



One Identity Manager 9.1.1

Administration Guide for Connecting to SharePoint Online

Copyright 2023 One Identity LLC.

ALL RIGHTS RESERVED.

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

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

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

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

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

Patents

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

Trademarks

One Identity and the One Identity logo are trademarks and registered trademarks of One Identity LLC. in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at www.OneIdentity.com/legal/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 SharePoint Online
Updated - 28 March 2023, 23:02

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

Contents

Mapping a SharePoint Online environment in One Identity Manager	8
Architecture overview	8
One Identity Manager users for managing SharePoint Online	9
Configuration parameters	11
Synchronizing a SharePoint Online environment	12
Setting up initial synchronization with a SharePoint Online tenant	13
Users and permissions for synchronizing with SharePoint Online	14
Integrating One Identity Manager as application in Azure Active Directory	15
Setting up the SharePoint Online synchronization server	16
System requirements for the SharePoint Online synchronization server	17
Installing One Identity Manager Service with a SharePoint Online connector	17
Preparing the administrative workstation for access to SharePoint Online	20
Preparing a remote connection server for access to the SharePoint Online tenant	21
Creating a synchronization project for initial synchronization of a SharePoint Online tenant	21
Information required for setting up a synchronization project	22
Creating an initial synchronization project for SharePoint Online	23
Configuring the synchronization log	27
SharePoint Online synchronization features	27
Customizing the synchronization configuration	28
Configuring synchronization with SharePoint Online tenants	29
Changing system connection settings of SharePoint Online tenants	30
Editing connection parameters in the variable set	30
Editing target system connection properties	31
Updating schemas	32
Configuring the provisioning of memberships	33
Configuring single object synchronization	34
Accelerating provisioning and single object synchronization	36
Running synchronization	37
Starting synchronization	37
Displaying synchronization results	38

Deactivating synchronization	39
Synchronizing single objects	40
Tasks following synchronization	41
Post-processing outstanding objects	41
Adding custom tables to the target system synchronization	43
Managing user accounts through account definitions	43
Troubleshooting	44
Ignoring data error in synchronization	44
Pausing handling of target system specific processes (Offline mode)	45
Managing SharePoint Online user accounts and employees	47
Account definitions for SharePoint Online user accounts	48
Creating account definitions	49
Editing account definitions	49
Main data for account definitions	49
Editing manage levels	52
Creating manage levels	53
Assigning manage levels to account definitions	54
Main data for manage levels	54
Creating mapping rules for IT operating data	55
Entering IT operating data	57
Modify IT operating data	58
Assigning account definitions to employees	59
Assigning account definitions to departments, cost centers, and locations	60
Assigning account definitions to business roles	60
Assigning account definitions to all employees	61
Assigning account definitions directly to employees	62
Assigning account definitions to system roles	62
Adding account definitions in the IT Shop	62
Assigning account definitions to SharePoint Online site collections	65
Deleting account definitions	65
Assigning employees automatically to SharePoint Online user accounts	68
Editing search criteria for automatic employee assignment	69
Changing manage levels for SharePoint Online user accounts	70
Finding employees and directly assigning them to user accounts	71
Assigning account definitions to linked SharePoint Online user accounts	72

Manually linking employees to SharePoint Online user accounts	73
Application cases for SharePoint Online user account	74
Supported user account types	75
Default user accounts	76
Administrative user accounts	77
Providing administrative user accounts for one employee	78
Providing administrative user accounts for several employees	79
Privileged user accounts	80
Specifying deferred deletion for SharePoint Online user accounts	81
Managing assignments of SharePoint Online groups and roles	83
Assigning SharePoint Online entitlements to SharePoint Online user accounts	84
Prerequisites for indirect assignment of SharePoint Online entitlements to SharePoint Online user accounts	85
Assigning SharePoint Online entitlements to departments, cost centers, and locations	86
Assigning SharePoint Online entitlements to business roles	88
Adding SharePoint Online entitlements to system roles	89
Adding SharePoint Online entitlements to the IT Shop	90
Assigning SharePoint Online user accounts directly to an entitlement	92
Assigning SharePoint Online entitlements directly to a user account	93
Assigning SharePoint Online roles to SharePoint Online groups	93
Assigning SharePoint Online groups to SharePoint Online roles	94
Effectiveness of SharePoint Online entitlement assignments	95
SharePoint Online group inheritance based on categories	97
Overview of all assignments	100
Mapping of SharePoint Online objects in One Identity Manager	102
SharePoint Online tenants	102
Displaying and editing SharePoint Online tenant main data	103
General main data of SharePoint Online tenants	103
Additional tasks for managing SharePoint Online tenant	105
Overview of SharePoint Online tenants	105
Editing the synchronization project for a SharePoint Online tenant	105
SharePoint Online user accounts	106
Creating SharePoint Online user accounts	107
Editing main data of SharePoint Online user accounts	107

Main data for user authenticated user accounts	108
Main data for group authenticated user accounts	111
Additional tasks for managing SharePoint Online user accounts	114
The SharePoint Online user account overview	114
Assigning extended properties to SharePoint Online user accounts	115
Deleting and restoring SharePoint Online user accounts	115
SharePoint Online groups	116
Creating SharePoint Online groups	117
Editing main data of SharePoint Online groups	117
SharePoint Online group main data	118
Additional tasks for managing SharePoint Online groups	119
Overview of SharePoint Online groups	120
Assigning extended properties to SharePoint Online groups	120
Deleting SharePoint Online groups	120
SharePoint Online permission levels	121
Creating SharePoint Online permission levels	121
Editing main data of SharePoint Online permission levels	122
Entering main data for SharePoint Online permission levels	122
Overview of SharePoint Online permission levels	123
Deleting and restoring SharePoint Online permission levels	123
SharePoint Online site collections	123
Editing main data of SharePoint Online site collections	124
General main data of a SharePoint Online site collection	124
Address data for a SharePoint Online site collection	126
Defining categories for the inheritance of SharePoint Online groups	126
Additional tasks for managing site collections	127
Overview of SharePoint Online site collections	127
SharePoint Online sites	127
Editing main data of SharePoint Online sites	128
General main data of SharePoint Online sites	128
Address data of SharePoint Online sites	129
Design information of SharePoint Online sites	130
Overview of SharePoint Online sites	130
Inheritance of SharePoint Online permissions by SharePoint Online sites	131
SharePoint Online roles	131

Editing main data of SharePoint Online roles	132
General main data of SharePoint Online roles	132
Additional tasks for managing SharePoint Online roles	133
Overview of SharePoint Online roles	134
Effectiveness of SharePoint Online roles	134
Setting up SharePoint Online site collections and sites	135
Reports about SharePoint Online objects	137
Handling of SharePoint Online objects in the Web Portal	139
Basic data for managing a SharePoint Online environment	141
SharePoint Online authentication modes	142
SharePoint Online site templates	142
Job server for SharePoint Online-specific process handling	143
General main data of Job servers	144
Specifying server functions	146
Target system managers	147
Troubleshooting a SharePoint Online connection	150
Error synchronizing after renaming a SharePoint Online site collection	150
Appendix: Configuration parameters for managing SharePoint Online	151
Appendix: Default project template for SharePoint Online	153
Appendix: Editing system objects	154
About us	155
Contacting us	155
Technical support resources	155
Index	156

Mapping a SharePoint Online environment in One Identity Manager

One Identity Manager offers simplified user administration for SharePoint Online environments. One Identity Manager concentrates on the mapping of site collections, sites, and groups that exist within a cloud environment.

One Identity Manager provides company employees with the user accounts required to allow you to use different mechanisms for connecting employees to their user accounts. You can also manage user accounts independently of employees and therefore set up administrator user accounts.

The system information for the SharePoint Online structure is loaded into the One Identity Manager database during data synchronization. It is only possible to customize certain system information in One Identity Manager due to the complex dependencies and far reaching effects of changes.

For more information about the SharePoint Online structure, see the *SharePoint Online documentation* from Microsoft.

Related topics

- [Editing system objects](#) on page 154

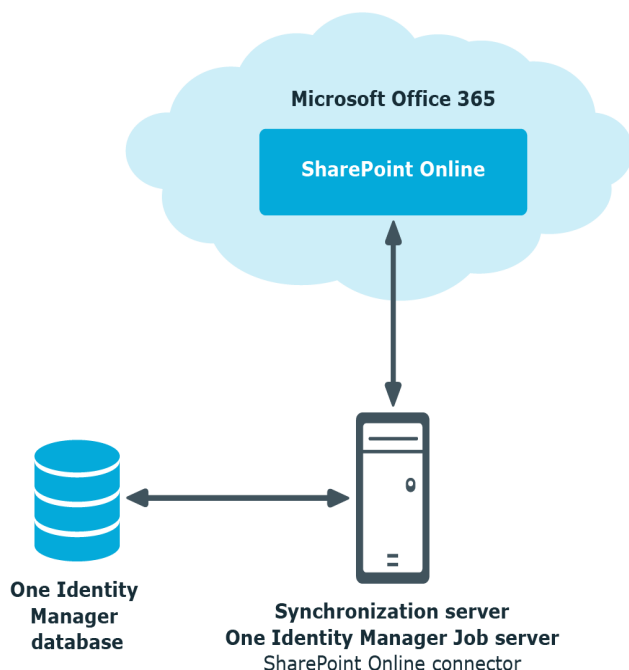
Architecture overview

To access SharePoint Online tenant data, the SharePoint Online connector is installed on a synchronization server. The synchronization server ensures data is compared between the One Identity Manager database and SharePoint Online. The SharePoint Online connector is part of the SharePoint Online Module and responsible for communicating with the SharePoint Online part of Microsoft Office 365 subscriptions in the cloud. The Microsoft CSOM (Client-side object model) is used for accessing the SharePoint Online data.

NOTE: For access to the data of a SharePoint Online tenant, the Azure Active Directory tenant to which the SharePoint Online tenant is connected must be synchronized.

For more information about synchronizing an Azure Active Directory tenant, see the *One Identity Manager Administration Guide for Connecting to Azure Active Directory*.

Figure 1: Architecture for synchronization



One Identity Manager users for managing SharePoint Online

The following users are used for setting up and administration of SharePoint Online.

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.

Users	Tasks
	<ul style="list-style-type: none"> • Set up other application roles for target system managers if required. • Specify which application roles for target system managers are mutually exclusive. • Authorize other employees 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 SharePoint Online 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 to add to the IT Shop. • Can add employees who have another identity than the Primary identity. • 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 employees 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> <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.

Users	Tasks
	<ul style="list-style-type: none"> • Create custom processes in the Designer as required. • Create and configure schedules as required. • Create and configure password policies as required.
Administrators for the IT Shop	<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 system entitlements to IT Shop structures.
Product owners for the IT Shop	<p>Product owners must be assigned to the Request & Fulfillment IT Shop Product owners application role or a child application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none"> • Approve through requests. • Edit service items and service categories under their management.
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 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 system entitlements to business roles.

Configuration parameters

Use configuration parameters to configure the behavior of the system's basic settings. One Identity Manager provides default settings for different configuration parameters. Check the configuration parameters and modify them as necessary to suit your requirements.

Configuration parameters are defined in the One Identity Manager modules. Each One Identity Manager module can also install configuration parameters. In the Designer, you can find an overview of all configuration parameters in the **Base data > General > Configuration parameters** category.

For more information, see [Configuration parameters for managing SharePoint Online](#) on page 151.

Synchronizing a SharePoint Online environment

One Identity Manager supports synchronization with SharePoint Online. The One Identity Manager Service is responsible for synchronizing data between the One Identity Manager database and SharePoint Online.

This section explains how to:

- Set up synchronization to import initial data from SharePoint Online tenant to the One Identity Manager database.
- Adjust a synchronization configuration.
- Start and deactivate the synchronization.
- Analyze synchronization results.

TIP: Before you set up synchronization with a SharePoint Online tenant, 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 SharePoint Online tenant](#) on page 13
- [Customizing the synchronization configuration](#) on page 28
- [SharePoint Online synchronization features](#) on page 27
- [Running synchronization](#) on page 37
- [Troubleshooting](#) on page 44
- [Editing system objects](#) on page 154

Setting up initial synchronization with a SharePoint Online tenant

The Synchronization Editor provides a project template that can be used to set up the synchronization of user accounts and permissions for the SharePoint Online environment. You use these project templates to create synchronization projects with which you import the data from a SharePoint Online tenant into your One Identity Manager database. In addition, the required processes are created that are used for the provisioning of changes to target system objects from the One Identity Manager database into the target system.

To load SharePoint Online objects into the One Identity Manager database for the first time

1. Prepare a user account in the Azure Active Directory tenant with sufficient permissions for synchronization. The Azure Active Directory tenant must be known in the One Identity Manager system.
2. If you want to use authentication through an Azure Active Directory application to log in to SharePoint Online, integrate the One Identity Manager as application in the Azure Active Directory tenant that is linked to the Office 365 tenant.
 - Load the certificate file with the private key (*.PFX) in the certificate store of the synchronization server and on the administrative workstation that is going to run the Synchronization Editor.
3. The One Identity Manager components for managing SharePoint Online systems are available if the **TargetSystem | SharePointOnline** configuration parameter is set.
 - In the Designer, check if the configuration parameter is set. Otherwise, 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 not 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*.
 - Other configuration parameters are installed when the module is installed. Check the configuration parameters and modify them as necessary to suit your requirements.
4. Install and configure a synchronization server and declare the server as a Job server in One Identity Manager.
5. Create a synchronization project with the Synchronization Editor.

Detailed information about this topic

- [Users and permissions for synchronizing with SharePoint Online](#) on page 14
- [Integrating One Identity Manager as application in Azure Active Directory](#) on page 15
- [System requirements for the SharePoint Online synchronization server](#) on page 17

- [Preparing the administrative workstation for access to SharePoint Online](#) on page 20
- [Creating a synchronization project for initial synchronization of a SharePoint Online tenant](#) on page 21
- [Configuration parameters for managing SharePoint Online](#) on page 151
- [Default project template for SharePoint Online](#) on page 153

Users and permissions for synchronizing with SharePoint Online

The following users are involved in synchronizing One Identity Manager with SharePoint Online.

Table 2: Users for synchronization

User	Permissions
Users for accessing SharePoint Online (synchronization users)	<p>For full synchronization of SharePoint Online tenant objects with the supplied One Identity Manager default configuration, you must provide a user account with the minimum required permissions. The following is required:</p> <ul style="list-style-type: none"> • An administrative user account of the corresponding Azure Active Directory tenant, which has the following administration roles. <ul style="list-style-type: none"> • SharePoint administrators • Azure Active Directory company administrator/global administrator <p>NOTE: This user account must be entered as the site collection administrator in all the site collections to be managed. You do this in SharePoint Online.</p> <p>For more information about site collection administrators, see the Microsoft documentation.</p>
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> <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</p>

User	Permissions
	<p>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) <p>For authentication through an Azure Active Directory application, the user account requires the certificate with the private key in the computer's certificate store (*.PFX file). The certificate must be the same certificate used by the synchronization user.</p>
User for accessing the One Identity Manager database	The Synchronization default system user is provided to run synchronization using an application server.

Integrating One Identity Manager as application in Azure Active Directory

To synchronize data between One Identity Manager and SharePoint Online, you must integrate One Identity Manager as an application in the Azure Active Directory tenant that is linked to the Office 365 tenant. The SharePoint Online connector authenticates itself in Azure Active Directory tenants using the One Identity Manager application. For more information about integrating an enterprise application in Azure Active Directory, see the *One Identity Manager Administration Guide for Connecting to Azure Active Directory*.

NOTE: An application ID is created when you add One Identity Manager as an application to Azure Active Directory. You need the application ID for setting up the synchronization project.

For more information about registering an application, see <https://docs.microsoft.com/de-de/azure/active-directory/develop/quickstart-register-app>.

To configure One Identity Manager for SharePoint Online as an application in Azure Active Directory

1. Create a self-signed X.509 certificate with the type **Server authentication** to use for authenticating the application against Azure Active Directory.

For more information, see the *SharePoint Online documentation* from Microsoft.

2. Register a new application as described in *One Identity Manager Administration Guide for Connecting to Azure Active Directory*.
 - Select the **Accounts in this organizational directory only** option.
3. Copy the application ID.
4. Load the certificate file (*.CER) and copy the certificate's thumbprint.

You will need the thumbprint for creating the synchronization project.
5. Add the following permissions to the application:
 - API permissions
 - Microsoft APIs > SharePoint
 - Application entitlements:
 - Sites.FullControl.All
 - TermStore.ReadWrite.All
 - User.ReadWrite.All
6. Grant administrator consent for these permissions (**API permissions > Grant consent > Grant admin consent for > Yes**).

Related topics

- [Creating an initial synchronization project for SharePoint Online](#) on page 23

Setting up the SharePoint Online 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 SharePoint Online connector must be installed on the synchronization server.

If authentication through an Azure Active Directory application is used for logging in to SharePoint Online, the One Identity Manager Service requires the certificate with the private key in the computer's certificate store (*.PFX file).

