



One Identity Manager 9.3

Administration Guide for Connecting to a Universal Cloud Interface

Copyright 2024 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 website (<http://www.OneIdentity.com>) for regional and international office information.


Patents


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

Trademarks

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

Legend

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

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

One Identity Manager Administration Guide for Connecting to a Universal Cloud Interface
Updated - 16 December 2024, 12:32

For the most recent documents and product information, see [Online product documentation](#).

Contents

Managing Universal Cloud Interface environments	9
Architecture overview	10
One Identity Manager users for managing cloud target systems	10
Synchronizing a cloud application in the Universal Cloud Interface	13
Setting up initial synchronization with a cloud application in the Universal Cloud Interface	14
Users and permissions for synchronizing with a cloud application	15
Setting up the synchronization server	16
System requirements for the synchronization server	16
Installing One Identity Manager Service with a Universal Cloud Interface connector	17
Creating a synchronization project for initial synchronization of a cloud application	20
Information required for setting up a synchronization project	20
Creating an initial synchronization project for a cloud application	22
Start up configurations for cloud application synchronization	27
Configuring the synchronization log	27
Customizing the synchronization configuration	28
How to configure Universal Cloud Interface synchronization	30
Configuring synchronization of multiple cloud applications	30
Changing system connection settings of cloud applications in the Universal Cloud Interface	31
Editing connection parameters in the variable set	31
Editing target system connection properties	32
Updating schemas	33
Speeding up synchronization with revision filtering	34
Configuring single object synchronization	36
Speeding up provisioning	36
Running synchronization	37
Starting synchronization	37
Deactivating synchronization	38
Displaying synchronization results	39
Tasks following synchronization	40

Post-processing outstanding objects	40
Displaying the target system synchronization configuration	42
Managing cloud user accounts through account definitions	43
Troubleshooting	43
Ignoring data error in synchronization	44
Pausing handling of target system specific processes (Offline mode)	45
Provisioning object changes	47
The provisioning sequence	47
Displaying pending changes	48
Retention time for pending changes	49
Managing cloud user accounts and identities	50
Account definitions for cloud user accounts	51
Creating account definitions	52
Editing account definitions	53
Main data for account definitions	53
Editing manage levels	56
Creating manage levels	57
Assigning manage levels to account definitions	57
Main data for manage levels	58
Creating mapping rules for IT operating data	59
Entering IT operating data	60
Modify IT operating data	61
Assigning account definitions to identities	62
Assigning account definitions to departments, cost centers, and locations	64
Assigning account definitions to business roles	64
Assigning account definitions to all identities	65
Assigning account definitions directly to identities	66
Assigning account definitions to system roles	66
Adding account definitions in the IT Shop	67
Assigning account definitions to cloud target systems	70
Deleting account definitions	70
Assigning identities automatically to user accounts	73
Editing search criteria for automatic identity assignment	75
Finding identities and directly assigning them to user accounts	76

Changing manage levels for cloud user accounts	77
Supported user account types	78
Default user accounts	79
Administrative user accounts	80
Providing an administrative user account for one identity	80
Providing an administrative user account for multiple identities	81
Privileged user accounts	82
Setting deferred deletion for cloud target system user accounts	84
Managing assignments of cloud groups and cloud system entitlements	86
System entitlements types in cloud target systems	86
Assigning cloud groups and system entitlements to cloud user accounts in One Identity Manager	88
Prerequisites for indirect assignments of cloud groups and system entitlements to cloud user accounts	90
Assigning cloud groups to departments, cost centers, and locations	91
Assigning cloud system entitlements to departments, cost centers, and locations	92
Assigning cloud groups to business roles	94
Assigning cloud system entitlements to business roles	95
Adding cloud groups to system roles	96
Adding cloud system entitlements to system roles	97
Adding cloud groups to the IT Shop	98
Adding cloud system entitlements to the IT Shop	100
Assigning cloud user accounts directly to cloud groups	103
Assigning cloud user account directly to cloud system entitlements	104
Assigning cloud groups directly to cloud user accounts	105
Assigning cloud system entitlements directly to cloud user accounts	105
Assigning default profiles to user accounts in Salesforce applications	106
Effectiveness of memberships in cloud groups and cloud system entitlements	107
Inheriting cloud group and system entitlement based on categories	110
Overview of all assignments	112
Login credentials for cloud user accounts	114
Password policies for cloud user accounts	114
Predefined password policies	115
Using password policies	116
Creating password policies	117

Editing password policies	118
General main data of password policies	118
Policy settings	119
Character classes for passwords	120
Custom scripts for password requirements	122
Checking passwords with a script	122
Generating passwords with a script	124
Password exclusion list	125
Checking passwords	125
Testing password generation	125
Initial password for new cloud user accounts	126
Email notifications about login data	126
Mapping cloud objects in One Identity Manager	128
Cloud target systems	128
General main data for cloud target systems	129
Defining categories for inheriting cloud groups and system entitlements	132
Specifying alternative names	132
Editing the synchronization project for a cloud target system	133
Container structures	133
Cloud user accounts	134
Creating and editing cloud user accounts	135
General main data for cloud user accounts	136
Login data for cloud user accounts	140
Details of cloud user account identification	141
Contact data for cloud user accounts	142
User-defined main data for cloud user accounts	142
Assigning permissions controls to cloud user accounts	143
Assigning extended properties to cloud user accounts	144
Locking and unlocking cloud user accounts	144
Deleting cloud user accounts	145
Displaying the cloud user account overview	146
Cloud groups	147
Creating and editing cloud groups	147
General main data for cloud groups	148
User-defined main data for cloud groups	149

Adding cloud groups to cloud groups	150
Assigning permissions controls to cloud groups	151
Assigning extended properties to cloud groups	151
Displaying the cloud group overview	152
Deleting cloud groups	152
Cloud system entitlements	153
Creating and editing cloud system entitlements	153
General main data for system entitlements	154
User-defined main data for cloud user accounts	155
Assigning cloud system entitlements to cloud system entitlements	156
Assigning extended properties to cloud system entitlements	157
Displaying cloud system entitlement overviews	158
Deleting cloud system entitlements	159
Cloud permissions controls	159
General main data for cloud permissions controls	160
User-defined main data for cloud permissions controls	160
Assigning cloud groups to cloud permissions controls	161
Assigning cloud user accounts to cloud permissions controls	161
Displaying an overview of the cloud permissions controls	162
Deleting cloud permissions controls	162
Reports about objects in cloud target systems	163
Handling cloud objects in the Web Portal	166
Basic data for managing a Universal Cloud Interface environment	168
Target system managers	169
Job server for Universal Cloud Interface-specific process handling	172
Editing Job server for cloud target systems	172
General main data of Job servers	173
Specifying server functions	176
Appendix: Configuration parameters for managing cloud target systems	177
Appendix: Default project template for cloud applications in the Universal Cloud Interface	180
About us	182
Contacting us	182
Technical support resources	182

Index183

Managing Universal Cloud Interface environments

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

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

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

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

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

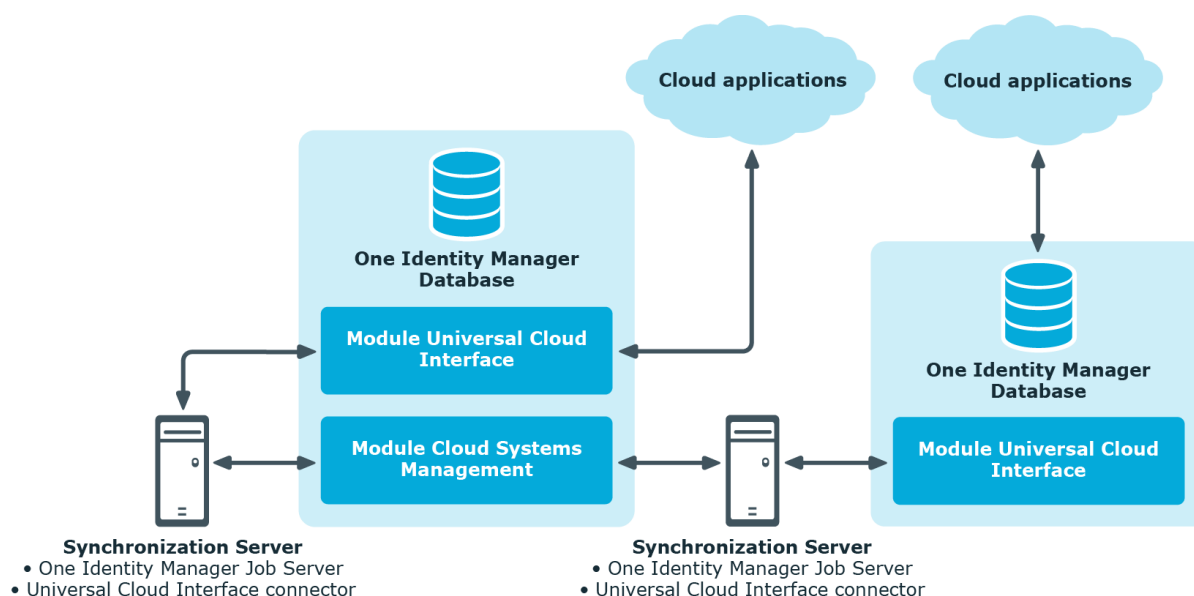
Since only data that must be available in the cloud application is saved in the Universal Cloud Interface Module, the module can be installed in a separate database. This database may be outside the company's infrastructure.

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

Architecture overview

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

Figure 1: Architecture for synchronization



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

One Identity Manager users for managing cloud target systems

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

Table 1: Users

Users	Tasks
Target system administrators	<p>Target system administrators must be assigned to the Target systems Administrators application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none">• Administer application roles for individual target system types.• Specify the target system manager.• Set up other application roles for target system managers if required.• Specify which application roles for target system managers are mutually exclusive.• Authorize other identities to be target system administrators.• Do not assume any administrative tasks within the target system.
Target system managers	<p>Target system managers must be assigned to the Target systems Cloud target systems application role or a child application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none">• Assume administrative tasks for the target system.• Create, change, or delete target system objects.• Edit password policies for the target system.• Prepare groups and system entitlements to add to the IT Shop.• Can add identities that do not have the Primary identity identity type.• Configure synchronization in the Synchronization Editor and define the mapping for comparing target systems and One Identity Manager.• Edit the synchronization's target system types and outstanding objects.• Authorize other identities within their area of responsibility as target system managers and create child application roles if required.
One Identity Manager administrators	<p>One Identity Manager administrator and administrative system users Administrative system users are not added to application roles.</p>

Users	Tasks
	<p>One Identity Manager administrators:</p> <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.
Administrators for the IT Shop	<p>Administrators must be assigned to the Request & Fulfillment IT Shop Administrators application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none"> • Assign groups to IT Shop structures. • Assign system entitlements to IT Shop structures.
Administrators for organizations	<p>Administrators must be assigned to the Identity Management Organizations Administrators application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none"> • Assign groups to departments, cost centers, and locations. • Assign system entitlements to departments, cost centers, and locations.
Business roles administrators	<p>Administrators must be assigned to the Identity Management Business roles Administrators application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none"> • Assign groups to business roles. • Assign system entitlements to business roles.

Synchronizing a cloud application in the Universal Cloud Interface

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

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

Table 2: Terms

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

The mapping defines how schema types of the connection systems are mapped to each other. For more information, see [Default project template for cloud applications in the Universal Cloud Interface](#) on page 180.

This section explains how to:

- Set up synchronization between the Universal Cloud Interface and Cloud Systems Management modules.
- Adapt a synchronization configuration, for example, to synchronize different target systems with the same synchronization project.
- Start and deactivate the synchronization.
- Evaluate the synchronization results.

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

Detailed information about this topic

- [Setting up initial synchronization with a cloud application in the Universal Cloud Interface](#) on page 14
- [Customizing the synchronization configuration](#) on page 28
- [Running synchronization](#) on page 37
- [Tasks following synchronization](#) on page 40
- [Troubleshooting](#) on page 43

Setting up initial synchronization with a cloud application in the Universal Cloud Interface

The Synchronization Editor provides a project template that can be used to set up the synchronization of user accounts and permissions. Use this project template to set up the initial synchronization project. In addition, the required processes are created that are used for the provisioning of changes to target system objects in the target system.

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

1. Provide One Identity Manager users with the required permissions for setting up synchronization and post-processing of synchronization objects.
2. The One Identity Manager components for managing cloud target systems are available if the **TargetSystem | CSM** configuration parameter is set.
 - In the Designer, check if the configuration parameter is set. Otherwise, set the configuration parameter and compile the database.
3. Install and configure a synchronization server and declare the server as Job server in One Identity Manager.
4. Create a synchronization project with the Synchronization Editor.

NOTE: The cloud application must already be available in the Universal Cloud Interface Module before the synchronization project can be created. For more information about setting up initial synchronization with a cloud

application, see the *One Identity Manager Administration Guide for Connecting to Cloud Applications*.

Detailed information about this topic

- [Users and permissions for synchronizing with a cloud application](#) on page 15
- [Setting up the synchronization server](#) on page 16
- [Creating a synchronization project for initial synchronization of a cloud application](#) on page 20
- [Start up configurations for cloud application synchronization](#) on page 27
- [Configuration parameters for managing cloud target systems](#) on page 177
- [Default project template for cloud applications in the Universal Cloud Interface](#) on page 180

Users and permissions for synchronizing with a cloud application

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

Table 3: Users for synchronization

User	Permissions
Users for accessing the Cloud Application in the Universal Cloud Interface	<p>To log on to the database containing the Universal Cloud Interface, use:</p> <ul style="list-style-type: none">• Role-based login: a user with the application role Universal Cloud Interface Administrators- OR -• Non role-based login: a system user with the DPR_EditRights_Methods permissions group.
One Identity Manager Service user account	<p>The user account for the One Identity Manager Service requires user permissions to carry out operations at file level (adding and editing directories and files).</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 permissions for the internal web service.</p>

User	Permissions
	<p>NOTE: If the One Identity Manager Service runs under the network service (NT Authority\NetworkService), you can grant permissions for the internal web service with the following command line call:</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)
User for accessing the One Identity Manager database	The Synchronization default system user is provided to run synchronization using an application server.

Setting up the synchronization server

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

The One Identity Manager Service with the Universal Cloud Interface connector must be installed on the synchronization server.

Detailed information about this topic

- [System requirements for the synchronization server](#) on page 16
- [Installing One Identity Manager Service with a Universal Cloud Interface connector](#) on page 17

System requirements for the synchronization server

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

- Windows operating system

The following versions are supported:

- Windows Server 2025
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012

- .NET 8 Desktop Runtime

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

Installing One Identity Manager Service with a Universal Cloud Interface connector

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

Table 4: Properties of the Job server

Property	Value
Server function	Universal Cloud Interface connector
Machine role	Server Job Server

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

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

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

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

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

- Configures the One Identity Manager Service.
- Starts the One Identity Manager Service.

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

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

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

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

1. Start the Server Installer program.

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

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

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

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

- a. Select a Job server from the **Server** drop-down.

- OR -

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

- b. Enter the following data for the Job server.

- **Server:** Name of the Job server.
- **Queue:** Name of the queue to handle the process steps. Each Job server within the network must have a unique queue identifier. The process steps are requested by the Job queue using this exact queue name. The queue identifier is entered in the One Identity Manager Service configuration file.
- **Full server name:** Full server name in accordance with DNS syntax.

Syntax:

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

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

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

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

For a direct connection to the database:

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

For a connection to the application server:

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

7. To configure the installation, click **Next**.
8. Confirm the security prompt with **Yes**.
9. On the **Select installation source** page, select the directory with the install files. Change the directory if necessary.
10. On the **Service access** page, enter the service's installation data.

- **Computer:** Select the server, on which you want to install and start the service, from the drop-down or enter the server's name or IP address.
To run the installation locally, select **Local installation** from the drop-down.
- **Service account:** Enter the details of the user account that the One Identity Manager Service is running under. Enter the user account, the user account's password and password confirmation.

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

You can also change the One Identity Manager Service details, such as the installation directory, name, display name, and the One Identity Manager Service description, using the advanced options.

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

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

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

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

Creating a synchronization project for initial synchronization of a cloud application

Use the Synchronization Editor to set up synchronization between the Cloud Systems Management Module and the Universal Cloud Interface Module. The following describes the steps for initial configuration of a synchronization project. For more information about setting up synchronization, see the *One Identity Manager Target System Synchronization Reference Guide*.

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

Related topics

- [Information required for setting up a synchronization project](#) on page 20
- [Creating an initial synchronization project for a cloud application](#) on page 22

Information required for setting up a synchronization project

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

Table 5: Information required for setting up a synchronization project

Data	Explanation
Cloud application	Name of the cloud application in the Universal Cloud Interface Module to synchronize.
Synchronization server	<p>All One Identity Manager Service actions are run against the target system environment on the synchronization server. Data entries required for synchronization and administration with the One Identity Manager database are processed by the synchronization server.</p> <p>The One Identity Manager Service with the Universal Cloud Interface 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 6: Additional properties for the Job server

Property	Value
Server function	Universal Cloud Interface connector
Machine role	Server Job Server

For more information, see [System requirements for the synchronization server](#) on page 16.

One Identity Manager database connection data	<ul style="list-style-type: none"> • Database server • Database name • SQL login and password • Specifies whether integrated Windows authentication is used <p>Use of the integrated Windows authentication is not recommended. If you decide to use it anyway, ensure that your environment supports Windows authentication.</p>
Remote connection server	To configure synchronization with a target system, One Identity Manager must load the data from the target system. One Identity Manager communicates directly with the target system to do this. Sometimes direct access from the workstation, on which the Synchronization Editor is installed, is not possible. For example, because of the firewall configuration or the workstation does not fulfill the necessary hardware and software requirements. If direct access is not possible from the workstation, you can set up a remote connection.

Data	Explanation
	<p>Remote connection server configuration:</p> <ul style="list-style-type: none"> • One Identity Manager Service is started • RemoteConnectPlugin is installed and an authentication method is set up • Universal Cloud Interface connector is installed <p>The remote connection server must be declared as a Job server in One Identity Manager. The Job server name is required.</p> <p>For more detailed information about setting up a remote connection, see the <i>One Identity Manager Target System Synchronization Reference Guide</i>.</p>

Creating an initial synchronization project for a cloud application

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

- Run in default mode
- Started from the Launchpad

If you run the project wizard in expert mode or directly from the Synchronization Editor, additional configuration settings can be made. Follow the project wizard instructions through these steps.

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

To set up initial synchronization project for a cloud application

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

NOTE: If synchronization is run by an application server, connect the database through the application server.
2. In the **Installation overview > Data synchronization** section, select the **Target system type Universal Cloud Interface** and click **Run**.
This starts the Synchronization Editor's project wizard.
3. On the wizard's start page, click **Next**.
4. On the **System access** page, specify how One Identity Manager can access the target system.
 - If access is possible from the workstation on which you started the Synchronization Editor, do not change any settings.


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

Select the **Connect using remote connection server** and enter the remote connection properties.

Remote connection properties

- **Access parameters**

- **Server:** Full server name or IP address of the server.

To select an existing Job server as the remote connection server, click  and select the server from the drop-down. This displays all the Job servers that have the **One Identity Manager Service installed** server function selected.

- **Port:** Port that is configured for the RemoteConnectPlugin.

- **Authentication**

If **SecretAuthentication** is configured for the RemoteConnectPlugin:

- **Secret:** Secret used by the Synchronization Editor to authenticate on the RemoteConnectPlugin.

If **ADGroupAuthentication** is configured for the RemoteConnectPlugin, no data is required.

- **Options**

- **Request timeout:** Maximum time allowed for a server query in seconds. If the time is exceeded, the request is canceled.
- **Accept self-signed certificates:** Specifies whether self-signed certificates can be accepted.

5. On the start page of the system connection wizard, click **Next**.
6. On the **Select database system** page, select the database system to which you want to connect.
7. On the **Connection parameters** page, enter the database credentials to the database containing the Universal Cloud Interface Module.
 - **Server:** Database server.
 - **Windows authentication:** (Optional) Specifies whether the integrated Windows authentication is used. This type of authentication is not recommended. If you decide to use it anyway, ensure that your environment supports Windows authentication.
 - **User:** User's SQL login name.
 - **Password:** Password for the SQL user's login.
 - **Database:** List of possible databases on the database server. Select the database.

- **Encrypt communication:** Specifies whether encryption is required for exchanging data between the client and server. Select the minimum encryption level. The encryption level that is actually used depends on the database server configuration. For more information, see the documentation from Microsoft.

Permitted values are:

- **Optional:** Communication is not encrypted.
 - **Mandatory:** Data exchange is encrypted. The **Trust server certificate** option, allows you to also specify whether to verify the server certificate.
 - **Strict (SQL Server 2022 and Azure SQL):** The data exchange is encrypted. The server certificate is always verified.
- **Trust server certificate:** If this option is enabled, the data exchange between the client and server is encrypted. However, the server certificate is not verified.
 - To enter additional information about the database connection, click **Advanced options**.
 - Click **Test** to test whether the database is accessible.
8. On the **Encryption** page, enter the private key for encrypting the database.
 9. On the last page of the system connection wizard, you can save the connection data.
 - Set the **Save connection locally** option to save the connection data. This can be reused when you set up other synchronization projects.
 - Click **Finish**, to end the system connection wizard and return to the project wizard.
 10. 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.


11. The wizard loads the target system schema. This may take a few minutes depending on the type of target system access and the size of the target system.
12. On the **Select cloud application** page, select the cloud application to synchronize.
13. On the **Restrict target system access** page, specify how system access should work. You have the following options:

Table 7: Specify target system access


Option	Meaning
Read-only access to target system.	<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.	<p>Specifies whether a provisioning workflow is set up in addition to the synchronization workflow for the initial loading of the target system.</p> <p>The provisioning workflow displays the following characteristics:</p> <ul style="list-style-type: none">• 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.

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

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

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

TIP: You can also implement an existing Job server as the synchronization server for this target system.

- To select a Job server, click .

This automatically assigns the server function matching this Job server.

- Click **OK**.

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

- d. **NOTE:** After you save the synchronization project, ensure that this server is set up as a synchronization server.
15. To close the project wizard, click **Finish**.
- Two start up configurations and two default schedules are created for regular synchronization.

Table 8: Start up configuration

Start configuration	Runtime interval
Synchronization of the cloud application	Daily
Synchronization of pending changes	Hourly

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

NOTE:

- If enabled, a consistency check is carried out. If errors occur, a message appears. You can decide whether the synchronization project can remain activated or not.
Check the errors before you use the synchronization project. To do this, in the **General** view on the Synchronization Editor's start page, click **Verify project**.
- If you do not want the synchronization project to be activated immediately, disable the **Activate and save the new synchronization project automatically option**. In this case, save the synchronization project manually before closing the Synchronization Editor.
- The connection data for the target system is saved in a variable set and can be modified in the Synchronization Editor in the **Configuration > Variables** category.

