One Identity Manager 8.1.3

Administration Guide for Connecting to SharePoint Online

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.

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 - June 2020
Version - 8.1.3

Contents

1

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 detailed information about the SharePoint Online structure, see the SharePoint Online documentation from Microsoft.

Related topics

- Editing system objects on page 134

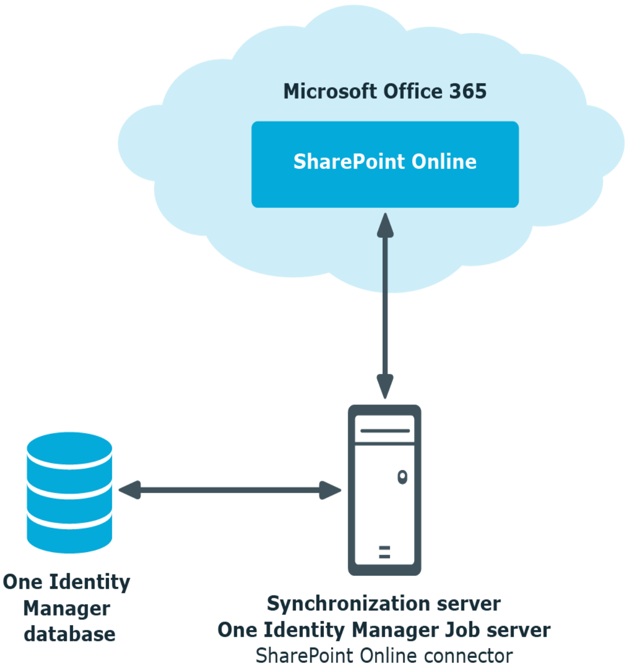
Architecture overview

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 SharePoint Online Microsoft subscriptions of Office 365 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 detailed 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

User	Tasks
Target system administrators	Target system administrators must be assigned to the **Target systems | Administrators** application role. Users with this application role: • Administer application roles for individual target system types. • Specify the target system manager. • Set up other application roles for target system managers

User	Tasks
	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	Target system managers must be assigned to the **Target systems | SharePoint Online** application role or a child application role. Users with this application role: • Assume administrative tasks for the target system. • Create, change, or delete target system objects like user accounts or groups. • Edit password policies for the target system. • Prepare groups to add to the IT Shop. • Can add employees who have an other 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	• Create customized permissions groups for application roles for role-based login to administration tools in the Designer as required. • Create system users and permissions groups for non role-based login to administration tools in the Designer as required. • Enable or disable additional configuration parameters in the Designer as required. • Create custom processes in the Designer as required. • Create and configure schedules as required. • Create and configure password policies as required.

Configuration parameter

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 131.

2

Synchronizing a SharePoint Online environment

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

This sections 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 the initial synchronization on page 12
- Customizing the synchronization configuration on page 25
- SharePoint Online synchronization features on page 24
- Executing synchronization on page 31
- Troubleshooting on page 37
- Editing system objects on page 134

Setting up the initial synchronization

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. 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.
    - Other configuration parameters are installed when the module is installed. Check the configuration parameters and modify them as necessary to suit your requirements.
3. Install and configure a synchronization server and declare the server as a Job server in One Identity Manager.
4. Create a synchronization project with the Synchronization Editor.

Detailed information about this topic

- Users and permissions for synchronizing with SharePoint Online on page 13
- System requirements for the synchronization server on page 15
- Creating a synchronization project for initial synchronization of a SharePoint Online tenant on page 19
- Configuration parameters for managing SharePoint Online on page 131
- Default project template for SharePoint Online on page 133

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
User for accessing SharePoint	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

<table>
<tr><th>User</th><th>Permissions</th></tr>
<tr><td>Online</td><td>is required:
An administrative user account of the corresponding Azure Active Directory tenant, which has the following administration roles.
SharePoint administrators
Azure Active Directory company administrator/global administrator
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.

For more detailed information about site collection administrators, see the Microsoft documentation.</td></tr>
<tr><td>One Identity Manager Service user account</td><td>The user account for One Identity Manager Service requires permissions to carry out operations at file level. For example, assigning permissions and creating and editing directories and files.

The user account must belong to the Domain users group.

The user account must have the Login as a service extended user permissions.

The user account requires access permissions to the internal web service.