Detailed information about this topic

- [System requirements for the SharePoint Online synchronization server](#) on page 17
- [Installing One Identity Manager Service with a SharePoint Online connector](#) on page 17
- [Integrating One Identity Manager as application in Azure Active Directory](#) on page 15

System requirements for the SharePoint Online synchronization server

To set up synchronization with a SharePoint Online tenant, a server must be available with the following software installed on it:

- Windows operating system

The following versions are supported:

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

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

Installing One Identity Manager Service with a SharePoint Online connector

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

Table 3: Properties of the Job server

Property	Value
Server function	SharePoint Online connector
Machine role	Server Job Server SharePoint Online

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

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

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

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

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

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

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

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

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

1. Start the Server Installer program.

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

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

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

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

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

- OR -

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

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

- **Server:** Name of the Job server.
- **Queue:** Name of the queue to handle the process steps. Each Job server within the network must have a unique queue identifier. The process

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

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

Syntax:

<Name of server>.<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 **SharePoint Online**.
5. On the **Server functions** page, select **SharePoint Online 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 string** 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 string** entry, then click the **Edit** button.
- e. Enter the address (URL) for the application server and click **OK**.
- f. Click the **Authentication string** entry and click the **Edit** button.
- g. In the **Authentication method** dialog, select the authentication module for logging in. Depending on the authentication module, other data may be required, such as user and password. For more information about One Identity Manager authentication modules, see the *One Identity Manager Authorization and Authentication Guide*.
- h. Click **OK**.

7. To configure the installation, click **Next**.

8. Confirm the security prompt with **Yes**.
9. On the **Select installation source** page, select the directory with the install files. Change the directory if necessary.
10. On the **Service access** page, enter the service's installation data.
 - **Computer:** Select the server, on which you want to install and start the service, from the menu or enter the server's name or IP address.
To run the installation locally, select **Local installation** from the menu.
 - **Service account:** Enter the details of the user account that the One Identity Manager Service is running under. Enter the user account, the user account's password and password confirmation.

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

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

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

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

Preparing the administrative workstation for access to SharePoint Online

To configure synchronization with SharePoint Online in the Synchronization Editor, One Identity Manager must load the data directly from the SharePoint Online environment. If authentication through an Azure Active Directory application is used for logging in to SharePoint Online, the user currently logged in on the administrative workstation requires the certificate with the private key in the computer's certificate store (*.PFX file). The certificate must be the same certificate used by the synchronization user.

If direct access from the workstation is not possible, you can set up a remote connection server.

Related topics

- [Users and permissions for synchronizing with SharePoint Online](#) on page 14
- [Preparing a remote connection server for access to the SharePoint Online tenant](#) on page 21

Preparing a remote connection server for access to the SharePoint Online tenant

To configure synchronization with a target system, One Identity Manager must load the data from the target system. One Identity Manager communicates directly with the target system to do this. Sometimes direct access from the workstation, on which the Synchronization Editor is installed, is not possible. For example, because of the firewall configuration or the workstation does not fulfill the necessary hardware and software requirements. If direct access is not possible from the workstation, you can set up a remote connection.

The remote connection server and the workstation must be in the same Active Directory domain.

Remote connection server configuration:

- One Identity Manager Service is started
- **RemoteConnectPlugin** is installed
- SharePoint Online connector is installed

The remote connection server must be declared as a Job server in One Identity Manager. The Job server name is required.

TIP: The remote connection server requires the same configuration as the synchronization server (with regard to the installed software and entitlements and user account certificate). Use the synchronization as remote connection server at the same time by installing the **RemoteConnectPlugin** as well.

For more detailed information about setting up a remote connection, see the *One Identity Manager Target System Synchronization Reference Guide*.

Related topics

- [Setting up the SharePoint Online synchronization server](#) on page 16
- [Users and permissions for synchronizing with SharePoint Online](#) on page 14

Creating a synchronization project for initial synchronization of a SharePoint Online tenant

Use the Synchronization Editor to configure synchronization between the One Identity Manager database and SharePoint Online tenant. The following describes the steps for initial configuration of a synchronization project.

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

Synchronization Editor also provides different configuration options for a synchronization project.

Information required for setting up a synchronization project

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

Table 4: Information required for setting up a synchronization project

Data	Explanation
Name of the base domain	Name of the Azure Active Directory base domain without .onmicrosoft.com.
Authentication method for logging in to SharePoint Online.	<ul style="list-style-type: none">• Application ID and certificate's thumbprint for authentication through an Azure Active Directory appliance.- OR -• User name and password for legacy authentication <p>Example:</p> <p><user name of the synchronization user>@yourorganization.onmicrosoft.com</p> <p>Make a user account available with sufficient permissions. For more information, see Users and permissions for synchronizing with SharePoint Online on page 14.</p>
Synchronization server for SharePoint Online	<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 SharePoint Online connector must be installed on the synchronization server.</p>

Table 5: Properties of the Job server

Property	Value
Server function	SharePoint Online connector
Machine role	Server Job Server SharePoint Online

For more information, see [Setting up the SharePoint Online synchronization server](#) on page 16.

One Identity Manager	<ul style="list-style-type: none">• Database server• Database name
----------------------	---

Data	Explanation
database connection data	<ul style="list-style-type: none"> • SQL Server 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	For more information, see Preparing a remote connection server for access to the SharePoint Online tenant on page 21.

Creating an initial synchronization project for SharePoint Online

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 an initial synchronization project for a SharePoint Online tenant

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

NOTE: If synchronization is run by an application server, connect the database through the application server.
2. Select the **Target system type SharePoint Online** entry and click **Start**.
This starts the Synchronization Editor's project wizard.
3. On the **System access** page, specify how One Identity Manager can access the target system.

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

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

4. Enter login data on the **Enter connection credentials** page to connect to SharePoint Online.
 - **Base domain:** Name of the Azure Active Directory base domain without .onmicrosoft.com.
 - **Authentication type:** Type of authentication that the SharePoint Online connector uses to log in to SharePoint Online. Select **Azure Active Directory application** or **Legacy**.

For authentication through an Azure Active Directory application, enter the following data:

- **Authentication endpoint:** Select the authentication endpoint of the Azure Active Directory application.
- **Application ID:** Application ID that was generated during integration of One Identity Manager as an Azure Active Directory tenant application.
- **Certificate thumbprint:** Thumbprint of the certificate that was created during integration of One Identity Manager as an application of the Azure Active Directory tenant.

Enter the following data for legacy authentication:

- **User name:** Enter the fully qualified name (FQDN) of the user account for logging in to SharePoint Online using the following format: user@domain.

Example:

<user name of the synchronization
user>@yourorganization.onmicrosoft.com

- **Password:** Password of the user account.

5. You can save the connection data on the last page of the system connection wizard.
 - Set the **Save connection locally** option to save the connection data. This can be reused when you set up other synchronization projects.
 - Click **Finish**, to end the system connection wizard and return to the project wizard.
6. 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.
7. 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.
 8. On the **Restrict target system access** page, specify how system access should work. You have the following options:

Table 6: Specify target system access

Option	Meaning
	<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.

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

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

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

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

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

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

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.

IMPORTANT: After you have set up the synchronization project, you must adjust the setting for the target system scope in the Synchronization Editor.

The scope should only include site collections in which the applicable synchronization user is entered in the SharePoint Online administration interface as the site collection administrator. There is no default user in SharePoint Online.

If the scope is not correctly set up, site collections cannot be loaded and synchronization is stopped.

To edit site collections in the scope of a SharePoint Online synchronization project

1. Open the Synchronization Editor.
2. Select the **Configuration > Target system** category.
3. Select the **Scope** view.
4. Click **Edit scope**. A list of site collections appears on the right-hand side.
5. Activate the site collections to synchronize.

In the list, select only the site collections for which the synchronization user is the same as the administrator in SharePoint Online.

6. Click **Commit to database** to save the changes.

Related topics

- [Users and permissions for synchronizing with SharePoint Online](#) on page 14
- [SharePoint Online synchronization features](#) on page 27
- [Setting up the SharePoint Online synchronization server](#) on page 16
- [Configuring the synchronization log](#) on page 27
- [Customizing the synchronization configuration](#) on page 28
- [Integrating One Identity Manager as application in Azure Active Directory](#) on page 15

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.

To configure the content of the synchronization log

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

- OR -

To configure the synchronization log for the database connection, select the **Configuration > One Identity Manager connection** category in the Synchronization Editor.

2. Select the **General** view and click **Configure**.
3. Select the **Synchronization log** view and 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**.

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 38

SharePoint Online synchronization features

There are a number of features for synchronizing SharePoint Online environments, which are described here.

- Only one SharePoint Online tenant is supported per synchronization project. You cannot add more base objects.
- The target system schema in One Identity Manager cannot be extended.

- After you have set up the synchronization project, you must adjust the setting for the target system scope in Synchronization Editor.

The scope should only include site collections in which the applicable synchronization user is entered in the SharePoint Online administration interface as the site collection administrator. There is no default user in SharePoint Online.

If the scope is not correctly set up, site collections cannot be loaded and synchronization is stopped.

To edit site collections in the scope of a SharePoint Online synchronization project

1. Open the Synchronization Editor.
2. Select the **Configuration > Target system** category.
3. Select the **Scope** view.
4. Click **Edit scope**. A list of site collections appears on the right-hand side.
5. Activate the site collections to synchronize.

In the list, select only the site collections for which the synchronization user is the same as the administrator in SharePoint Online.

6. Click **Commit to database** to save the changes.

Related topics

- [Users and permissions for synchronizing with SharePoint Online](#) on page 14
- [Error synchronizing after renaming a SharePoint Online site collection](#) on page 150

Customizing the synchronization configuration

Having used the Synchronization Editor to set up a synchronization project for initial synchronization of a SharePoint Online tenant, you can use the synchronization project to load SharePoint Online site collections into the One Identity Manager database. If you manage sites, users, and groups with One Identity Manager, the changes are provisioned to the SharePoint Online tenant.

Adjust the synchronization configuration in order to compare the One Identity Manager database with the SharePoint Online tenant on a regular basis and to synchronize changes.

- To use One Identity Manager as the primary system during synchronization, create a workflow with synchronization in the direction of the **Target system**.
- To specify which SharePoint Online objects and One Identity Manager database objects are included in the synchronization, edit the scope of the target system connection and the One Identity Manager database connection. To prevent data

inconsistencies, define the same scope in both systems. If no scope is defined, all objects will be synchronized.

- You can use variables to create generally applicable synchronization configurations that contain the necessary information about the synchronization objects when synchronization starts. Variables can be implemented in base objects, schema classes, or processing method, for example.
- Update the schema in the synchronization project if the One Identity Manager schema or target system schema has changed. Then you can add the changes to the mapping.
- To synchronize additional schema properties, update the schema in the synchronization project. Include the schema extensions in the mapping.

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

Detailed information about this topic

- [Configuring synchronization with SharePoint Online tenants](#) on page 29
- [Changing system connection settings of SharePoint Online tenants](#) on page 30
- [Updating schemas](#) on page 32
- [Configuring the provisioning of memberships](#) on page 33
- [Configuring single object synchronization](#) on page 34
- [Accelerating provisioning and single object synchronization](#) on page 36

Configuring synchronization with SharePoint Online tenants

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 SharePoint Online

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.

Changing system connection settings of SharePoint Online tenants

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 30
- [Editing target system connection properties](#) on page 31

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.

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 31

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 30

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.

Configuring the provisioning of memberships

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

- Memberships are saved as an object property in list form in the target system.
Example: List of user accounts in the Member property of a SharePoint Online group (Group)
- Memberships can be modified in either of the connected systems.
- A provisioning workflow and provisioning processes are set up.

If one membership in One Identity Manager changes, by default, the complete list of members is transferred to the target system. Therefore, memberships that were previously added to the target system are removed in the process and previously deleted memberships are added again.

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

To allow separate provisioning of memberships

1. In the Manager, select the **SharePoint Online > Basic configuration data > Target system types** category.
2. In the result list, select the **SharePoint Online** target system type.

3. Select the **Configure tables for publishing** task.
4. Select the assignment tables that you want to set up for single provisioning. Multi-select is possible.
5. Click **Merge mode**.


NOTE:

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

6. Save the changes.

For each assignment table labeled like this, the changes made in One Identity Manager are saved in a separate table. Therefore, only newly added and deleted assignments are processed. During modification provisioning, the members list in the target system is compared to the entries in this table. This means that only modified memberships are provisioned and not the entire members list.

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

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

To restore the original condition

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

NOTE: To create the reference to the added or deleted assignments in the condition, use the *i* table alias.

Example of a condition on the O3SUserInGroup assignment table:

```
exists (select top 1 1 from O3SGroup g
        where g.UID_O3SGroup = i.UID_O3SGroup
        and <limiting condition>)
```

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

Configuring single object synchronization

Changes made to individual objects in the target system can be immediately applied in the One Identity Manager database without having to start a full synchronization of the target

system environment. Individual objects can only be synchronized if the object is already present in the One Identity Manager database. The changes are applied to the mapped object properties. If a membership list belongs to one of these properties, the entries in the assignment table will also be updated. If the object is no longer present in the target system, then it is deleted from the One Identity Manager database.

Prerequisites

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

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

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

1. In the Manager, select the **SharePoint Online > Basic configuration data > Target system types** category.
2. In the result list, select the **SharePoint Online** target system type.
3. Select the **Assign synchronization tables** task.
4. In the **Add assignments** pane, assign the custom table for which you want to use single object synchronization.
5. Save the changes.
6. Select the **Configure tables for publishing** task.
7. Select the custom table and enter the **Root object path**.
Enter the path to the base object in the ObjectWalker notation of the VI.DB.
Example: `FK(UID_03STenant).XObjectKey`
8. Save the changes.

Related topics

- [Synchronizing single objects](#) on page 40
- [Post-processing outstanding objects](#) on page 41

Accelerating provisioning and single object synchronization

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

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

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

To configure load balancing

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

All Job servers must access the same SharePoint Online tenant as the synchronization server for the respective base object.

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

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

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

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

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

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

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

To use the synchronization server without load balancing.

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

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

Detailed information about this topic

- [Server bearbeiten](#)

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.

Before you run synchronization of the SharePoint Online environments, the Azure Active Directory environment in One Identity Manager must have the latest status.

NOTE: Synchronize the Azure Active Directory environment on a regular basis. Synchronization must take place in the following order:

1. Azure Active Directory
2. SharePoint Online

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 39
- [Displaying synchronization results](#) on page 38
- [Pausing handling of target system specific processes \(Offline mode\)](#) on page 45

Starting synchronization

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

To synchronize on a regular basis

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

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

To start initial synchronization manually

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

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

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

Displaying synchronization results

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

To display a synchronization log

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

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

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

To display a provisioning log

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Logs** category.

3. Click  in the navigation view toolbar.

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

4. Select a log by double-clicking it.

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

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

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

Related topics

- [Configuring the synchronization log](#) on page 27
- [Troubleshooting](#) on page 44

Deactivating synchronization

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

To prevent regular synchronization

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

Now you can only start synchronization manually.

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

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

To deactivate the synchronization project

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

Related topics

- [Pausing handling of target system specific processes \(Offline mode\)](#) on page 45

Synchronizing single objects

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

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

To synchronize a single object

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

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

Features of synchronizing memberships

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

Example:

Base object for assigning SharePoint Online user accounts to SharePoint Online groups is the group.

In the target system, a user account was assigned to a group. To synchronize this assignment, in the Manager, select the group that the user account was assigned to and run single object synchronization. In the process, all of the group's memberships are synchronized.

The user account must already exist as an object in the One Identity Manager database for the assignment to be made.

Detailed information about this topic

- [Configuring single object synchronization](#) on page 34

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 41
- [Adding custom tables to the target system synchronization](#) on page 43
- [Managing 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 **SharePoint Online > Target system synchronization: SharePoint Online** category.

The navigation view lists all the synchronization tables assigned to the **SharePoint Online** 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 object 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. 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 7: 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.

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.

Adding custom tables to the target system synchronization

You must customize your target system synchronization to synchronize custom tables.

To add custom tables to target system synchronization

1. In the Manager, select the **SharePoint Online > Basic configuration data > Target system types** category.
2. In the result list, select the **SharePoint Online** target system type.
3. Select the **Assign synchronization tables** task.
4. In the Add assignments pane, assign **custom** tables to the outstanding objects you want to handle.
5. Save the changes.
6. Select the **Configure tables for publishing** task.
7. Select the custom tables that contain the outstanding objects that can be published in the target system and set the **Publishable** option.
8. Save the changes.

Related topics

- [Post-processing outstanding objects](#) on page 41

Managing user accounts through account definitions

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

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

Detailed information about this topic

- [Assigning account definitions to linked SharePoint Online user accounts](#) on page 72

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 38
- [SharePoint Online synchronization features](#) on page 27

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 39

Managing SharePoint Online user accounts and employees

The main feature of One Identity Manager is to map employees 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 employees. This provides an overview of the permissions for each employee in all of the connected target systems. One Identity Manager offers the option of managing user accounts and their permissions. You can provision modifications in the target systems. Employees are supplied with the necessary permissions in the connected target systems according to their function in the company. Regular synchronization keeps data consistent between target systems and the One Identity Manager database.