Detailed information about this topic

- [Information required for setting up a synchronization project](#) on page 20
- [Users and permissions for synchronizing with a cloud application](#) on page 15
- [Setting up the synchronization server](#) on page 16
- [Start up configurations for cloud application synchronization](#) on page 27
- [Configuring the synchronization log](#) on page 27
- [Customizing the synchronization configuration](#) on page 28
- [Running synchronization](#) on page 37
- [Tasks following synchronization](#) on page 40
- [Default project template for cloud applications in the Universal Cloud Interface](#) on page 180

Start up configurations for cloud application synchronization

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

- Synchronization of the cloud application
Cloud application objects, such as user accounts, groups, group memberships, are synchronized. This is done by the **Initial synchronization** workflow. Synchronization is run on a daily basis by the default schedule.
- Synchronization of pending changes
If cloud objects are changed in the Cloud Systems Management Module, these changes must first be transferred to the Universal Cloud Interface Module and can then be provisioned in the cloud application itself. To track whether the changes have been successfully provisioned in the cloud application, they are labeled with **Pending changes**. The details, time of creation, and processing status of every pending change are saved. Once provisioning is complete, the processing status must be transferred from the Universal Cloud Interface to the Cloud Systems Management Module. To do this, run the **Synchronization of pending changes** start up configuration. This is done by the **State synchronization** workflow. Synchronization is run on an hourly basis with the default schedule.

Related topics

- [Provisioning object changes](#) on page 47
- [Starting synchronization](#) on page 37

Configuring the synchronization log

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

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

1. To configure the synchronization log for target system connection, in the Synchronization Editor, select the **Configuration > Target system** category.
- OR -
To configure the synchronization log for the database connection, in the Synchronization Editor, select the **Configuration > One Identity Manager connection** category.
2. In the **General** section, click **Setup**.

3. In the **Synchronization log** section, set **Create synchronization log**.
4. Enable the data to be logged.

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

5. Click **OK**.

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

1. In the Synchronization Editor, select the **Workflows** category.
2. Select a workflow in the navigation view.
3. In the **General** section, click **Edit**.
4. Select the **Synchronization log** tab.
5. Enable the data to be logged.

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

6. Click **OK**.

Synchronization logs are stored for a fixed length of time.

To modify the retention period for synchronization logs

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

Related topics

- [Displaying synchronization results](#) on page 39

Customizing the synchronization configuration

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

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

- To use Cloud Systems Management Module as the primary system during synchronization, create a workflow with synchronization in the direction of the **Target system**.
- You can use variables to create generally applicable synchronization configurations that contain the necessary information about the synchronization objects when synchronization starts. Variables can be implemented in base objects, schema classes, or processing method, for example.
- Use variables to set up a synchronization project for synchronizing different cloud applications. Store the connection parameter as a variable for logging in to the databases.
- To specify which target system objects and database objects are included in synchronization, edit the scope of the target system connection and the One Identity Manager database connection. To prevent data inconsistencies, define the same scope in both systems. If no scope is defined, all objects will be synchronized.
- 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.
- Add your own schema types if you want to synchronize data, which does not have schema types in the connector schema. Include the schema extensions in the mapping.
- If the cloud application schema cannot be adequately represented by the default project template, customize the synchronization configuration. At the same time, define how the system entitlements are mapped in the One Identity Manager schema. When you are setting up synchronization, ensure that the base object for the cloud application(CSMRoot) is created in the database and the **System entitlements types used** (GroupUsageMask) and **User account has memberships** (UserContainsGroupList) properties are set correctly.

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

Detailed information about this topic

- [How to configure Universal Cloud Interface synchronization](#) on page 30
- [Configuring synchronization of multiple cloud applications](#) on page 30
- [Updating schemas](#) on page 33
- [Changing system connection settings of cloud applications in the Universal Cloud Interface](#) on page 31

How to configure Universal Cloud Interface synchronization

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

To create a synchronization configuration for synchronizing Universal Cloud Interface

1. In the Synchronization Editor, open the synchronization project.
2. Check whether the existing mappings can be used to synchronize into the target system. Create new maps if required.
3. Create a new workflow with the workflow wizard.
This creates a workflow with **Target system** as its direction of synchronization.
4. Create a new start up configuration. Use the new workflow to do this.
5. Save the changes.
6. Run a consistency check.

Related topics

- [Configuring synchronization of multiple cloud applications](#) on page 30

Configuring synchronization of multiple cloud applications

Prerequisites

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

To customize a synchronization project for synchronizing another cloud application

1. In the Synchronization Editor, open the synchronization project.
2. Create a new base object the other cloud application.
 - Use the wizard to attach a base object.
 - In the wizard, select the Universal Cloud Interface connector.

- Declare the connection parameters. The connection parameters are saved in a special variable set.

A start up configuration is created that uses the newly created variable set.

3. Change other elements of the synchronization configuration as required.
4. Save the changes.
5. Run a consistency check.

Related topics

- [How to configure Universal Cloud Interface synchronization](#) on page 30

Changing system connection settings of cloud applications in the Universal Cloud Interface

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

- a. Specify a specialized variable set and change the values of the affected variables.
The default values remain untouched in the default variable set. The variables can be reset to the default values at any time. (Recommended action).
- b. Edit the target system connection with the system connection wizard and change the effected values.

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

Detailed information about this topic

- [Editing connection parameters in the variable set](#) on page 31
- [Editing target system connection properties](#) on page 32

Editing connection parameters in the variable set





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

NOTE: To guarantee data consistency in the connected target system, ensure that the start-up configuration for synchronization and the base object for provisioning use the same variable set. This especially applies if a synchronization project is used for synchronizing different cloud applications.

To customize connection parameters in a specialized variable set

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

Some connection parameters can be converted to variables here. For other parameters, variables are already created.
4. Select a parameter and click **Convert**.
5. Select the **Configuration > Variables** category.

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

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

Related topics

- [Editing target system connection properties](#) on page 32

Editing target system connection properties

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

| NOTE: In the following circumstances, the default values cannot be restored:

- The connection parameters are not defined as variables.
- The default variable set is selected as an active variable set.

In both these cases, the system connection wizard overwrites the default values. They cannot be restored at a later time.

To edit connection parameters using the system connection wizard

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

NOTE: If the default variable set is selected, the default values are overwritten and cannot be restored at a later time.
3. Select the **Configuration > Target system** category.
4. Click **Edit connection**.
 This starts the system connection wizard.
5. Follow the system connection wizard instructions and change the relevant properties.
6. Save the changes.

Related topics

- [Editing connection parameters in the variable set](#) on page 31

Updating schemas

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

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

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

- A schema was changed by:
 - Changes to a target system schema
 - Customizations to the One Identity Manager schema

- A One Identity Manager update migration
- A schema in the synchronization project was shrunk by:
 - Enabling the synchronization project
 - Saving the synchronization project for the first time
 - Compressing a schema

To update a system connection schema

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Configuration > Target system** category.
 - OR -
 - Select the **Configuration > One Identity Manager connection** category.
3. Select the **General** view and click **Update schema**.
4. Confirm the security prompt with **Yes**.

This reloads the schema data.

To edit a mapping

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

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

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

Speeding up synchronization with revision filtering

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

One Identity Manager supports revision filtering. The date of the last target system object change (column XDateUpdated) is used as revision counter. Each synchronization saves its last run 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 target system objects' change date is compared with the revision saved in the One Identity Manager database. Only those objects that have been changed since this date are loaded from the target system.

Synchronization is even faster if the change information on the schema type also takes deleted objects into account. If a schema type's objects were neither added, changed nor deleted, the synchronization step can be skipped. Objects must not be loaded for comparison. To take advantage of this optimization, the revision data for tables must be saved in both of the connected databases.

To use optimized revision filtering

1. Start the Designer and connect to the target system database.
2. Set the **Common | TableRevision** configuration parameter.
3. Save the changes.
4. Connect the Designer to the One Identity Manager database.
5. Set the **Common | TableRevision** configuration parameter.
6. Save the changes.

Now each time a table changes, the table's revision date updates. This information is stored in the QBMTTableRevision table, RevisionDate column. In this way, One Identity Manager identifies whether a table object has been added, changed, or deleted.

Synchronization with revision filtering compares a table's revision date against the revision saved in the One Identity Manager database. If the revision date is older, no objects have been changed in this table since the previous synchronization. Therefore, synchronization does not carry out this step for the affected schema type. If the revision date is newer, synchronization carries out this step and the changed objects are determined as described above.

The revision is found at start of synchronization. Objects modified by synchronization are loaded and checked by the next synchronization. This means that the second synchronization after initial synchronization is not significantly faster.

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

To permit revision filtering on a workflow

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

To permit revision filtering for a start up configuration

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

NOTE: If the **Common | TableRevision** is not set, all revision data in the QBMTTableRevision table is deleted.

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

Configuring single object synchronization

Single object synchronization is not supported.

Speeding up provisioning

To smooth out spikes in data traffic, handling of processes for provisioning can be distributed over several Job servers. This can speed up the provisioning process.

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

Once load balancing is no longer required, ensure that the synchronization server runs the provisioning processes.

To configure load balancing

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

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

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

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

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

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

3. In the Manager, assign this server function to all the Job servers that will be handling provisioning 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 again.

To use the synchronization server without load balancing.

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

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

Detailed information about this topic

- [Job server for Universal Cloud Interface-specific process handling](#) on page 172

Running synchronization

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

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

Detailed information about this topic

- [Starting synchronization](#) on page 37
- [Deactivating synchronization](#) on page 38
- [Displaying synchronization results](#) on page 39
- [Start up configurations for cloud application synchronization](#) on page 27
- [Pausing handling of target system specific processes \(Offline mode\)](#) on page 45

Starting synchronization

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

To synchronize on a regular basis

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

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

To start initial synchronization manually

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

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

- If another synchronization process is started with the same start up configuration, the process is stopped and is assigned **Frozen** status. An error message is written to the One Identity Manager Service log file.
 - Ensure that start up configurations that are used in start up sequences are not started individually at the same time. Assign start up sequences and start up configurations different schedules.
- Starting another synchronization process with different start up configuration that addresses same target system may lead to synchronization errors or loss of data. Specify One Identity Manager behavior in this case, in the start up configuration.
 - Use the schedule to ensure that the start up configurations are run in sequence.
 - Group start up configurations with the same start up behavior.

Deactivating synchronization

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

To prevent regular synchronization

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

Now you can only start synchronization manually.

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

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

To deactivate the synchronization project

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

3. Click **Deactivate project**.


Detailed information about this topic

- [Creating a synchronization project for initial synchronization of a cloud application](#) on page 20
- [Pausing handling of target system specific processes \(Offline mode\)](#) on page 45


Displaying synchronization results

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

To display a synchronization log

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

To display a provisioning log

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

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

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

Related topics

- [Configuring the synchronization log](#) on page 27
- [Troubleshooting](#) on page 43

Tasks following synchronization

After the synchronization of data from the target system into the One Identity Manager database, rework may be necessary. Check the following tasks:

- [Post-processing outstanding objects](#) on page 40
- [Displaying the target system synchronization configuration](#) on page 42
- [Managing cloud user accounts through account definitions](#) on page 43

Post-processing outstanding objects

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

Outstanding objects:

- Cannot be edited in One Identity Manager.
- Are ignored by subsequent synchronizations.
- Are ignored by inheritance calculations.

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

Start target system synchronization to do this.

To post-process outstanding objects

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

The navigation view lists all the synchronization tables assigned to the **Universal Cloud Interface** target system type.

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

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

- The synchronization log has already been deleted.
- OR -
- An assignment from a member list has been deleted from the target system.

The base object of the assignment was updated during the synchronization. A corresponding entry appears in the synchronization log. The entry in the

assignment table is marked as outstanding, but there is no entry in the synchronization log.

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




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

TIP:

To display the properties of an outstanding object

1. Select the object on the target system synchronization form.
 2. Open the context menu and click **Show object**.
 3. For memberships, select the object whose properties you want to display.
3. Select the objects you want to rework. Multi-select is possible.
 4. Click on one of the following icons in the form toolbar to run the respective method.

Table 9: Methods for handling outstanding objects

Icon	Method	Description
	Delete	The object is immediately deleted from the One Identity Manager database. Deferred deletion is not taken into account. Indirect memberships cannot be deleted.
	Publish	The object is added to the target system. The Outstanding label is removed from the object. This runs a target system specific process that triggers the provisioning process for the object. Prerequisites: <ul style="list-style-type: none">• The table containing the object can be published.• The target system connector has write access to the target system.
	Reset	The Outstanding label is removed for the object.

TIP: If a method cannot be run due to certain restrictions, the respective icon is disabled.


- To display the constraint's details, click the **Show** button in the **Constraints** column.

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

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

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

To disable bulk processing

- Disable the  icon in the form's toolbar.

NOTE: The target system connector must have write access to the target system in order to publish outstanding objects that are being post-processed. That means, the **Connection is read-only** option must not be set for the target system connection.

Related topics

- For more information, see [Displaying the target system synchronization configuration](#) on page 42.

Displaying the target system synchronization configuration

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

To display the target system synchronization configuration

1. In the Manager, select the **Cloud target systems > Basic configuration data > Target system types** category.
2. Select Universal Cloud Interface in the result list.
3. Select the **Assign synchronization tables** task.
All the tables that could be synchronized are enabled.
4. Select the **Configure tables for publishing** task.
The **Can be published** option is set for all tables with outstanding objects in the target system.

Related topics

- [Post-processing outstanding objects](#) on page 40

Managing cloud user accounts through account definitions

In the default installation, after synchronizing, identities are automatically created for user accounts and contacts. If an account definition for the domain is not known at the time of synchronization, user accounts and contacts are linked to identities. However, account definitions are not assigned. The user accounts and contacts are therefore in a **Linked** state.

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

To manage user accounts through account definitions

1. Create an account definition.
2. Assign a user account in the **Linked** state to the account definition. The account definition's default manage level is applied to the user account.
 - a. In the Manager, select the **Cloud target systems > Target system > User accounts > Linked but not configured > <target system>** category.
 - b. Select the **Assign account definition to linked accounts** task.
 - c. In the **Account definition** drop-down, select the account definition.
 - d. Select the user accounts that contain the account definition.
 - e. Save the changes.

Related topics

- [Account definitions for cloud user accounts](#) on page 51

Troubleshooting

Synchronization Editor helps you to analyze and eliminate synchronization errors.

- Simulating synchronization

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

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

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

- Reset start information

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

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

Related topics

- [Displaying synchronization results](#) on page 39

Ignoring data error in synchronization

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

To ignoring data errors during synchronization in One Identity Manager

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

This starts the system connection wizard.

4. On the **Additional options** page, enable **Try to ignore data errors**.

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

Default columns, such as primary keys, UID columns, or mandatory input columns cannot be ignored.

5. Save the changes.

IMPORTANT: If this option is set, One Identity Manager tries to ignore commit errors that could be related to data errors in a single column. This causes the data changed in the affected column to be discarded and the object is subsequently saved again. This effects performance and leads to loss of data.

Only set this option in the exceptional circumstance of not being able to correct the data before synchronization.

Pausing handling of target system specific processes (Offline mode)

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

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


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

Prerequisites

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

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

To allow offline mode for a base object

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

IMPORTANT: To prevent data inconsistencies, the offline phase should be kept as short as possible.

The number of processes to handle depends on the extent of the changes in the One Identity Manager database and their effect on the target system during the offline phase. To establish data consistency between the One Identity Manager database and the target system, all pending processes must be handled before synchronization can start.

Only use offline mode, if possible, for short system downtimes such as maintenance windows.

To flag a target system as offline

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

This opens the **Manage offline systems** dialog. The **Base objects** section displays the base objects of target system connections that can be switched to offline.

4. Select the base object whose target system connection is not available.
5. Click **Switch offline**.
6. Confirm the security prompt with **OK**.

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

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

Related topics

- [Deactivating synchronization](#) on page 38

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.

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

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.

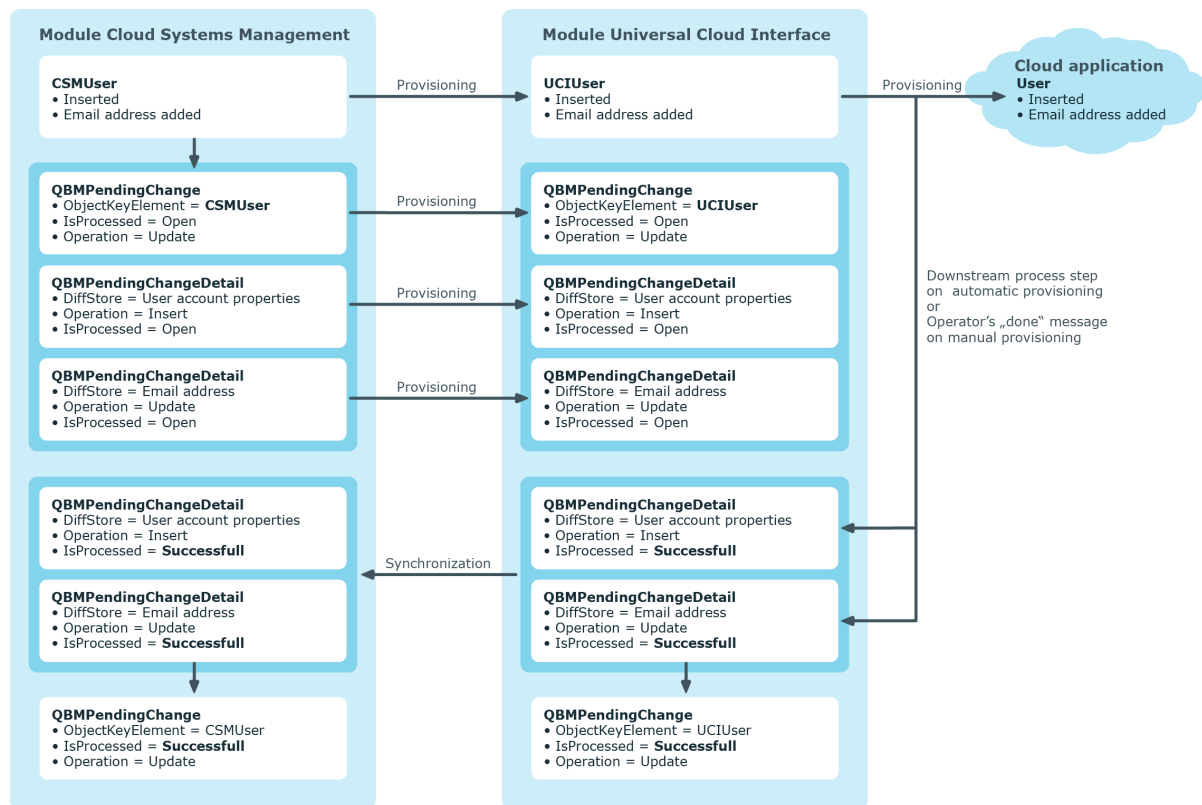
Detailed information about this topic

- [The provisioning sequence](#) on page 47
- [Retention time for pending changes](#) on page 49

The provisioning sequence

The following visual shows how object changes are provisioned and how the pending changes associated with it are processed. The sequence does not depend on whether the Cloud System Management and the Universal Cloud Interface modules are installed in the same or in separate databases.

Figure 2: Provisioning sequence for pending changes



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

Related topics

- [Provisioning object changes](#) on page 47



Displaying pending changes

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

To display pending changes

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

Table 10: Meaning of the icons in the toolbar

Icon	Meaning
	Show selected object.
	Reload the data.

Related topics

- [Provisioning object changes](#) on page 47

Retention time for pending changes

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

To configure the retention period for pending changes

1. To change the retention period for successful provisioning processes, in the Designer, edit the value of the **QBM | PendingChange | LifeTimeSuccess** configuration parameter. Enter a retention period in days. The default is **2** days.
2. To change the retention period for failed provisioning processes, in the Designer, edit the value of the **QBM | PendingChange | LifeTimeError** configuration parameter and enter the retention period in days. The default is **30** days.
3. To change the retention period for pending provisioning processes, in the Designer, edit the value of the **QBM | PendingChange | LifeTimeRunning** configuration parameter and enter the retention period in days. The default is **60** days.

Related topics

- [Provisioning object changes](#) on page 47

Managing cloud user accounts and identities

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

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

- Identities can automatically obtain their account definitions using user account resources.

If an identity does not yet have a user account in a target system, a new user account is created. This is done by assigning account definitions to an identity using the integrated inheritance mechanisms and subsequent process handling.

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

- When user accounts are inserted, they can be automatically assigned to an existing identity or a new identity can be created if necessary. In the process, the identity main data is created on the basis of existing user account main data. This mechanism can be implemented if a new user account is created manually or by synchronization. However, this is not the One Identity Manager default method. You must define criteria for finding identities for automatic identity assignment.
- Identities and user accounts can be entered manually and assigned to each other.

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

Related topics

- [Account definitions for cloud user accounts](#) on page 51
- [Assigning identities automatically to user accounts](#) on page 73
- [Setting deferred deletion for cloud target system user accounts](#) on page 84
- [Creating and editing cloud user accounts](#) on page 135

Account definitions for cloud user accounts

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

The data for the user accounts in the respective target system comes from the basic identity main data. The identities must have a central user account. The assignment of the IT operating data to the identity's user account is controlled through the primary assignment of the identity to a location, a department, a cost center, or a business role. Processing is done through templates. There are predefined templates for determining the data required for user accounts included in the default installation. You can customize templates as required.

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

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

For more information about the principles of account definitions, manage levels, and determining the valid IT operating data, see the *One Identity Manager Target System Base Module Administration Guide*.

The following steps are required to implement an account definition:

- Creating account definitions
- Configuring manage levels
- Creating the formatting rules for IT operating data
- Collecting IT operating data
- Assigning account definitions to identities and target systems


Detailed information about this topic

- [Creating account definitions](#) on page 52
- [Editing account definitions](#) on page 53
- [Main data for account definitions](#) on page 53
- [Editing manage levels](#) on page 56
- [Creating manage levels](#) on page 57
- [Assigning manage levels to account definitions](#) on page 57
- [Creating mapping rules for IT operating data](#) on page 59
- [Entering IT operating data](#) on page 60
- [Modify IT operating data](#) on page 61
- [Assigning account definitions to identities](#) on page 62
- [Assigning account definitions to cloud target systems](#) on page 70
- [Deleting account definitions](#) on page 70

Creating account definitions

Create one or more account definitions for the target system.

To create a new account definition

1. In the Manager, select the **Cloud Target Systems > Basic configuration data > Account definitions > Account definitions** category.
2. Click  in the result list.
3. On the main data form, enter the main data of the account definition.
4. Save the changes.

Detailed information about this topic

- [Main data for account definitions](#) on page 53
- [Editing account definitions](#) on page 53
- [Assigning manage levels to account definitions](#) on page 57

Editing account definitions

You can edit the main data of account definitions.

To edit an account definition

1. In the Manager, select the **Cloud Target Systems > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Change main data** task.
4. Enter the account definition's main data.
5. Save the changes.