NOTE: If One Identity Manager Service runs under the network service (NT Authority\NetworkService), you can issue access permissions for the internal web service with the following command line call:

<code>netsh http add urlacl url=http://<IP address>:<port number>/ user="NT AUTHORITY\NETWORKSERVICE"</code>

The user account needs full access to the One Identity Manager Service installation directory in order to automatically update One Identity Manager.

In the default installation, One Identity Manager is installed under:
<code>%ProgramFiles(x86)%\One Identity</code> (on 32-bit operating systems)
<code>%ProgramFiles%\One Identity</code> (on 64-bit operating systems)</td></tr>
<tr><td>User for accessing the One Identity Manager database</td><td>The Synchronization default system user is provided to execute synchronization with an application server.</td></tr>
</table>

Setting up the SharePoint Online synchronization server

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

Detailed information about this topic

- System requirements for the synchronization server on page 15
- Installing the One Identity Manager Service on page 15

System requirements for the 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 2008 R2 (non-Itanium based 64-bit) service pack 1 or later
  - Windows Server 2012
  - Windows Server 2012 R2
  - Windows Server 2016
  - Windows Server 2019
- Microsoft .NET Framework Version 4.7.2 or later

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

Installing the One Identity Manager Service

The One Identity Manager Service with the SharePoint Online connector must be installed on the synchronization server. 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).

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

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

NOTE: To generate processes for the Job server, you need the provider, connection parameters, and the authentication data. By default, this information is determined from the database connection data. If the Job server runs through an application server, you must configure extra connection data in the Designer. For detailed information about setting up Job servers, see the *One Identity Manager Configuration Guide*.

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

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

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

1. Start the Server Installer program on your administrative workstation.
2. On the **Database connection** page, enter the valid connection credentials for the One Identity Manager database.
3. On the **Server properties** page, specify the server on which you want to install the One Identity Manager Service.
    a. Select a Job server from the **Server** menu.

       - OR -

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

b. Enter the following data for the Job server.

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

     Syntax:

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

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

4. On the **Machine roles** page, select **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 detailed information about configuring the service, see the *One Identity Manager Configuration Guide*.

   - For a direct connection to the database:
     a. Select **Process collection | sqlprovider**.
     b. Click the **Connection parameter** entry, then click the **Edit** button.
     c. Enter the connection data for the One Identity Manager database.
   - For a connection to the application server:
     a. Select **Process collection**, click the **Insert** button and select **AppServerJobProvider**.
     b. Click the **Connection parameter** entry, then click the **Edit** button.
     c. Enter the connection data for the application server.
     d. Click the **Authentication data** entry and click the **Edit** button.
     e. Select the authentication module. Depending on the authentication module, other data may be required, such as user and password. For detailed information about the One Identity Manager authentication modules, see the *One Identity Manager Authorization and Authentication Guide*.
7. To configure remote installations, click **Next**.
8. Confirm the security prompt with **Yes**.
9. On the **Select installation source** page, select the directory with the install files.
10. On the **Select private key file** page, select the file with the private key.

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

11. On the **Service access** page, enter the service's installation data.
    - **Computer**: Name or IP address of the server that the service is installed and started on.
    - **Service account**: User account data for the One Identity Manager Service.
        - To start the service under another account, disable the **Local system account** option and enter the user account, password and password confirmation.
    - **Installation account**: Data for the administrative user account to install the service.
        - To use the current user’s account, set the **Current user** option.
        - To use another user account, disable the **Current user** option and enter the user account, password and password confirmation.
    - To change the install directory, names, display names, or description of the One Identity Manager Service, use the other options.
12. Click **Next** to start installing the service.

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

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

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). Use the synchronization as remote connection server at the same time, by simply 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 15
- Users and permissions for synchronizing with SharePoint Online on page 13

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`.
User account and password for logging in	User account and password for logging in to SharePoint Online. Example: `<user name of the synchronization user>@yourorganization.onmicrosoft.com` Make a user account available with sufficient permissions. For more

Data	Explanation
	information, see Users and permissions for synchronizing with SharePoint Online on page 13.
Synchronization server for SharePoint Online	All One Identity Manager Service actions are executed against the target system environment on the synchronization server. Data entries required for synchronization and administration with the One Identity Manager database are processed by the synchronization server. The One Identity Manager Service with the SharePoint Online connector must be installed on the synchronization server. **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 15.
One Identity Manager database connection data	• Database server • Database • SQL Server login and password • Specifies whether integrated Windows authentication is used. This type of authentication is not recommended. If you decide to use it anyway, ensure that your environment supports Windows authentication.
Remote connection server	For more information, see Preparing a remote connection server for access to the SharePoint Online tenant on page 18.