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

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

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

- When user accounts are inserted, they can be automatically assigned to an existing employee. 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 employees for automatic employee assignment.
- Employees and user accounts can be entered manually and assigned to each other.

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

Related topics

- [Account definitions for SharePoint Online user accounts](#) on page 48
- [Assigning employees automatically to SharePoint Online user accounts](#) on page 68
- [SharePoint Online user accounts](#) on page 106

Account definitions for SharePoint Online user accounts

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

The data for the user accounts in the respective target system comes from the basic employee data. The assignment of the IT operating data to the employee's user account is controlled through the primary assignment of the employee to a location, a department, a cost center, or a business role. 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 employee's properties that are inherited by the user account. This allows an employee to have several user accounts in one target system, for example:

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

For more detailed 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 employees and target systems

Detailed information about this topic

- [Creating account definitions](#) on page 49
- [Editing manage levels](#) on page 52
- [Creating mapping rules for IT operating data](#) on page 55
- [Entering IT operating data](#) on page 57
- [Assigning account definitions to employees](#) on page 59
- [Assigning account definitions to SharePoint Online site collections](#) on page 65

Creating account definitions

To create a new account definition

1. In the Manager, select the **SharePoint Online > 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.

Related topics

- [Main data for account definitions](#) on page 49
- [Editing account definitions](#) on page 49
- [Assigning manage levels to account definitions](#) on page 54

Editing account definitions

To edit an account definition

1. In the Manager, select the **SharePoint Online > 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 49
- [Creating account definitions](#) on page 49
- [Assigning manage levels to account definitions](#) on page 54

Main data for account definitions

Enter the following data for an account definition:

Table 8: 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	<p>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.</p> <p>TIP: You can enter the account definition of the corresponding Azure Active Directory tenant here. In this case, an Azure Active Directory user account is first created for the employee. Once this user account exists, the SharePoint Online user account is added.</p>
Description	Text field for additional explanation.
Manage level (initial)	Manage level to use by default when you add new user accounts.
Risk index	<p>Value for evaluating the risk of assigning the account definition to employees. 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. The account definition can be requested by an employee through the Web Portal and distributed using a defined approval process. The resource can also be assigned directly to employees 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. The account definition can be requested by an employee through the Web Portal and distributed using a defined approval process. The account definition cannot be directly assigned to roles outside the IT Shop.
Automatic assignment to employees	Specifies whether the account definition is automatically

Property	Description
	<p>assigned to all internal employees. To automatically assign the account definition to all internal employee, use the Enable automatic assignment to employees. The account definition is assigned to every employee that is not marked as external. Once a new internal employee is created, they automatically obtain this account definition.</p> <p>To automatically remove the account definition assignment from all employees, use the Disable automatic assignment to employees. The account definition cannot be reassigned to employees 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 employees.</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. The associated user account is deleted.</p>
Retain account definition if temporarily disabled	<p>Specifies the account definition assignment to temporarily deactivated employees.</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. The associated user account is deleted.</p>
Retain account definition on deferred deletion	<p>Specifies the account definition assignment on deferred deletion of employees.</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. The associated user account is deleted.</p>
Retain account definition on security risk	<p>Specifies the account definition assignment to employees 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. The associated user account is deleted.</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

Property	Description
	input fields.
Groups can be inherited	<p>Specifies whether the user account can inherit groups through the linked employee. If the option is set, the user account inherits groups through hierarchical roles, in which the employee is a member, or through IT Shop requests.</p> <ul style="list-style-type: none"> • If you add an employee with a user account to a department, for example, and you have assigned groups to this department, the user account inherits these groups. • If an employee has requested group membership in the IT Shop and the request is granted approval, the employee's user account only inherits the group if the option is set.
Roles can be inherited	<p>Specifies whether the user account can inherit SharePoint Online roles through the linked employee. If the option is set, the user account inherits the roles through hierarchical roles, in which the employee is a member, or through IT Shop requests.</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 employee but they do not inherit any further properties. When a new user account is added with this manage level and an employee is assigned, some of the employee's properties are transferred initially. If the employee properties are changed at a later date, the changes are not passed onto the user account.
- **Full managed:** User accounts with the **Full managed** manage level inherit defined properties of the assigned employee. When a new user account is created with this manage level and an employee is assigned, the employee's properties are transferred in an initial state. If the employee properties are changed at a later date, the changes are passed onto the user account.

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

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

Specify the effect of temporarily or permanently disabling, deleting, or the security risk of an employee on its user accounts and group memberships for each manage level. For more information about manage levels, see the *One Identity Manager Target System Base Module Administration Guide*.

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

To edit a manage level

1. In the Manager, select the **SharePoint Online > 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 54
- [Entering IT operating data](#) on page 57
- [Assigning manage levels to account definitions](#) on page 54

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 **SharePoint Online > 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 account definitions](#) on page 49
- [Editing account definitions](#) on page 49
- [Assigning manage levels to account definitions](#) on page 54

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 **SharePoint Online > 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 9: 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.

Property	Description
	<ul style="list-style-type: none"> • 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 employees are locked.
Retain groups if permanently disabled	Specifies whether user accounts of permanently deactivated employees retain group memberships.
Lock user accounts if permanently disabled *)	Specifies whether user accounts of permanently deactivated employees are locked.
Retain groups on deferred deletion	Specifies whether user accounts of employees marked for deletion retain their group memberships.
Lock user accounts if deletion is deferred*)	Specifies whether user accounts of employees marked for deletion are locked.
Retain groups on security risk	Specifies whether user accounts of employees posing a security risk retain their group memberships.
Lock user accounts if security is at risk*)	Specifies whether user accounts of employees posing a security risk are locked.
Retain groups if user account disabled	Specifies whether disabled user accounts retain their group memberships.

NOTE:*) SharePoint Online user accounts cannot be locked!

When an employee is disabled, deleted, or rated as a security risk their SharePoint Online user accounts remain enabled. For logging into a SharePoint Online site collection, you need to know if the user account referenced as an authentication object is locked or disabled. To prevent a disabled, deleted, or security risk employee logging into a SharePoint Online site collection, manage the user accounts linked as authentication objects using account definitions.

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 employee's primary roles.

The following IT operating data is used in the One Identity Manager default configuration for automatically creating user accounts for an employee in the target system and modifying them.

- SharePoint Online authentication mode
- Groups can be inherited
- Roles can be inherited
- Privileged user account.

To create a mapping rule for IT operating data

1. In the Manager, select the **SharePoint Online > 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 menu, you can select the columns that use the TSB_ITDataFromOrg script in their template.
 - **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 employee'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 **Employee - new user account with default properties created** mail template is used.

To change the mail template, in the Designer, adjust the **TargetSystem | SharePoint Online | Accounts | MailTemplateDefaultValues** configuration parameter.
5. Save the changes.

Entering IT operating data

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

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

Example:

Normally, each employee in department A obtains a default user account in the tenant A. In addition, certain employees in department A obtain administrative user accounts in the tenant A.

Create an account definition A for the default user account of the tenant A and an account definition B for the administrative user account of tenant 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 tenant 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 menu, you can select the columns that use the TSB_ITDataFromOrg script in their template.

- **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 55

Modify IT operating data

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

Prerequisites

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

NOTE: If the assignment of an employee to a primary department, cost center, 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 **SharePoint Online > 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 employees

Account definitions are assigned to company employees.

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

You can automatically assign special account definitions to all company employees. It is possible to assign account definitions to the IT Shop as requestable products. 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 employees 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 employee already has a user account in the target system that has an account definition. If no user account exists, a new user account is created with the account definition's default manage level.

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

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

Prerequisites for indirect assignment of account definitions to employees

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

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 60
- [Assigning account definitions to business roles](#) on page 60
- [Assigning account definitions to all employees](#) on page 61
- [Assigning account definitions directly to employees](#) on page 62
- [Assigning account definitions to system roles](#) on page 62
- [Adding account definitions in the IT Shop](#) on page 62


Assigning account definitions to departments, cost centers, and locations

To add account definitions to hierarchical roles

1. In the Manager, select the **SharePoint Online > 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.


Assigning account definitions to business roles

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

To add account definitions to hierarchical roles

1. In the Manager, select the **SharePoint Online > 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.

Assigning account definitions to all employees

Use this task to assign the account definition to all internal employees. Employees that are marked as external do not obtain this account definition. Once a new internal employee 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 employees in the database and all pending newly added internal employees obtain a user account in this target system.

To assign an account definition to all employees

1. In the Manager, select the **SharePoint Online > 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 employees** task.
5. Confirm the security prompt with **Yes**.
6. Save the changes.

NOTE: To automatically remove the account definition assignment from all employees, run the **DISABLE AUTOMATIC ASSIGNMENT TO EMPLOYEES** task. The account definition cannot be reassigned to employees from this point on. Existing assignments remain intact.


Assigning account definitions directly to employees

To assign an account definition directly to employees

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

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

To remove an assignment

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

Assigning account definitions to system roles

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


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

To add account definitions to a system role

1. In the Manager, select the **SharePoint Online > 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.

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 employees using IT Shop assignments, you must also set the **Only for use in IT Shop** option. Direct assignment to hierarchical roles may not be possible.

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

To add an account definition to the IT Shop (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. In the **Add assignments** pane, assign the account definitions to the IT Shop shelves.
5. Save the changes.

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

1. In the Manager, select the **SharePoint Online > 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. In the **Add assignments** pane, assign the account definitions to the IT Shop shelves.
5. 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. In the **Remove assignments** pane, remove the account definitions from the IT Shop shelves.
5. Save the changes.

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

1. In the Manager, select the **SharePoint Online > 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. In the **Remove assignments** pane, remove the account definitions from the IT Shop shelves.
5. 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 **SharePoint Online > 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 49

Assigning account definitions to SharePoint Online site collections

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

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

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

To assign the account definition to a target system

1. In the Manager, select the site collection in the **SharePoint Online > Site collections** category.
2. Select the **Change main data** task.
3. From the **Account definition (initial)** menu, select the account definition for user accounts.
4. Save the changes.

Related topics

- [Assigning employees automatically to SharePoint Online user accounts](#) on page 68

Deleting account definitions

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

To delete an account definition

1. Remove automatic assignments of the account definition from all employees.
 - a. In the Manager, select the **SharePoint Online > 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 employees** task.
 - e. Confirm the security prompt with **Yes**.
 - f. Save the changes.
2. Remove direct assignments of the account definition to employees.

- a. In the Manager, select the **SharePoint Online > Basic configuration data > Account definitions > Account definitions** category.
 - b. Select an account definition in the result list.
 - c. Select the **Assign to employees** task.
 - d. In the **Remove assignments** pane, remove employees.
 - e. Save the changes.
3. Remove the account definition's assignments to departments, cost centers, and locations.
 - a. In the Manager, select the **SharePoint Online > 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 **SharePoint Online > 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. Remove the assignment of the account definition to IT operating data.
 - a. In the Manager, select the **SharePoint Online > Basic configuration data > Account definitions > Account definitions** category.
 - b. Select an account definition in the result list.
 - c. Select the **Edit IT operating data mapping** task.
 - d. Select a column and click **Delete** to remove the mapping rule.
 - e. Delete all mapping rules.
 - f. Save the changes.
6. If the account definition was requested through the IT Shop, it must be canceled and removed from all IT Shop shelves.

For more detailed information about unsubscribing requests, see the *One Identity Manager Web Designer 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 **SharePoint Online > 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.

7. 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 **SharePoint Online > 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** menu, remove the account definition.
 - e. Save the changes.
8. Remove the account definition's assignments to target systems.
 - a. In the Manager, select the site collection in the **SharePoint Online > Site collections** category.
 - b. Select the **Change main data** task.
 - c. On the **General** tab, remove the assigned account definitions.
 - d. Save the changes.
9. Delete the account definition.

- a. In the Manager, select the **SharePoint Online > 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 employees automatically to SharePoint Online user accounts

When you add a user account, an existing employee can automatically be assigned to it. This mechanism can be triggered after a new user account is created either manually or through synchronization.

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

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

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

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

Prerequisites

- The user accounts are principals of **User** type.
- The user accounts are not assigned an authentication object

Run the following tasks to assign employees automatically.

- If you want employees to be assigned during the synchronization of user accounts, in the Designer, set the **TargetSystem | SharePointOnline | PersonAutoFullsync** configuration parameter and select the required mode.
- If you want employees to be assigned outside synchronization, in the Designer, set the **TargetSystem | SharePointOnline | PersonAutoDefault** configuration parameter and select the required mode.
- Assign an account definition to the site collection. Ensure that the manage level to be used is entered as the default manage level.
- Define the search criteria for employees assigned to the site collection.

NOTE:

The following applies for synchronization:

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

The following applies outside synchronization:

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

NOTE:

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

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

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

Related topics

- [Creating account definitions](#) on page 49
- [Assigning account definitions to SharePoint Online site collections](#) on page 65
- [Changing manage levels for SharePoint Online user accounts](#) on page 70
- [Editing search criteria for automatic employee assignment](#) on page 69

Editing search criteria for automatic employee assignment

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

The search criterion is written in XML notation to the **Search criteria for automatic employee assignment** column (AccountToPersonMatchingRule) in the 03SSite table.

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

NOTE: 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 specify criteria for employee assignment

1. In the Manager, select the **SharePoint Online > Site collections** category.
2. Select the site collection in the result list.
3. Select the **Define search criteria for employee assignment** task.
4. Specify which user account properties must match with which employee so that the employee is linked to the user account.

Table 10: Search criteria for user accounts

Apply to	Column for employee	Column for user account
SharePoint Online user account (user authenticated)	Default email address (DefaultEmailAddress)	Email address (EMail)

5. Save the changes.

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

Related topics

- [Assigning employees automatically to SharePoint Online user accounts](#) on page 68
- [Finding employees and directly assigning them to user accounts](#) on page 71

Changing manage levels for SharePoint Online user accounts

The default manage level is applied if you create user accounts using automatic employee 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 **SharePoint Online > User accounts (user authenticated)** 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.

Finding employees and directly assigning them to user accounts

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

Table 11: Manual assignment view

View	Description
Suggested assignments	This view lists all user accounts to which One Identity Manager can assign an employee. All employees are shown who were found using the search criteria and can be assigned.
Assigned user accounts	This view lists all user accounts to which an employee is assigned.
Without employee assignment	This view lists all user accounts to which no employee is assigned and for which no employee was found using the search criteria.

To apply search criteria to user accounts

1. In the Manager, select the **SharePoint Online > Site collections** category.
2. Select the site collection in the result list.
3. Select the **Define search criteria for employee 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 employee main data.

The assignment of employees 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 employees directly over a suggestion list

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

3. Click **Assign selected**.

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

The employees 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 employee assignment**.

1. Click **Select employee** for the user account to which you want to assign an employee. Select an employee from the menu.

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

3. (Optional) Select an account definition in the **Assign this account definition** menu, and select a manage level in the **Assign this account manage level** menu.

4. Click **Assign selected**.

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

The employees displayed in the **Employee** 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 you want to delete the employee assignment from. Multi-select is possible.

2. Click **Remove selected**.

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

The assigned employees are removed from the selected user accounts.

Assigning account definitions to linked SharePoint Online user accounts

An account definition can be subsequently assigned to user accounts with **Linked** status. This may be necessary, for example, if:

- Employees and user accounts were linked manually
- Automatic employee assignment is configured, but when a user account is inserted, no account definition is assigned in the SharePoint Online system.

To manage user accounts through account definitions

1. Create an account definition.
2. Assign an account definition to the site collection.
3. 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 **SharePoint Online > User accounts (user authenticated) > Linked but not configured > <site collection>** category.
 - b. Select the **Assign account definition to linked accounts** task.
 - c. In the **Account definition** menu, select the account definition.
 - d. Select the user accounts that contain the account definition.
 - e. Save the changes.

Detailed information about this topic

- [Assigning account definitions to SharePoint Online site collections](#) on page 65

Manually linking employees to SharePoint Online user accounts

An employee can be linked to multiple SharePoint Online user accounts, for example, so that you can assign an administrative user account in addition to the default user account. One employee can also use default user accounts with different types.

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

To manually assign user accounts to an employee

1. In the Manager, select the **Employees > Employees** category.
2. Select the employee in the result list and run the **Assign SharePoint Online user accounts** task.
3. Assign the user accounts.
4. Save the changes.

Related topics

- [Application cases for SharePoint Online user account](#) on page 74
- [Supported user account types](#) on page 75

Application cases for SharePoint Online user account

Example:

Set up guest access to a site collection with read-only permissions. To do this, a SharePoint Online user account is added. The Azure Active Directory **Guests** group is assigned as authentication object to the user account. Jo User1 owns an Azure Active Directory user account, which is a member in this group. They can log in to the site collection with this and obtain all the SharePoint Online user account's permissions.

Jan User3 also obtain a guest login for the site collection. They own an Azure Active Directory user account in the same domain. In the Web Portal, they request membership of the Azure Active Directory **Guests** group. Once the request is granted approval and assigned, they can log in on the site collection.