Related topics

- [Main data for account definitions](#) on page 53
- [Creating account definitions](#) on page 52
- [Assigning manage levels to account definitions](#) on page 57

Main data for account definitions

Enter the following data for an account definition:

Table 11: Main data for an account definition

Property	Description
Account definition	Account definition name.
User account table	Table in the One Identity Manager schema that maps user accounts.
Target system	Target system to which the account definition applies.
Required account definition	Specifies the required account definition. Define the dependencies between account definitions. When this account definition is requested or assigned, the required account definition is assigned automatically. Leave empty for cloud target systems.
Description	Text field for additional explanation.
Manage level (initial)	Manage level to use by default when you add new user accounts.
Risk index	Value for evaluating the risk of assigning the account

Property	Description
	<p>definition to identities. Set a value in the range 0 to 1. This input field is only visible if the QER CalculateRiskIndex configuration parameter is set.</p> <p>For more information, see the <i>One Identity Manager Risk Assessment Administration Guide</i>.</p>
Service item	Service item through which you can request the account definition resource in the IT Shop. Assign an existing service item or add a new one.
IT Shop	Specifies whether the account definition can be requested through the IT Shop. This account definition can be requested through the Web Portal and allocated by defined approval processes. The resource can also be assigned directly to identities and roles outside the IT Shop.
Only for use in IT Shop	Specifies whether the account definition can only be requested through the IT Shop. This account definition can be requested through the Web Portal and allocated by defined approval processes. The account definition cannot be directly assigned to roles outside the IT Shop.
Automatic assignment to identities	<p>Specifies whether the account definition is automatically assigned to all internal identities. To automatically assign the account definition to all internal identity, use the Enable automatic assignment to identities. The account definition is assigned to every identity that is not marked as external. Once a new internal identity is created, they automatically obtain this account definition.</p> <p>To automatically remove the account definition assignment from all identities, use the Disable automatic assignment to identities. The account definition cannot be reassigned to identities from this point on. Existing account definition assignments remain intact.</p>
Retain account definition if permanently disabled	<p>Specifies the account definition assignment to permanently deactivated identities.</p> <p>Option set: The account definition assignment remains in effect. The user account remains intact.</p> <p>Option not set (default): The account definition assignment is not in effect.</p>
Retain account definition if temporarily disabled	<p>Specifies the account definition assignment to temporarily deactivated identities.</p> <p>Option set: The account definition assignment remains in effect. The user account remains intact.</p>

Property	Description
	Option not set (default): The account definition assignment is not in effect.
Retain account definition on deferred deletion	<p>Specifies the account definition assignment on deferred deletion of identities.</p> <p>Option set: The account definition assignment remains in effect. The user account remains intact.</p> <p>Option not set (default): The account definition assignment is not in effect.</p>
Retain account definition on security risk	<p>Specifies the account definition assignment to identities posing a security risk.</p> <p>Option set: The account definition assignment remains in effect. The user account remains intact.</p> <p>Option not set (default): The account definition assignment is not in effect.</p>
Resource type	Resource type for grouping account definitions.
Spare field 01 - spare field 10	Additional company-specific information. Use the Designer to customize display names, formats, and templates for the input fields.
Groups can be inherited	<p>Specifies whether the user account can inherit groups through the linked identity. If the option is set, the user account inherits groups through hierarchical roles, in which the identity is a member, or through IT Shop requests.</p> <ul style="list-style-type: none"> • If you add an identity with a user account to a department, for example, and you have assigned groups to this department, the user account inherits these groups. • If an identity has requested group membership in the IT Shop and the request is granted approval, the identity's user account only inherits the group if the option is set.
System entitlements 1 can be inherited	<p>Specifies whether the user account may inherit system entitlements of the corresponding type through the linked identity. If the option is set, the user account inherits groups through hierarchical roles, in which the identity is a member, or through IT Shop requests.</p> <ul style="list-style-type: none"> • For example, if you add an identity with a user account to a department and you have assigned system entitlements to that department, the user account inherits those system entitlements.
System entitlements 2 can be inherited	
System entitlements 3 can be inherited	

Property	Description
	<ul style="list-style-type: none"> If an identity has requested an assignment to a system entitlement in the IT Shop and this request is approved and assigned, then the identity's user account inherits this system entitlement only if the option is enabled. <p>The options are only displayed if the respective system entitlement type is used in the target system.</p>

Editing manage levels

One Identity Manager supplies a default configuration for manage levels:

- **Unmanaged:** User accounts with the **Unmanaged** manage level are linked to the identity but they do not inherit any further properties. When a new user account is added with this manage level and an identity is assigned, some of the identity's properties are transferred initially. If the identity properties are changed at a later date, the changes are not passed onto the user account.
- **Full managed:** User accounts with the **Full managed** manage level inherit defined properties of the assigned identity. When a new user account is created with this manage level and an identity is assigned, the identity's properties are transferred in an initial state. If the identity properties are changed at a later date, the changes are passed onto the user account.

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

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

Specify how an identity's temporary deactivation, permanent deactivation, deletion, and security risks affect its user accounts and group memberships at each manage level. For more information about manage levels, see the *One Identity Manager Target System Base Module Administration Guide*.

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

To edit a manage level

1. In the Manager, select the **Cloud Target Systems > Basic configuration data > Account definitions > Manage levels** category.
2. Select the manage level in the result list.

3. Select the **Change main data** task.
4. Edit the manage level's main data.
5. Save the changes.

Related topics


- [Main data for manage levels](#) on page 58
- [Creating manage levels](#) on page 57
- [Assigning manage levels to account definitions](#) on page 57

Creating manage levels

One Identity Manager supplies a default configuration for the **Unmanaged** and **Full managed** manage levels. You can define other manage levels depending on your requirements.

IMPORTANT: In the Designer, extend the templates by adding the procedure for the additional manage levels. For more information about templates, see the *One Identity Manager Configuration Guide*

To create a manage level

1. In the Manager, select the **Cloud Target Systems > Basic configuration data > Account definitions > Manage levels** category.
2. Click  in the result list.
3. On the main data form, edit the main data of the manage level.
4. Save the changes.

Related topics

- [Main data for manage levels](#) on page 58
- [Editing manage levels](#) on page 56
- [Assigning manage levels to account definitions](#) on page 57

Assigning manage levels to account definitions


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

To assign manage levels to an account definition

1. In the Manager, select the **Cloud Target Systems > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Assign manage level** task.
4. In the **Add assignments** pane, assign the manage level.

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

To remove an assignment

- Select the manage level and double-click .
5. Save the changes.

Main data for manage levels

Enter the following data for a manage level.

Table 12: Main data for manage levels

Property	Description
Manage level	Name of the manage level.
Description	Text field for additional explanation.
IT operating data overwrites	Specifies whether user account data formatted from IT operating data is automatically updated. Permitted values are: <ul style="list-style-type: none">• Never: Data is not updated. (Default)• Always: Data is always updated.• Only initially: Data is only determined at the start.
Retain groups if temporarily disabled	Specifies whether user accounts of temporarily deactivated retain their group memberships.
Lock user accounts if temporarily disabled	Specifies whether user accounts of temporarily deactivated identities are locked.
Retain groups if permanently disabled	Specifies whether user accounts of permanently deactivated identities retain group memberships.
Lock user accounts if permanently disabled	Specifies whether user accounts of permanently deactivated identities are locked.
Retain groups on deferred deletion	Specifies whether user accounts of identities marked for deletion retain their group memberships.
Lock user accounts if	Specifies whether user accounts of identities marked for

Property	Description
deletion is deferred	deletion are locked.
Retain groups on security risk	Specifies whether user accounts of identities posing a security risk retain their group memberships.
Lock user accounts if security is at risk	Specifies whether user accounts of identities posing a security risk are locked.
Retain groups if user account disabled	Specifies whether disabled user accounts retain their group memberships.

Creating mapping rules for IT operating data

An account definition specifies which rules are used to form the IT operating data and which default values will be used if no IT operating data can be found through the identity's primary roles.

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

To create a mapping rule for IT operating data

1. In the Manager, select the **Cloud Target Systems > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Edit IT operating data mapping** task.
4. Click **Add** and enter the following information:
 - **Column:** User account property for which the value is set. In the drop-down, you can select the columns that use the TSB_ITDataFromOrg script in their template. For more information about this, see the *One Identity Manager Target System Base Module Administration Guide*.
 - **Source:** Specifies which roles to use in order to find the user account properties. You have the following options:
 - Primary department
 - Primary location
 - Primary cost center
 - Primary business roles

NOTE: The business role can only be used if the Business Roles Module is available.

- Empty

If you select a role, you must specify a default value and set the **Always use default value** option.

- **Default value:** Default value of the property for an identity's user account if the value is not determined dynamically from the IT operating data.
- **Always use default value:** Specifies whether the user account property is always set with the default value. IT operating data is not determined dynamically from a role.
- **Notify when applying the default:** Specifies whether an email is sent to a specific mailbox when the default value is used. The **Identity - new user account with default properties created** mail template is used.

To change the mail template, in the Designer, adjust the **TargetSystem | CMS | Accounts | MailTemplateDefaultValues** configuration parameter.

5. Save the changes.

Related topics

- [Entering IT operating data](#) on page 60

Entering IT operating data

To create user accounts for an identity with the **Full managed** manage level, you need to know which IT operating data is required. The operating data required for each specific target system is defined with its business roles, departments, locations, or cost centers. An identity is assigned a primary business role, primary location, primary department, or primary cost center. The necessary IT operating data is ascertained from these assignments and used in creating the user accounts. Default values are used if valid IT operating data cannot be found over the primary roles.

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

Example: Mapping IT operating data

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

Create an account definition A for the default user account of the cloud target system A and an account definition B for the administrative user account of cloud target

system A. In the IT operating data mapping rule for the account definitions A and B, specify the **Department** property in order to determine the valid IT operating data.

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

To define IT operating data

1. In the Manager, select the role in the **Organizations** or **Business roles** category.
2. Select the **Edit IT operating data** task.
3. Click **Add** and enter the following data.
 - **Effects on:** Specify an IT operating data application scope. The IT operating data can be used for a target system or a defined account definition.

To specify an application scope

- a. Click ➔ next to the field.
 - b. Under **Table**, select the table that maps the target system for select the TSBAccountDef table or an account definition.
 - c. Select the specific target system or account definition under **Effects on**.
 - d. Click **OK**.
- **Column:** Select the user account property for which the value is set.

In the drop-down, you can select the columns that use the TSB_ITDataFromOrg script in their template. For more information about this, see the *One Identity Manager Target System Base Module Administration Guide*.
 - **Value:** Enter a fixed value to assign to the user account's property.
4. Save the changes.

Related topics

- [Creating mapping rules for IT operating data](#) on page 59

Modify IT operating data

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

Prerequisites

- The IT operating data of a department, a cost center, a business role, or a location have been changed.
 - OR -
- The default values in the IT operating data template were modified for an account definition.

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

To run the template

1. In the Manager, select the **Cloud Target Systems > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Run templates** task.

This displays a list of all user accounts that were created with the selected account definition and whose properties were changed by modifying the IT operating data. That means:

- **Old value:** Value of the object property before changing the IT operating data.
 - **New value:** Value of the object property after changing the IT operating data.
 - **Selection:** Specifies whether the new value is copied to the user account.
4. Mark all the object properties in the **selection** column that will be given the new value.
 5. Click **Apply**.

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

Assigning account definitions to identities

Account definitions are assigned to company identities.

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

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

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

NOTE: If a user account already exists and is disabled, then it is re-enabled. In this case, you must change the user account manage level afterward.

As long as an account definition for an identity is valid, the identity retains the user account that was created by it. If the account definition assignment is removed, the user account that was created from this account definition, is deleted. User accounts marked as **Outstanding** are only deleted if the **QER | Person | User | DeleteOptions | DeleteOutstanding** configuration parameter is set.

Prerequisites for indirect assignment of account definitions to identities

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

To configure assignments to roles of a role class

1. In the Manager, select role classes in the **Organizations > Basic configuration data > Role classes** category.
- OR -
In the Manager, select role classes in the **Business roles > Basic configuration data > Role classes** category.
2. Select the **Configure role assignments** task and configure the permitted assignments.
 - To generally allow an assignment, enable the **Assignments allowed** column.
 - To allow direct assignment, enable the **Direct assignments permitted** column.
3. Save the changes.

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

Detailed information about this topic

- [Assigning account definitions to departments, cost centers, and locations](#) on page 64
- [Assigning account definitions to business roles](#) on page 64
- [Assigning account definitions to all identities](#) on page 65
- [Assigning account definitions directly to identities](#) on page 66
- [Assigning account definitions to system roles](#) on page 66
- [Adding account definitions in the IT Shop](#) on page 67
- [Assigning account definitions to cloud target systems](#) on page 70

Assigning account definitions to departments, cost centers, and locations


Assign account definitions to departments, cost centers, and locations in order to assign identities to them through these organizations.

To add account definitions to hierarchical roles

1. In the Manager, select the **Cloud Target Systems > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Assign organizations** task.
4. In the **Add assignments** pane, assign the organizations:
 - On the **Departments** tab, assign departments.
 - On the **Locations** tab, assign locations.
 - On the **Cost centers** tab, assign cost centers.

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

To remove an assignment

- Select the organization and double-click .
5. Save the changes.

Related topics

- [Assigning account definitions to business roles](#) on page 64
- [Assigning account definitions to all identities](#) on page 65
- [Assigning account definitions directly to identities](#) on page 66
- [Assigning account definitions to system roles](#) on page 66
- [Adding account definitions in the IT Shop](#) on page 67

Assigning account definitions to business roles


NOTE: This function is only available if the Business Roles Module is installed.

You can assign account definitions to business roles in order to assign them to identities through business roles.

To add account definitions to hierarchical roles

1. In the Manager, select the **Cloud Target Systems > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.

3. Select the **Assign business roles** task.
4. In the **Add assignments** pane, select the role class and assign business roles.

TIP: In the **Remove assignments** pane, you can remove assigned business roles.
To remove an assignment
 - Select the business role and double-click .
5. Save the changes.

Related topics

- [Assigning account definitions to departments, cost centers, and locations](#) on page 64
- [Assigning account definitions to all identities](#) on page 65
- [Assigning account definitions directly to identities](#) on page 66
- [Assigning account definitions to system roles](#) on page 66
- [Adding account definitions in the IT Shop](#) on page 67

Assigning account definitions to all identities

Use this task to assign the account definition to all internal identities. Identities that are marked as external do not obtain this account definition. Once a new internal identity is created, they automatically obtain this account definition. The assignment is calculated by the DBQueue Processor.

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

To assign an account definition to all identities

1. In the Manager, select the **Cloud Target Systems > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Change main data** task.
4. Select the **Disable automatic assignment to identities** task.
5. Confirm the security prompt with **Yes**.
6. Save the changes.

NOTE: To automatically remove the account definition assignment from all identities, run the [DISABLE AUTOMATIC ASSIGNMENT TO IDENTITIES](#) task. The account definition cannot be reassigned to identities from this point on. Existing assignments remain intact.

Related topics

- [Assigning account definitions to departments, cost centers, and locations](#) on page 64
- [Assigning account definitions to business roles](#) on page 64
- [Assigning account definitions directly to identities](#) on page 66
- [Assigning account definitions to system roles](#) on page 66
- [Adding account definitions in the IT Shop](#) on page 67

Assigning account definitions directly to identities

Account definitions can be assigned directly or indirectly to identities. Indirect assignment is carried out by allocating identities and account definitions in company structures, like departments, cost centers, locations, or business roles.


To react quickly to special requests, you can assign account definitions directly to identities.

To assign an account definition directly to identities

1. In the Manager, select the **Cloud Target Systems > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Assign to identities** task.
4. In the **Add assignments** pane, add identities.

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

To remove an assignment

- Select the identity and double-click .
5. Save the changes.

Related topics

- [Assigning account definitions to departments, cost centers, and locations](#) on page 64
- [Assigning account definitions to business roles](#) on page 64
- [Assigning account definitions to all identities](#) on page 65
- [Assigning account definitions to system roles](#) on page 66
- [Adding account definitions in the IT Shop](#) on page 67

Assigning account definitions to system roles

NOTE: This function is only available if the System Roles Module is installed.

Use this task to add an account definition to system roles.


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

To add account definitions to a system role

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

TIP: In the **Remove assignments** pane, you can remove the system role assignment.

To remove an assignment

- Select the system role and double-click .
5. Save the changes.

Related topics

- [Assigning account definitions to departments, cost centers, and locations](#) on page 64
- [Assigning account definitions to business roles](#) on page 64
- [Assigning account definitions to all identities](#) on page 65
- [Assigning account definitions directly to identities](#) on page 66
- [Adding account definitions in the IT Shop](#) on page 67

Adding account definitions in the IT Shop

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

- The account definition must be labeled with the **IT Shop** option.
- The account definition must be assigned to a service item.

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

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

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

To add an account definition to the IT Shop (role-based login)

1. In the Manager, select the **Entitlements > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Add to IT Shop** task.
4. To assign the account definition to shelves, select the **IT Shop shelves** tab and, in the **Add assignments** section, select the shelves with a double-click.
5. To assign the account definition to IT Shop templates, select the **IT Shop templates** tab and, in the **Add assignments** section, select the template with a double-click.
6. Save the changes.

To add an account definition to the IT Shop (non role-based login)

1. In the Manager, select the **Cloud Target Systems > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Add to IT Shop** task.
4. To assign the account definition to shelves, select the **IT Shop shelves** tab and, in the **Add assignments** section, select the shelves with a double-click.
5. To assign the account definition to IT Shop templates, select the **IT Shop templates** tab and, in the **Add assignments** section, select the template with a double-click.
6. Save the changes.

To remove an account definition from individual IT Shop shelves (role-based login)

1. In the Manager, select the **Entitlements > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Add to IT Shop** task.
4. To remove the account definition from the shelves, select the **IT Shop shelves** tab and, in the **Remove assignments** section, double-click the shelves.
5. To remove the account definition from the IT Shop templates, select the **IT Shop templates** tab and, in the **Remove assignments** section, double-click the templates.
6. Save the changes.

To remove an account definition from individual IT Shop shelves (non role-based login)

1. In the Manager, select the **Cloud Target Systems > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Add to IT Shop** task.

4. To remove the account definition from the shelves, select the **IT Shop shelves** tab and, in the **Remove assignments** section, double-click the shelves.
5. To remove the account definition from the IT Shop templates, select the **IT Shop templates** tab and, in the **Remove assignments** section, double-click the templates.
6. Save the changes.

To remove an account definition from all IT Shop shelves (role-based login)

1. In the Manager, select the **Entitlements > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Remove from all shelves (IT Shop)** task.
4. Confirm the security prompt with **Yes**.
5. Click **OK**.

The account definition is removed from all shelves by the One Identity Manager Service. At the same time, any requests and assignment requests with this account definition are canceled.

To remove an account definition from all IT Shop shelves (non role-based login)

1. In the Manager, select the **Cloud Target Systems > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Remove from all shelves (IT Shop)** task.
4. Confirm the security prompt with **Yes**.
5. Click **OK**.

The account definition is removed from all shelves by the One Identity Manager Service. At the same time, any requests and assignment requests with this account definition are canceled.

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

Related topics

- [Main data for account definitions](#) on page 53
- [Assigning account definitions to departments, cost centers, and locations](#) on page 64
- [Assigning account definitions to business roles](#) on page 64
- [Assigning account definitions directly to identities](#) on page 66
- [Assigning account definitions to system roles](#) on page 66

Assigning account definitions to cloud target systems

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

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

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

To assign the account definition to a target system

1. In the Manager, select the target system in the **Cloud target systems** category.
2. Select the **Change main data** task.
3. From the **Account definition (initial)** drop-down, select the account definition for user accounts.
4. Save the changes.

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

Detailed information about this topic

- [Assigning identities automatically to user accounts](#) on page 73

Deleting account definitions

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

To delete an account definition

1. Remove automatic assignments of the account definition from all identities.
 - a. In the Manager, select the **Cloud Target Systems > Basic configuration data > Account definitions > Account definitions** category.
 - b. Select an account definition in the result list.
 - c. Select the **Change main data** task.
 - d. Select the **Disable automatic assignment to identities** task.

- e. Confirm the security prompt with **Yes**.
 - f. Save the changes.
2. Remove direct assignments of the account definition to identities.
 - a. In the Manager, select the **Cloud Target Systems > Basic configuration data > Account definitions > Account definitions** category.
 - b. Select an account definition in the result list.
 - c. Select the **Assign to identities** task.
 - d. In the **Remove assignments** pane, remove identities.
 - e. Save the changes.
3. Remove the account definition's assignments to departments, cost centers, and locations.
 - a. In the Manager, select the **Cloud Target Systems > Basic configuration data > Account definitions > Account definitions** category.
 - b. Select an account definition in the result list.
 - c. Select the **Assign organizations** task.
 - d. In the **Remove assignments** pane, remove the relevant departments, cost centers, and locations.
 - e. Save the changes.
4. Remove the account definition's assignments to business roles.
 - a. In the Manager, select the **Cloud Target Systems > Basic configuration data > Account definitions > Account definitions** category.
 - b. Select an account definition in the result list.
 - c. Select the **Assign business roles** task.
 - d. In the **Remove assignments** pane, remove the business roles.
 - e. Save the changes.
5. If the account definition was requested through the IT Shop, it must be canceled and removed from all IT Shop shelves.

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

To remove an account definition from all IT Shop shelves (role-based login)


- a. In the Manager, select the **Entitlements > Account definitions** category.
- b. Select an account definition in the result list.
- c. Select the **Remove from all shelves (IT Shop)** task.
- d. Confirm the security prompt with **Yes**.
- e. Click **OK**.

The account definition is removed from all shelves by the One Identity Manager Service. At the same time, any requests and assignment requests with this account definition are canceled.

To remove an account definition from all IT Shop shelves (non role-based login)

- a. In the Manager, select the **Cloud Target Systems > Basic configuration data > Account definitions > Account definitions** category.
- b. Select an account definition in the result list.
- c. Select the **Remove from all shelves (IT Shop)** task.
- d. Confirm the security prompt with **Yes**.
- e. Click **OK**.

The account definition is removed from all shelves by the One Identity Manager Service. At the same time, any requests and assignment requests with this account definition are canceled.

6. Remove the required account definition assignment. As long as the account definition is required for another account definition, it cannot be deleted. Check all the account definitions.
 - a. In the Manager, select the **Cloud Target Systems > Basic configuration data > Account definitions > Account definitions** category.
 - b. Select an account definition in the result list.
 - c. Select the **Change main data** task.
 - d. From the **Required account definition** drop-down, remove the account definition.
 - e. Save the changes.
7. Remove the account definition's assignments to target systems.
 - a. In the Manager, select the target system in the **Cloud target systems** category.
 - b. Select the **Change main data** task.
 - c. On the **General** tab, remove the assigned account definitions.
 - d. Save the changes.
8. Delete the account definition.
 - a. In the Manager, select the **Cloud Target Systems > Basic configuration data > Account definitions > Account definitions** category.
 - b. Select an account definition in the result list.
 - c. Click  to delete an account definition.

Assigning identities automatically to user accounts

When you add a user account, an existing identity can automatically be assigned to it. If necessary, a new identity can be created. The identity main data is created on the basis of existing user account main data. This mechanism can be triggered after a new user account is created either manually or through synchronization.

Define criteria for finding identities to apply to automatic identity assignment. If a user account is linked to an identity through the current mode, the user account is given, through an internal process, the default manage level of the account definition entered in the user account's target system. You can customize user account properties depending on how the behavior of the manage level is defined.

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

NOTE: It is not recommended to assign identities using automatic identity assignment in the case of administrative user accounts. Use **Change main data** to assign identities to administrative user accounts for the respective user account.

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

Run the following tasks to assign identities automatically.