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:

- Executed in default mode
- Started from the Launchpad

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

To set up an initial synchronization project for a SharePoint Online tenant

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

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

2. Select the **Target system type 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 the following login data on the **Enter connection credentials** page to connect to SharePoint Online.

   - **Base domain**: Enter the name of the Azure Active Directory base domain without `.onmicrosoft.com`.
   - **User name**: Enter the fully qualified domain name 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**: Enter the pass word 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
Read-only access to target system.	Specifies that a synchronization workflow is only to be set up for the initial loading of the target system into the One Identity Manager database. The synchronization workflow has the following characteristics: • Synchronization is in the direction of **One Identity Manager**. • Processing methods in the synchronization steps are only defined for synchronization in the direction of **One Identity Manager**.
Read/write access to target system. Provisioning available.	Specifies whether a provisioning workflow is to be set up in addition to the synchronization workflow for the initial loading of the target system. The provisioning workflow displays the following characteristics: • Synchronization is in the direction of the **Target system**. • Processing methods are only defined in the 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 a synchronization server to execute synchronization.

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

   a. Click to add a new Job server.

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

   c. Click **OK**.

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

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

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

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

NOTE: If enabled, a consistency check is carried out. If errors occur, a message appears. You can decide whether the synchronization project can remain activated or not.

Check the errors before you use the synchronization project. To do this, in the **General** view on the Synchronization Editor‘s start page, click **Verify project**.

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

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 exclude site collections from 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. 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 your changes.

Related topics

- Users and permissions for synchronizing with SharePoint Online on page 13
- SharePoint Online synchronization features on page 24
- Setting up the SharePoint Online synchronization server on page 15
- Configuring the synchronization log on page 23
- Customizing the synchronization configuration on page 25

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 Synchronization Editor.

   - OR -

   To configure the synchronization log for the database connection, select the **Configuration | Synchronization Editor connection** category in One Identity Manager.
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 32

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 pro 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 exclude site collections from 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. 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 your changes.

Related topics

- Users and permissions for synchronizing with SharePoint Online on page 13

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 master 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 methods, for example.
- Update the schema in the synchronization project if the One Identity Manager schema or target system schema has changed. Then you can add the changes to the mapping.
- To synchronize additional schema properties, update the schema in the synchronization project. Include the schema extensions in the mapping.

- Add your own schema types if you want to synchronize data, which does not have schema types in the connector schema. Include the schema extensions in the mapping.

For more detailed 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 26
- Updating schemas on page 26
- Configuring the provisioning of memberships on page 27
- Configuring single object synchronization on page 29
- Accelerating provisioning and single object synchronization on page 30

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 master system during synchronization, you also require a workflow with synchronization in the direction of the **Target system**.

To create a synchronization configuration for synchronizing SharePoint Online

1. Open the synchronization project in the Synchronization Editor.
2. Check whether existing mappings can be used for synchronizing 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 synchronization direction.
4. Create a new start up configuration. Use the new workflow to do this.
5. Save the changes.
6. Run a consistency check.

Updating schemas

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

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

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

- A schema was changed by:
  - Changes to a target system schema
  - Customizations to the One Identity Manager schema
  - A One Identity Manager update migration
- A schema in the synchronization project was shrunk by:
  - Enabling the synchronization project
  - Saving the synchronization project for the first time
  - Compressing a schema

To update a system connection schema

1. Select the **Configuration | Target system** category.

   - OR -

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

   This reloads the schema data.

To edit a mapping

1. Select the **Mappings** category.
2. Select a mapping in the navigation view.

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

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

Configuring the provisioning of memberships

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

- Memberships are saved in the target system as an object property in list form (Example: List of user accounts in the `Members` property of a SharePoint Online`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. Select **SharePoint Online** in the result list.
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.
    - This option can only be enabled for assignment tables that have a base table with `XDateSubItem` or `CCC_XDateSubItem` column.
    - Assignment tables that are grouped together in a virtual schema property in the mapping must be marked identically.
5. Click **Merge mode**.
6. Save the changes.