SharePoint Online access permissions are supplied in different ways in the One Identity Manager, depending on the referenced authentication object.

Case 1: The associated authentication object is a group. The authentication system is managed in One Identity Manager. (Default case)

- The user account represents an Azure Active Directory group. This group can be assigned in the One Identity Manager as authentication object.
- The user account cannot be assigned to an employee. This means, the user account can only become a member in SharePoint Online roles and groups through direct assignment.
- Before an employee can log in to the SharePoint Online system, they require an Azure Active Directory user account. This user account must be a member of the Azure Active Directory group that is used as an authentication object.
- A new SharePoint Online user account can be created manually.
- The user account cannot be managed through an account definition.

Case 2: The authentication object is a user account. The authentication system is managed in One Identity Manager.

- The user account represents an Azure Active Directory user account. The user account is not assigned as an authentication object in One Identity Manager.
- The SharePoint Online user account can be assigned to an employee. This means that the user account can become a member in SharePoint Online roles and groups

through inheritance and direct assignment.

If an authentication object is assigned, the connected employee is found through the authentication object.

If there is no authentication object assigned, the employee can be assigned automatically or manually. Automatic employee assignment depends on the **TargetSystem | SharePointOnline | PersonAutoFullsync** and **TargetSystem | SharePointOnline | PersonAutoDefault** configuration parameters.

- A new SharePoint Online user account can be manually created or by using an account definition. The Azure Active Directory user account used as the authentication object must belong to a domain trusted by the referenced authentication system.
- The user account can be managed through an account definition.

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

Supported user account types

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

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

- Identity

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

Table 12: Identities of user accounts

Identity	Description	Value of the IdentityType column
Primary identity	Employee's default user account.	Primary
Organizational identity	Secondary user account used for different roles in the organization, for example for subcontracts with other functional areas.	Organizational
Personalized admin identity	User account with administrative permissions, used by one employee.	Admin
Sponsored identity	User account used for a specific purpose. For example, for training purposes.	Sponsored

Identity	Description	Value of the IdentityType column
Shared identity	User account with administrative permissions, used by several employees.	Shared
Service identity	Service account.	Service

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

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

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

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

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

- Privileged user account

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

Detailed information about this topic

- [Default user accounts](#) on page 76
- [Administrative user accounts](#) on page 77
- [Privileged user accounts](#) on page 80

Default user accounts

Normally, each employee obtains a default user account, which has the permissions they require for their regular work. The user accounts are linked to the employee. By default, the link between employee and SharePoint Online user account is set up through the authentication objects to which the user account is assigned. Alternatively, employees can

also be directly linked to the user accounts. Such user accounts can be managed through account definitions. The effect of the link and the scope of the employee's inherited properties on the user accounts can be configured through an account definition and its manage levels.

To create default user accounts through account definitions

1. Create an account definition and assign the **Unmanaged** and **Full managed** manage levels.
2. Specify the effect of temporarily or permanently disabling, deleting, or the security risk of an employee on its user accounts and group memberships for each manage level.
3. Create a formatting rule for IT operating data.

You use the mapping rule to define which rules are used to map IT operating data for user accounts and which default values are used if no IT operating data can be determined through a person'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 rules for the `IsGroupAccount_Group` and `IsGroupAccount_RLAsgn` columns, use the default value **1** and set the **Always use default value** option.
 - In the mapping rule for the `IdentityType` column, use the default value **Primary** and enable **Always use default value**.
4. Enter the effective IT operating data for the target system. Select the concrete target system under **Effects on**.
Specify in the departments, cost centers, locations, or business roles that IT operating data should apply when you set up a user account.
 5. Assign the account definition to employees.
When the account definition is assigned to an employee, a new user account is created through the inheritance mechanism and subsequent processing.

Related topics

- [Account definitions for SharePoint Online user accounts](#) on page 48

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 administrative user accounts for one employee](#) on page 78
- [Providing administrative user accounts for several employees](#) on page 79

Providing administrative user accounts for one employee


Prerequisites

- The user account must be labeled as a personalized admin identity.
- The employee who will be using the user account must be labeled as a personalized admin identity.
- The employee who will be using the user account must be linked to a main identity.

To prepare an administrative user account for a person

1. Label the user account as a personalized admin identity.
 - a. In the Manager, select the **SharePoint Online > User accounts (user authenticated)** category.
- OR -
In the Manager, select the **SharePoint Online > User accounts (group authenticated)** 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 employee who will be using this administrative user account.
 - a. In the Manager, select the **SharePoint Online > User accounts (user authenticated)** category.
- OR -
In the Manager, select the **SharePoint Online > User accounts (group authenticated)** category.
 - b. Select the user account in the result list.
 - c. Select the **Change main data** task.

- d. On the **General** tab, in the **Person** selection list, select the employee who will be using this administrative user account.

TIP: If you are the target system manager, you can choose  to create a new person.

Related topics

- [Providing administrative user accounts for several employees](#) on page 79
- For more information about mapping employee identities, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Providing administrative user accounts for several employees


Prerequisite

- The user account must be labeled as a shared identity.
- A pseudo employee must exist. The pseudo employee must be labeled as a shared identity and must have a manager.
- The employees who are permitted to use the user account must be labeled as a primary identity.

To prepare an administrative user account for multiple employees


1. Label the user account as a shared identity.
 - a. In the Manager, select the **SharePoint Online > User accounts (user authenticated)** category.
- OR -
In the Manager, select the **SharePoint Online > User accounts (group authenticated)** 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** menu, select **Shared identity**.
2. Link the user account to a pseudo employee.
 - a. In the Manager, select the **SharePoint Online > User accounts (user authenticated)** category.
- OR -
In the Manager, select the **SharePoint Online > User accounts (group authenticated)** category.
 - b. Select the user account in the result list.

- c. Select the **Change main data** task.
 - d. On the **General** tab, select the pseudo employee from the **Employee** menu.

TIP: If you are the target system manager, you can choose  to create a new pseudo employee.
3. Assign the employees who will use this administrative user account to the user account.
- a. In the Manager, select the **SharePoint Online > User accounts (user authenticated)** category.
 - OR -
 - In the Manager, select the **SharePoint Online > User accounts (group authenticated)** category.
 - b. Select the user account in the result list.
 - c. Select the **Assign employees authorized to use** task.
 - d. In the **Add assignments** pane, add employees.

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

To remove an assignment

 - Select the employee and double-click .

Related topics

- [Providing administrative user accounts for one employee](#) on page 78
- For more information about mapping employee identities, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Privileged user accounts

Privileged user accounts are used to provide employees with additional privileges. This includes administrative user accounts or service accounts, for example. The user accounts are 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 the effect of temporarily or permanently disabling or deleting, or the security risk of an employee on its user accounts and group memberships for each manage level.
4. Create a formatting rule for 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 a person'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_Group` and `IsGroupAccount_RLAsgn` columns with a default value of **0** and set the **Always use default value** option.
5. Enter the effective IT operating data for the target system.

Specify in the departments, cost centers, locations, or business roles which IT operating data should apply when you set up a user account.
 6. Assign the account definition directly to employees who work with privileged user accounts.

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

| **TIP:**

Related topics

- [Account definitions for SharePoint Online user accounts](#) on page 48

Specifying deferred deletion for SharePoint Online 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 blocked. 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.

In the Designer, enter a different value for deferred deletion in the Deferred deletion [days] property of the **O3SUser** table.

- 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 **O3SUser** table.

Example:

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*.

Managing assignments of SharePoint Online groups and roles

User accounts inherit SharePoint Online permissions through SharePoint Online roles and SharePoint Online groups. SharePoint Online groups are always defined for one site collection in this way. SharePoint Online roles are defined for sites. They are assigned to groups, and the user accounts that are members of these groups inherit SharePoint Online permissions through them. SharePoint Online roles can also be assigned directly to user accounts. User account permissions on individual sites in a site collection are restricted through the SharePoint Online roles that are assigned to it.

In SharePoint Online, the users can have different entitlements that are mapped in One Identity Manager as follows:

- Entitlement for the use of SharePoint Online groups (03SGroup table)
- Entitlement for the use of SharePoint Online roles (03SRLAsgn)

Terms

- A SharePoint Online Role is the permission level linked to a fixed site.
- The assignment of user account or groups to a SharePoint Online role is called a role assignment.
- Entitlement assignments refer to the assignment of the various entitlements to user accounts. These include:
 - Group assignments to user accounts (03SUserInGroup table)
 - Role assignments to user accounts (03SUserHasRLAsgn table)

Detailed information about this topic

- [Assigning SharePoint Online entitlements to SharePoint Online user accounts](#) on page 84
- [Effectiveness of SharePoint Online entitlement assignments](#) on page 95
- [SharePoint Online group inheritance based on categories](#) on page 97
- [Overview of all assignments](#) on page 100

Assigning SharePoint Online entitlements to SharePoint Online user accounts

In One Identity Manager, SharePoint Online entitlements can be assigned directly or indirectly to employees.

In the case of indirect assignment, employees and entitlements are organized in hierarchical roles. The number of entitlements assigned to an employee is calculated from the position in the hierarchy and the direction of inheritance. If the employee has a SharePoint Online user account, the entitlements are assigned to this user account.

Entitlements can also be assigned to employees through IT Shop requests. To enable the assignment of entitlements using IT Shop requests, employees are added as customers in a shop. All entitlements assigned to this shop as products can be requested by the customers. After approval is granted, requested entitlements are assigned to the employees.

You can use system roles to group entitlements together and assign them to employees as a package. You can create system roles that contain only SharePoint Online entitlements. You can also group any number of company resources into a system role.

To react quickly to special requests, you can also assign the entitlements directly to user accounts.

For more information see the following guides:

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 assignment of SharePoint Online entitlements to SharePoint Online user accounts](#) on page 85
- [Assigning SharePoint Online entitlements to departments, cost centers, and locations](#) on page 86
- [Assigning SharePoint Online entitlements to business roles](#) on page 88
- [Assigning SharePoint Online user accounts directly to an entitlement](#) on page 92

- [Adding SharePoint Online entitlements to system roles](#) on page 89
- [Adding SharePoint Online entitlements to the IT Shop](#) on page 90
- [Assigning SharePoint Online entitlements directly to a user account](#) on page 93
- [Assigning SharePoint Online roles to SharePoint Online groups](#) on page 93

Prerequisites for indirect assignment of SharePoint Online entitlements to SharePoint Online user accounts

In the case of indirect assignment, employees, groups SharePoint Online, and SharePoint Online roles are assigned to hierarchical roles, such as departments, cost centers, locations, or business roles. When assigning SharePoint Online groups and SharePoint Online roles indirectly, check the following settings and modify them if necessary.

Prerequisites for indirect assignment of SharePoint Online groups to SharePoint Online user accounts

1. Assignment of employees and SharePoint Online groups is permitted for role classes (departments, cost centers, locations, or business roles).
2. The SharePoint Online user account does not have the **Groups can be inherited** option set.
3. The SharePoint Online user account is labeled with the **Groups can be inherited** option.
4. The SharePoint Online user account is linked to an employee.
5. The SharePoint Online user account and the SharePoint Online groups belong to the same site collection.

Prerequisites for indirect assignment of SharePoint Online roles to SharePoint Online user accounts

- Assignment of employees and SharePoint Online roles is permitted for role classes (departments, cost centers, locations, or business roles).
- The SharePoint Online user account does not have the **Groups can be inherited** option set.
- The SharePoint Online user account is labeled with the **Groups can be inherited** option.
- The SharePoint Online user account is linked to an employee.
- The SharePoint Online user account and the SharePoint Online roles belong to the same site collection.

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.

NOTE: If a SharePoint Online role refers to a permission level for which the **Hidden** option is set, no business roles and organizations can be assigned. These SharePoint Online roles can be neither directly nor indirectly assigned to user accounts or groups.

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 employees not allowed. For more detailed information about the basic principles for assigning company resources, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Related topics

- [Editing main data of SharePoint Online user accounts](#) on page 107
- [Main data for user authenticated user accounts](#) on page 108

Assigning SharePoint Online entitlements to departments, cost centers, and locations

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

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

1. In the Manager, select one of the following categories:
 - **SharePoint Online > Groups**
 - **SharePoint Online > Roles**
2. Select the entitlements 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 permissions to a department, cost center or location (role-based login)

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

- OR -

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

- OR -

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

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

3. Select one of the following tasks.

- **Assign SharePoint Online groups**
- **Assign SharePoint Online roles**

4. In the **Add assignments** pane, assign the entitlements.

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

To remove an assignment

- Select the entitlement and double-click .

5. Save the changes.

Related topics

- [Prerequisites for indirect assignment of SharePoint Online entitlements to SharePoint Online user accounts](#) on page 85
- [Assigning SharePoint Online entitlements to business roles](#) on page 88
- [Adding SharePoint Online entitlements to system roles](#) on page 89
- [Adding SharePoint Online entitlements to the IT Shop](#) on page 90
- [Assigning SharePoint Online user accounts directly to an entitlement](#) on page 92
- [Assigning SharePoint Online entitlements directly to a user account](#) on page 93
- [One Identity Manager users for managing SharePoint Online](#) on page 9

Assigning SharePoint Online entitlements to business roles

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


You assign entitlements to business roles so that these entitlements are assigned to user accounts through these business roles.

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

1. In the Manager, select one of the following categories.
 - **SharePoint Online > Groups**
 - **SharePoint Online > Roles**
2. Select the entitlements 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 entitlements to a business role (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 one of the following tasks.
 - **Assign SharePoint Online groups**
 - **Assign SharePoint Online roles**
4. In the **Add assignments** pane, assign the entitlements.

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

To remove an assignment

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

Related topics

- [Prerequisites for indirect assignment of SharePoint Online entitlements to SharePoint Online user accounts](#) on page 85
- [Assigning SharePoint Online entitlements to departments, cost centers, and locations](#) on page 86

- [Adding SharePoint Online entitlements to system roles on page 89](#)
- [Adding SharePoint Online entitlements to the IT Shop on page 90](#)
- [Assigning SharePoint Online user accounts directly to an entitlement on page 92](#)
- [Assigning SharePoint Online entitlements directly to a user account on page 93](#)
- [One Identity Manager users for managing SharePoint Online on page 9](#)

Adding SharePoint Online entitlements to system roles

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

Use this task to add an entitlement to system roles. If you assign a system role to employees, all user accounts owned by these employees inherit the entitlement.


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 one of the following categories.
 - **SharePoint Online > Groups**
 - **SharePoint Online > Roles**
2. Select the entitlements 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 assignment of SharePoint Online entitlements to SharePoint Online user accounts on page 85](#)
- [Assigning SharePoint Online entitlements to departments, cost centers, and locations on page 86](#)
- [Assigning SharePoint Online entitlements to business roles on page 88](#)
- [Adding SharePoint Online entitlements to the IT Shop on page 90](#)

- [Assigning SharePoint Online user accounts directly to an entitlement](#) on page 92
- [Assigning SharePoint Online entitlements directly to a user account](#) on page 93

Adding SharePoint Online entitlements to the IT Shop

When you assign a permission 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 permissions must be labeled with the **IT Shop** option.
 - The permission 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 permission easier to find in the Web Portal, assign a service category to the service item.
- If you only want the permission to be assigned to employees through IT Shop requests, the permissions 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 permissions to IT Shop shelves. Target system administrators are not authorized to add permissions to IT Shop.

To add a permission to the IT Shop.

1. In the Manager, select the one of the following categories (non role-based login).
 - **SharePoint Online > Groups**
 - **SharePoint Online > Roles**

- OR -

In the Manager, select one of the following categories (role-based login).

 - **Entitlements > SharePoint Online groups**
 - **Entitlements > SharePoint Online roles**
2. In the result list, select the permission.
3. Select the **Add to IT Shop** task.
4. Select the **IT Shop structures** tab.
5. In the **Add assignments** pane, the entitlement to the IT Shop shelves.
6. Save the changes.

To remove, an entitlement from individual shelves of the IT Shop

1. In the Manager, select the one of the following categories (non role-based login).
 - **SharePoint Online > Groups**
 - **SharePoint Online > Roles**- OR -

In the Manager, select one of the following categories (role-based login).

 - **Entitlements > SharePoint Online groups**
 - **Entitlements > SharePoint Online roles**
2. In the result list, select the permission.
3. Select the **Add to IT Shop** task.
4. Select the **IT Shop structures** tab.
5. In the **Remove assignments** pane, the entitlement from the IT Shop shelves.
6. Save the changes.

To remove, an entitlement from all shelves of the IT Shop

1. In the Manager, select the one of the following categories (non role-based login).
 - **SharePoint Online > Groups**
 - **SharePoint Online > Roles**- OR -

In the Manager, select one of the following categories (role-based login).

 - **Entitlements > SharePoint Online groups**
 - **Entitlements > SharePoint Online roles**
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 this group are canceled.