- If you want identities to be assigned during the synchronization of user accounts, in the Designer, set the **TargetSystem | CSM | PersonAutoFullsync** configuration parameter and select the required mode.
- If you want identities to be assigned outside synchronization, in the Designer, set the **TargetSystem | CSM | PersonAutoDefault** configuration parameter and select the required mode.
- In the **TargetSystem | CSM | PersonExcludeList** configuration parameter, define the user accounts for which no automatic assignment to identities shall take place.

Example:




```
ADMINISTRATOR|GUEST|KRBGT|TSINTERNETUSER|IUSR_.*|IWAM_.*|SUPPORT_.*|. * | $
```

TIP: You can edit the value of the configuration parameter in the **Exclude list for automatic identity assignment** dialog.

To edit the exclude list for automatic identity assignment

1. In the Designer, edit the **PersonExcludeList** configuration parameter.
2. Click ... next to the **Value** field.

This opens the **Exclude list for Cloud user accounts** dialog.

3. To add a new entry, click  **Add**.
To edit an entry, select it and click  **Edit**.
4. Enter the name of the user account that does not allow identities to be assigned automatically.
Each entry in the list is handled as part of a regular expression. You are allowed to use the usual special characters for regular expressions.
5. To delete an entry, select it and click  **Delete**.
6. Click **OK**.

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

NOTE:

The following applies for synchronization:

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

The following applies outside synchronization:

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

NOTE:

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

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

For more information, see [Managing cloud user accounts through account definitions](#) on page 43.

Related topics

- [Creating account definitions](#) on page 52
- [Assigning account definitions to cloud target systems](#) on page 70
- [Changing manage levels for cloud user accounts](#) on page 77
- [Editing search criteria for automatic identity assignment](#) on page 75
- [Finding identities and directly assigning them to user accounts](#) on page 76

Editing search criteria for automatic identity assignment

The criteria for identity assignments are defined for the target system. You specify which user account properties must match the identity's properties such that the identity can be assigned to the user account. You can limit search criteria further by using format definitions.

The search criterion is written in XML notation to the **Search criteria for automatic identity assignment** column (AccountToPersonMatchingRule) in the CSMRoot table.

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

NOTE: Object definitions for user accounts that can have search criteria applied to them are predefined. For example, if you require other objects definitions that limit a preselection of user accounts, set up the respective custom object definitions in the Designer. For more information, see the *One Identity Manager Configuration Guide*.

To define identity assignment criteria for a cloud target system

1. In the Manager, select the **Cloud target systems > Basic configuration data > Cloud target systems** category.
2. Select the target system in the result list.
3. Select the **Define search criteria for identity assignment** task.
4. Specify which user account properties must match with which identity so that the identity is linked to the user account.

Table 13: Example of search criteria for user accounts

Apply to	Identity column	Column for user account
Cloud user accounts	First name (FirstName) AND Last name (LastName)	First name (FirstName) AND Last name (LastName)

5. Save the changes.

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

Related topics

- [Finding identities and directly assigning them to user accounts](#) on page 76
- [Assigning identities automatically to user accounts](#) on page 73

Finding identities and directly assigning them to user accounts

Based on the search criteria, you can create a suggestion list for the assignment of identities to user accounts and make the assignment directly. User accounts are grouped in different views for this.

- **Suggested assignments:** This view lists all user accounts to which One Identity Manager can assign an identity. All identities are shown that were found using the search criteria and can be assigned.
- **Assigned user accounts:** This view lists all user accounts to which an identity is assigned.
- **No identity assignment:** This view lists all user accounts to which no identity is assigned and for which no identity was found using the search criteria.

NOTE: To display disabled user accounts or deactivated identities in the view, enable the **Even locked accounts are mapped** option.

If you assign a deactivated identity to a user account, it might be locked or deleted depending on the configuration.

To apply search criteria to user accounts

1. In the Manager, select the **Cloud Target Systems > <target system>** category.
2. Select the target system in the result list.
3. Select the **Define search criteria for identity assignment** task.
4. At the bottom of the form, click **Reload**.

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

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

The assignment of identities to user accounts creates connected user accounts (**Linked** state). To create managed user accounts (**Linked configured** state), you can assign an account definition at the same time.

To assign identities directly to user accounts

- Click **Suggested assignments**.
 1. Click the **Selection** box of all user accounts to which you want to assign the suggested identities. Multi-select is possible.
 2. (Optional) Select an account definition in the **Assign this account definition** drop-down, and select a manage level in the **Assign this account manage level** drop-down.
 3. Click **Assign selected**.

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

The identities determined using the search criteria are assigned to the selected user accounts. If an account definition was selected, this is assigned to all selected user accounts.

- OR -

- Click **No identity assignment**.

1. Click **Select identity** for the user account to which you want to assign an identity. Select an identity from the drop-down.
2. Click the **Selection** box of all user accounts to which you want to assign the selected identities. Multi-select is possible.
3. (Optional) Select an account definition in the **Assign this account definition** drop-down, and select a manage level in the **Assign this account manage level** drop-down.
4. Click **Assign selected**.
5. Confirm the security prompt with **Yes**.

The identities displayed in the **Identity** column are assigned to the selected user accounts. If an account definition was selected, this is assigned to all selected user accounts.

To remove assignments

- Click **Assigned user accounts**.

1. Click the **Selection** box of all the user accounts with the identity assignment you want to delete. Multi-select is possible.
2. Click **Remove selected**.
3. Confirm the security prompt with **Yes**.

The assigned identities are removed from the selected user accounts.

Changing manage levels for cloud user accounts

The default manage level is applied if you create user accounts using automatic identity assignment. You can change a user account manage level later.

To change the manage level for a user account

1. In the Manager, select the **Cloud Target Systems > target system > User accounts** category.
2. Select the user account in the result list.
3. Select the **Change main data** task.

4. Select the manage level in the **Manage level** list on the **General** tab.
5. Save the changes.

Related topics

- [Creating and editing cloud user accounts](#) on page 135

Supported user account types

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

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

- Identity type

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

Table 14: Identity types of user accounts

Identity type	Description	Value of the IdentityType column
Primary identity	Identity's default user account.	Primary
Organizational identity	Secondary user account used for different roles in the company, for example for subcontracts with other functional areas.	Organizational
Personalized administrator identity	User account with administrative permissions, used by an identity.	Admin
Sponsored identity	User account used for a specific purpose. For example, for training purposes.	Sponsored
Shared identity	User account with administrative permissions, used by multiple identities.	Shared
Service identity	Service account.	Service

- Privileged user account

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

Detailed information about this topic

- [Default user accounts](#) on page 79
- [Administrative user accounts](#) on page 80
- [Providing an administrative user account for one identity](#) on page 80
- [Providing an administrative user account for multiple identities](#) on page 81
- [Privileged user accounts](#) on page 82

Default user accounts

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

To create default user accounts through account definitions

1. Create an account definition and assign the **Unmanaged** and **Full managed** manage levels.
2. Specify how an identity's temporary deactivation, permanent deactivation, deletion, and security risks affect its user accounts and group memberships at each manage level.
3. Create a formatting rule for IT operating data.

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

The type of IT operating data required depends on the target system. The following settings are recommended for default user accounts:

- In the mapping rule for the `IsGroupAccount` column, use the default value **1** and enable the **Always use default value** option.
 - In the mapping rule for the `IdentityType` column, use the default value **Primary** and enable **Always use default value**.
4. Enter the effective IT operating data for the target system. Select the concrete target system under **Effects on**.
Specify in the departments, cost centers, locations, or business roles that IT operating data should apply when you set up a user account.
 5. Assign the account definition to identities.

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

Related topics

- [Account definitions for cloud user accounts](#) on page 51

Administrative user accounts

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

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

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

Related topics

- [Providing an administrative user account for one identity](#) on page 80
- [Providing an administrative user account for multiple identities](#) on page 81

Providing an administrative user account for one identity


Use this task to create an administrative user account that can be used by an identity.

Prerequisites

- The user account must be labeled as a personalized administrator identity.
- The identity that will be using the user account must be marked as a personalized administrator identity.
- The identity that will be using the user account must be linked to a main identity.

To prepare an administrative user account for an identity

1. Label the user account as a personalized administrator identity.
 - a. In the Manager, select the **Cloud Target Systems > target system > User accounts** category.
 - b. Select the user account in the result list.
 - c. Select the **Change main data** task.

- d. On the **General** tab, in the **Identity** selection list, select **Personalized administrator identity**.
 2. Link the user account to the identity that will be using this administrative user account.
 - a. In the Manager, select the **Cloud Target Systems > target system > User accounts** category.
 - b. Select the user account in the result list.
 - c. Select the **Change main data** task.
 - d. On the **General** tab, in the **Identity** selection list, select the identity that will be using this administrative user account.
- TIP:** If you are the target system manager, you can select  to create a new identity.

Related topics

- [Providing an administrative user account for multiple identities](#) on page 81
- For more information about mapping identity, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Providing an administrative user account for multiple identities

Use this task to create an administrative user account that can be used by more than one identity.


Prerequisites

- The user account must be labeled as a shared identity.
- There must be an identity with the type **Shared identity** available. The shared identity must have a manager.
- The identities who are permitted to use the user account must be labeled as a primary identity.

To prepare an administrative user account for multiple identities

1. Label the user account as a shared identity.
 - a. In the Manager, select the **Cloud Target Systems > target system > User accounts** category.
 - b. Select the user account in the result list.
 - c. Select the **Change main data** task.
 - d. On the **General** tab, in the **Identity** drop-down, select **Shared identity**.

2. Link the user account to an identity.
 - a. In the Manager, select the **Cloud Target Systems > target system > User accounts** category.
 - b. Select the user account in the result list.
 - c. Select the **Change main data** task.
 - d. On the **General** tab, in the **Identity** drop-down, select an identity the type **Shared identity**.

TIP: If you are the target system manager, you can use the  button to create a new shared identity.

3. Assign the identities who will use this administrative user account to the user account.
 - a. In the Manager, select the **Cloud Target Systems > target system > User accounts** category.
 - b. Select the user account in the result list.
 - c. Select the **Assign identities authorized to use** task.
 - d. In the **Add assignments** pane, add identities.

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

To remove an assignment

- Select the identity and double-click .

Related topics

- [Providing an administrative user account for one identity](#) on page 80
- For more information about mapping identity, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Privileged user accounts

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

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

To create privileged users through account definitions

1. Create an account definition. Create a new manage level for privileged user accounts and assign this manage level to the account definition.
2. If you want to prevent the properties for privileged user accounts from being overwritten, set the **IT operating data overwrites** property for the manage level to **Only initially**. In this case, the properties are populated just once when the user accounts are created.
3. Specify how an identity's temporary deactivation, permanent deactivation, deletion, and security risks affect its user accounts and group memberships in the manage level.
4. Create a formatting rule for the IT operating data.

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

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

- In the mapping rule for the `IsPrivilegedAccount` column, use the default value **1** and set the **Always use default value** option.
 - You can also specify a mapping rule for the `IdentityType` column. The column owns different permitted values that represent user accounts.
 - To prevent privileged user accounts from inheriting the entitlements of the default user, define a mapping rule for the `IsGroupAccount` column with a default value of **0** and set the **Always use default value** option.
5. Enter the effective IT operating data for the target system.

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

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

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

TIP: If customization requires that the login names of privileged user accounts follow a defined naming convention, specify how the login names are formatted in the template.

- To use a prefix for the login name, in the Designer, set the **TargetSystem | CSM | Accounts | PrivilegedAccount | SAMAccountName_PrefixTargetSystem** configuration parameter.
- To use a postfix for the login name, in the Designer, set the **TargetSystem | CSM | Accounts | PrivilegedAccount | SAMAccountName_Postfix** configuration parameter.

These configuration parameters are evaluated in the default installation, if a user account is marked with the **Privileged user account** property (`IsPrivilegedAccount` column). The user account login names are renamed according to the formatting rules. This also

occurs if the user accounts are labeled as privileged using the **Mark selected user accounts as privileged** schedule. If necessary, modify the schedule in the Designer.

Related topics

- [Account definitions for cloud user accounts](#) on page 51

Setting deferred deletion for cloud target system user accounts

You can use deferred deletion to specify how long the user accounts remain in the database after deletion is triggered before they are finally removed. By default, user accounts are finally deleted from the database after 30 days. First, the user accounts are disabled or locked. You can reenable the user accounts up until deferred deletion runs. After deferred deletion is run, the user accounts are deleted from the database and cannot be restored anymore.

You have the following options for configuring deferred deletion.

- Global deferred deletion: Deferred deletion applies to user accounts in all target system. The default value is **30** days.
- Target system specific deferred deletion: Deferred deletion can be configured individually for each target system. This deferred deletion overrides global deferred deletion.

To enable deferred deletion separately for each target system

1. In the Manager, configure deferred deletion for the target system.
 - a. In the Manager, select the **Cloud target systems > Basic configuration data > Cloud target systems** category.
 - b. In the result list, select a target system and run the **Change main data** task.
 - c. On the **General** tab, under **Deferred deletion [days]**, enter the deferred deletion value in days.
 - d. Save the changes.
2. In the Designer, create a **Script (deferred deletion)** in the CSUser table.

Example: Script for target system-specific deferred deletion

Deferred deletion of user accounts in a cloud target system depends on the deferred deletion of the target system (UNSRotB.DeleteDelayDays). The following script is given in the CSMUser table.

```
If $FK(UID_CSMRoot).DeleteDelayDays:Int$ > 0 Then
    Value = $FK(UID_CSMRoot).DeleteDelayDays:Int$
End If
```

- Object-specific deferred deletion: Deferred deletion can be configured depending on certain properties of the accounts.

To use object-specific deferred deletion, in the Designer, create a **Script (deferred deletion)** for the CSMUser table.

Example: Script for object-specific deferred deletion

Deferred deletion of privileged user accounts is 10 days. The following **Script (deferred deletion)** is entered in the table.

```
If Not $IsPrivilegedAccount:Bool$ Then
    Value = 10
End If
```

For more information on editing table definitions and configuring deferred deletion in the Designer, see the *One Identity Manager Configuration Guide*.

Related topics

- [General main data for cloud target systems](#) on page 129
- [Deleting cloud user accounts](#) on page 145

Managing assignments of cloud groups and cloud system entitlements

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

In One Identity Manager, you can assign cloud groups and system entitlements directly to user accounts or they can be inherited through departments, cost centers, locations, or business roles. Users can also request the groups and system entitlements through the Web Portal. To do this, groups and system entitlements are provided in the IT Shop.

Detailed information about this topic

- [System entitlements types in cloud target systems](#) on page 86
- [Assigning cloud groups and system entitlements to cloud user accounts in One Identity Manager](#) on page 88
- [Effectiveness of memberships in cloud groups and cloud system entitlements](#) on page 107
- [Inheriting cloud group and system entitlement based on categories](#) on page 110
- [Overview of all assignments](#) on page 112

System entitlements types in cloud target systems

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

Table 15: Mapping system entitlements in the Cloud Systems Management Module

Table in the Universal Cloud Interface	Table in the Cloud Systems Management Module	Display name
UCIGroup	CSMGroup	Groups
UCIGroup1	CSMGroup1	System entitlements 1
UCIGroup2	CSMGroup2	System entitlements 2
UCIGroup3	CSMGroup3	System entitlements 3
UCIItem	CSMItem	Permissions controls

A user account obtains the required entitlements for accessing target system resources through its assignments to groups or system entitlements. Depending on the target system, assignments are maintained either on user accounts (user-based assignment) or on system entitlements (entitlement-based assignment). When setting up synchronization with the default project template, the Universal Cloud Interface connector determines which object type is used to store the assignments. Assignments are mapped in the following tables:

Table 16: User-based assignment

CSMUserHasGroup	Groups: Assignments to user accounts
CSMUserHasGroup1	System entitlements 1: Assignments to user accounts
CSMUserHasGroup2	System entitlements 2: Assignments to user accounts
CSMUserHasGroup3	System entitlements 3: Assignments to user accounts
CSMUserHasItem	User accounts: Permission control assignments

Table 17: Entitlement-based assignment

CSMUserInGroup	User accounts: Assignment to groups
CSMUserInGroup1	User accounts: Assignment to system entitlements 1
CSMUserInGroup2	User accounts: Assignment to system entitlements 2
CSMUserInGroup3	User accounts: Assignment to system entitlements 3

Assignments to permissions controls are always user-based.

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

To display the types of system entitlements used

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

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

NOTE: When setting up attestation procedures, compliance rules, or company policies using system entitlements, be sure to select the correct assignment tables to look at both user-based and entitlement-based assignments.

To set up functions independently of the target system configurations, use the target system mapping in the Unified Namespace. Both user-based and entitlement-based assignments for all types of system entitlements are mapped in the UNSAccountInUNSGroup table; the UNSGroup table contains all system entitlements regardless of type.

For more information about the Unified Namespace, see the *One Identity Manager Target System Base Module Administration Guide*.

Detailed information about the attestation functions, compliance rules, and company policies can be found in the following guides:

One Identity Manager Attestation Administration Guide
One Identity Manager Compliance Rules Administration Guide
One Identity Manager Company Policies Administration Guide

Related topics

- [General main data for cloud target systems](#) on page 129

Assigning cloud groups and system entitlements to cloud user accounts in One Identity Manager

Cloud groups and system entitlements can be assigned to identities directly or indirectly.

In the case of indirect assignment, identities as well as groups and entitlements are organized in hierarchical roles. The number of groups and system entitlements assigned to an identity is calculated from the position in the hierarchy and the direction of inheritance. If you add an identity to hierarchical roles and that identity owns a cloud user account, this user account is added to the cloud groups and system entitlements.

Cloud groups and system entitlements can also be requested in the Web Portal. To do this, add identities to a shop as customers. All cloud groups and system entitlements assigned to this shop as products can be requested by the customers. After approval is granted, requested cloud groups and system entitlements are assigned to the identities.

Through system roles, cloud groups and system entitlements can be grouped together and assigned to identities as a package. You can create system roles that contain only cloud groups or system entitlements. You can also group any number of company resources into a system role.

To react quickly to special requests, you can assign cloud groups and system entitlements directly to user accounts.

Topic	Guide
Basic principles for assigning and inheriting company resources	<i>One Identity Manager Identity Management Base Module Administration Guide</i> <i>One Identity Manager Business Roles Administration Guide</i>
Assigning company resources through IT Shop requests	<i>One Identity Manager IT Shop Administration Guide</i>
System roles	<i>One Identity Manager System Roles Administration Guide</i>

Detailed information about this topic

- [Prerequisites for indirect assignments of cloud groups and system entitlements to cloud user accounts](#) on page 90
- [Assigning cloud groups to departments, cost centers, and locations](#) on page 91
- [Assigning cloud system entitlements to departments, cost centers, and locations](#) on page 92
- [Assigning cloud groups to business roles](#) on page 94
- [Assigning cloud system entitlements to business roles](#) on page 95
- [Adding cloud groups to system roles](#) on page 96
- [Adding cloud system entitlements to system roles](#) on page 97
- [Adding cloud groups to the IT Shop](#) on page 98
- [Adding cloud system entitlements to the IT Shop](#) on page 100
- [Assigning cloud user accounts directly to cloud groups](#) on page 103
- [Assigning cloud user account directly to cloud system entitlements](#) on page 104

- [Assigning cloud groups directly to cloud user accounts](#) on page 105
- [Assigning cloud system entitlements directly to cloud user accounts](#) on page 105

Prerequisites for indirect assignments of cloud groups and system entitlements to cloud user accounts

In the case of indirect assignment, identities as well as cloud groups and entitlements are organized in hierarchical roles. When assigning cloud groups and system entitlements indirectly, check the following settings and modify them if necessary.

1. Identity, cloud group, and system entitlement assignment is permitted for role classes (department, cost center, location, or business roles).

For more information, see the *One Identity Manager Identity Management Base Module Administration Guide*.

To configure assignments to roles of a role class

1. In the Manager, select role classes in the **Organizations > Basic configuration data > Role classes** category.

- OR -

In the Manager, select role classes in the **Business roles > Basic configuration data > Role classes** category.

2. Select the **Configure role assignments** task and configure the permitted assignments.
 - To generally allow an assignment, enable the **Assignments allowed** column.
 - To allow direct assignment, enable the **Direct assignments permitted** column.

3. Save the changes.

2. Settings for assigning cloud groups and system entitlements to cloud user accounts.

- Cloud user accounts are linked to identities.
- The options **Groups can be inherited, System entitlements 1 can be inherited, System entitlements 1 can be inherited** are set on the cloud user accounts.
- Cloud user accounts, cloud groups, and system entitlements belong to the same target system.

NOTE: There are other configuration settings that play a role when company resources are inherited through departments, cost centers, locations, and business roles. For example, role inheritance might be blocked or inheritance of identities not allowed. For more information about the basic principles for assigning company resources, see the

Related topics

- [Creating and editing cloud user accounts](#) on page 135
- [General main data for cloud user accounts](#) on page 136

Assigning cloud groups to departments, cost centers, and locations


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

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

1. In the Manager, select the **Cloud Target Systems > <target system> > Groups** category.
2. Select the group in the result list.
3. Select the **Assign organizations** task.
4. In the **Add assignments** pane, assign the organizations:
 - On the **Departments** tab, assign departments.
 - On the **Locations** tab, assign locations.
 - On the **Cost centers** tab, assign cost centers.

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

To remove an assignment

- Select the organization and double-click .
5. Save the changes.

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

1. In the Manager, select the **Organizations > Departments** category.
- OR -
In the Manager, select the **Organizations > Cost centers** category.
- OR -
In the Manager, select the **Organizations > Locations** category.
2. Select the department, cost center, or location in the result list.
3. Select the **Assign cloud groups and system entitlements** task.

4. Select the **Cloud Groups** tab.
5. In the **Add assignments** pane, assign groups.

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

To remove an assignment

- Select the group and double-click .

6. Save the changes.

Related topics

- [Prerequisites for indirect assignments of cloud groups and system entitlements to cloud user accounts](#) on page 90
- [Assigning cloud system entitlements to departments, cost centers, and locations](#) on page 92
- [Assigning cloud user accounts directly to cloud groups](#) on page 103
- [Adding cloud groups to system roles](#) on page 96
- [Adding cloud groups to the IT Shop](#) on page 98
- [Assigning cloud groups to business roles](#) on page 94
- [Assigning cloud groups directly to cloud user accounts](#) on page 105
- [One Identity Manager users for managing cloud target systems](#) on page 10

Assigning cloud system entitlements to departments, cost centers, and locations

Assign a system entitlement to departments, cost centers, or location such that the system entitlement can be inherited by user accounts through these organizations.


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

1. In the Manager, select the **Cloud target systems > <target system> > System entitlements 1** category.
- OR -
In the Manager, select the **Cloud target systems > <target system> > System entitlements 2** category.
- OR -
In the Manager, select the **Cloud target systems > <target system> > System entitlements 3** category.
2. Select the system entitlement in the result list.

3. Select the **Assign organizations** task.
4. In the **Add assignments** pane, assign the organizations:
 - On the **Departments** tab, assign departments.
 - On the **Locations** tab, assign locations.
 - On the **Cost centers** tab, assign cost centers.

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

To remove an assignment


- Select the organization and double-click .
5. Save the changes.