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

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

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

To restore the default condition

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

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

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 member list is belongs to one of these properties, then 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 detailed information, see *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_O3STenant).XObjectKey`

8. Save the changes.

Related topics

- Synchronizing single objects on page 34
- Post-processing outstanding objects on page 34

Accelerating provisioning and single object synchronization

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

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

To configure load balancing

1. Configure the server and declare it as a Job server in One Identity Manager.
    - Assign the **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 detailed information about load balancing, see the *One Identity Manager Target System Synchronization Reference Guide*.

Detailed information about this topic

- Editing SharePoint Online Job servers on page 124

Executing 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 was terminated unexpectedly, you must reset the start information to be able to restart synchronization.

Before you execute 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 of execution. For detailed information about start up configurations, see the *One Identity Manager Target System Synchronization Reference Guide*.

Detailed information about this topic

- Starting synchronization on page 31
- Deactivating synchronization on page 33
- Displaying synchronization results on page 32

Starting synchronization

When setting up the initial synchronization project using the Launchpad, a default schedule for regular synchronizations is created and assigned. To execute regular synchronizations, activate this schedule.

To synchronize on a regular basis

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

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

To start initial synchronization manually

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

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. Open the synchronization project in the Synchronization Editor.
2. Select the **Logs** category.
3. Click in the navigation view toolbar.

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

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

To display a provisioning log

1. Open the synchronization project in the Synchronization Editor.
2. Select the **Logs** category.
3. Click in the navigation view toolbar.

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

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

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

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

Related topics

- Configuring the synchronization log on page 23
- Troubleshooting on page 37

Deactivating synchronization

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

To prevent regular synchronization

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

   Now you can only start synchronization manually.

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

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

To deactivate the synchronization project

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

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 member list is belongs to one of these properties, then 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.

Detailed information about this topic

- Configuring single object synchronization on page 29

Tasks after a 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 34
- Adding custom tables to the target system synchronization on page 36
- Managing user accounts through account definitions on page 37

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.

   All the synchronization tables assigned to the **SharePoint Online** target system type are displayed in the navigation view.

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 executed. 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***
   >
   > a. Select the object on the target system synchronization form.
   >
   > b. 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 execute 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. The **Outstanding** label is removed from the object. Indirect memberships cannot be deleted.
	Publish	The object is added to the target system. The **Outstanding** label is removed from the object. The method triggers the `HandleOutstanding` event. This runs a target system specific process that triggers the provisioning process for the object. Prerequisites: • 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 execution of 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

- In the form's toolbar, click to disable bulk processing.

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 34

Managing user accounts through account definitions

Following a synchronization, employees are automatically assigned in the default installation. If an account definition for the site collection is not yet 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 62

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 was terminated 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 32
- SharePoint Online synchronization features on page 24

3

Managing SharePoint Online user accounts and employees

The main feature of One Identity Manager is to map employees together with the master 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. If an employee does not yet have a user account in a tenant, a new user account is created. This is done by assigning account definitions to an employee using the integrated inheritance mechanism and subsequent process handling.

  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 40
- Automatic assignment of employees to SharePoint Online user accounts on page 58

Account definitions for SharePoint Online user accounts

One Identity Manager has account definitions for automatically allocating user accounts to employees during working hours. 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.

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 41
- Editing manage levels on page 43
- Creating mapping rules for IT operating data on page 46
- Entering IT operating data on page 47
- Assigning account definitions to employees on page 50
- Assigning account definitions to target systems on page 55

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 master data form, enter the master data for the account definition.
4. Save the changes.

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 master data** task.
4. Enter the account definition's master data.
5. Save the changes.

Related topics

- Master data for account definitions on page 41
- Creating account definitions on page 41

Master data for account definitions

Enter the following data for an account definition:

Table 8: Master 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	Target system to which the account definition applies.