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

Related topics

- [SharePoint Online group main data](#) on page 118
- [General main data of SharePoint Online roles](#) on page 132
- [Prerequisites for indirect assignment of SharePoint Online entitlements to SharePoint Online user accounts](#) on page 85

- [Assigning SharePoint Online entitlements to departments, cost centers, and locations](#) on page 86
- [Assigning SharePoint Online entitlements to business roles](#) on page 88
- [Adding SharePoint Online entitlements to system roles](#) on page 89
- [Assigning SharePoint Online user accounts directly to an entitlement](#) on page 92
- [Assigning SharePoint Online entitlements directly to a user account](#) on page 93
- [One Identity Manager users for managing SharePoint Online](#) on page 9

Assigning SharePoint Online user accounts directly to an entitlement


To react quickly to special requests, you can assign the entitlements directly to user accounts.

To assign an entitlement directly to user accounts

1. In the Manager, select one of the following categories.
 - **SharePoint Online > Groups**
 - **SharePoint Online > Roles**
2. Select the entitlements in the result list.
3. Select in 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 SharePoint Online entitlements directly to a user account](#) on page 93
- [Assigning SharePoint Online entitlements to departments, cost centers, and locations](#) on page 86
- [Assigning SharePoint Online entitlements to business roles](#) on page 88
- [Adding SharePoint Online entitlements to system roles](#) on page 89
- [Adding SharePoint Online entitlements to the IT Shop](#) on page 90

Assigning SharePoint Online entitlements directly to a user account

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

To assign entitlements directly to a user account

1. In the Manager, select the **SharePoint Online > User accounts** category.
2. Select the user account in the result list.
3. Select one of the following tasks.

- **Assign groups**
- **Assign SharePoint Online roles**

4. In the **Add assignments** pane, assign the entitlements.

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

To remove an assignment

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

Related topics

- [Assigning SharePoint Online user accounts directly to an entitlement on page 92](#)
- [Assigning SharePoint Online entitlements to departments, cost centers, and locations on page 86](#)
- [Assigning SharePoint Online entitlements to business roles on page 88](#)
- [Adding SharePoint Online entitlements to system roles on page 89](#)
- [Adding SharePoint Online entitlements to the IT Shop on page 90](#)

Assigning SharePoint Online roles to SharePoint Online groups

In order for SharePoint Online user accounts to obtain permissions for individual websites, assign SharePoint Online roles to the groups. SharePoint Online roles and groups must belong to the same site collection.


NOTE: SharePoint Online roles with the **Hidden** option that reference permission levels, cannot be assigned to groups.

To assign SharePoint Online roles to a group

1. In the Manager, select the **SharePoint Online > Groups** category.
2. Select the group in the result list.
3. Select the **Assign SharePoint Online roles** task.
4. In the **Add assignments** pane, assign the roles.

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

To remove an assignment

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

Related topics

- [Entering main data for SharePoint Online permission levels on page 122](#)
- [Assigning SharePoint Online groups to SharePoint Online roles on page 94](#)
- [Assigning SharePoint Online entitlements to departments, cost centers, and locations on page 86](#)
- [Assigning SharePoint Online entitlements to business roles on page 88](#)
- [Adding SharePoint Online entitlements to system roles on page 89](#)
- [Adding SharePoint Online entitlements to the IT Shop on page 90](#)
- [Assigning SharePoint Online user accounts directly to an entitlement on page 92](#)
- [Assigning SharePoint Online entitlements directly to a user account on page 93](#)

Assigning SharePoint Online groups to SharePoint Online roles

In order for SharePoint Online user accounts to obtain permissions for individual websites, assign SharePoint Online roles to the groups. SharePoint Online roles and groups must belong to the same site collection.

NOTE: SharePoint Online roles with the **Hidden** option that reference permission levels, cannot be assigned to groups.

To assign groups to a SharePoint Online role

1. In the Manager, select the category **SharePoint Online > Roles**.
2. Select the role in the result list.
3. Select the **Assign groups** task.
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

- [Entering main data for SharePoint Online permission levels on page 122](#)
- [Assigning SharePoint Online roles to SharePoint Online groups on page 93](#)
- [Assigning SharePoint Online entitlements to departments, cost centers, and locations on page 86](#)
- [Assigning SharePoint Online entitlements to business roles on page 88](#)
- [Adding SharePoint Online entitlements to system roles on page 89](#)
- [Adding SharePoint Online entitlements to the IT Shop on page 90](#)
- [Assigning SharePoint Online user accounts directly to an entitlement on page 92](#)
- [Assigning SharePoint Online entitlements directly to a user account on page 93](#)

Effectiveness of SharePoint Online entitlement assignments

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

It is possible to assign an excluded group 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.

The effectiveness of the assignments is mapped in the `03SUserIn03SGroup` and `03SBaseTreeHasGroup` 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 site collection. 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 employee from obtaining authorizations of groups A and group B at the same time. That means, groups A, B, and C are mutually exclusive. A user, who is a member of group C cannot be a member of group B at the same time. That means, groups B and C are mutually exclusive.

Table 13: Specifying excluded groups (03SGroupExclusion table)

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

Table 14: Effective assignments

Employee	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. If this should not be allowed, define further exclusion for group C.

Table 15: Excluded groups and effective assignments

Employee	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 site collection.

To exclude a group

1. In the Manager, select the **SharePoint Online > 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.

SharePoint Online group inheritance based on categories

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 template contains two tables; the user account table and the group table.

Use the user account table to specify categories for target system dependent user accounts. In the group table, enter your categories for the target system-dependent groups. Each table contains the category positions **position 1** to **position 63**.

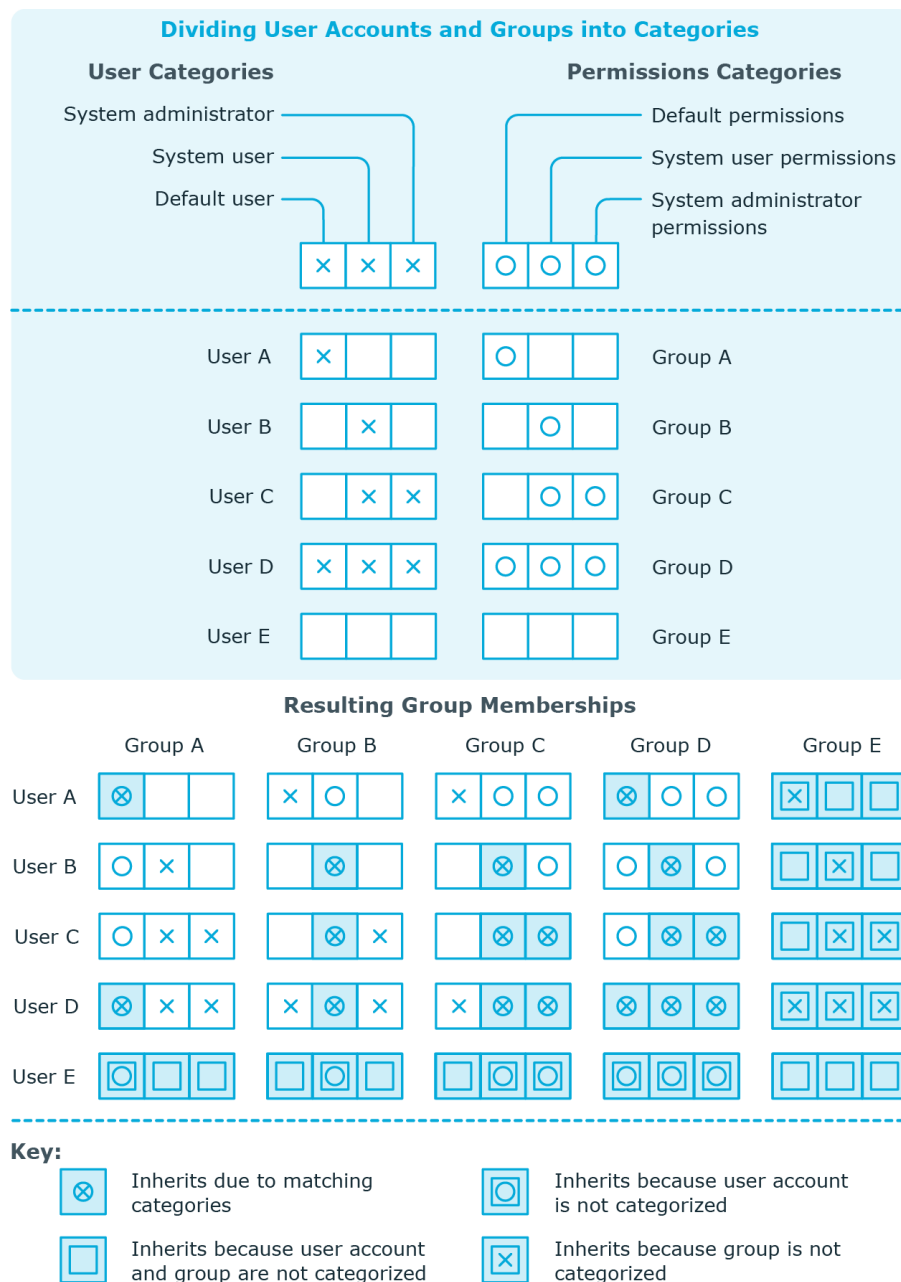
Every user account can be assigned to one or more categories. Each group can also be assigned to one or more categories. The group is inherited by the user account when at least one user account category items matches an assigned group. The group is also inherited by the user account if the group or 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 16: 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 2: Example of inheriting through categories.



To use inheritance through categories

1. In the Manager, define the categories in the site collection.
2. Assign categories to user accounts through their main data.
3. Assign categories to groups through their main data.

Related topics

- [Defining categories for the inheritance of SharePoint Online groups](#) on page 126
- [Main data for group authenticated user accounts](#) on page 111
- [Main data for user authenticated user accounts](#) on page 108
- [SharePoint Online group main data](#) on page 118


Overview of all assignments


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

Examples:

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

To display detailed information about assignments

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

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



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

Figure 3: Toolbar of the Overview of all assignments report.

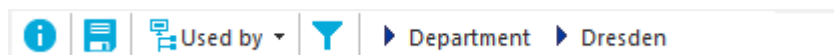






Table 17: Meaning of icons in the report toolbar

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.

Mapping of SharePoint Online objects in One Identity Manager

You use One Identity Manager to manage all objects of the SharePoint Online that are required for the optimization of access control in the target system. These objects are imported into the One Identity Manager database during synchronization. You cannot display or edit their properties in the Manager.

Detailed information about this topic

- [SharePoint Online tenants](#) on page 102
- [SharePoint Online user accounts](#) on page 106
- [SharePoint Online groups](#) on page 116
- [SharePoint Online permission levels](#) on page 121
- [SharePoint Online site collections](#) on page 123
- [SharePoint Online sites](#) on page 127
- [SharePoint Online roles](#) on page 131

SharePoint Online tenants

A SharePoint Online tenant is the base object of a SharePoint Online system. A SharePoint Online tenant must have a direct relationship to an Azure Active Directory tenant. There is only one tenant for each connected SharePoint Online system.

SharePoint Online tenants are used to configure provisioning processes, automatic assignment of employees to user accounts, and to pass down groups to user accounts through categories within a SharePoint Online.

NOTE: SharePoint Online tenants cannot be created in One Identity Manager. The Synchronization Editor sets up SharePoint Online the tenants in the One Identity Manager database.

Detailed information about this topic

- [Displaying and editing SharePoint Online tenant main data](#) on page 103
- [General main data of SharePoint Online tenants](#) on page 103
- [Synchronizing a SharePoint Online environment](#) on page 12
- [Editing system objects](#) on page 154

Displaying and editing SharePoint Online tenant main data

You can edit the main data of each tenant separately. However, you cannot create new tenants.

To edit SharePoint Online tenant main data

1. In the Manager, select the **SharePoint Online > Tenants** category.
2. Select the tenant in the result list.
3. Select the **Change main data** task.
4. Edit the tenant's main data.
5. Save the changes.

Related topics


- [General main data of SharePoint Online tenants](#) on page 103

General main data of SharePoint Online tenants

On the **General** tab, you can see the following main data:

Table 18: General main data of SharePoint Online tenants

Property	Description
Name	Name of the organization that is used for logging on to Office 365.
Azure Active Directory tenant	Unique identifier of the Azure Active Directory tenant.
Target system managers	Application role, in which target system managers are specified for the tenant. Target system managers only edit the objects from tenants to

Property	Description									
	<p>which they are assigned. A different target system manager can be assigned to each tenant.</p> <p>Select the One Identity Manager application role whose members are responsible for administration of this tenant. Use the  button to add a new application role.</p>									
Synchronized by	<p>Type of synchronization through which data is synchronized between the tenant and One Identity Manager. Once objects are available for this tenant in One Identity Manager, the type of synchronization can no longer be changed.</p> <p>If you create a tenant with Synchronization Editor, it uses One Identity Manager.</p> <p>Table 19: Permitted values</p> <table><tr><th>Value</th><th>Synchronization by</th><th>Provisioned by</th></tr><tr><td>One Identity Manager</td><td>SharePoint Online connector</td><td>SharePoint Online connector</td></tr><tr><td>No synchronization</td><td>none</td><td>none</td></tr></table> <p>NOTE: If you select No synchronization, you can define custom processes to exchange data between One Identity Manager and the target system.</p>	Value	Synchronization by	Provisioned by	One Identity Manager	SharePoint Online connector	SharePoint Online connector	No synchronization	none	none
Value	Synchronization by	Provisioned by								
One Identity Manager	SharePoint Online connector	SharePoint Online connector								
No synchronization	none	none								
Default website URL	Root site collection for the tenants.									
Compatibility range	Specifies which compatibility range is available for new website collections.									
Resource quota	Specifies the value of the resource quota for the tenant.									
Resource consumption quota	Specifies the value of the resource quota used by all of the tenant's websites.									
Show "All users" claim	Enables the administrator to hide the All users option in the person selection.									
Show "Everyone" claim	Enables the administrator to hide the Everyone group in the person selection.									
Show "Everyone except external users" claim	Enables the administrator to hide the Everyone except external users group in the person selection.									

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

except
external users"

Related topics

- [Target system managers](#) on page 147

Additional tasks for managing SharePoint Online tenant

After you have entered the main data, you can run the following tasks.

Task	Topic
Overview of SharePoint Online tenants	Overview of SharePoint Online tenants on page 105
Define search criteria for employee assignment	Editing search criteria for automatic employee assignment on page 69
How to Edit a Synchronization Project	Editing the synchronization project for a SharePoint Online tenant on page 105
Synchronize this object	Synchronizing single objects on page 40

Overview of SharePoint Online tenants

To obtain an overview of a tenant

1. In the Manager, select the **SharePoint Online > Tenants** category.
2. Select the tenant in the result list.
3. Select the **SharePoint Online tenant overview** task.

Editing the synchronization project for a SharePoint Online tenant

Synchronization projects in which an Azure Active Directory tenant 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 **SharePoint Online > Tenants** category.
2. Select the tenant 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

SharePoint Online user accounts

SharePoint Online user accounts provide the information necessary for user authentication, such as, the authentication mode and login names. In addition, permissions of users in a site collection are specified in the user accounts.

Each SharePoint Online user account represents an object from an authentication system trusted by the SharePoint Online system. In SharePoint Online, the authentication system is Azure Active Directory. The Azure Active Directory target system must be administrated in One Identity Manager, so that the object used for authentication on the usSharePoint Online account can be saved as the authentication object. This means the SharePoint Online user account permissions are mapped to employees managed in One Identity Manager. One Identity Manager makes it possible for you to obtain an overview of all an employee's SharePoint Online access permissions. SharePoint Online permissions can be attested and checked for compliance. Employees can request or obtain the SharePoint Online permissions they requires through their memberships in hierarchical roles or through the Web Portal when appropriately configured.

By default, the following objects can be assigned as authentication objects in One Identity Manager.

- Azure Active Directory groups of **Security group** type (AADGroup table)
- Azure Active Directory user accounts (AADUser table)

During synchronization, One Identity Manager tries to assign the matching authentication object using the login name.

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

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


| NOTE:

Related topics

- [Application cases for SharePoint Online user account](#) on page 74
- [Managing SharePoint Online user accounts and employees](#) on page 47
- [Account definitions for SharePoint Online user accounts](#) on page 48
- [Creating SharePoint Online user accounts](#) on page 107
- [Editing main data of SharePoint Online user accounts](#) on page 107
- [Deleting and restoring SharePoint Online user accounts](#) on page 115
- [Managing assignments of SharePoint Online groups and roles](#) on page 83

Creating SharePoint Online user accounts

To create a user account

1. In the Manager, select the **SharePoint Online > User accounts (user authenticated)** category.
- OR -
In the Manager, select the **SharePoint Online > User accounts (group authenticated)** 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.

Related topics

- [Main data for user authenticated user accounts](#) on page 108
- [Main data for group authenticated user accounts](#) on page 111
- [Editing main data of SharePoint Online user accounts](#) on page 107

Editing main data of SharePoint Online user accounts

To edit main data of a user account

1. In the Manager, select the **SharePoint Online > User accounts (user authenticated)** category.

- OR -

In the Manager, select the **SharePoint Online > User accounts (group authenticated)** 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.