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

1. In the Manager, select the **Organizations > Departments** category.
 - OR -
 - In the Manager, select the **Organizations > Cost centers** category.
 - OR -
 - In the Manager, select the **Organizations > Locations** category.
2. Select the department, cost center, or location in the result list.
3. Select the **Assign cloud groups and system entitlements** task.
4. In the **Add assignments** pane, assign the system entitlements.
 - On the **Cloud system entitlement 1** tab, assign the system entitlement 1.
 - On the **Cloud system entitlement 2** tab, assign the system entitlement 2.
 - On the **Cloud system entitlement 3** tab, assign the system entitlement 3.

TIP: In the **Remove assignments** pane, you can remove system entitlement assignments.

To remove an assignment

- Select the system entitlement and double-click .
5. Save the changes.

Related topics

- [Prerequisites for indirect assignments of cloud groups and system entitlements to cloud user accounts](#) on page 90
- [Assigning cloud groups to departments, cost centers, and locations](#) on page 91
- [Assigning cloud system entitlements to business roles](#) on page 95
- [Adding cloud system entitlements to system roles](#) on page 97
- [Adding cloud system entitlements to the IT Shop](#) on page 100

- [Assigning cloud user account directly to cloud system entitlements](#) on page 104
- [Assigning cloud system entitlements directly to cloud user accounts](#) on page 105

Assigning cloud groups to business roles


NOTE: This function is only available if the Business Roles Module is installed.

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

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

1. In the Manager, select the **Cloud Target Systems > <target system> > Groups** category.
 2. Select the group in the result list.
 3. Select the **Assign business roles** task.
 4. In the **Add assignments** pane, select the role class and assign business roles.
- TIP:** In the **Remove assignments** pane, you can remove assigned business roles.


To remove an assignment

- Select the business role and double-click .
5. Save the changes.

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

1. In the Manager, select the **Business roles > <role class>** category.
 2. Select the business role in the result list.
 3. Select the **Assign cloud groups and system entitlements** task.
 4. Select the **Cloud Groups** tab.
 5. In the **Add assignments** pane, assign the groups.
- TIP:** In the **Remove assignments** pane, you can remove the assignment of groups.

To remove an assignment

- Select the group and double-click .
6. Save the changes.

Related topics

- [Prerequisites for indirect assignments of cloud groups and system entitlements to cloud user accounts](#) on page 90
- [Assigning cloud system entitlements to business roles](#) on page 95
- [Assigning cloud groups to departments, cost centers, and locations](#) on page 91

- [Adding cloud groups to system roles](#) on page 96
- [Adding cloud groups to the IT Shop](#) on page 98
- [Assigning cloud user accounts directly to cloud groups](#) on page 103
- [Assigning cloud groups directly to cloud user accounts](#) on page 105
- [One Identity Manager users for managing cloud target systems](#) on page 10

Assigning cloud system entitlements to business roles

| NOTE: This function is only available if the Business Roles Module is installed.


Assign a system entitlement to business roles such that the group is inherited by user accounts through these business roles.

To assign a system entitlement to business roles (non role-based login):

1. In the Manager, select the **Cloud target systems > <target system> > System entitlements 1** category.
- OR -
In the Manager, select the **Cloud target systems > <target system> > System entitlements 2** category.
- OR -
In the Manager, select the **Cloud target systems > <target system> > System entitlements 3** category.
2. Select the system entitlement in the result list.
3. Select the **Assign business roles** task.
4. In the **Add assignments** pane, select the role class and assign business roles.

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

To remove an assignment

- Select the business role and double-click .
5. Save the changes.


To assign system entitlements to a business role (non role-based login or role-based login)

1. In the Manager, select the **Business roles > <role class>** category.
2. Select the business role in the result list.
3. Select the **Assign cloud groups and system entitlements** task.
4. In the **Add assignments** pane, assign the system entitlements.

- On the **Cloud system entitlement 1** tab, assign the system entitlement 1.
- On the **Cloud system entitlement 2** tab, assign the system entitlement 2.
- On the **Cloud system entitlement 3** tab, assign the system entitlement 3.

TIP: In the **Remove assignments** pane, you can remove system entitlement assignments.

To remove an assignment

- Select the system entitlement and double-click .

5. Save the changes.

Related topics

- [Prerequisites for indirect assignments of cloud groups and system entitlements to cloud user accounts](#) on page 90
- [Assigning cloud groups to business roles](#) on page 94
- [Assigning cloud system entitlements to departments, cost centers, and locations](#) on page 92
- [Adding cloud system entitlements to system roles](#) on page 97
- [Adding cloud system entitlements to the IT Shop](#) on page 100
- [Assigning cloud user account directly to cloud system entitlements](#) on page 104
- [Assigning cloud system entitlements directly to cloud user accounts](#) on page 105

Adding cloud groups to system roles

NOTE: This function is only available if the System Roles Module is installed.

Use this task to add a group to system roles.

If you assign a system role to identities, all user accounts owned by these identities inherit the group.

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

To assign a group to system roles

1. In the Manager, select the **Cloud Target Systems > <target system> > Groups** category.
2. Select the group in the result list.
3. Select the **Assign system roles** task.

4. In the **Add assignments** pane, assign system roles.

TIP: In the **Remove assignments** pane, you can remove the system role assignment.

To remove an assignment

- Select the system role and double-click .

5. Save the changes.

Related topics

- [Prerequisites for indirect assignments of cloud groups and system entitlements to cloud user accounts](#) on page 90
- [Adding cloud system entitlements to system roles](#) on page 97
- [Assigning cloud groups to departments, cost centers, and locations](#) on page 91
- [Assigning cloud groups to business roles](#) on page 94
- [Adding cloud groups to the IT Shop](#) on page 98
- [Assigning cloud user accounts directly to cloud groups](#) on page 103
- [Assigning cloud groups directly to cloud user accounts](#) on page 105

Adding cloud system entitlements to system roles

NOTE: This function is only available if the System Roles Module is installed.

Use this task to add a system entitlement to system roles.

If you assign a system role to identities, all custom target system user accounts owned by these identities inherit the system entitlement.

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


To assign a system entitlement to system roles

1. In the Manager, select the **Cloud target systems > <target system> > System entitlements 1** category.
- OR -
In the Manager, select the **Cloud target systems > <target system> > System entitlements 2** category.
- OR -
In the Manager, select the **Cloud target systems > <target system> > System entitlements 3** category.

2. Select the system entitlement in the result list.
3. Select the **Assign system roles** task.
4. In the **Add assignments** pane, assign system roles.

TIP: In the **Remove assignments** pane, you can remove the system role assignment.

To remove an assignment

- Select the system role and double-click .
5. Save the changes.

Related topics

- [Prerequisites for indirect assignments of cloud groups and system entitlements to cloud user accounts](#) on page 90
- [Adding cloud groups to system roles](#) on page 96
- [Assigning cloud system entitlements to departments, cost centers, and locations](#) on page 92
- [Assigning cloud system entitlements to business roles](#) on page 95
- [Adding cloud system entitlements to the IT Shop](#) on page 100
- [Assigning cloud user account directly to cloud system entitlements](#) on page 104
- [Assigning cloud system entitlements directly to cloud user accounts](#) on page 105

Adding cloud groups to the IT Shop

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

- The group must be labeled with the **IT Shop** option.
- The group must be assigned a service item.

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

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

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

To add a group to the IT Shop.

1. In the Manager, select the **Cloud Target Systems > <Target system> > Groups** (non role-based login) category.
- OR -
In the Manager, select the **Entitlements > Cloud groups** (role-based login) category.
2. In the result list, select the group.
3. Select the **Add to IT Shop** task.
4. To assign the group to shelves, select the **IT Shop shelves** tab and, in the **Add assignments** section, double-click on the shelves.
5. To assign the group to IT Shop templates, select the **IT Shop templates** tab and, in the **Add assignments** section, double-click on the templates.
6. Save the changes.

To remove a group from individual shelves of the IT Shop

1. In the Manager, select the **Cloud Target Systems > <Target system> > Groups** (non role-based login) category.
- OR -
In the Manager, select the **Entitlements > Cloud groups** (role-based login) category.
2. In the result list, select the group.
3. Select the **Add to IT Shop** task.
4. To remove the group from the shelves, select the **IT Shop shelves** tab and, in the **Remove assignments** section, double-click the shelves.
5. To remove the group from the IT Shop templates, select the **IT Shop templates** tab and, in the **Remove assignments** section, double-click the templates.
6. Save the changes.

To remove a group from all shelves of the IT Shop

1. In the Manager, select the **Cloud Target Systems > <Target system> > Groups** (non role-based login) category.
- OR -
In the Manager, select the **Entitlements > Cloud groups** (role-based login) category.
2. In the result list, select the group.
3. Select the **Remove from all shelves (IT Shop)** task.
4. Confirm the security prompt with **Yes**.
5. Click **OK**.

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

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

Related topics

- [Prerequisites for indirect assignments of cloud groups and system entitlements to cloud user accounts](#) on page 90
- [General main data for cloud groups](#) on page 148
- [Adding cloud system entitlements to the IT Shop](#) on page 100
- [Assigning cloud groups to departments, cost centers, and locations](#) on page 91
- [Assigning cloud groups to business roles](#) on page 94
- [Adding cloud groups to system roles](#) on page 96
- [Assigning cloud user accounts directly to cloud groups](#) on page 103
- [Assigning cloud groups directly to cloud user accounts](#) on page 105

Adding cloud system entitlements to the IT Shop

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

- The system entitlement must be labeled with the **IT Shop** option.
- The system entitlement must be assigned to a service item.

TIP: In the Web Portal, all products that can be requested are grouped together by service category. To make the system entitlement easier to find in the Web Portal, assign a service category to the service item.
- If the system entitlement can only be assigned to identities using IT Shop requests, the system entitlement must be also labeled with the **Only use in IT Shop** option. Direct assignment to hierarchical roles or user accounts is then no longer permitted.

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

To add a system entitlement to the IT Shop

1. Non role-based login:

In the Manager, select the **Cloud target systems > <target system> > System entitlements 1** category.

- OR -

In the Manager, select the **Cloud target systems > <target system> > System entitlements 2** category.

- OR -

In the Manager, select the **Cloud target systems > <target system> > System entitlements 3** category.

Role-based login:

In the Manager, select the **Entitlements > Cloud system entitlements 1** category.

- OR -

In the Manager, select the **Entitlements > Cloud system entitlements 2** category.

- OR -

In the Manager, select the **Entitlements > Cloud system entitlements 3** category.

2. Select the system entitlement in the result list.
3. Select the **Add to IT Shop** task.
4. Select the **IT Shop structures** tab.
5. In the **Add assignments** pane, assign the system entitlement to IT Shop shelves.
6. Save the changes.

To remove a system entitlement from individual IT Shop shelves

1. Non role-based login:

In the Manager, select the **Cloud target systems > <target system> > System entitlements 1** category.

- OR -

In the Manager, select the **Cloud target systems > <target system> > System entitlements 2** category.

- OR -

In the Manager, select the **Cloud target systems > <target system> > System entitlements 3** category.

Role-based login:

In the Manager, select the **Entitlements > Cloud system entitlements 1** category.

- OR -

In the Manager, select the **Entitlements > Cloud system entitlements 2** category.

- OR -

In the Manager, select the **Entitlements > Cloud system entitlements 3** category.

2. Select the system entitlement in the result list.
3. Select the **Add to IT Shop** task.
4. Select the **IT Shop structures** tab.
5. In the **Remove assignments** pane, remove the system entitlement from the IT Shop shelves.
6. Save the changes.

To remove a system entitlement from all IT Shop shelves

1. Non role-based login:

In the Manager, select the **Cloud target systems > <target system> > System entitlements 1** category.

- OR -

In the Manager, select the **Cloud target systems > <target system> > System entitlements 2** category.

- OR -

In the Manager, select the **Cloud target systems > <target system> > System entitlements 3** category.

Role-based login:

In the Manager, select the **Entitlements > Cloud system entitlements 1** category.

- OR -

In the Manager, select the **Entitlements > Cloud system entitlements 2** category.

- OR -

In the Manager, select the **Entitlements > Cloud system entitlements 3** category.

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

The system entitlement is removed from all shelves by the One Identity Manager Service. All requests and assignment requests with this system entitlement are unsubscribed in the process.

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

Related topics

- [Prerequisites for indirect assignments of cloud groups and system entitlements to cloud user accounts](#) on page 90
- [General main data for cloud groups](#) on page 148
- [Adding cloud groups to the IT Shop](#) on page 98
- [Assigning cloud system entitlements to departments, cost centers, and locations](#) on page 92
- [Assigning cloud system entitlements to business roles](#) on page 95
- [Adding cloud system entitlements to system roles](#) on page 97
- [Assigning cloud user account directly to cloud system entitlements](#) on page 104
- [Assigning cloud system entitlements directly to cloud user accounts](#) on page 105

Assigning cloud user accounts directly to cloud groups

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


To react quickly to special requests, you can assign groups directly to user accounts. You cannot directly assign groups that have the **Only use in IT Shop** option.

To assign user accounts directly to a group

1. In the Manager, select the **Cloud Target Systems > <target system> > Groups** category.
2. Select the group in the result list.
3. Select the **Assign user accounts** task.
4. In the **Add assignments** pane, assign the user accounts.

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

To remove an assignment

- Select the user account and double-click .
5. Save the changes.

Related topics

- [Assigning cloud user account directly to cloud system entitlements](#) on page 104
- [Assigning cloud groups directly to cloud user accounts](#) on page 105
- [Assigning cloud groups to departments, cost centers, and locations](#) on page 91

- [Assigning cloud groups to business roles](#) on page 94
- [Adding cloud groups to system roles](#) on page 96
- [Adding cloud groups to the IT Shop](#) on page 98

Assigning cloud user account directly to cloud system entitlements


To react quickly to special requests, you can assign the system entitlements directly to user accounts. You cannot directly assign system entitlements that have the **Only use in IT Shop** option set.

To assign user accounts directly to a system entitlement

1. In the Manager, select the **Cloud target systems > <target system> > System entitlements 1** category.
- OR -
In the Manager, select the **Cloud target systems > <target system> > System entitlements 2** category.
- OR -
In the Manager, select the **Cloud target systems > <target system> > System entitlements 3** category.
2. Select the system entitlement in the result list.
3. Select the **Assign user accounts** task.
4. In the **Add assignments** pane, assign the user accounts.

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

To remove an assignment

- Select the user account and double-click .
5. Save the changes.

Related topics

- [Assigning cloud user accounts directly to cloud groups](#) on page 103
- [Assigning cloud system entitlements to departments, cost centers, and locations](#) on page 92
- [Assigning cloud system entitlements to business roles](#) on page 95
- [Adding cloud system entitlements to system roles](#) on page 97
- [Adding cloud system entitlements to the IT Shop](#) on page 100
- [Assigning cloud system entitlements directly to cloud user accounts](#) on page 105

Assigning cloud groups directly to cloud user accounts


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

To assign groups directly to user accounts

1. In the Manager, select the **Cloud Target Systems > target system > User accounts** category.
2. Select the user account in the result list.
3. Select the **Assign cloud groups and system entitlements** task.
4. Select the **Cloud Groups** tab.
5. In the **Add assignments** pane, assign the groups.

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

To remove an assignment

- Select the group and double-click .

6. Save the changes.

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

Related topics

- [Assigning cloud groups and system entitlements to cloud user accounts in One Identity Manager on page 88](#)
- [Assigning cloud system entitlements directly to cloud user accounts on page 105](#)
- [Assigning cloud groups to departments, cost centers, and locations on page 91](#)
- [Assigning cloud groups to business roles on page 94](#)
- [Adding cloud groups to system roles on page 96](#)
- [Adding cloud groups to the IT Shop on page 98](#)

Assigning cloud system entitlements directly to cloud user accounts

To react quickly to special requests, you can assign system entitlements directly to a user account. You cannot directly assign system entitlements that have the **Only use in**


IT Shop option set.

To assign system entitlements directly to a user account

1. In the Manager, select the **Cloud Target Systems > target system > User accounts** category.
2. Select the user account in the result list.
3. Select the **Assign cloud groups and system entitlements** task.
4. Select the **Cloud system entitlements 1** tab.
 - OR -
 - Select the **Cloud system entitlements 2** tab.
 - OR -
 - Select the **Cloud system entitlements 3** tab.
5. In the **Add assignments** pane, assign the system entitlements.

TIP: In the **Remove assignments** pane, you can remove system entitlement assignments.

To remove an assignment

- Select the system entitlement and double-click .
6. Save the changes.

Related topics

- [Assigning cloud groups directly to cloud user accounts](#) on page 105
- [Assigning cloud system entitlements to departments, cost centers, and locations](#) on page 92
- [Assigning cloud system entitlements to business roles](#) on page 95
- [Adding cloud system entitlements to system roles](#) on page 97
- [Adding cloud system entitlements to the IT Shop](#) on page 100
- [Assigning cloud user account directly to cloud system entitlements](#) on page 104

Assigning default profiles to user accounts in Salesforce applications

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

Prerequisites

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

To change the default profile for new user accounts

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

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

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

Effectiveness of memberships in cloud groups and cloud system entitlements

NOTE: The functionality described here for groups applies equally to system entitlements.

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

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

NOTE:

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

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

Example: The effect of group memberships

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

Jo User1 has a user account in this target system. They primarily belong to the "Marketing" department. The "Control group" business role and the "Finance" department are assigned to them secondarily. Without an exclusion definition, the user account obtains all the permissions of groups A, B, and C.

By using suitable controls, you want to prevent an identity from being able to trigger a request and to pay invoices. That means, groups A, B, and C are mutually exclusive. An identity that checks invoices may not be able to make invoice payments as well. That means, groups B and C are mutually exclusive.

Table 18: Specifying excluded groups (CSMGroupExclusion table)

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

Table 19: Effective assignments

Identity	Member in role	Effective group
Pat Identity1	Marketing	Group A
Jan User3	Marketing, finance	Group B
Jo User1	Marketing, finance, control group	Group C
Chris User2	Marketing, control group	Group A, Group C

Only the group C assignment is in effect for Jo User1. It is published in the target system. If Jo User1 leaves the "control group" business role at a later date, group B also takes effect.

The groups A and C are in effect for Chris User2 because the groups are not defined as mutually exclusive. That means that the identity is authorized to trigger requests and to check invoices. If this should not be allowed, define further exclusion for group C.

Table 20: Excluded groups and effective assignments

Identity	Member in role	Assigned group	Excluded group	Effective group
Chris User2	Marketing	Group A		Group C
	Control group	Group C	Group B Group A	

Prerequisites

- The **QER | Structures | Inherit | GroupExclusion** configuration parameter is set.

In the Designer, set the configuration parameter and compile the database.

NOTE: If you disable the configuration parameter at a later date, model components and scripts that are no longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*.

- Mutually exclusive groups belong to the same cloud target system.

To exclude a group

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

- OR -

In the **Remove assignments** pane, remove the groups that are no longer mutually exclusive.

5. Save the changes.

To exclude system entitlements

1. In the Manager, select the **Cloud target systems > <target system> > System entitlements 1** category.
- OR -
In the Manager, select the **Cloud target systems > <target system> > System entitlements 2** category.
- OR -
In the Manager, select the **Cloud target systems > <target system> > System entitlements 3** category.
2. Select a system entitlement in the result list.
3. Select the **Exclude system entitlements 1** task, **Exclude system entitlements 2** task, or **Exclude system entitlements 3** task to match the selected system entitlement.
4. In the **Add assignments** pane, assign system entitlements that are mutually exclusive to the selected system entitlement.
- OR -
In the **Remove assignments** pane, remove the system entitlements that are no longer mutually exclusive.
5. Save the changes.

Inheriting cloud group and system entitlement based on categories

NOTE: The functionality described here for groups applies equally to system entitlements.

In One Identity Manager, user accounts can selectively inherit groups. To do this, groups and user accounts are divided into categories. The categories can be freely selected and are specified using a mapping rule. Each category is given a specific position within the template. The mapping rule contains different tables. Use the user account table to specify categories for target system dependent user accounts. In the group table, enter your categories for the target system-dependent groups. Each table contains the category positions **position 1** to **position 63**.

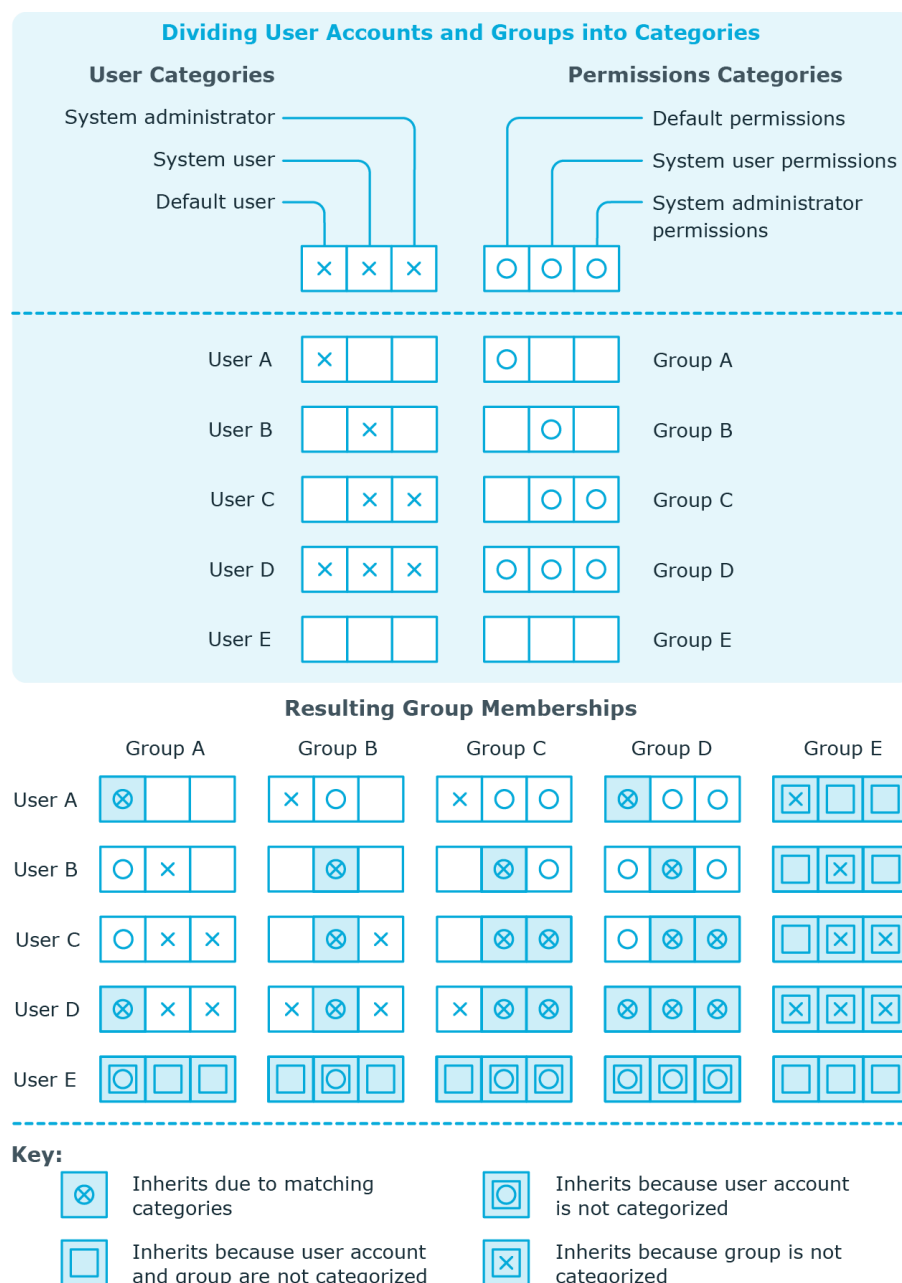
Every user account can be assigned to one or more categories. Each group can also be assigned to one or more categories. The group is inherited by the user account when at least one user account category items matches an assigned group. The group is also inherited by the user account if the group or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

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

Table 21: Category examples

Category item	Categories for user accounts	Categories for groups
1	Default user	Default permissions
2	System users	System user permissions
3	System administrator	System administrator permissions

Figure 3: Example of inheriting through categories.