Property	Description
system	
Required account definition	Required account definition. Define the dependencies between account definitions. When this account definition is requested or assigned, the required account definition is automatically requested or assigned with it. 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. If this exists, the SharePoint Online user account is added.
Description	Text field for additional explanation.
Manage level (initial)	Manage level to use by default when you add new user accounts.
Risk index	Value for evaluating the risk of assignments to employees. Enter a value between 0 and 1. This input field is only visible if the **QER | CalculateRiskIndex** configuration parameter is set. For more detailed information, see the *One Identity Manager Risk Assessment Administration Guide*.
Service item	Service item through which you can request the account definition 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 ordered by an employee over the Web Portal and distributed using a defined approval process. The account definition 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 ordered by an employee over the Web Portal and distributed using a defined approval process. This means, the account definition cannot be directly assigned to roles outside the IT Shop.
Automatic assignment to employees	Specifies whether the account definition is assigned automatically to all internal employees. The account definition is assigned to every employee not marked as external, on saving. New employees automatically obtain this account definition as soon as they are added. IMPORTANT: Only set this option 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. Disable this option to remove automatic assignment of the account definition to all employees. The account definition cannot be reassigned to employees from this point on. Existing account definition assignments

Property	Description
	remain intact.
Retain account definition if permanently disabled	Specifies the account definition assignment to permanently disabled employees. Option set: the account definition assignment remains in effect. The user account stays the same. Option not set: the account definition assignment is not in effect. The associated user account is deleted.
Retain account definition if temporarily disabled	Specifies the account definition assignment to temporarily disabled employees. Option set: the account definition assignment remains in effect. The user account stays the same. Option not set: the account definition assignment is not in effect. The associated user account is deleted.
Retain account definition on deferred deletion	Specifies the account definition assignment on deferred deletion of employees. Option set: the account definition assignment remains in effect. The user account stays the same. Option not set: the account definition assignment is not in effect. The associated user account is deleted.
Retain account definition on security risk	Specifies the account definition assignment to employees posing a security risk. Option set: the account definition assignment remains in effect. The user account stays the same. Option not set: the account definition assignment is not in effect. The associated user account is deleted.
Resource type	Resource type for grouping .
Spare field 01 - spare field 10	Additional company-specific information. Use the Designer to customize display names, formats, and templates for the input fields.

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 no 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.

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 master data** task.
4. Edit the manage level's master data.
5. Save the changes.

Related topics

- Master data for manage levels on page 45
- Entering IT operating data on page 47

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 detailed 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 master data form, edit the master data for the manage level.
4. Save the changes.

Related topics

- Master data for account definitions on page 41
- Editing account definitions on page 41

Master data for manage levels

Enter the following data for a manage level.

Table 9: Master 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: • **Never**: Data is not updated. • **Always**: Data is always updated. • **Only initially**: Data is only determined at the start.
Retain groups if temporarily disabled	Specifies whether user accounts of temporarily disabled employees retain their group memberships.
Lock user accounts if temporarily disabled *)	Specifies whether user accounts of temporarily disabled employees are locked.
Retain groups if permanently disabled	Specifies whether user accounts of permanently disabled employees retain group memberships.
Lock user accounts if permanently disabled *)	Specifies whether user accounts of permanently disabled 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 (with delay) 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
- 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 and enter the following data.

Table 10: Mapping rule for IT operating data

Property	Description
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: Only use the primary business role if the Business Roles Module is installed. • 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 user account properties are always filled with the default value. IT operating data is not determined dynamically from a role.
Notify when applying the standard	Specifies whether email notification to a defined mailbox is sent when the default value is used. The **Employee - new user account with default properties created** mail template is used. To change the mail template, adjust the **TargetSystem | SharePointOnline | Accounts | MailTemplateDefaultValues** configuration parameter.

4. 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 A and an account definition B for the administrative user account of tenant A. Specify the "Department" property in the IT operating data formatting rule for the account definitions A and B 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.

Table 11: IT operating data

Property	Description
Effects on	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	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	Concrete value which is assigned to the user account property.

4. Save the changes.

Related topics

- Creating mapping rules for IT operating data on page 46

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 changes, the templates are automatically executed.

To execute 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 **Execute 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.

Old value:	Current value of the object property.
New value:	Value that the object property would have following modification of the IT operating data.
Selection:	Specifies whether or not the new value is transferred 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.

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).

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 assignment of an account definition is removed, the user account that was created from this account definition is deleted.