Related topics

- [Main data for user authenticated user accounts](#) on page 108
- [Main data for group authenticated user accounts](#) on page 111
- [Creating SharePoint Online user accounts](#) on page 107
- [Deleting and restoring SharePoint Online user accounts](#) on page 115

Main data for user authenticated user accounts

Enter the following main data of a user authenticated user account.

Table 20: User authenticated user account main data

Property	Description
Employee	<p>Employee that uses this user account. An employee is already entered if the user account was generated by an account definition. If you create the user account manually, you can select an employee in the menu. If an authentication object is assigned, the connected employee is found through the authentication object by using a template. If there is no authentication object assigned, the employee can be assigned automatically or manually.</p> <p>You can create a new employee for a user account with an identity of type Organizational identity, Personalized administrator identity, Sponsored identity, Shared identity, or Service identity. To do this, click  next to the input field and enter the required employee main data. Which login data is required depends on the selected identity type.</p>
No link to an employee required	<p>Specifies whether the user account is intentionally not assigned an employee. The option is automatically set if a user account is included in the exclusion list for automatic employee 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</p>

Property	Description
	<p>linked with an employee (for example, if several employees 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 employee can be filtered according to various criteria.</p>
Not linked to an employee	<p>Indicates why the No link to an employee 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 employee due to an exclusion criterion. For example, the user account is included in the exclude list for automatic employee assignment (configuration parameter PersonExcludeList).
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 employee 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 employee. 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> <p>NOTE: If employees obtain their SharePoint Online user accounts through account definitions, the employees must have user accounts in the corresponding Azure Active Directory tenant that is specified in the SharePoint Online tenant.</p>
Manage level	<p>Manage level of the user account. Select a manage level from the menu. You can only specify the manage level can if you have also entered an account definition. All manage levels of the selected account definition are available in the menu.</p>
Site collection	<p>Site collection the user account is used in.</p>
Principal type	<p>Type of the principal (user, domain group)</p>
Authentication	<p>Authentication mode used for logging in to SharePoint Online with this</p>

Property	Description
mode	user account. For SharePoint Online, AzureAD is the only authentication mode.
Authentication object	<p>Authentication object referencing the user account.</p> <p>The authentication object is assigned during automatic synchronization. You can assign an authentication object when setting up a new user account in the Manager. The authentication object cannot be changed after saving.</p> <p>The following authentication objects can be assigned to a user-authenticated user account:</p> <ul style="list-style-type: none"> • Azure Active Directory user accounts from the tenant that is assigned to the SharePoint Online tenant <p>NOTE: The SharePoint Online user account is also created if the user account that is used as the authentication object is disabled or locked.</p>
Title	Any display name for the user account. By default, the title is taken from the authentication object's display name. Enter the display name by hand if no authentication object is assigned.
Login name	User account login name. The login name is determined by using a template. Enter the login name by hand if no authentication object is assigned.
Email address	User account email address. The email address is formatted using templates from the authentication object's email address.
Risk index (calculated)	Maximum risk index value of all assigned SharePoint Online roles and 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 menu.
Identity	<p>User account's identity type Permitted values are:</p> <ul style="list-style-type: none"> • Primary identity: Employee's default user account. • Organizational identity: Secondary user account used for different roles in the organization, for example for subcontracts with other functional areas. • Personalized administrator identity: User account with administrative permissions, used by one employee. • Sponsored identity: User account to use for a specific purpose.

Property	Description
	<p>Training, for example.</p> <ul style="list-style-type: none"> • Shared identity: User account with administrative permissions, used by several employees. Assign all employees 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 employee. If the option is set, the user account inherits groups through hierarchical roles, in which the employee is a member, or through IT Shop requests.</p> <ul style="list-style-type: none"> • If you add an employee with a user account to a department, for example, and you have assigned groups to this department, the user account inherits these groups. • If an employee has requested group membership in the IT Shop and the request is granted approval, the employee's user account only inherits the group if the option is set.
Roles can be inherited	Specifies whether the user account can inherit SharePoint Online roles through the linked employee. If the option is set, the user account inherits the roles through hierarchical roles, in which the employee is a member, or through IT Shop requests.
Administrator	Specifies whether the user account is a site collection administrator.
Hidden	Specifies if the user account is displayed in the user interface.


Related topics

- [Account definitions for SharePoint Online user accounts](#) on page 48
- [Defining categories for the inheritance of SharePoint Online groups](#) on page 126
- [Prerequisites for indirect assignment of SharePoint Online entitlements to SharePoint Online user accounts](#) on page 85
- [Assigning employees automatically to SharePoint Online user accounts](#) on page 68
- [Supported user account types](#) on page 75

Main data for group authenticated user accounts

Enter the following main data of a group authenticated user account.

Table 21: Group authenticated user account main data

Property	Description
Employee	<p>Employee that uses this user account. An employee is already entered if the user account was generated by an account definition. If you create the user account manually, you can select an employee in the menu. If an authentication object is assigned, the connected employee is found through the authentication object by using a template. If there is no authentication object assigned, the employee can be assigned automatically or manually.</p> <p>You can create a new employee for a user account with an identity of type Organizational identity, Personalized administrator identity, Sponsored identity, Shared identity, or Service identity. To do this, click  next to the input field and enter the required employee main data. Which login data is required depends on the selected identity type.</p>
No link to an employee required	<p>Specifies whether the user account is intentionally not assigned an employee. You can set the option manually. Enable the option if the user account does not need to be linked with an employee (for example, if several employees 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 employee can be filtered according to various criteria.</p>
Not linked to an employee	Indicates why the No link to an employee required option is enabled for this user account. The user account is not associated with an employee due to an exclusion criterion.
Site collection	Site collection the user account is used in.
Group authenticated	Specifies whether the user account's authentication object is a group.
Authentication mode	Authentication mode used for logging in on the SharePoint Online server with this user account. For SharePoint Online, AzureAD is the only authentication mode.
Authentication object	<p>Authentication object referencing the user account.</p> <p>The authentication object is assigned during automatic synchronization. You can assign an authentication object when setting up a new user account in the Manager. The authentication object cannot be changed after saving.</p> <p>The following authentication objects can be assigned to a group authenticated user account:</p> <ul style="list-style-type: none"> • Azure Active Directory groups with the Security group group type from the tenant that is assigned to the SharePoint Online

Property	Description
	tenant
Title	Any display name for the user account. The title is taken from the authentication object's display name by default. Enter the display name by hand if no authentication object is assigned.
Login name	User account login name. The login name is determined by using a template. Enter the login name by hand if no authentication object is assigned.
Email address	User account email address. The email address is formatted using templates from the authentication object's email address.
Risk index (calculated)	Maximum risk index value of all assigned SharePoint Online roles and 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 menu.
Advice	Text field for additional explanation.
Identity	User account's identity type Permitted values are: <ul style="list-style-type: none"> • Primary identity: Employee's default user account. • Organizational identity: Secondary user account used for different roles in the organization, for example for subcontracts with other functional areas. • Personalized administrator identity: User account with administrative permissions, used by one employee. • Sponsored identity: User account to use for a specific purpose. Training, for example. • Shared identity: User account with administrative permissions, used by several employees. Assign all employees that use this user account. • Service identity: Service account.
Privileged user account.	Specifies whether this is a privileged user account.
Administrator	Specifies whether the user account is a site collection administrator.
Hidden	Specifies whether the user account is displayed in the user interface.

Related topics

- [Defining categories for the inheritance of SharePoint Online groups](#) on page 126
- [Supported user account types](#) on page 75

Additional tasks for managing SharePoint Online user accounts

After you have entered the main data, you can run the following tasks.

Task	Topic
Overview of SharePoint Online user accounts	The SharePoint Online user account overview on page 114
Assigning extended properties	Assigning extended properties to SharePoint Online user accounts on page 115
Assign groups	Assigning SharePoint Online entitlements directly to a user account on page 93
Assign SharePoint Online roles	Assigning SharePoint Online entitlements directly to a user account on page 93
Synchronize object	Synchronizing single objects on page 40

The SharePoint Online user account overview

To obtain an overview of a user account

1. In the Manager, select the **SharePoint Online > User accounts (user authenticated)** category.
- OR -
In the Manager, select the **SharePoint Online > User accounts (group authenticated)** category.
2. Select the user account in the result list.
3. Select the **SharePoint Online user account overview** task.

Assigning extended properties to SharePoint Online 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 Identity Management Base Module Administration Guide*.

To specify extended properties for a user account

1. In the Manager, select the **SharePoint Online > User accounts (user authenticated)** category.

- OR -

In the Manager, select the **SharePoint Online > User accounts (group authenticated)** 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.


Deleting and restoring SharePoint Online user accounts

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


You can delete a user account that was not created using an account definition through the result list or from the menu bar. 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 permanently deleted from the One Identity Manager database and the target system depending on the deferred deletion setting.

For more information about deactivating and deleting employees and user accounts, see the *One Identity Manager Target System Base Module Administration Guide*.

To delete a user account that is not managed using an account definition

1. In the Manager, select the **SharePoint Online > User accounts (user authenticated)** category.
- OR -
In the Manager, select the **SharePoint Online > User accounts (group authenticated)** category.
2. Select the user account in the result list.
3. Click  in the result list.
4. Confirm the security prompt with **Yes**.

To restore a user account

1. In the Manager, select the **SharePoint Online > User accounts (user authenticated)** category.
- OR -
In the Manager, select the **SharePoint Online > User accounts (group authenticated)** category.
2. Select the user account in the result list.
3. Click  in the result list.

Related topics

- [Specifying deferred deletion for SharePoint Online user accounts](#) on page 81

SharePoint Online groups

You can use groups in SharePoint Online to provide users with the same permissions. Groups that you add for site collections are valid for all sites in that site collection. SharePoint Online roles that you define for a site are assigned directly to groups. All user accounts that are members of these groups obtain the permissions defined in the SharePoint Online roles for this site. To add users to groups, you assign the groups directly to users. You can assign groups to departments, cost centers, locations, business roles, system roles, or the IT Shop.

You can edit the following group data in the One Identity Manager:


- Object properties like display name, owner, or visibility of memberships
- Assigned SharePoint Online role and user accounts
- Usage in the IT Shop
- Risk assessment
- Inheritance through roles and inheritance restrictions

Related topics

- [Creating SharePoint Online groups](#) on page 117
- [Editing main data of SharePoint Online groups](#) on page 117
- [SharePoint Online group main data](#) on page 118
- [Deleting SharePoint Online groups](#) on page 120
- [Managing assignments of SharePoint Online groups and roles](#) on page 83

Creating SharePoint Online groups

To create a group

1. In the Manager, select the **SharePoint Online > 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.

Related topics

- [SharePoint Online group main data](#) on page 118
- [Editing main data of SharePoint Online groups](#) on page 117
- [Deleting SharePoint Online groups](#) on page 120

Editing main data of SharePoint Online groups

To edit group main data

1. In the Manager, select the **SharePoint Online > Groups** category.
2. Select the group in the result list.
3. Select the **Change main data** task.
4. Enter the required data on the main data form.
5. Save the changes.

Related topics

- [SharePoint Online group main data](#) on page 118
- [Creating SharePoint Online groups](#) on page 117
- [Deleting SharePoint Online groups](#) on page 120

SharePoint Online group main data

Enter the following main data of a group.

Table 22: SharePoint Online group main data

Property	Description
Title	Display name of the group.
Site collection	Site collection the group is used in.
Owner	Owner of the group. A SharePoint Online user account or a SharePoint Online group can be selected.
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. <i>For more information about risk assessment, see the 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 menu.
Description	Text field for additional explanation.
Hidden	Specifies whether the group is shown in the user interface.
Memberships only visible to members	Specifies whether only group members can see the list of members.
Group members can edit memberships	Specifies whether all group members can edit the group memberships.
Request for membership permitted	Specifies whether SharePoint Online users can request or end membership in these groups themselves.
Automatic membership on request	Specifies whether SharePoint Online users automatically become members in the group once they request membership. The same applies when user end their membership.
Email address membership requested	Email address that the group membership request or closure is sent to.
IT Shop	Specifies whether the group can be requested through the IT Shop. If

Property	Description
	this option is set, the group can be requested by the employees through the Web Portal and distributed with a defined approval process. The group can still be assigned directly to hierarchical roles.
Only for use in IT Shop	Specifies whether the group can only be requested through the IT Shop. If this option is set, the group can be requested by the employees through the Web Portal and distributed with a defined approval process. Direct assignment of the group to hierarchical roles or user accounts is not permitted.

Detailed information about this topic

- [SharePoint Online group inheritance based on categories](#) on page 97
- [Adding SharePoint Online entitlements to the IT Shop](#) on page 90

Additional tasks for managing SharePoint Online groups

After you have entered the main data, you can run the following tasks.

Task	Topic
Overview of SharePoint Online Groups	Overview of SharePoint Online groups on page 120
Assign user accounts	Assigning SharePoint Online user accounts directly to an entitlement on page 92
Assign SharePoint Online roles	Assigning SharePoint Online roles to SharePoint Online groups on page 93
Assign system roles	Adding SharePoint Online entitlements to system roles on page 89
Assign business roles	Assigning SharePoint Online entitlements to business roles on page 88
Assign organizations	Assigning SharePoint Online entitlements to departments, cost centers, and locations on page 86
Exclude groups	Effectiveness of SharePoint Online entitlement assignments on page 95
Add to IT Shop	Adding SharePoint Online entitlements to the IT Shop on page 90
Assigning extended	Assigning extended properties to SharePoint Online groups on

Task	Topic
properties	page 120
Synchronize object	Synchronizing single objects on page 40

Overview of SharePoint Online groups

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 **SharePoint Online > Groups** category.
2. Select the group in the result list.
3. Select the **SharePoint Online group overview** task.

Assigning extended properties to SharePoint Online 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 setting up extended properties, see the *One Identity Manager Identity Management Base Module Administration Guide*.

To specify extended properties for a group

1. In the Manager, select the **SharePoint Online > Groups** category.
2. Select the group 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.

Deleting SharePoint Online groups

Groups are deleted permanently from the One Identity Manager database and from SharePoint Online.

To delete a group

1. In the Manager, select the **SharePoint Online > Groups** category.
2. Select the group in the result list.
3. Click  in the result list.
4. Confirm the security prompt with **Yes**.

SharePoint Online permission levels


To assign permissions to the objects of a site collection and their child sites, permission levels are defined in SharePoint Online. These permission levels group together different permissions that are permanently defined in SharePoint Online.

Related topics

- [Creating SharePoint Online permission levels](#) on page 121
- [Editing main data of SharePoint Online permission levels](#) on page 122
- [Entering main data for SharePoint Online permission levels](#) on page 122
- [Deleting and restoring SharePoint Online permission levels](#) on page 123
- [Synchronizing single objects](#) on page 40

Creating SharePoint Online permission levels

To create a permission level

1. In the Manager, select the **SharePoint Online > Permission levels** category.
2. Click  in the result list.
3. On the main data form, edit the main data of the permission level.
4. Save the changes.

Related topics

- [Entering main data for SharePoint Online permission levels](#) on page 122
- [Editing main data of SharePoint Online permission levels](#) on page 122
- [Deleting and restoring SharePoint Online permission levels](#) on page 123

Editing main data of SharePoint Online permission levels

To edit main data of a permission level

1. In the Manager, select the **SharePoint Online > Permission levels** category.
2. Select the permission level in the result list and run the **Change main data** task.
3. Edit the main data of the permission level.
4. Save the changes.

Related topics

- [Entering main data for SharePoint Online permission levels](#) on page 122
- [Creating SharePoint Online permission levels](#) on page 121
- [Deleting and restoring SharePoint Online permission levels](#) on page 123

Entering main data for SharePoint Online permission levels

Enter the following properties for a permission level on the main data form:

Table 23: General main data of a permission level

Property	Description
Permission level	Name of the permission level.
Site collection	Unique identifier for the site collection in which the permission level is created.
Permissions	SharePoint Online permissions that are assigned to the permission level.
Description	Text field for additional explanation.
Type	Type of permission level.
Hidden	Specifies whether a SharePoint Online role with the permission level can be assigned to user accounts or groups.

Related topics

- [SharePoint Online permission levels](#) on page 121

Overview of SharePoint Online permission levels


To obtain an overview of a permission level

1. In the Manager, select the **SharePoint Online > Permission levels** category.
2. Select the permission level in the result list.
3. Select the **SharePoint Online permission level overview** task.

Deleting and restoring SharePoint Online permission levels


You cannot delete SharePoint Online roles in the Manager. They are deleted by the DBQueue Processor when the associated permission level is deleted.

To delete a permission level

1. In the Manager, select the **SharePoint Online > Permission levels** category.
2. Select the permission level in the result list.
3. Click  to delete the permission level.
4. Confirm the security prompt with **Yes**.

If deferred deletion is configured, the permission level is marked for deletion and finally deleted after the deferred deletion period has expired. During this period, the permission level can be restored. Permission levels with deferred deletion of 0 days are deleted immediately.

To restore a permission level

1. In the Manager, select the **SharePoint Online > Permission levels** category.
2. Select the permission level marked for deletion in the result list.
3. Click  in the result list.