To use inheritance through categories

- In the Manager, define the categories in the cloud target system.
- Assign categories to user accounts through their main data.
- Assign categories to groups and system entitlements through their main data.

Related topics

- [Defining categories for inheriting cloud groups and system entitlements](#) on page 132
- [General main data for cloud user accounts](#) on page 136
- [General main data for cloud groups](#) on page 148


Overview of all assignments

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

Example: Assignment overview

- If the report is created for a resource, all roles are determined in which there are identities with this resource.
- If the report is created for a group or another system entitlement, all roles are determined in which there are identities with this group or system entitlement.
- If the report is created for a compliance rule, all roles are determined in which there are identities who violate this compliance rule.
- If the report is created for a department, all roles are determined in which identities of the selected department are also members.
- If the report is created for a business role, all roles are determined in which identities of the selected business role are also members.

To display detailed information about assignments

- To display the report, select the base object from the navigation or the result list and select the **Overview of all assignments** report.
- Click the  **Used by** button in the report toolbar to select the role class for which you want to determine whether roles exist that contain identities with the selected base object.

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

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

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



Table 22: Meaning of icons in the report toolbar

Icon	Meaning
	Show the legend with the meaning of the report control elements
	Saves the current report view as a graphic.
	Selects the role class used to generate the report.
	Displays all roles or only the affected roles.

Login credentials for cloud user accounts

When new user accounts are created in One Identity Manager, the passwords needed to log in to the target system are created immediately also. Various options are available for assigning the initial password. Predefined password policies are applied to the passwords, and you can adjust these policies to suit your individual requirements if necessary. You can set up email notifications to distribute the login credentials generated to users.

Detailed information about this topic

- [Password policies for cloud user accounts](#) on page 114
- [Initial password for new cloud user accounts](#) on page 126
- [Email notifications about login data](#) on page 126

Password policies for cloud user accounts

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

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

Detailed information about this topic

- [Predefined password policies](#) on page 115
- [Using password policies](#) on page 116
- [Creating password policies](#) on page 117
- [Custom scripts for password requirements](#) on page 122

- [Password exclusion list](#) on page 125
- [Checking passwords](#) on page 125
- [Testing password generation](#) on page 125

Predefined password policies

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

Password for logging in to One Identity Manager

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

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

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

Password policy for forming identities' central passwords

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

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

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

Password policies for user accounts

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

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

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

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

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

Using password policies

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

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

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

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

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

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

To reassign a password policy

1. In the Manager, select the **Cloud target systems > Basic configuration data > Password policies** category.
2. Select the password policy in the result list.
3. Select **Assign objects**.
4. Click **Add** in the **Assignments** section and enter the following data.
 - **Apply to:** Application scope of the password policy.

To specify an application scope

1. Click ➔ next to the field.
2. Select one of the following references under **Table**:
 - The table that contains the base objects of synchronization.
 - To apply the password policy based on the account definition, select the **TSBAccountDef** table.

- To apply the password policy based on the manage level, select the **TSBBehavior** table.
3. Under **Apply to**, select the table that contains the base objects.
 - If you have selected the table containing the base objects of synchronization, next select the specific target system.
 - If you have selected the **TSBAccountDef** table, next select the specific account definition.
 - If you have selected the **TSBBehavior** table, next select the specific manage level.
 4. Click **OK**.
 - **Password column**: Name of the password column.
 - **Password policy**: Name of the password policy to use.
 5. Save the changes.


To change a password policy's assignment

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

Creating password policies

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

To create a password policy

1. In the Manager, select the **Cloud target systems > Basic configuration data > Password policies** category.
2. Click  in the result list.
3. On the main data form, enter the main data of the password policy.
4. Save the changes.

Detailed information about this topic

- [General main data of password policies](#) on page 118
- [Policy settings](#) on page 119
- [Character classes for passwords](#) on page 120
- [Custom scripts for password requirements](#) on page 122

Editing password policies

Predefined password policies are supplied with the default installation that you can use or customize if required.

To edit a password policy

1. In the Manager, select the **Cloud target systems > Basic configuration data > Password policies** category.
2. In the result list, select the password policy.
3. Select the **Change main data** task.
4. Edit the password policy's main data.
5. Save the changes.


Detailed information about this topic



- [General main data of password policies](#) on page 118
- [Policy settings](#) on page 119
- [Character classes for passwords](#) on page 120
- [Custom scripts for password requirements](#) on page 122
- [Creating password policies](#) on page 117

General main data of password policies

Enter the following main data of a password policy.

Table 23: main data for a password policy

Property	Meaning
Display name	Password policy name. Translate the given text using the  button.
Description	Text field for additional explanation. Translate the given text

Property	Meaning
	using the  button.
Error Message	Custom error message generated if the policy is not fulfilled. Translate the given text using the  button.
Owner (Application Role)	Application roles whose members can configure the password policies.
Default policy	Mark as default policy for passwords. This option cannot be changed. NOTE: The One Identity Manager password policy is marked as the default policy. This password policy is applied if no other password policy can be found for identities, user accounts, or system users.

Policy settings

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

Table 24: Policy settings

Property	Meaning
Initial password	Initial password for newly created user accounts. The initial password is used if a password is not entered when you create a user account or if a random password is not generated.
Password confirmation	Reconfirm password.
Minimum Length	Minimum length of the password. Specify the number of characters a password must have. If the value is 0 , no password is required.
Max. length	Maximum length of the password. Specify the number of characters a password can have. The maximum permitted value is 256 .
Max. errors	Maximum number of errors. Set the number of invalid passwords attempts. The number of failed logins is only taken into account when logging in to One Identity Manager. If the value is 0 , the number of failed logins is not taken into account. This data is only taken into account if the One Identity Manager login was through a system user or identity based authentication module. If a user has exceeded the maximum number of failed logins, the identity or system

Property	Meaning
	<p>user will not be able to log in to One Identity Manager.</p> <p>You can use the Password Reset Portal to reset the passwords of identities and system users who have been locked. For more information, see the <i>One Identity Manager Web Portal User Guide</i>.</p>
Validity period	Maximum age of the password. Enter the length of time a password can be used before it expires. If the value is 0 , then the password does not expire.
Password history	Enter the number of passwords to be saved. If, for example, a value of 5 is entered, the user's last five passwords are stored. If the value is 0 , then no passwords are stored in the password history.
Minimum password strength	Specifies how secure the password must be. The higher the password strength, the more secure it is. The value 0 means that the password strength is not tested. The values 1 , 2 , 3 and 4 specify the required complexity of the password. The value 1 represents the lowest requirements in terms of password strength. The value 4 requires the highest level of complexity.
Name properties denied	Specifies whether name properties are permitted in the password. If this option is set, name properties are not permitted in passwords. The values of these columns are taken into account if the Contains name properties for password check option is set. In the Designer, adjust this option in the column definition. For more information, see the <i>One Identity Manager Configuration Guide</i> .

Character classes for passwords

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

Table 25: Character classes for passwords

Property	Meaning
Required number of character classes	<p>Number of rules for character classes that must be fulfilled so that a password adheres to the password policy. The following rules are taken into account for Min. number letters, Min. number lowercase, Min. number uppercase, Min. number digits, and Min. number special characters.</p> <p>That means:</p>

Property	Meaning
	<ul style="list-style-type: none"> Value 0: All character class rules must be fulfilled. Value >0: Minimum number of character class rules that must be fulfilled. At most, the value can be the number of rules with a value >0. <p> NOTE: Generated passwords are not tested for this.</p>
Min. number letters	Specifies the minimum number of alphabetical characters the password must contain.
Min. number lowercase	Specifies the minimum number of lowercase letters the password must contain.
Min. number uppercase	Specifies the minimum number of uppercase letters the password must contain.
Min. number digits	Specifies the minimum number of digits the password must contain.
Min. number special characters	Specifies the minimum number of special characters the password must contain.
Permitted special characters	List of permitted special characters.
Max. identical characters in total	Specifies the maximum number of identical characters that can be present in the password in total.
Max. identical characters in succession	Specifies the maximum number of identical character that can be repeated after each other.
Denied special characters	List of special characters that are not permitted.
Do not generate lowercase letters	Specifies whether a generated password can contain lowercase letters. This setting only applies when passwords are generated.
Do not generate uppercase	Specifies whether a generated password can contain uppercase letters. This setting only applies when passwords are generated.

Property	Meaning
letters	
Do not generate digits	Specifies whether a generated password can contain digits. This setting only applies when passwords are generated.
Do not generate special characters	Specifies whether a generated password can contain special characters. If this option is set, only letters, numbers, and spaces are allowed in passwords. This setting only applies when passwords are generated.

Custom scripts for password requirements

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

Detailed information about this topic

- [Checking passwords with a script](#) on page 122
- [Generating passwords with a script](#) on page 124

Checking passwords with a script

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

Syntax of check scripts

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

With parameters:

policy = password policy object

spwd = password to check

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

Example: Script that checks a password

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

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

To use a custom script for checking a password

1. In the Designer, create your script in the **Script Library** category.
2. Edit the password policy.
 - a. In the Manager, select the **Cloud target systems > Basic configuration data > Password policies** category.
 - b. On the **Scripts** tab, enter the name of the script to be used to check a password in the **Check script** field.
 - c. (Optional) On the **Scripts** tab, in the **Additional requirements** field, enter the description of the additional requirements for the password that are checked by the script.
 - d. Save the changes.

Related topics

- [Generating passwords with a script](#) on page 124

Generating passwords with a script

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

Syntax for generating script

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

With parameters:

policy = password policy object

spwd = generated password

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

Example: Script that generates a password

In random passwords, this script replaces the invalid characters ? and ! at the beginning of a password with _.

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

```
    Dim pwd = spwd.ToInsecureArray()
```

```
    ' replace invalid characters at first position
```

```
    If pwd.Length>0
```

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

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

```
        End If
```

```
    End If
```

```
End Sub
```

To use a custom script for generating a password

1. In the Designer, create your script in the **Script Library** category.
2. Edit the password policy.
 - a. In the Manager, select the **Cloud target systems > Basic configuration data > Password policies** category.
 - b. On the **Scripts** tab, enter the name of the script to be used to generate a password in the **Generating script** field.
 - c. Save the changes.

Related topics

- [Checking passwords with a script](#) on page 122

Password exclusion list

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

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

To add a term to the restricted list

1. In the Designer, select the **Base data > Security settings > Password policies** category.
2. Create a new entry with the **Object > New** menu item and enter the term you want to exclude from the list.
3. Save the changes.

Checking passwords

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

To verify if a password conforms to the password policy

1. In the Manager, select the **Cloud target systems > Basic configuration data > Password policies** category.
2. Select the **Test** tab.
3. Select the table and object to be tested in **Base object for test**.
4. Enter a password in **Enter password to test**.

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

Testing password generation

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

To generate a password that conforms to the password policy

1. In the Manager, select the **Cloud target systems > Basic configuration data > Password policies** category.
2. Select the **Test** tab.
3. Click **Generate**.

This generates and displays a password.

Initial password for new cloud user accounts

You can issue an initial password for a new user account in the following ways:

- When you create the user account, enter a password in the main data.
- Assign a randomly generated initial password to enter when you create user accounts.
 - In the Designer, set the **TargetSystem | CSM | Accounts | InitialRandomPassword** configuration parameter.
 - Apply target system specific password policies and define the character sets that the password must contain.
 - Specify which identity will receive the initial password by email.

Related topics

- [Password policies for cloud user accounts](#) on page 114
- [Email notifications about login data](#) on page 126

Email notifications about login data

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

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

1. Ensure that the email notification system is configured in One Identity Manager. For more information, see the *One Identity Manager Installation Guide*.

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

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

To send initial login data by email

1. In the Designer, set the **TargetSystem | CSM | Accounts | InitialRandomPassword** configuration parameter.
2. In the Designer, set the **TargetSystem | CSM | Accounts | InitialRandomPassword | SendTo** configuration parameter and enter the message recipient as a value.
3. In the Designer, set the **TargetSystem | CSM | Accounts | InitialRandomPassword | SendTo | MailTemplateAccountName** configuration parameter.
By default, the message sent uses the mail template **Identity - new user account created**. The message contains the name of the user account.
4. In the Designer, set the **TargetSystem | CSM | Accounts | InitialRandomPassword | SendTo | MailTemplatePassword** configuration parameter.
By default, the message sent uses the mail template **Identity - initial password for new user account**. The message contains the initial password for the user account.

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

Mapping cloud objects in One Identity Manager

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

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

Detailed information about this topic

- [Cloud target systems](#) on page 128
- [Container structures](#) on page 133
- [Cloud user accounts](#) on page 134
- [Cloud groups](#) on page 147
- [Cloud permissions controls](#) on page 159
- [Reports about objects in cloud target systems](#) on page 163

Cloud target systems

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

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

To edit a cloud system's main data

1. In the Manager, select the **Cloud target systems > Basic configuration data > Cloud target systems** category.
2. Select the target system in the result list.

3. Select the **Change main data** task.
4. Edit the target system type main data.
5. Save the changes.

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

Detailed information about this topic

- [General main data for cloud target systems](#) on page 129
- [Defining categories for inheriting cloud groups and system entitlements](#) on page 132
- [Specifying alternative names](#) on page 132
- [Setting deferred deletion for cloud target system user accounts](#) on page 84
- [Editing the synchronization project for a cloud target system](#) on page 133

General main data for cloud target systems

Enter the following main data for a cloud target system.

Table 26: Cloud target system main data

Property	Description
Cloud target system	Name of the target system.
Canonical name	Name of the target system conforming with DNS syntax. target system name.parent target system name.primary system name Example: DHW2k01.Testlab.com
Distinguished name	Cloud target system's distinguished name. This distinguished name is used to form distinguished names for child objects. If the target system does not supply any distinguished names, you can enter the target system identifier here, for example. Syntax example: DC = <target system>
Display name	Name that is displayed in the One Identity Manager tools for the target system.
Account definition (initial)	Initial account definition for creating user accounts. This account definition is used if automatic assignment of identities to user accounts is used for this cloud target system and user accounts should be created which are already managed (Linked configured state). The account definition's default manage level is applied. User accounts are only linked to the identity (Linked) if no account


Property	Description
	definition is given. This is the case on initial synchronization, for example.
Deferred deletion [days]	Number of days to defer deletion operations for this target system. For more information, see Setting deferred deletion for cloud target system user accounts on page 84.
Target system managers	<p>Application role in which target system managers are specified. The target system managers only modify the cloud target system objects assigned to them. Therefore, each cloud target system can have a different target system manager assigned to it.</p> <p>Select the One Identity Manager application role whose members are responsible for administration of this cloud target system. Use the  button to add a new application role.</p>
Synchronized by	<p>Type of synchronization through which the data is synchronized between the target system and One Identity Manager. You can no longer change the synchronization type once objects for this target system are present in One Identity Manager.</p> <p>If you create a cloud target system with the Synchronization Editor, One Identity Manager is used.</p>

Table 27: Permitted values

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

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

Types of system entitlements used	Types of system entitlements to which user accounts can be assigned in this cloud target system.
User account has memberships	<p>Specifies for which types of system entitlements, assignments are maintained in the user accounts.</p> <p>Enable the types with assignments that are maintained in the user accounts.</p> <p>Disable the types with system entitlement assignments to be maintained.</p>

Property	Description
	<div> <p>Example:</p> <p>In the System entitlement types used menu, the values Group and System entitlement 1 are selected. In the User account has memberships menu, only the value System entitlement 1 is selected.</p> <p>The assignments of user accounts to groups are saved with the groups, the assignment of user accounts to system entitlements 1 are saved with the user accounts.</p> </div>
Description	Text field for additional explanation.
Manual provisioning	<p>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.</p> <p>Set this option, if object modifications are not allowed to be published automatically in the cloud application. Use the Web Portal to transfer the changes to the cloud application. For more information about provisioning object modifications, see the <i>One Identity Manager Administration Guide for Connecting to Cloud Applications</i>.</p> <p>IMPORTANT: If you set this option, ensure that data, using regular and frequent synchronization,</p> <ul style="list-style-type: none"> • between the Universal Cloud Interface Module and the cloud application and • between the modules Universal Cloud Interface and Cloud Systems Management <p>is kept consistent!</p>
User account deletion not permitted	Specifies whether user accounts in the cloud target system can be deleted. If this option is set, user account can only be disabled.

Related topics


- [Assigning identities automatically to user accounts](#) on page 73
- [Target system managers](#) on page 169
- [System entitlements types in cloud target systems](#) on page 86

Defining categories for inheriting cloud groups and system entitlements

NOTE: The functionality described here for groups applies equally to system entitlements.

In One Identity Manager, user accounts can selectively inherit groups. To do this, groups and user accounts are divided into categories. The categories can be freely selected and are specified using a mapping rule. Each category is given a specific position within the template. The mapping rule contains different tables. Use the user account table to specify categories for target system dependent user accounts. In the group table, enter your categories for the target system-dependent groups. Each table contains the category positions **position 1** to **position 63**.

To define a category

1. In the Manager, select the target system in the **Cloud target systems** category.
2. Select the **Change main data** task.
3. Switch to the **Mapping rule category** tab.
4. Extend the relevant roots of a table.
5. To enable the category, double-click .
6. Enter a category name of your choice for user accounts and groups in the login language that you use.
7. Save the changes.

Detailed information about this topic

- [Inheriting cloud group and system entitlement based on categories](#) on page 110

Specifying alternative names

You can use alternative names for each target system to improve how different objects types of a custom target system are presented.

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

To specify alternative column names

1. In the Manager, select the **Cloud target systems > Basic configuration data > Cloud target systems** category.
2. In the result list, select a target system and run the **Change main data** task.

3. Switch to the **Alternative names** tab.
This displays all the default names for the tables and columns.
4. Enter any name in the login language in use.
5. Save the changes.

Editing the synchronization project for a cloud target system

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

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

To open an existing synchronization project in the Synchronization Editor:

1. In the Manager, select the **Cloud target systems > Basic configuration data > Cloud target systems** category.
2. Select the target system in the result list.
3. Select the **Change main data** task.
4. Select the **Edit synchronization project** task.


Related topics

- [Customizing the synchronization configuration](#) on page 28

Container structures

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

To edit or create a container

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

3. Edit the container's main data.
4. Save the changes.

Enter the following main data of a container.

Table 28: Main data for a container

Property	Description
Name	Container name.
Distinguished name	Container's distinguished name.
Parent container	Parent container for mapping a hierarchical container structure.
Cloud target system	The container's cloud target system.
Description	Text field for additional explanation.
Account manager	Manager responsible for the container. To specify an account manager <ol style="list-style-type: none">1. Click ➔ next to the field.2. In the Table menu, select the table that maps the account manager.3. In the Account manager menu, select the manager.4. Click OK.
Target system managers	Application role in which target system managers are specified for the container. Target system managers only edit container objects that are assigned to them. Each container can have a different target system manager assigned to it. Select the One Identity Manager application role whose members are responsible for administration of this container. Use the ➕ button to add a new application role.

Related topics

- [Target system managers](#) on page 169

Cloud user accounts

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

Detailed information about this topic

- [Managing cloud user accounts and identities](#) on page 50
- [Supported user account types](#) on page 78
- [Creating and editing cloud user accounts](#) on page 135
- [Assigning permissions controls to cloud user accounts](#) on page 143
- [Assigning extended properties to cloud user accounts](#) on page 144
- [Locking and unlocking cloud user accounts](#) on page 144
- [Deleting cloud user accounts](#) on page 145
- [Displaying the cloud user account overview](#) on page 146


Creating and editing cloud user accounts

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

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

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

To create a user account

1. In the Manager, select the **Cloud Target Systems > target system > User accounts** category.
2. Click  in the result list.
3. On the main data form, edit the main data of the user account.
4. Save the changes.

To edit main data of a user account

1. In the Manager, select the **Cloud Target Systems > target system > User accounts** category.
2. Select the user account in the result list.
3. Select the **Change main data** task.
4. Edit the user account's resource data.
5. Save the changes.

To manually assign a user account for an identity

1. In the Manager, select the **Identities > Identities** category.
2. Select the identity in the result list.
3. Select the **Assign cloud user accounts** task.
4. Assign a user account.
5. Save the changes.

Detailed information about this topic

- [General main data for cloud user accounts](#) on page 136
- [Login data for cloud user accounts](#) on page 140
- [Details of cloud user account identification](#) on page 141
- [Contact data for cloud user accounts](#) on page 142
- [User-defined main data for cloud user accounts](#) on page 142

Related topics


- [Deleting cloud user accounts](#) on page 145

General main data for cloud user accounts

Enter the following general main data.

Table 29: User account properties

Property	Description
Identity	<p>Identity that uses this user account.</p> <ul style="list-style-type: none">• An identity is already entered if the user account was generated by an account definition.• If you are using automatic identity assignment, an associated identity is found and added to the user account when you save the user account.• If you create the user account manually, you can select an identity in the drop-down. <p>The drop-down displays activated and deactivated identities by default. If you do not want to see any deactivated identities, set the QER Person HideDeactivatedIdentities configuration parameter.</p> <p>NOTE: If you assign a deactivated identity to a user account, it might be locked or deleted depending on the configuration.</p>

Property	Description
	<p>You can create a new identity for a user account with an identity of type Organizational identity, Personalized administrator identity, Sponsored identity, Shared identity, or Service identity. To do this, click  next to the input field and enter the required identity main data. Which login data is required depends on the selected identity type.</p>
No link to an identity required	<p>Specifies whether the user account is intentionally not assigned an identity. The option is automatically set if a user account is included in the exclusion list for automatic identity assignment or a corresponding attestation is carried out. You can set the option manually. Enable the option if the user account does not need to be linked with an identity (for example, if several identities use the user account).</p> <p>If attestation approves these user accounts, these user accounts will not be submitted for attestation in the future. In the Web Portal, user accounts that are not linked to an identity can be filtered according to various criteria.</p>
Not linked to an identity	<p>Indicates why the No link to an identity required option is enabled for this user account. Possible values:</p> <ul style="list-style-type: none"> • By administrator: The option was set manually by the administrator. • By attestation: The user account was attested. • By exclusion criterion: The user account is not associated with an identity due to an exclusion criterion. For example, the user account is included in the exclude list for automatic identity assignment (configuration parameter PersonExcludeList).
Target system	The user account's cloud target system.
Account definition	<p>Account definition through which the user account was created.</p> <p>Use the account definition to automatically fill user account main data and to specify a manage level for the user account. One Identity Manager finds the IT operating data of the assigned identity and enters it in the corresponding fields in the user account.</p> <p>NOTE: The account definition cannot be changed once the user account has been saved.</p> <p>NOTE: Use the user account's Remove account definition task to reset the user account to Linked status. This removes the account definition from both the user account and the identity. The user account remains but is not managed by the account definition anymore. The task only removes account definitions that are directly assigned (XOrigin=1).</p>
Manage level	Manage level of the user account. Select a manage level from the drop-down. You can only specify the manage level can if you have also entered

Property	Description
	an account definition. All manage levels of the selected account definition are available in the drop-down.
Form of address	Identity's form of address.
First name	The user's first name. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
Last name	The user's last name. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
Full name	Full name of the user account.
Initials	The user's initials. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
Job description	The user's job description. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
Nickname	Additional information about the user account.
Surname prefix	A prefix to the user's surname, for example von or de .
Display name	User account display name.
Alias	Alias for further identification of the user account.
Name	User account identifier.
Container	Container in which to create the user account. If you have assigned an account definition, the container is determined from the company IT data for the assigned identity depending on the manage level of the user account.
First primary group	User account's primary group.
Second primary group	Additional primary group for the user account. If there group with different groups types in the target system, you can assign another primary group here.
Email address	User account's email address.
Email encoding	Type of email encoding.
Account expiry date	The date from which the user account can no longer be used to log in. If a leaving date is specified for an identity, this date is used as the account expiration date depending on the manage level. Any existing account expiry date is overwritten in this case.