For detailed 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 51
- Assigning account definitions to business roles on page 52
- Assigning account definitions to all employees on page 52
- Assigning account definitions directly to employees on page 53
- Assigning account definitions to system roles on page 53
- Adding account definitions in the IT Shop on page 53

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

Installed modules: Business Roles Module

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, 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

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 master data** task.
4. On the **General** tab, enable the **Automatic assignment to employees** option.

   IMPORTANT: Only set this option 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.
5. Save the changes.

The account definition is assigned to every employee that is not marked as external. New employees automatically obtain this account definition as soon as they are added. The assignment is calculated by the DBQueue Processor.

NOTE: Disable **Automatic assignment to employees** to remove automatic assignment of the account definition to all employees. 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

Installed modules: System Roles Module

NOTE: 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 assigned system roles.

   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

1. In the Manager, select the **SharePoint Online | Basic configuration data | Account definitions | Account definitions** (non role-based login) category.

   - OR -

   In the Manager, select the **Entitlements | Account definitions** (role-based login) 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

1. In the Manager, select the **SharePoint Online | Basic configuration data | Account definitions | Account definitions** (non role-based login) category.

   - OR -

   In the Manager, select the **Entitlements | Account definitions** (role-based login) 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

1. In the Manager, select the **SharePoint Online | Basic configuration data | Account definitions | Account definitions** (non role-based login) category.

   - OR -

In the Manager, select the **Entitlements | Account definitions** (role-based login) 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 requests from company resources through the IT Shop, see the *One Identity Manager IT Shop Administration Guide*.

Related topics

- Master data for account definitions on page 41

Assigning account definitions to target systems

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 master data** task.
3. From the **Account definition (initial)** menu, select the account definition for user accounts.
4. Save the changes.

Related topics

- Automatic assignment of employees to SharePoint Online user accounts on page 58
- Master data for manage levels on page 45

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 master data** task.
    d. On the **General** tab, disable the **Automatic assignment to employees** option.
    e. 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 the 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.

       In the **Remove assignments** pane, remove the business roles.
    d. 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 Portal User Guide*.

    To remove an account definition from all IT Shop shelves

    a. In the Manager, select the **SharePoint Online | Basic configuration data | Account definitions | Account definitions** (non role-based login) category.

        - OR -

        In the Manager, select the **Entitlements | Account definitions** (role-based login) 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 master 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 master 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.

Automatic assignment of employees to SharePoint Online user accounts

When you add a user account, an existing employee can be assigned automatically. 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 master data** to assign employees to administrative user accounts for the respective user account.

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:

Following a synchronization, employees are automatically assigned in the default installation. If an account definition for the site collection is not yet 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 37.

Related topics

- Creating account definitions on page 41
- Assigning account definitions to target systems on page 55
- Changing the manage level in SharePoint Online user accounts on page 62
- Editing search criteria for automatic employee assignment on page 59

Editing search criteria for automatic employee assignment

The criteria for employee assignments are defined for the site collection. In this case, 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 `O3SSite` 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: When the employees are assigned to user accounts on the basis of search criteria, user accounts are given 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.

It is not recommended to make assignments to administrative user accounts based on search criteria. Use **Change master data** to assign employees to administrative user accounts for the respective user account.

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 12: Search criteria for user accounts

Apply to	Column for employee	Column for user account
SharePoint Online user account (user authenticated)	Default email address (`DefaultEmailAddress`)	E-Mail Address (`EMail`)

5. Save the changes.

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

Related topics

- Automatic assignment of employees to SharePoint Online user accounts on page 58
- Finding employees and directly assigning them to user accounts on page 60

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 13: 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

View	Description
	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. In the result list, select the site collection.
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 master 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.

Changing the manage level in 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 master data** task.
4. On the **General** tab, select the manage level in the **Manage level** menu.
5. Save the changes.

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 select 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 target systems on page 55

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 64
- Supported user account types on page 65

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. Clara Harris owns an Azure Active Directory user account, which is a member in this group. She can log in to the site collection with this and obtain all the SharePoint Online user account's permissions.
>
> Jan Bloggs is also requires guest access to the site collection. He owns an Azure Active Directory user account in the same domain. In the Web Portal, he requests membership of the Azure Active Directory **Guests** group. Once the request is granted approval and assigned, he 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 Onlineroles 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 detailed 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 14: Identities of user accounts

Identity	Description	Value of the IdentityType column
Primary identity	Employee's default user account.	Primary

Identity	Description	Value of the IdentityType column
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 that is used for a specific purpose, such as training.	Sponsored
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, group identity, or service identity are linked to dummy employees that do not refer to a real person. These dummy employees are needed so that permissions can be inherited by the user accounts. When evaluating reports, attestations, or compliance checks, check whether dummy employees need to be considered separately.