SharePoint Online site collections

Site collections and sites are mapped with their access rights to One Identity Manager. You cannot edit their properties in One Identity Manager. You can edit access rights managed within a site collection in One Identity Manager. To do this, SharePoint Online roles, groups, and user accounts are loaded into the One Identity Manager database.

A site collection groups child sites together. User account and their access permissions are managed on the sites. To automatically assign used accounts and employees, assign an account definition to the site collection.

Related topics

- [Editing main data of SharePoint Online site collections](#) on page 124
- [Synchronizing single objects](#) on page 40

Editing main data of SharePoint Online site collections

To edit site collection main data

1. In the Manager, select the **SharePoint Online > Site collections** category.
2. Select the site collection in the result list. Select the **Change main data** task.
3. Enter the required data on the main data form.
4. Save the changes.

Related topics

- [General main data of a SharePoint Online site collection](#) on page 124
- [Address data for a SharePoint Online site collection](#) on page 126
- [Defining categories for the inheritance of SharePoint Online groups](#) on page 126

General main data of a SharePoint Online site collection

The following properties are displayed for site collections.

| **NOTE:** Only the account definition of the site collection can be edited.

Table 24: General main data of a site collection

Property	Description
Title	Title of the site collection.
Account definition	Initial account definition for creating user accounts. This account definition is used if automatic assignment of employees to user accounts is used for this site collection and if user accounts are to be created that are already managed (Linked configured). The account

Property	Description
	definition's default manage level is applied. User accounts are only linked to the employee (Linked) if no account definition is given. This is the case on initial synchronization, for example.
Tenant	Unique identifier of the Azure Active Directory tenant.
Root site	Link to the site collection root site. Links to a site that is set as root site .
Administrator	Administrator user account for the site collection.
Language	Name of the language, for example ES-es
Time zones	Unique identifier for the time zone.
Geolocation	Details of the geographical location.
Main version	The main version of this site collection for the purpose of compatibility checks at main version level.
Status information	Status of the site collection.
Site template	Unique identifier of SharePoint Online site template.
Used storage	Information about the storage taken up by the site collection on the server.
Used storage (%)	Percentage of storage space used.
Max. disk space	Maximum amount of disk space that this site collection can use in bytes.
Warn as from	Threshold in bytes above which a warning is sent to the site collection administrator before the maximum available storage space is exceeded.
Max usage quota	Maximum number of time users access can access the site collection per day.
Warn as from	Threshold in bytes above which a warning is sent to the site collection administrator before the maximum usage quota is exceeded.
Last content-relevant change	Time of last content-relevant change that was made to an object in this site collection.

Related topics

- [Account definitions for SharePoint Online user accounts](#) on page 48

Address data for a SharePoint Online site collection

The following address data is mapped on the **Addresses** tab.

Table 25: Address data for a site collection


Properties	Description
URL	Complete URL of the site collection.
URL relative to server	URL of the site collection relative to the server URL.

If the server declared in the URL can be resolved by DNS, you can open the site in the default browser.

Defining categories for the inheritance of SharePoint Online groups

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 template contains two tables; the user account table and the group table. Use the user account table to specify categories for target system dependent user accounts. In the group table, enter your categories for the target system-dependent groups. Each table contains the category positions **position 1** to **position 63**.

To define a category

1. In the Manager, select the site collection in the **SharePoint Online > Site collections** category.
2. Select the **Change main data** task.
3. Switch to the **Mapping rule category** tab.
4. Extend the relevant roots of the user account table or group table.
5. To enable the category, double-click .
6. Enter a category name of your choice for user accounts and groups in the login language that you use.
7. Save the changes.

Related topics

- [SharePoint Online group inheritance based on categories](#) on page 97

Additional tasks for managing site collections

After you have entered the main data, you can run the following tasks.

Task	Theme
Overview of the SharePoint Online site collection	Overview of SharePoint Online site collections on page 127
Define Search Criteria for Employee Assignment	Editing search criteria for automatic employee assignment on page 69
Synchronize object	Synchronizing single objects on page 40

Overview of SharePoint Online site collections

Authorized user accounts and groups are displayed on the site collection overview as well as the tenant and the root site linked to the site collection. The overview form also shows the quota template, and the site collection administrators assigned to the site collection.

To view an overview of a site collection:

1. In the Manager, select the **SharePoint Online > Site collections** category.
2. Select the user account in the result list.
3. Select the **SharePoint Online site collection overview** task.

SharePoint Online sites

SharePoint Online sites are organized into site collections. A site collection manages access rights and characterization templates for all sites in the site collection. You can structure sites hierarchically. There is always a site labeled as **root site** in every site collection. The other sites in the site collection are sorted below the root site.

Related topics

- [Editing main data of SharePoint Online sites](#) on page 128
- [Synchronizing single objects](#) on page 40

Editing main data of SharePoint Online sites

To edit a site's main data

1. In the Manager, select the **SharePoint Online > Sites** category.
2. Select the site in the result list.
3. Select the **Change main data** task.
4. Enter the required data on the main data form.
5. Save the changes.

Related topics

- [General main data of SharePoint Online sites](#) on page 128
- [Address data of SharePoint Online sites](#) on page 129
- [Design information of SharePoint Online sites](#) on page 130

General main data of SharePoint Online sites

The following main data is displayed for sites.

Table 26: General main data of a site

Property	Description
Title	Display name of the site.
Created	Specifies when the site was created.
User interface version	Version of the user interface (UI) of the website.
Parent site	Unique ID for the parent site.
Site collection	Unique identifier for the site collection to which the site belongs.
SharePoint Online site collection	The parent site of the selected website.
Language	Name of the language, for example ES-es
Time zones	Unique identifier for the time zone.
Unique role assignments	Specifies whether user accounts and groups can be given direct permission for the website. If this option is not set, the role assignments are

Property	Description
	inherited from the parent site. No other user accounts or groups have permissions for this site.
Member group	Determines the users who have been assigned permissions for contributions to the website.
Owner group	The owner groups belonging to the site.
Visitor group	The visitor group belonging to the site.
Author	Link to user account that created the site.
Request access email	Email address to which the access requests are sent.
Description	Text field for additional explanation.
RSS feeds	Specifies whether RSS feeds are permitted on the site.
Contains confidential info	Specifies whether the site contains confidential information.
Multilingual	Information about whether a multilingual user interface is activated for the site.

Related topics

- [Managing assignments of SharePoint Online groups and roles](#) on page 83

Address data of SharePoint Online sites

The following address data is mapped on the **Addresses** tab.

Table 27: Address data for a site

Properties	Description
URL relative to server	URL of the site relative to the server URL.
URL	Absolute site URL.
System master page URL	System master page URL, relative to the web application URL.
Site master page URL	Site master page URL, relative to the web application URL.

If the server declared in the URL can be resolved by DNS, you can open the site in the default browser.

Related topics

- [Overview of SharePoint Online sites](#) on page 130

Design information of SharePoint Online sites

The following design information is displayed on the **Design** tab.

Table 28: Site design properties

Property	Description
Site template	Unique identifier for the site template to be used when the site is created. A value is only shown if you add the site through One Identity Manager.
URL for logo	URL for the site logo relative to the web application URL.
Logo icon description	Description of the site's logo.

Overview of SharePoint Online sites

You can view all the roles and permission levels that are valid for this site on the overview form. Use **Open URL** to open the site in a standard web browser. Prerequisite for this is that the server in the URL can be resolved per DNS.

To obtain an overview of an site

1. In the Manager, select the **SharePoint Online > Sites** category.
2. Select the site in the result list.
3. Select the **SharePoint Online site overview** task.

If the server declared in the URL can be resolved by DNS, you can open the site in the default browser.

To open the site

1. In the Manager, select the **SharePoint Online > Site collections** category.
2. Select the site in the result list.
3. Select **Open URL**.

Related topics

- [Address data of SharePoint Online sites](#) on page 129

Inheritance of SharePoint Online permissions by SharePoint Online sites

SharePoint Online roles are defined at site level. There are always roles defined for the root site of a site collection. Child sites can inherit these role definitions. In the same way, roles on the root site of a site collection are also assigned to groups or user accounts. These assignments can inherit child sites.

The **Unique role assignment** option specifies whether user accounts and groups are explicitly authorized for a site or whether the role assignments are inherited by the parent website.

Child sites can inherit permissions from the sites that the user accounts have on those sites. Every root site of a site collection or every site that has a child site.

This permits the following scenarios:

1. The child site inherits the role assignments.

The permission levels and role definitions of the (bequeathing) parent site apply. User and groups cannot be explicitly authorized for the site. Only user accounts that have permissions for the (bequeathing) parent site have access to the site.

2. The child site does not inherit role assignments.

In this case unique permission levels can be created in the same way as the root site of a site collection. The SharePoint Online roles based on the definitions are assigned to user accounts and groups.

Related topics

- [General main data of SharePoint Online sites](#) on page 128
- [Managing assignments of SharePoint Online groups and roles](#) on page 83

SharePoint Online roles

Permission levels with a unique reference to a site are mapped in the One Identity Manager database as SharePoint Online roles. You can assign SharePoint Online roles through groups, or directly to user accounts. SharePoint Online users obtain their permissions for site objects in this way.

NOTE: SharePoint Online roles and role assignments are handled as dependent objects by synchronization. That means, SharePoint Online roles must also be synchronized in order to synchronize role assignments.

Related topics

- [SharePoint Online permission levels](#) on page 121

Editing main data of SharePoint Online roles

To edit SharePoint Online role main data

1. In the Manager, select the category **SharePoint Online > Roles**.
2. Select the SharePoint Online role in the result list and run the **Change main data** task.
3. Edit the main data of the role.
4. Save the changes.

NOTE: If the SharePoint Online role references a permission level for which the **Hidden** option is set, the **IT Shop** options and **Only use in IT Shop** cannot be set. You cannot assign these SharePoint Online roles to user accounts or groups.

Related topics

- [General main data of SharePoint Online roles](#) on page 132
- [Entering main data for SharePoint Online permission levels](#) on page 122

General main data of SharePoint Online roles

The following properties are displayed for SharePoint Online roles.

Table 29: General main data of a SharePoint Online role

Property	Description
Display name	SharePoint Online role display name.
Permission level	Unique identifier for the permission level on which the SharePoint Online role is based.
Site	Unique identifier for the site that inherits its permissions from the SharePoint Online role.
Service item	Service item data for requesting the role through the IT Shop.
Category	Categories for role inheritance. User accounts can inherit roles selectively. To do this, roles, and user accounts are divided into categories. Select one or more categories from the menu.
Description	Text field for additional explanation.
IT Shop	Specifies whether the SharePoint Online role can be requested through the

Property	Description
	IT Shop. This SharePoint Online role can be requested by staff through the Web Portal and granted through a defined approval procedure. The SharePoint Online role can still be assigned directly to employees and hierarchical roles.
Only for use in IT Shop	Specifies whether the SharePoint Online role can only be requested through the IT Shop. This SharePoint Online role can be requested by staff through the Web Portal and granted through a defined approval procedure. The SharePoint Online role may not be assigned directly to hierarchical roles.

NOTE: If the SharePoint Online role references a permission level for which the **Hidden** option is set, the **IT Shop** options and **Only use in IT Shop** cannot be set. You cannot assign these SharePoint Online roles to user accounts or groups.

Detailed information about this topic

- [Entering main data for SharePoint Online permission levels](#) on page 122

Additional tasks for managing SharePoint Online roles

After you have entered the main data, you can run the following tasks.

Task	Topic
Overview of SharePoint Online Groups	Overview of SharePoint Online roles on page 134
Assign user accounts	Assigning SharePoint Online user accounts directly to an entitlement on page 92
Assign groups	Assigning SharePoint Online groups to SharePoint Online roles on page 94
Assign system roles	Adding SharePoint Online entitlements to system roles on page 89
Assign business roles	Assigning SharePoint Online entitlements to business roles on page 88
Assign organizations	Assigning SharePoint Online entitlements to departments, cost centers, and locations on page 86
Exclude SharePoint Online roles	Effectiveness of SharePoint Online roles on page 134

Task	Topic
Assigning extended properties	Assigning extended properties to SharePoint Online groups on page 120
Synchronize object	Synchronizing single objects on page 40

Overview of SharePoint Online roles

To obtain an overview of a role

1. In the Manager, select the category **SharePoint Online > Roles**.
2. Select the role in the result list.
3. Select the **SharePoint Online role overview** task.

Effectiveness of SharePoint Online roles

The behavior described under [Effectiveness of SharePoint Online entitlement assignments](#) on page 95 can also be used for SharePoint Online roles.

The effect of the assignments is mapped in the `03SUserHas03SRLAssign` and `BaseTreeHas03SRLAssign` tables through the `XIsInEffect` column.

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 not 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 SharePoint Online roles belong to the same site collection.

To exclude SharePoint Online roles

1. In the Manager, select the category **SharePoint Online > Roles**.
 2. Select the role in the result list.
 3. Select the **Exclude SharePoint Online roles** task.
 4. In the **Add assignments** pane, assign the roles that are mutually exclusive to the selected role.
- OR -

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

5. Save the changes.

Setting up SharePoint Online site collections and sites

Site collections and sites are loaded into the One Identity Manager database through synchronization in the default installation of One Identity Manager. You can add new site collections and site in the One Identity Manager and publish them in the SharePoint Online target system. Predefined scripts and processes are provided for this purpose. You can use these as templates to make the site collections and sites requestable through the IT Shop.

NOTE: Customize these scripts and processes as required.

Table 30: Example scripts and processes

Script/Process	Description
Script 03S_ Create03SSite	<p>Creates a new site collection and the associate root site in the One Identity Manager database. Creates a user account that is entered as site collection administrator or root site author.</p> <p>NOTE: Enter a valid SharePoint Online timezone value for the UID_DialogTimeZone parameter. If the timezone is invalid, UTC is used. You will find a list of permitted timezones in the script commentary.</p>
Script 03S_ Create03SWeb	Creates a new site within a site collection in the One Identity Manager database.
Process 03S_ 03SWeb_ (De-)Provision	<p>Creates a new site within a site collection. The process is triggered by the PROVISION event if the site in the One Identity Manager database is not labeled as the root site.</p> <p>Deletes a site. The process is triggered by the DEPROVISION event if the site in the One Identity Manager database is not labeled as the root site.</p>
Process 03S_ 03SSite_ (De-)Provision	<p>Creates a new site collection in a web application and the associated root site. The process is triggered by the PROVISION event.</p> <p>Deletes a site collection in a web application and the associated root site. The process is triggered by the DEPROVISION event.</p>

The following step are required in additions:

- Define a requestable product through which the site collection/site is requested from the IT Shop.
- Define product properties that are mapped to the script parameter (for example, URL or site template). You must include these product properties when the site collection/site is requested.
- Create a process for the PersonWantsOrg table that is started when the request is approved (event OrderGranted). This process call the matching script and sets the parameter values with the defined product properties you have defined. Then the site collection/site is added to the One Identity Manager database.
- To add a new site collection to an existing synchronization project, extend the scope of the target system connection in the synchronization project.

Extending the scope

The scope should only include site collections in which the applicable synchronization user is entered in the SharePoint Online administration interface as the site collection administrator. There is no default user in SharePoint Online.

If the scope is not correctly set up, site collections cannot be loaded and synchronization is stopped.

To edit site collections in the scope of a SharePoint Online synchronization project

1. Open the Synchronization Editor.
2. Select the **Configuration > Target system** category.
3. Select the **Scope** view.
4. Click **Edit scope**. A list of site collections appears on the right-hand side.
5. Activate the site collections to synchronize.

In the list, select only the site collections for which the synchronization user is the same as the administrator in SharePoint Online.

6. Click **Commit to database** to save the changes.

For more information about the IT Shop, see the *One Identity Manager IT Shop Administration Guide*. For more information about defining processes, see the *One Identity Manager Configuration Guide*.

Related topics

- [SharePoint Online synchronization features](#) on page 27

Reports about SharePoint Online objects

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 SharePoint Online.

NOTE: Other sections may be available depending on the which modules are installed.

Table 31: 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.
Overview of all assignments	group Role	This report finds all roles containing employees who have the selected system entitlement.
Show overview	group Role	This report shows an overview of the system entitlement and its assignments.
Show overview including origin	group Role	This report shows an overview of the system entitlement and origin of the assigned user accounts.
Show overview including history	group Role	This report shows an overview of the system entitlement and 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)	Site collection Site	This report returns all the 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.
Show system	Site collection	This report shows the system entitlements with the

Report	Published for	Description
entitlements overview (incl. history)	tion Site	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	Site collec- tion Tenant	This report finds all roles containing employees with at least one user account in the selected target system.

Handling of SharePoint Online objects in the Web Portal

One Identity Manager enables its users to perform various tasks simply using a Web Portal.

- Managing user accounts and employees

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 person, such as a manager.

- Managing entitlement assignments

When an entitlement is assigned to an IT Shop shelf, the entitlement can be requested by the customer in the Web Portal. The request undergoes a defined approval process. The entitlement is not assigned until it has been approved by an authorized person.