Property	Description
	<p>NOTE: If the identity's leaving date is deleted at a later point in time, the user account expiration date remains intact!</p>
Resource type	Type of the resource, for example, user .
Risk index (calculated)	Maximum risk index value of all assigned groups. The property is only visible if the QER CalculateRiskIndex configuration parameter is set. For more information, see the <i>One Identity Manager Risk Assessment Administration Guide</i> .
Category	Categories for the inheritance of groups by the user account. Groups can be selectively inherited by user accounts. To do this, groups and user accounts or contacts are divided into categories. Select one or more categories from the drop-down.
Description	Text field for additional explanation.
Login name	Name the user uses to log onto the target system. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
Identity type	<p>User account's identity type Permitted values are:</p> <ul style="list-style-type: none"> • Primary identity: Identity's default user account. • Organizational identity: Secondary user account used for different roles in the organization, for example for subcontracts with other functional areas. • Personalized administrator identity: User account with administrative permissions, used by one identity. • Sponsored identity: User account to use for a specific purpose. Training, for example. • Shared identity: User account with administrative permissions, used by several identities. Assign all identities that use this user account. • Service identity: Service account.
Privileged user account.	Specifies whether this is a privileged user account.
Groups can be inherited	<p>Specifies whether the user account can inherit groups through the linked identity. If the option is set, the user account inherits groups through hierarchical roles, in which the identity is a member, or through IT Shop requests.</p> <ul style="list-style-type: none"> • If you add an identity with a user account to a department, for example, and you have assigned groups to this department, the user account inherits these groups.

Property	Description
	<ul style="list-style-type: none"> If an identity has requested group membership in the IT Shop and the request is granted approval, the identity's user account only inherits the group if the option is set.
System entitlements 1 can be inherited	Specifies whether the user account may inherit system entitlements of the corresponding type through the linked identity. If the option is set, the user account inherits groups through hierarchical roles, in which the identity is a member, or through IT Shop requests.
System entitlements 2 can be inherited	<ul style="list-style-type: none"> For example, if you add an identity with a user account to a department and you have assigned system entitlements to that department, the user account inherits those system entitlements.
System entitlements 3 can be inherited	<ul style="list-style-type: none"> If an identity has requested an assignment to a system entitlement in the IT Shop and this request is approved and assigned, then the identity's user account inherits this system entitlement only if the option is enabled. <p>The options are only displayed if the respective system entitlement type is used in the target system.</p>
User account is disabled	Specifies whether the user account is locked. If a user account is not required for a period of time, you can temporarily disable the user account by using the <User account is deactivated> option.

Related topics

- [Assigning identities automatically to user accounts](#) on page 73
- [Prerequisites for indirect assignments of cloud groups and system entitlements to cloud user accounts](#) on page 90
- [Locking and unlocking cloud user accounts](#) on page 144
- [System entitlements types in cloud target systems](#) on page 86
- [General main data for cloud target systems](#) on page 129

Login data for cloud user accounts

NOTE: One Identity Manager password policies are taken into account when a user password is being verified. Ensure that the password policy does not violate the target system's requirements.

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

Table 30: User account login data

Property	Description
Password/Password confirmation	<p>Password for the user account. The identity's central password can be mapped to the user account password. For more information about an identity's central password, see <i>One Identity Manager Identity Management Base Module Administration Guide</i>.</p> <p>If you use a random generated initial password for the user accounts, it is automatically entered when a user account is created.</p> <p>The password is deleted from the database after publishing to the target system.</p>
Password last changed	Date on which the password was last changed.
Last login	Date and time of the last login to the cloud application.

Related topics

- [Password policies for cloud user accounts](#) on page 114

Details of cloud user account identification

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

Table 31: 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.

Property	Description
Room	Room.
Department	Identity's department
Division	Division the accounts belongs to.
Organization	Organization the accounts belongs to.
Personnel number	Number for identifying the identity, in addition to their ID.
Employment	Type of job.
Account manager	Manager responsible for the user account.

To specify an account manager

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

Contact data for cloud user accounts

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

Table 32: Contact data for a user account

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

User-defined main data for cloud user accounts

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

Table 33: Customized main data of a user account

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

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

Assigning permissions controls to cloud user accounts


Use this task to assign permissions controls directly to user accounts.

To assign permissions controls to a user account

1. In the Manager, select the **Cloud Target Systems > target system > User accounts** category.
2. Select the user account in the result list.
3. Select **Assign permissions controls**.
4. In the **Add assignments** pane, assign permissions controls.

TIP: In the **Remove Assignments** pane, you can remove the assigned permission controls.

To remove an assignment

- Select the permissions control and double-click .
5. Save the changes.

Related topics

- [Assigning cloud user accounts to cloud permissions controls](#) on page 161

Assigning extended properties to cloud user accounts

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


For more information about using extended properties, see the *One Identity Manager Compliance Rules Administration Guide*.

To specify extended properties for a user account

1. In the Manager, select the **Cloud Target Systems > target system > User accounts** category.
2. Select the user account in the result list.
3. Select **Assign extended properties**.
4. In the **Add assignments** pane, assign extended properties.

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

To remove an assignment

- Select the extended property and double-click .
5. Save the changes.

Locking and unlocking cloud user accounts

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

Scenario: The user accounts are linked to identities and are managed through account definitions.

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

Scenario: The user accounts are linked to identities. No account definition is applied.

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

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

To disable the user account when the configuration parameter is disabled

1. In the Manager, select the **Cloud Target Systems > target system > User accounts** category.
2. Select the user account in the result list.
3. Select the **Change main data** task.
4. On the **General** tab, set the **Account is disabled** option.
5. Save the changes.

Scenario: The user accounts are not linked to identities.

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

1. In the Manager, select the **Cloud Target Systems > target system > User accounts** category.
2. Select the user account in the result list.
3. Select the **Change main data** task.
4. On the **General** tab, set the **Account is disabled** option.
5. Save the changes.

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


Related topics

- [Account definitions for cloud user accounts](#) on page 51
- [Creating manage levels](#) on page 57

Deleting cloud user accounts

You can delete a user account from the result list or the menu base. After you have confirmed the security alert the user account is marked for deletion in the One Identity Manager. The user account is locked in One Identity Manager and finally deleted from the database and the One Identity Manager depending on the deferred deletion setting.

To delete a user account

1. In the Manager, select the **Cloud Target Systems > target system > User accounts** category.
2. Select the user account in the result list.
3. Click  in the result list.
4. Confirm the security prompt with **Yes**.

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

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

To prevent user accounts from being deleted

1. In the Manager, select the **Cloud target systems > Basic configuration data > Cloud target systems** category.
2. Select the target system in the result list.
3. Select the **Change main data** task.
4. Set the **User account deletion not permitted** option.
5. Save the changes.

Detailed information about this topic

- [Provisioning object changes](#) on page 47
- [General main data for cloud target systems](#) on page 129
- [Locking and unlocking cloud user accounts](#) on page 144
- [Setting deferred deletion for cloud target system user accounts](#) on page 84

Displaying the cloud user account overview

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

To obtain an overview of a user account

1. In the Manager, select the **Cloud Target Systems > target system > User accounts** category.
2. Select the user account in the result list.
3. Select the **User account overview** task.

Cloud groups

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

Detailed information about this topic


- [Adding cloud groups to cloud groups](#) on page 150
- [Assigning permissions controls to cloud groups](#) on page 151
- [Assigning extended properties to cloud groups](#) on page 151
- [Deleting cloud groups](#) on page 152
- [Displaying the cloud group overview](#) on page 152
- [Managing assignments of cloud groups and cloud system entitlements](#) on page 86

Related topics

- [Cloud system entitlements](#) on page 153

Creating and editing cloud groups

To create a group

1. In the Manager, select the **Cloud Target Systems > <target system> > Groups** category.
2. Click  in the result list.
3. On the main data form, edit the main data of the group.
4. Save the changes.

To edit group main data

1. In the Manager, select the **Cloud Target Systems > <target system> > Groups** category.
2. Select the group in the result list.
3. Select the **Change main data** task.
4. On the main data form, edit the main data of the group.
5. Save the changes.

Detailed information about this topic

- [General main data for cloud groups](#) on page 148
- [User-defined main data for cloud groups](#) on page 149
- [Deleting cloud groups](#) on page 152

General main data for cloud groups

Enter the following main data of a group.

Table 34: Entering main data of a group

Property	Description
Name	Name of the group.
Container	Container in which to create the group.
Target system	The group's cloud target system
Distinguished name	Distinguished name of the group.
Display name	Name for displaying the group in the user interface of One Identity Manager tools.
Group name	Additional name for the group.
Email address	Group's email address
Account manager	Manager responsible for the group. To specify an account manager <ol style="list-style-type: none">1. Click ➔ next to the field.2. In the Table menu, select the table that maps the account manager.3. In the Account manager menu, select the manager.4. Click OK.
IT Shop	Specifies whether the group can be requested through the IT Shop. If this option is set, the group can be requested through the Web Portal and allocated by defined approval processes. The group can still be assigned directly to hierarchical roles. For more information, see the <i>One Identity Manager IT Shop Administration Guide</i> .
Only for use in IT Shop	Specifies whether the group can only be requested through the IT Shop. If this option is set, the group can be requested through the Web Portal and allocated by defined approval processes. Direct assignment of the

Property	Description
	group to hierarchical roles or user accounts is not permitted.
Service item	Service item data for requesting the group through the IT Shop.
Risk index	Value for evaluating the risk of assigning the group to user accounts. Set a value in the range 0 to 1. This input field is only visible if the QER CalculateRiskIndex configuration parameter is activated. For more information, see the <i>One Identity Manager Risk Assessment Administration Guide</i> .
Category	Categories for group inheritance. Groups can be selectively inherited by user accounts. To do this, groups and user accounts are divided into categories. Select one or more categories from the drop-down. For more information, see the <i>One Identity Manager Target System Base Module Administration Guide</i> .
Description	Text field for additional explanation.
Group type	Name of the group type. This is only required if different group types are recognized in the cloud application.
Resource type	Type of resource, for example, Group .

Detailed information about this topic

- [Defining categories for inheriting cloud groups and system entitlements](#) on page 132

User-defined main data for cloud groups

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

Table 35: User-defined main data of a group

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

Property	Description
- Spare option no. 05	customize display names, formats, and templates for the input fields.

Adding cloud groups to cloud groups


Use this task to add a group to another group. This means that the groups can be hierarchically structured.

To assign groups directly to a group as members

1. In the Manager, select the **Cloud Target Systems > <target system> > Groups** category.
2. Select the group in the result list.
3. Select the **Assign groups** category.
4. Select the **Has members** tab.
5. Assign child groups in **Add assignments**.

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

To remove an assignment


- Select the group and double-click .
6. Save the changes.

To add a group as a member of other groups

1. In the Manager, select the **Cloud Target Systems > <target system> > Groups** category.
2. Select the group in the result list.
3. Select the **Assign groups** task.
4. Select the **Is member of** tab.
5. In the **Add assignments** pane, assign parent groups.

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

To remove an assignment

- Select the group and double-click .
6. Save the changes.

Related topics

- [Assigning cloud system entitlements to cloud system entitlements](#) on page 156

Assigning permissions controls to cloud groups


Use this task to assign permissions controls to groups.

To assign permissions controls to a group

1. In the Manager, select the **Cloud Target Systems > <target system> > Groups** category.
2. Select the group in the result list.
3. Select the **Assign permissions controls** task.
4. In the **Add assignments** pane, assign permissions controls.

TIP: In the **Remove Assignments** pane, you can remove the assigned permission controls.

To remove an assignment

- Select the permissions control and double-click .
5. Save the changes.

Related topics

- [Cloud permissions controls](#) on page 159
- [Assigning cloud groups to cloud permissions controls](#) on page 161

Assigning extended properties to cloud groups

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


For more information about using extended properties, see the *One Identity Manager Compliance Rules Administration Guide*.

To specify extended properties for a group

1. In the Manager, select the **Cloud Target Systems > <target system> > Groups** category.
2. Select the group in the result list.
3. Select the **Assign extended properties** task.
4. In the **Add assignments** pane, assign extended properties.

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

To remove an assignment

- Select the extended property and double-click .
5. Save the changes.

Related topics

- [Assigning extended properties to cloud system entitlements](#) on page 157

Displaying the cloud group overview

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


To obtain an overview of a group

1. In the Manager, select the **Cloud Target Systems > <target system> > Groups** category.
2. Select the group in the result list.
3. Select the **Group overview** task.

Deleting cloud groups

Groups are deleted permanently from the One Identity Manager database. Once you have deleted a group, it is also deleted in the Universal Cloud Interface Module through the provisioning process and then in the cloud application. The deletion is logged as a pending change. You can display whether the group has been deleted in the cloud application from the process status for the pending change. The same applies if user account assignments to groups are deleted.

To delete a group

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

Related topics

- [Provisioning object changes](#) on page 47
- [Deleting cloud system entitlements](#) on page 159

Cloud system entitlements

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

Detailed information about this topic


- [Creating and editing cloud system entitlements](#) on page 153
- [Assigning cloud user account directly to cloud system entitlements](#) on page 104
- [Assigning cloud system entitlements to cloud system entitlements](#) on page 156
- [Displaying cloud system entitlement overviews](#) on page 158

Related topics

- [Cloud groups](#) on page 147

Creating and editing cloud system entitlements

To create a system entitlement

1. In the Manager, select the **Cloud target systems > <target system> > System entitlements 1** category.
- OR -
In the Manager, select the **Cloud target systems > <target system> > System entitlements 2** category.
- OR -
In the Manager, select the **Cloud target systems > <target system> > System entitlements 3** category.
2. Click  in the result list.
3. On the main data form, edit the system entitlement's main data.
4. Save the changes.

To edit the main data of a system entitlement:

1. In the Manager, select the **Cloud target systems > <target system> > System entitlements 1** category.
- OR -

In the Manager, select the **Cloud target systems > <target system> > System entitlements 2** category.

- OR -

In the Manager, select the **Cloud target systems > <target system> > System entitlements 3** category.

2. Select the system entitlement in the result list.
3. Select the **Change main data** task.
4. On the main data form, edit the system entitlement's main data.
5. Save the changes.

Detailed information about this topic

- [General main data for system entitlements](#) on page 154
- [User-defined main data for cloud user accounts](#) on page 155

General main data for system entitlements

Enter the following main data for a system entitlement.

Table 36: General main data of a system entitlement

Property	Description
Name	Name of the system entitlement.
Container	Container in which the system entitlement is added.
Target system	Cloud target system of the system entitlement.
Distinguished name	Distinguished name of the system entitlement.
Display name	The display name is used to display the system entitlement in the One Identity Manager tools' user interface.
System entitlement name	Additional identifier for the system entitlement.
Email address	E-mail address of the system entitlement.
Account manager	Manager responsible for the system entitlement. To specify an account manager <ol style="list-style-type: none">1. Click ➔ next to the field.2. In the Table menu, select the table that maps the account manager.3. In the Account manager menu, select the manager.

Property	Description
	4. Click OK .
IT Shop	Specifies whether the system entitlement can be requested through the IT Shop. If this option is set, the system entitlement can be requested through the Web Portal and allocated by defined approval processes. The system entitlement can still be assigned directly to user accounts and hierarchical roles. For more information, see the <i>One Identity Manager IT Shop Administration Guide</i> .
Only for use in IT Shop	Specifies whether the system entitlement can only be requested through the IT Shop. If this option is set, the system entitlement can be requested through the Web Portal and allocated by defined approval processes. Direct assignment of the system entitlement to hierarchical roles or user accounts is not permitted.
Service item	Service item for requesting the system entitlement through the IT Shop.
Risk index	Value for evaluating the risk of assigning the system entitlement to user accounts. Set a value in the range 0 to 1. This input field is only visible if the QER CalculateRiskIndex configuration parameter is set. For more information, see the <i>One Identity Manager Risk Assessment Administration Guide</i> .
Category	Category for inheriting system entitlements. System entitlements can be selectively inherited by user accounts. To do this, system entitlements and user accounts are divided into categories. Select one or more categories from the menu. For more information, see the <i>One Identity Manager Target System Base Module Administration Guide</i> .
Description	Text field for additional explanation.
System entitlement type	Unique identifier of the system entitlement type. This is only required if different system entitlement types are recognized in the cloud application.
Resource type	Name of the resource type such as /Roles.

Detailed information about this topic

- [Defining categories for inheriting cloud groups and system entitlements](#) on page 132
- [System entitlements types in cloud target systems](#) on page 86

User-defined main data for cloud user accounts

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

Table 37: User-defined main data of a system entitlement

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

Assigning cloud system entitlements to cloud system entitlements

System entitlements can be members of other system entitlements. This means that the system entitlements can be hierarchically structured. Only system entitlements that have the same type can be assigned.

To assign system entitlements as members to a system entitlement

1. In the Manager, select the **Cloud target systems > <target system> > System entitlements 1** category.
- OR -
In the Manager, select the **Cloud target systems > <target system> > System entitlements 2** category.
- OR -
In the Manager, select the **Cloud target systems > <target system> > System entitlements 3** category.
2. Select the system entitlement in the result list.
3. Select the **System entitlements 1 overview** task, **System entitlements 2 overview** task, or **System entitlements 3 overview** task to match the selected system entitlement.
4. Select the **Has members** tab.
5. In the **Add assignments** pane, assign the child system entitlements.

TIP: In the **Remove assignments** pane, you can remove system entitlement assignments.

To remove an assignment

- Select the system entitlement and double-click .

6. Save the changes.

To add a system entitlement as a member to another system entitlement

1. In the Manager, select the **Cloud target systems > <target system> > System entitlements 1** category.

- OR -

In the Manager, select the **Cloud target systems > <target system> > System entitlements 2** category.

- OR -

In the Manager, select the **Cloud target systems > <target system> > System entitlements 3** category.

2. Select the system entitlement in the result list.

3. Select the **System entitlements 1 overview** task, **System entitlements 2 overview** task, or **System entitlements 3 overview** task to match the selected system entitlement.

4. Select the **Is member of** tab.

5. In the **Add assignments** pane, assign the parent system entitlements.

TIP: In the **Remove assignments** pane, you can remove system entitlement assignments.

To remove an assignment

- Select the system entitlement and double-click .

6. Save the changes.

Related topics

- [Adding cloud groups to cloud groups](#) on page 150

Assigning extended properties to cloud system entitlements

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

For more information about using extended properties, see the *One Identity Manager Compliance Rules Administration Guide*.

To specify extended properties for a system entitlement

1. In the Manager, select the **Cloud target systems > <target system> > System entitlements 1** category.

- OR -

In the Manager, select the **Cloud target systems > <target system> > System entitlements 2** category.

- OR -

In the Manager, select the **Cloud target systems > <target system> > System entitlements 3** category.

2. Select the system entitlement in the result list.
3. Select **Assign extended properties**.
4. In the **Add assignments** pane, assign extended properties.

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

To remove an assignment

- Select the extended property and double-click .

5. Save the changes.

Related topics

- [Assigning extended properties to cloud groups](#) on page 151

Displaying cloud system entitlement overviews

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

To obtain an overview of a system entitlement

1. In the Manager, select the **Cloud target systems > <target system> > System entitlements 1** category.

- OR -

In the Manager, select the **Cloud target systems > <target system> > System entitlements 2** category.

- OR -

In the Manager, select the **Cloud target systems > <target system> > System entitlements 3** category.


2. Select the system entitlement in the result list.

3. Select the **System entitlement 1 overview** task, **System entitlement 2 overview** task, or **System entitlement 3 overview** task to match the selected system entitlement.

Deleting cloud system entitlements

This deletes the system entitlement permanently from the One Identity Manager database. Once you have deleted a system entitlement, it is also deleted in the Universal Cloud Interface Module by the provisioning process and then in the cloud application. The deletion is logged as a pending change. You can display whether the system entitlement has been deleted in the cloud application from the process status of the pending change. The same applies if user account assignments to system entitlements are deleted.

To delete a system entitlement

1. In the Manager, select the **Cloud target systems > <target system> > System entitlements 1** category.
- OR -
In the Manager, select the **Cloud target systems > <target system> > System entitlements 2** category.
- OR -
In the Manager, select the **Cloud target systems > <target system> > System entitlements 3** category.
2. Select the system entitlement in the result list.
3. Click  to delete the system entitlement.
4. Confirm the security prompt with **Yes**.

Related topics


- [Provisioning object changes](#) on page 47
- [Deleting cloud groups](#) on page 152

Cloud permissions controls

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

To create or edit permissions controls

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

2. Select the permissions control in the result list. Select the **Change main data** task.
- OR -
Click  in the result list.
3. Edit the permissions controls' main data.
4. Save the changes.

Detailed information about this topic

- [General main data for cloud permissions controls](#) on page 160
- [User-defined main data for cloud permissions controls](#) on page 160

General main data for cloud permissions controls

Enter the following main data of a permissions control.

Table 38: Permissions control main data

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

User-defined main data for cloud permissions controls

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

Table 39: User-defined main data of permissions controls

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

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

Assigning cloud groups to cloud permissions controls


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

To assign permissions controls to groups

1. In the Manager, select the **Cloud Target Systems > <target system> > Permissions controls** category.
2. Select the permissions control in the result list.
3. Select **Assign groups** category.
4. In the **Add assignments** pane, assign the groups.

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

To remove an assignment

- Select the group and double-click .
5. Save the changes.

Related topics

- [Assigning permissions controls to cloud groups](#) on page 151

Assigning cloud user accounts to cloud permissions controls


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

To assign permissions controls to user accounts

1. In the Manager, select the **Cloud Target Systems > <target system> > Permissions controls** category.
2. Select the permissions control in the result list.
3. Select the **Assign user accounts** task.
4. In the **Add assignments** pane, assign the user accounts.

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

To remove an assignment

- Select the user account and double-click .
5. Save the changes.