In the Web Portal, managers and administrators of organizations can assign entitlements to the departments, cost centers, or locations for which they are responsible. The entitlements are inherited by all persons who are members of these departments, cost centers, or locations.

If the Business Roles Module is available, managers and administrators of business roles in the Web Portal can assign entitlements to the business roles for which they are responsible. The entitlements are inherited by all persons who are members of these business roles.

If the System Roles Module is available, supervisors of system roles in the Web Portal can assign entitlements to the system roles. The entitlements are inherited by all persons to whom these system roles are assigned.

- Attestation

To enable this, attestation policies are configured in the Manager. The attestors use the Web Portal to approve attestation cases.

- Governance administration

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 and resolve 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 entitlements 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 employees, user accounts, and their entitlements and risks.

For more information about the named topics, refer to the following guides:

- *One Identity Manager Web Designer 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 SharePoint Online environment

To manage SharePoint Online in One Identity Manager, the following basic data is relevant.

- Authentication modes

Authentication mode used for logging in on the SharePoint Online server with this user account. For SharePoint Online, **AzureAD** is the only authentication mode.

For more information, see [SharePoint Online authentication modes](#) on page 142.

- 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 41.

- Account definitions

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

For more information, see [Account definitions for SharePoint Online user accounts](#) on page 48.

- Server

In order to handle target system specific processes in One Identity Manager, the synchronization server and its server functionality must be declared.

For more information, see [Job server for SharePoint Online-specific process handling](#) on page 143.

- Target system managers

A default application role exists for the target system manager in One Identity Manager. Assign employees to this application role who have permission to edit all tenants in One Identity Manager.

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

For more information, see [Target system managers](#) on page 147.

SharePoint Online authentication modes

To display main data for an authentication mode

1. In the Manager, select the **SharePoint Online > Basic configuration data > Authentication modes** category.
2. Select the authentication mode in the result list.
3. Select the **Change main data** task.

The following main data is supplied for the authentication mode.

Table 32: Authentication mode properties

Property	Description
System ID	Name of the authentication mode. For SharePoint Online, AzureAD is the only authentication mode.
User prefix	Prefix for formatting a login name for new user accounts. The associated authentication object is not a group. This means, the user account's Group option is not set.
Group prefix	Prefix for formatting a login name for new user accounts. The associated authentication object is a group. This means, the user account's Group option is set.
Column for login name	Column in the Person table used to format the login name for new user accounts. This information is required if employees are linked to user accounts through automatic employee assignment.

SharePoint Online site templates

To be able to add site and site collections in One Identity Manager, web templates are loaded into One Identity Manager.

To obtain an overview of a site template

1. In the Manager, select the **SharePoint Online > Basic configuration data > Site templates** category.

2. In the result list, select the web template.
3. Select the **SharePoint Online web template overview** task.

Related topics

- [Setting up SharePoint Online site collections and sites](#) on page 135

Job server for SharePoint Online-specific process handling

In order to handle target system 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 **SharePoint Online > Basic configuration data > Server** category and edit the Job server's 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.

To edit a Job server and its functions

1. In the Manager, select the **SharePoint Online > 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 144
- [Specifying server functions](#) on page 146

Related topics

- [System requirements for the SharePoint Online synchronization server](#) on page 17

General main data of Job servers

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

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

Table 33: Job server properties

Property	Meaning
Server	Job server name.
Full server name	Full server name in accordance with DNS syntax. Syntax: <Name of server>.<Fully qualified domain name>
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 (target server)	Permitted copying methods that can be used when this server is the destination of a copy action.
Coding	Character set coding that is used to write files to the server.
Parent Job server	Name of the parent Job server.
Executing server	Name of the implementing server. The name of the server that exists physically and where the processes are handled. This input is evaluated when the One Identity Manager Service is automatically updated. If the server is handling several queues, the process steps are not supplied until all the queues that are being processed on the same server have completed their automatic update.
Queue	Name of the queue to handle the process steps. The process steps are requested by the Job queue using this queue identifier. The queue identifier is entered in the One Identity Manager Service configuration file.
Server operating system	Operating system of the server. This input is required to resolve the path name for replicating software profiles. The values Win32 , Windows , Linux , and Unix are permitted. If no value is specified, Win32 is used.

Property	Meaning
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	<p>Specifies whether a One Identity Manager Service is installed on this server. This option is enabled by the QBM_PJobQueueLoad procedure the moment the queue is called for the first time.</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	Specifies whether a software update is currently running.
Server function	Server functionality in One Identity Manager. One Identity Manager processes are handled with respect to the server function.

Related topics

- [Specifying server functions](#) on page 146

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 34: Permitted server functions

Server function	Remark
Azure Active Directory connector (via Microsoft Graph)	Server on which the Azure Active Directory connector is installed. This server synchronizes the Azure Active Directory target system.
CSV connector	Server on which the CSV connector for synchronization is installed.
Domain controller	The Active Directory domain controller. Servers that are not labeled as domain controllers are considered to be member servers.
Printer server	Server that acts as a print server.
Generic server	Server for generic synchronization with a custom target system.
Home server	Server for adding home directories for user accounts.
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	This server can process CSV files using the ScriptComponent process component.
Generic database connector	This server can connect to an ADO.Net database.
One Identity Manager database connector	Server on which the One Identity Manager connector is installed. This server synchronizes the One Identity Manager target system.

Server function	Remark
One Identity Manager Service installed	Server on which a One Identity Manager Service is installed.
Primary domain controller	Primary domain controller.
Profile server	Server for setting up profile directories for user accounts.
SAM synchronization Server	Server for synchronizing an SMB-based target system.
SharePoint Online connector	Server on which the SharePoint Online connector is installed. This server synchronizes the SharePoint Online target system.
SMTP host	Server from which One Identity Manager Service sends email notifications. Prerequisite for sending mails using One Identity Manager Service is SMTP host configuration.
Default report server	Server on which reports are generated.
Windows PowerShell connector	The server can run Windows PowerShell version 3.0 or later.
SCIM connector	This server can connect to a cloud application.

Related topics

- [General main data of Job servers](#) on page 144

Target system managers

A default application role exists for the target system manager in One Identity Manager. Assign employees to this application role who have permission to edit all tenants in One Identity Manager.

Define additional application roles if you want to limit the permissions for target system managers to individual tenants. 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 employees to be target system administrators.
2. These target system administrators add employees to the default application role for target system managers.

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

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

Table 35: Default application roles for target system managers

User	Tasks
Target system managers	<p>Target system managers must be assigned to the Target systems SharePoint Online 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 to add to the IT Shop.• Can add employees who have another identity than the Primary identity.• 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 employees within their area of responsibility as target system managers and create child application roles if required.

To initially specify employees to be target system administrators

1. Log in to 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 employees** task.
4. Assign the employee you want and save the changes.

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

1. Log in to the Manager as a target system administrator (**Target systems | Administrators** application role).
2. Select the **One Identity Manager Administration > Target systems > SharePoint Online** category.
3. Select the **Assign employees** task.
4. Assign the employees you want and save the changes.

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

1. Log in to the Manager as a target system manager.
2. Select the application role in the **SharePoint Online > Basic configuration data > Target system managers** category.
3. Select the **Assign employees** task.
4. Assign the employees you want and save the changes.

To specify target system managers for individual tenants

1. Log in to the Manager as a target system manager.
2. Select the **SharePoint Online > Tenants** category.
3. Select the tenant 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** menu.

- OR -

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

- a. Enter the application role name and assign the **Target systems | SharePoint Online** parent application role.
 - b. Click **OK** to add the new application role.
6. Save the changes.
 7. Assign employees to this application role who are permitted to edit the tenant in One Identity Manager.

Related topics

- [One Identity Manager users for managing SharePoint Online](#) on page 9

Troubleshooting a SharePoint Online connection

Error synchronizing after renaming a SharePoint Online site collection

After renaming a site collection in SharePoint Online that has already been read into the One Identity Manager database, synchronization fails with an error message.

Probable reason

In the synchronization project's scope, the site collection's old name is still referenced.

Solution

- Correct the synchronization project's scope and select the site collection whose URL contains the new name.

Related topics

- [SharePoint Online synchronization features](#) on page 27

Configuration parameters for managing SharePoint Online

The following configuration parameters are additionally available in One Identity Manager after the module has been installed.

Table 36: Configuration parameters

Configuration parameter	Meaning
TargetSystem SharePointOnline	Preprocessor relevant configuration parameter for controlling database model components for SharePoint Online target system administration. If the parameter is set, the target system components are available. Changes to this parameter require the database to be recompiled. If you disable the configuration parameter at a later date, model components and scripts that are not 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> .
TargetSystem SharePointOnline Accounts	Parameter for configuring SharePoint Online user account data.
TargetSystem SharePointOnline 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 Employee - new user account with default properties created mail template is used.
TargetSystem SharePointOnline DefaultAddress	Default email address of the recipient for notifications about actions in the target system.
TargetSystem SharePointOnline	Maximum runtime of a synchronization in minutes. No recalculation of group memberships by the DBQueue

Configuration parameter	Meaning
MaxFullsyncDuration	Processor can take place during this time. If the maximum runtime is exceeded, group membership are recalculated.
TargetSystem SharePointOnline PersonAutoDefault	Mode for automatic employee assignment for user accounts added to the database outside synchronization.
TargetSystem SharePointOnline PersonAutoFullsync	Mode for automatic employee assignment for user accounts that are added to or updated in the database by synchronization.

Default project template for SharePoint Online

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.

NOTE: There is only one synchronization template in the One Identity Manager for the target system SharePoint Online.

To synchronize SharePoint Online user accounts and permissions, you use the **SharePoint Online synchronization** project template. The project template uses mappings for the following schema types.

Table 37: Mapping SharePoint Online schema types to tables in the One Identity Manager schema

Schema type in SharePoint Online	Table in the One Identity Manager Schema
Tenant	O3STenant
Site	O3SSite
Group	O3SGroup
Web	O3SWeb
RoleAssignment	O3SRLAsgn
RoleDefinition	O3SRole
User	O3SUser
WebTemplate	O3SWebTemplate

Editing system objects

The following table describes permitted editing methods for SharePoint Online schema types and names restrictions on editing system objects in the Manager.

Table 38: Methods available for editing objects types

Type	Read	Add	Delete	Change
Tenant	Yes	No	No	No
Site collection	Yes	(Yes)	(Yes)	No
User account	Yes	Yes	Yes	Yes
Group	Yes	Yes	Yes	Yes
Site	Yes	(Yes)	(Yes)	Yes
Role	Yes	Yes	Yes	Yes
Role assignment	Yes	No	No	Yes

(Yes): It is technically possible to create and delete site collections and sites. However, the scripts and processes required for this must be customized. For more information, see [Setting up SharePoint Online site collections and sites](#) on page 135.

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 48
 - add to IT Shop 62
 - assign automatically 61
 - assign to all employees 61
 - assign to business role 60
 - assign to cost center 60
 - assign to customers 65
 - assign to department 60
 - assign to employee 59, 62
 - assign to location 60
 - assign to system roles 62
 - assign to user account 72
- create 49
- delete 65
- edit 49
- editing manage level 52
- IT operating data 55, 57
- manage level 53

architecture overview 8

authentication

- authentication mode 142

authentication mode 142

authentication object 74

authorization assignment

- direct 92-93

B

- base object 30, 34

C

- calculation schedule 37
 - deactivate 39
- category 126
- configuration parameter 11, 151
- convert connection parameter 30
- customer
 - account definition (initial) 65

D

- default user accounts 76
- direction of synchronization
 - direction target system 21, 23, 29
 - in the Manager 21, 23

E

- employee
 - assign user account 73
 - group identity 79
 - main identity 78
 - personalized admin identity 78
 - primary identity 79
- employee assignment
 - manual 71
 - remove 71
 - search criteria 69
- exclusion definition 95, 134
- extended property
 - assign group 120

user account 115

G

group

- about IT Shop requests 118
- add to IT Shop 90
- assign business role 88
- assign category 118
- assign cost center 86
- assign department 86
- assign extended properties 120
- assign location 86
- assign SharePoint Online role 93
- assign system role 89
- assign user account 84, 92
- category 97
- create 117
- delete 120
- effective 95
- exclusion 95
- inheriting through categories 126
- inheriting through roles 84
- inheriting through system roles 89
- overview form 120
- overview of all assignments 100
- owner 118
- risk index 118
- role assignment 131
- set up 116
- work 117

group identity 77, 79

group prefix 142

I

identity 75

IT operating data

- change 58

IT Shop shelf

- assign account definition 62
- assign group 90
- assign role 90

J

Job server

- edit 17
- load balancing 36
- properties 144

L

load balancing 36

log file 44

M

manage level

- edit 52

membership

- modify provisioning 33

N

NLog 44

O

object

- delete immediately 41

- outstanding 41
- publish 41
- offline mode 45
- One Identity Manager
 - register as application 15
- outstanding object 41

P

- permission
 - add to IT Shop 90
 - assign business role 88
 - assign organizations 86
 - assign system role 89
 - assign user account 92
 - effective 95
 - exclusion 95
 - group 84
 - inheriting through system roles 89
 - overview of all assignments 100
 - role 84
- permissions level 121-122
 - assign to group 121
 - assign to user account 121
 - delete 123
 - role definition 131
 - site 121-122
 - site collection 121-122
- personalized admin identity 77-78
- prefix 142
 - create site 129
- product and SKU
 - assign business role 88
 - overview of all assignments 100
- project template 153

- provisioning
 - accelerate 36
 - members list 33
- pseudo employee 79

R

- reset revision 44
- reset start up data 44
- role
 - about IT Shop requests 132
 - add to IT Shop 90
 - assign cost center 86
 - assign department 86
 - assign group 94
 - assign location 86
 - assign system role 89
 - assign user account 84, 92
 - effective 134
 - exclusion 134
 - inheriting through roles 84
 - inheriting through system roles 89
 - map in One Identity Manager 131
 - overview 134
 - permissions inheritance 131
 - permissions level 131-132
 - role assignment 94, 131
 - site 132
- root site 128
 - site 127
 - site collection 124

S

- schema
 - changes 32

- shrink 32
- update 32
- server function 146
- SharePoint Online
 - troubleshooting 150
- SharePoint Online connector 8
- SharePoint Online server 8
- SharePoint Online tenant
 - overview 105
 - report 137
 - target system manager 147
- SharePoint Online user account
 - deferred deletion 81
- single object synchronization 34, 40
 - accelerate 36
- site 127
 - anonymous access 128
 - author 128
 - prefix 129
 - role assignment 128, 131
 - role definition 128
 - root site 127-128
 - permissions inheritance 131
 - site template 130
 - subordinate 131
 - URL 129-130
 - open 130
- site (SharePoint Online)
 - about IT Shop requests 135
 - create 135
- site collection 123
 - account definition 124
 - administrator 124
 - category 97
 - overview 127
 - root site 124
 - permissions inheritance 131
 - server 124
 - specify category 126
 - URL 124, 126
- site collection (SharePoint Online)
 - about IT Shop requests 135
 - create 135
 - rename 150
- site template
 - create site 130
- site template (SharePoint Online) 142
- start up configuration 30
- synchronization
 - calculation schedule 37
 - configure 21, 23, 28
 - connection parameter 21, 23, 28
 - prerequisite 12
 - prevent 39
 - scope 28
 - simulate 44
 - start 21, 23, 37
 - synchronization project
 - create 21, 23
 - variable 28
 - workflow 21, 23, 29
- synchronization analysis report 44
- synchronization configuration
 - customize 28-29
- synchronization log 38, 44
 - contents 27
 - create 27
- synchronization project
 - create 21, 23
 - deactivate 39

- edit 105
- project template 153
- synchronization server 8, 16
 - configure 17
 - edit 143
 - install 17
 - Job server 17
 - server function 146
 - system requirements 17
- synchronization workflow
 - create 21, 23, 29
- synchronize single object 40
- system
 - account definition 103
 - edit 102
 - employee assignment 69
 - synchronization type 103
- system connection
 - change 30
 - enabled variable set 31

T

- target system
 - not available 45
- target system manager 147
 - specify 103
- target system synchronization 41
- template
 - IT operating data, modify 58

U

- URL
 - site 129-130
 - site collection 124, 126

- user account 74, 106
 - administrative user account 77
 - administrator 108, 111
 - apply template 58
 - assign category 108, 111
 - assign employee 68, 108
 - assign extended properties 115
 - assign group 93
 - assign permissions 93
 - assign role 93
 - auditor 108, 111
 - authentication object 74, 108, 111
 - authentication system 108, 111
 - category 97
 - connected 72
 - create 107
 - default user accounts 76
 - deferred deletion 115
 - delete 115
 - edit 107
 - group identity 77, 79
 - identity 75, 108, 111
 - lock 115
 - login name 108, 111
 - manage level 70
 - more than 1 per employee 74
 - overview 114
 - personalized admin identity 77-78
 - privileged user account 75, 80, 108, 111
 - restore 115
 - risk index 108, 111
 - role assignment 131
 - type 75-77, 80
- user prefix 142

V

variable set 30

active 31