Related topics

- [Assigning permissions controls to cloud user accounts](#) on page 143

Displaying an overview of the cloud permissions controls

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


To obtain an overview of a permissions control

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

Deleting cloud permissions controls

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

To delete a permissions control

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

Related topics

- [Provisioning object changes](#) on page 47

Reports about objects in cloud target systems

One Identity Manager makes various reports available containing information about the selected base object and its relations to other One Identity Manager database objects. The following reports are available for cloud systems.

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

Table 40: Data quality target system report

Report	Published for	Description
Show overview	User account	This report shows an overview of the user account and the assigned permissions.
Show overview including origin	User account	This report shows an overview of the user account and origin of the assigned permissions.
Show overview including history	User account	This report shows an overview of the user accounts including its history. Select the end date for displaying the history (Min. date). Older changes and assignments that were removed before this date, are not shown in the report.
Show user accounts overview (incl. history)	Container	This report shows all the container's user accounts with their permissions including a history. Select the end date for displaying the history (Min. date). Older changes and assignments that were removed before this date, are not shown in the report.

Report	Published for	Description
Show system entitlements overview (incl. history)	Container	<p>This report shows the container's system entitlements with the assigned user accounts including a history.</p> <p>Select the end date for displaying the history (Min. date). Older changes and assignments that were removed before this date, are not shown in the report.</p>
Overview of all assignments	Container	This report finds all roles containing identities with at least one user account in the selected container.
Overview of all assignments	System entitlement group	This report finds all roles containing identities who have the selected system entitlement.
Show overview	System entitlement group	This report shows an overview of the system entitlement and its assignments.
Show overview including origin	System entitlement group	This report shows an overview of the system entitlement and origin of the assigned user accounts.
Show overview including history	System entitlement group	<p>This report shows an overview of the system entitlement and including its history.</p> <p>Select the end date for displaying the history (Min. date). Older changes and assignments that were removed before this date, are not shown in the report.</p>
Show entitlement drifts	Cloud target system	This report shows all system entitlements that are the result of manual operations in the target system rather than provisioned by One Identity Manager.
Show user accounts overview (incl. history)	Cloud target system	<p>This report returns all the user accounts with their permissions including a history.</p> <p>Select the end date for displaying the history (Min. date). Older changes and assignments that were removed before this date, are not shown in the report.</p>
Show user accounts with an above average	Cloud target system	This report contains all user accounts with an above average number of system entitlements.

Report	Published for	Description
number of system entitlements		
Show identities with multiple user accounts	Cloud target system	This report shows all the identities that have multiple user accounts. The report contains a risk assessment.
Show system entitlements overview (incl. history)	Cloud target system	This report shows the system entitlements with the assigned user accounts including a history. Select the end date for displaying the history (Min. date). Older changes and assignments that were removed before this date, are not shown in the report.
Overview of all assignments	Cloud target system	This report finds all roles containing identities with at least one user account in the selected target system.
Show unused user accounts	Cloud target system	This report contains all user accounts, which have not been used in the last few months.
Show orphaned user accounts	Cloud target system	This report shows all user accounts to which no identity is assigned.

Table 41: Additional reports for the target system

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

Related topics

- [Overview of all assignments](#) on page 112

Handling cloud objects in the Web Portal

One Identity Manager enables its users to perform various tasks simply using a Web Portal.

- Managing user accounts and identities

An account definition can be requested by shop customers in the Web Portal if it is assigned to an IT Shop shelf. The request undergoes a defined approval process. The user account is not created until it has been agreed by an authorized identity, such as a manager.

- Managing assignments of groups and system entitlements

These products can be requested in the Web Portal by the shop's customers by assigning groups and system entitlements to an IT Shop shelf. The request undergoes a defined approval process. The group or system entitlement is not assigned until it has been approved by an authorized identity.

In the Web Portal, managers and administrators of organizations can assign system entitlements to the departments, cost centers, or locations for which they are responsible. The system entitlements and groups are inherited by all identities who are members of these departments, cost centers, or locations.

If the Business Roles Module is available, managers and administrators of business roles can assign groups and system entitlements to the business roles in the Web Portal for which they are responsible. The groups and system entitlements are inherited by all identities who are members of these business roles.

If the System Roles Module is available, those with system roles responsibilities can assign groups and system entitlements to the system roles in the Web Portal. The groups and system entitlements are inherited by all identities to whom these system roles are assigned.

- Attestation

If the Attestation Module is available, the correctness of the properties of target system objects and of entitlement assignments can be verified on request. To enable this, attestation policies are configured in the Manager. The attestors use the Web Portal to approve attestation cases.

- Governance administration

If the Compliance Rules Module is available, you can define rules that identify the invalid group memberships and evaluate their risks. The rules are checked regularly, and if changes are made to the objects in One Identity Manager. Compliance rules are defined in the Manager. Supervisors use the Web Portal to check rule violations and to grant exception approvals.

If the Company Policies Module is available, company policies can be defined for the target system objects mapped in One Identity Manager and their risks evaluated. Company policies are defined in the Manager. Supervisors use the Web Portal to check policy violations and to grant exception approvals.

- Risk assessment

You can use the risk index of groups to evaluate the risk of entitlement assignments for the company. One Identity Manager provides default calculation functions for this. The calculation functions can be modified in the Web Portal.

- Reports and statistics

The Web Portal provides a range of reports and statistics about the identities, user accounts, and their entitlements and risks.

For more information about the named topics, see [Managing cloud user accounts and identities](#) on page 50, [Managing assignments of cloud groups and cloud system entitlements](#) on page 86, and the following guides:

- *One Identity Manager Web Portal User Guide*
- *One Identity Manager Attestation Administration Guide*
- *One Identity Manager Compliance Rules Administration Guide*
- *One Identity Manager Company Policies Administration Guide*
- *One Identity Manager Risk Assessment Administration Guide*

Basic data for managing a Universal Cloud Interface environment

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

- Configuration parameter

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

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

For more information, see [Configuration parameters for managing cloud target systems](#) on page 177.

- Target system types

Target system types are required for configuring target system comparisons. Tables with outstanding objects are maintained with the target system types and settings are configured for provisioning memberships and single objects synchronization. Target system types also map objects in the Unified Namespace.

For more information, see [Post-processing outstanding objects](#) on page 40.

- Account definitions

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

For more information, see [Account definitions for cloud user accounts](#) on page 51.

- Password policy

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

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

For more information, see [Password policies for cloud user accounts](#) on page 114.

- Initial password for new user accounts

You have the different options for issuing an initial password for user accounts. Enter a password or use a random generated initial password when you create a user account.

For more information, see [Initial password for new cloud user accounts](#) on page 126.

- Email notifications about credentials

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

For more information, see [Email notifications about login data](#) on page 126.

- Target system managers

A default application role exists for the target system manager in One Identity Manager. Assign identities to this application role who have permission to edit all cloud target system in One Identity Manager.

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

For more information, see [Target system managers](#) on page 169.

- Servers

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

For more information, see [Job server for Universal Cloud Interface-specific process handling](#) on page 172.

Target system managers

A default application role exists for the target system manager in One Identity Manager. Assign identities to this application role who have permission to edit all cloud target system in One Identity Manager.

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

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

Implementing application roles for target system managers

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

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

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

NOTE: If no identities are assigned to a child application role for target system administrators, the identities of the parent application role are granted the permissions.

Table 42: Default application roles for target system managers

User	Tasks
Target system managers	<p>Target system managers must be assigned to the Target systems Cloud target systems application role or a child application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none">• Assume administrative tasks for the target system.• Create, change, or delete target system objects.• Edit password policies for the target system.• Prepare groups and system entitlements to add to the IT Shop.• Can add identities that do not have the Primary identity identity type.• Configure synchronization in the Synchronization Editor and define the mapping for comparing target systems and One Identity Manager.• Edit the synchronization's target system types and outstanding objects.• Authorize other identities within their area of responsibility as target system managers and create child application roles if required.

To initially specify identities to be target system administrators

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

2. Select the **One Identity Manager Administration > Target systems > Administrators** category.
3. Select the **Assign identities** task.
4. Assign the identity and save the changes.

To add the first identities to the default application as target system managers

1. Log in to the Manager as a target system administrator (**Target systems | Administrators** application role).
2. Select the **One Identity Manager Administration > Target systems > Cloud target systems** category.
3. Select the **Assign identities** task.
4. Assign the identities you want and save the changes.

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

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

To specify target system managers for individual cloud target systems

1. Log in to the Manager as a target system manager.
2. Select the **Cloud Target Systems > Basic configuration data > Cloud target systems** category.
3. Select the target system in the result list.
4. Select the **Change main data** task.
5. On the **General** tab, select the application role in the **Target system manager** drop-down.

- OR -

Next to the **Target system manager** drop-down, click  to create a new application role.

- a. Enter the application role name and assign the **Target systems | Cloud target systems** parent application role.
 - b. Click **OK** to add the new application role.
6. Save the changes.
 7. Assign identities to this application role who are permitted to edit the target system in One Identity Manager.

Related topics

- [One Identity Manager users for managing cloud target systems](#) on page 10
- [General main data for cloud target systems](#) on page 129
- [Container structures](#) on page 133

Job server for Universal Cloud Interface-specific process handling

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

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

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

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

Related topics

- [Setting up the synchronization server](#) on page 16

Editing Job server for cloud target systems

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

To edit a Job server and its functions

1. In the Manager, select the **Cloud target systems > Basic configuration data > Server** category.
2. Select the Job server entry in the result list.
3. Select the **Change main data** task.

4. Edit the Job server's main data.
5. Select the **Assign server functions** task and specify server functionality.
6. Save the changes.

Detailed information about this topic

- [General main data of Job servers](#) on page 173
- [Specifying server functions](#) on page 176

General main data of Job servers

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

The following properties are displayed for Job servers.

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

Table 43: Job server properties

Property	Meaning
Server	Job server name.
Full server name	Full server name in accordance with DNS syntax. Syntax: <Name of servers>.<Fully qualified domain name>
Target system	Computer account target system.
Language	Language of the server.
Server is cluster	Specifies whether the server maps a cluster.
Server belongs to cluster	Cluster to which the server belongs. NOTE: The Server is cluster and Server belongs to cluster properties are mutually exclusive.
IP address (IPv6)	Internet protocol version 6 (IPv6) server address.
IP address (IPv4)	Internet protocol version 4 (IPv4) server address.
Copy process (source server)	Permitted copying methods that can be used when this server is the source of a copy action. At present, only copy methods that support the Robocopy and rsync programs are supported. If no method is given, the One Identity Manager Service determines the

Property	Meaning
	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	<p>Name of the executing server. The name of the server that exists physically and where the processes are handled.</p> <p>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.</p>
Queue	Name of the queue to handle the process steps. The process steps are requested by the Job queue using this queue identifier. The queue identifier is entered in the One Identity Manager Service configuration file.
Server operating system	Operating system of the server. This input is required to resolve the path name for replicating software profiles. The values Win32 , Windows , Linux , and Unix are permitted. If no value is specified, Win32 is used.
Service account data	One Identity Manager Service user account information. In order to replicate between non-trusted systems (non-trusted domains, Linux server), the One Identity Manager Service user information has to be declared for the servers in the database. This means that the service account, the service account domain, and the service account password have to be entered for the server.
One Identity Manager Service installed	Specifies whether a One Identity Manager Service is installed

Property	Meaning
	<p>installed on this server. This option is enabled by the QBM_PJobQueueLoad procedure the moment the queue is called for the first time.</p> <p>The option is not automatically removed. If necessary, you can reset this option manually for servers whose queue is no longer enabled.</p>
Stop One Identity Manager Service	<p>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.</p> <p>You can make the service start and stop with the appropriate administrative permissions in the Job Queue Info program. For more information, see the <i>One Identity Manager Process Monitoring and Troubleshooting Guide</i>.</p>
Paused due to unavailability of a target system	<p>Specifies whether task processing for this queue has been stopped because the target system that uses this Job server as a synchronization server is temporarily unavailable. As soon as the target system is available again, processing starts and all outstanding tasks are performed.</p> <p>For more information about offline mode, see the <i>One Identity Manager Target System Synchronization Reference Guide</i>.</p>
No automatic software update	<p>Specifies whether to exclude the server from automatic software updating.</p> <p>NOTE: Servers must be manually updated if this option is set.</p>
Software update running	<p>Specifies whether a software update is currently running.</p>
Server function	<p>Server functionality in One Identity Manager. One Identity Manager processes are handled with respect to the server function.</p>

Related topics

- [Specifying server functions](#) on page 176

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 44: Permitted server functions

Server function	Remark
Update server	<p>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.</p> <p>The server with the One Identity Manager database installed on it is labeled with this functionality during initial installation of the schema.</p>
SQL processing server	<p>It can run SQL tasks. The server requires a direct connection to the database server that One Identity Manager database is installed on.</p> <p>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.</p>
CSV script server	<p>This server can process CSV files using the ScriptComponent process component.</p>
One Identity Manager Service installed	<p>Server on which a One Identity Manager Service is installed.</p>
SMTP host	<p>Server from which One Identity Manager Service sends email notifications. Prerequisite for sending mails using One Identity Manager Service is SMTP host configuration.</p>
Default report server	<p>Server on which reports are generated.</p>
Universal Cloud Interface connector	<p>This server can connect to the Universal Cloud Interface Module.</p>

Related topics

- [General main data of Job servers](#) on page 173

Configuration parameters for managing cloud target systems

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

Table 45: Configuration parameters for managing cloud target systems

Configuration parameters	Meaning
TargetSystem CSM	<p>Preprocessor relevant configuration parameter for controlling the database model components for the administration of the cloud target systems. If the parameter is set, the target system components are available. Changes to this parameter require the database to be recompiled.</p> <p>If you disable the configuration parameter at a later date, model components and scripts that are no longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the <i>One Identity Manager Configuration Guide</i>.</p>
TargetSystem CSM Accounts	Allows configuration of user account data.
TargetSystem CSM Accounts InitialRandomPassword	Specifies whether a random password is generated when a new user account is added. The password must contain at least those character sets that are defined in the password policy.
TargetSystem CSM Accounts InitialRandomPassword SendTo	Identity to receive an email with the random generated password (manager cost center/department/location/business role, identity's manager or XUserInserted). If no recipient can be found, the password is sent to the address stored in the TargetSystem CSM DefaultAddress configuration parameter.
TargetSystem CSM	Mail template name that is sent to supply users with the login

Configuration parameters	Meaning
Accounts InitialRandomPassword SendTo MailTemplateAccountName	credentials for the user account. The Identity - new user account created mail template is used.
TargetSystem CSM Accounts InitialRandomPassword SendTo MailTemplatePassword	Mail template name that is sent to supply users with the initial password. The Identity - initial password for new user account mail template is used.
TargetSystem CSM Accounts MailTemplateDefaultValues	Mail template used to send notifications about whether default IT operating data mapping values are used for automatically creating a user account. The Identity - new user account with default properties created mail template is used.
TargetSystem CSM Accounts PrivilegedAccount	Allows configuration of privileged user account settings.
TargetSystem CSM Accounts PrivilegedAccount SAMAccountName_ Postfix	Postfix for formatting the login name of privileged user accounts.
TargetSystem CSM Accounts PrivilegedAccount SAMAccountName_ Prefix	Prefix for formatting a login name of privileged user accounts.
TargetSystem CSM ApplicationType	Configuration of the different cloud applications.
TargetSystem CSM ApplicationType Salesforce	Salesforce application settings
TargetSystem CSM ApplicationType Salesforce DefaultProfileName	Name of the default profile assigned to new Salesforce users.
TargetSystem CSM DefaultAddress	Default email address of the recipient for notifications about actions in the target system.
TargetSystem CSM	Maximum runtime of a synchronization in minutes. No

Configuration parameters	Meaning
MaxFullsyncDuration	recalculation of group memberships by the DBQueue Processor can take place during this time. If the maximum runtime is exceeded, group membership are recalculated.
TargetSystem CSM PersonAutoDefault	Mode for automatic identity assignment for user accounts added to the database outside synchronization.
TargetSystem CSM PersonAutoDisabledAccounts	Specifies whether identities are automatically assigned to disabled user accounts. User accounts are not given an account definition.
TargetSystem CSM PersonAutoFullSync	Mode for automatic identity assignment for user accounts that are added to or updated in the database by synchronization.
TargetSystem CSM PersonExcludeList	Listing of all user account without automatic identity assignment. Names are listed in a pipe () delimited list that is handled as a regular search pattern. Example: ADMINISTRATOR GUEST KRBTGT TSINTERNETUSER IUSR_.* IWAM_.* SUPPORT_.* . * \$

The following configuration parameters are also required.

Table 46: Additional configuration parameters

Configuration parameters	Meaning
QBM PendingChange	General configuration parameter for configuring pending changes.
QBM PendingChange LifeTimeError	This configuration parameter specifies the maximum retention period (in days) for failed provisioning processes. The default is 30 days.
QBM PendingChange LifeTimeRunning	This configuration parameter specifies the maximum retention period (in days) for open provisioning processes. The default is 60 days.
QBM PendingChange LifeTimeSuccess	This configuration parameter specifies the maximum retention period (in days) for successful provisioning processes. The default is 2 days.

Default project template for cloud applications in the Universal Cloud Interface

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

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

The project template uses mappings for the following schema types.

Table 47: Mapping Universal Cloud Interface schema types to tables in the One Identity Manager schema

Schema type in Universal Cloud Interface	Table in the One Identity Manager Schema
UCIRoot	CSMRoot
UCIContainer	CSMContainer
UCIGroup	CSMGroup
UCIGroupInGroup	CSMGroupInGroup
UCIGroupHasItem	CSMGroupHasItem
UCIGroup1	CSMGroup1
UCIGroup1InGroup1	CSMGroup1InGroup1
UCIGroup2	CSMGroup2
UCIGroup2InGroup2	CSMGroup2InGroup2
UCIGroup3	CSMGroup3

Schema type in Universal Cloud Interface	Table in the One Identity Manager Schema
UCIGroup3InGroup3	CSMGroup3InGroup3
UCIItem	CSMItem
UCIUser	CSMUser
UCIUserInGroup	CSMUserInGroup
UCIUserInGroup1	CSMUserInGroup1
UCIUserInGroup2	CSMUserInGroup2
UCIUserInGroup3	CSMUserInGroup3
UCIUserHasGroup	CSMUserHasGroup
UCIUserHasGroup1	CSMUserHasGroup1
UCIUserHasGroup2	CSMUserHasGroup2
UCIUserHasGroup3	CSMUserHasGroup3
UCIUserHasItem	CSMUserHasItem
QBMPendingChange	QBMPendingChange
QBMPendingChangeDetail	QBMPendingChangeDetail

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 definition 51

- add to IT Shop 67

- assign automatically 65

- assign to all identities 65

- assign to business role 64

- assign to cost center 64

- assign to department 64

- assign to identities 62, 66

- assign to location 64

- assign to system roles 66

- create 52

- delete 70

- edit 53

- IT operating data 59-60

- manage level 56-57

account manager 141

application role 10

B

base object 31

C

calculation schedule 37

- deactivate 38

cloud container 133

- account manager 133

- target system manager 133

cloud group 147

- add to IT Shop 98

- assign business roles 94

- assign cloud user account 88

- assign cost center 91

- assign department 91

- assign extended properties 151

- assign hierarchical role 88

- assign location 91

- assign permissions control 151

- assign system role 96

- assign to cloud group 150

- assign user account 103, 105

- category 110

- cloud container 148

- create 147

- delete 152

- edit 147

- effective 107

- exclusion 107

- group membership 103

- inheriting through system roles 96

cloud permissions control 159

- assign cloud group 151, 161

- assign cloud user account 161

- assign user account 143

- delete 162

- permissions type 160

cloud system entitlement 153

- assign extended properties 157

- assign system entitlements 156

- assign system role 97

- assign to business role 95

- assign to cost center 92

- assign to department 92
- assign to location 92
- assign to user account 104-105
- assignment
 - permissions-based 86
 - save 86
 - user-based 86
- container 154
- create 153
- delete 159
- edit 153
- effective 107
- exclusion 107
- type 86
- cloud target system
 - account definition 70, 129
 - alternative column description 132
 - category 110, 132
 - deferred deletion 84, 129
 - display name 129
 - edit 128
 - identity assignment 75
 - overview of all assignments 112
 - synchronized by 129
 - target system managers 129
 - target system type 129
 - user 10
- cloud user account 134
 - account definition 136
 - account manager 141
 - administrative user account 78, 80-81
 - assign extended properties 144
 - assign group 105
 - assign identity 73
 - assign permissions control 143
 - assign system entitlements 105
 - category 110
 - deactivate identity 144
 - default profile 106
 - default user accounts 78-79
 - delete 145
 - identity 78, 136
 - lock 144
 - login 140
 - login name 136
 - manage level 77
 - password 126, 140
 - privileged user account 78, 82, 136
 - set up 135
 - target system 136
 - type 78
 - unlock 144
- configuration parameter 177
- convert connection parameter 31

D

- direction of synchronization
 - direction target system 20, 30
 - in the One Identity Manager 20

E

- email notification 126
- exclusion definition 107
- extended property
 - cloud group 151
 - cloud user account 144

I

identity

- deactivate 144

identity assignment

- manual 76

- remove 76

- search criteria 75

inheritance

- category 110

IT operating data

- change 61

IT Shop shelf

- assign account definition 67

- assign cloud group 98

J

Job server

- edit 16-17

- load balancing 36

- properties 173

L

- load balancing 36

- login data 126

N

- notification 126

O

object

- delete immediately 40

- outstanding 40

- publish 40

- offline mode 45

- outstanding object 40

P

password

- initial 126

password policy 114

- assign 116

- character sets 120

- check password 125

- conversion script 122, 124

- default policy 116, 118

- display name 118

- edit 117-118

- error message 118

- excluded list 125

- failed logins 119

- generate password 125

- initial password 119

- name components 119

- password age 119

- password cycle 119

- password length 119

- password strength 119

- predefined 115

- test script 122

pending changes 47-48

- retention period 49

project template 180

provisioning 47

- accelerate 36

provisioning process

- delete 49

- display 48

- failed 48
- open 48

R

- report 163
 - overview of all assignments 112
- revision filter 34

S

- schema
 - changes 33
 - shrink 33
 - update 33
- server function 176
- single object synchronization 36
- start up configuration 31
- synchronization
 - accelerate 34
 - authorizations 15
 - base object
 - create 30
 - calculation schedule 37
 - configure 20, 28
 - connection parameter 20, 28, 30
 - different cloud applications 30
 - extended schema 30
 - only changes 34
 - prevent 38
 - scope 28
 - set up 14
 - start 20, 37
 - synchronization project
 - create 20
 - target system schema 30

- user 15
- variable 28
- variable set 30
- workflow 20, 30
- synchronization configuration
 - customize 28, 30
- synchronization log 39
 - contents 27
 - create 27
- synchronization project
 - create 20
 - deactivate 38
 - edit 133
 - project template 180
- synchronization server 172
 - configure 16
 - edit 172
 - install 16-17
 - Job server 16-17
 - server function 176
- synchronization workflow
 - create 20, 30
- system connection
 - change 31
 - enabled variable set 32

T

- target system
 - not available 45
- target system manager 169
- target system managers 10
- target system synchronization 40
- template
 - IT operating data, modify 61

U

user account

- apply template 61

- password

 - notification 126

V

variable set 31

- active 32