For detailed 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 67
- Administrative user accounts on page 68
- Privileged user accounts on page 70

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 the IT operating data for the user accounts, and which default values are used if no IT operating data can be determined through a person's primary roles.

   Which IT operating data is required depends on the target system. The following setting are recommended for default user accounts:

   - In the mapping rule for the `IsGroupAccount` column, use the default value **1** and enable the **Always use default value** option.
   - In the mapping rule for the `IdentityType` column, use the default value **Primary** and enable **Always use default value**.
4. Enter the effective IT operating data for the target system. Select the concrete target system under **Effects on**.

   Specify in the departments, cost centers, locations, or business roles that IT operating data should apply when you set up a user account.
5. Assign the account definition to 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 40

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 68
- Providing administrative user accounts for several employees on page 69

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 master 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 master 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 69
- 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 dummy employee must exist. The dummy 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 master data** task.
   d. On the **General** tab, in the **Identity** menu, select **Shared identity**.
2. Link the user account to a dummy 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 master data** task.

d. On the **General** tab, select the dummy employee from the **Employee** menu.

   TIP: If you are the target system manager, you can choose to create a new dummy 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 68
- For detailed 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 the IT operating data for the user accounts, and which default values are used if no IT operating data can be determined through a person's primary roles.

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

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

   Specify in the departments, cost centers, locations, or business roles which IT operating data should apply when you set up a user account.
6. Assign the account definition directly to 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: If customization requires that the of privileged user accounts follow a defined naming convention, create the template according to which the are formed.

Related topics

- Account definitions for SharePoint Online user accounts on page 40

4

Managing the 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 (`O3SGroup` table)
- Entitlement for the use of SharePoint Online roles (`O3SRLAsgn`)

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 (`O3SUserInGroup` table)
    - Role assignments to user accounts (`O3SUserHasRLAsgn` table)

Assigning SharePoint Online entitlements to SharePoint Online user accounts in One Identity Manager

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. System entitlements from different target systems can also be grouped together in a system role.

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

Prerequisites

- The assignment of employees, SharePoint Online roles, and SharePoint Online groups is permitted for departments, cost centers, locations, or business roles.

  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.
- **Group authenticated** is not set in the user accounts.
- User accounts are marked with the **Groups can be inherited** option.
- User accounts and SharePoint Online entitlements belong to the same site collection.

For detailed information see the following guides:

Theme	Guide
Inheritance of company resources	*One Identity Manager Identity Management Base Module Administration Guide* *One Identity Manager Business Roles Administration Guide*
Assigning company resources through IT Shop requests	*One Identity Manager IT Shop Administration Guide*
System roles	*One Identity Manager System Roles Administration Guide*

Detailed information about this topic

- Assigning SharePoint Online entitlements to departments, cost centers, and locations on page 74
- Assigning SharePoint Online entitlements to business roles on page 75
- Assigning SharePoint Online user accounts directly to an entitlement on page 79
- Adding SharePoint Online entitlements to system roles on page 77
- Adding SharePoint Online entitlements to the IT Shop on page 77
- Assigning SharePoint Online entitlements directly to a user account on page 80
- Assigning SharePoint Online roles to SharePoint Online groups on page 81

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.

   - OR -

   In the **Remove assignments** pane, remove the entitlements.
5. Save the changes.

Related topics

- Assigning SharePoint Online entitlements to business roles on page 75
- Adding SharePoint Online entitlements to system roles on page 77
- Adding SharePoint Online entitlements to the IT Shop on page 77
- Assigning SharePoint Online user accounts directly to an entitlement on page 79
- Assigning SharePoint Online entitlements directly to a user account on page 80
- One Identity Manager users for managing SharePoint Online on page 9

Assigning SharePoint Online entitlements to business roles

Installed modules: Business Roles Module

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, 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.

   \- OR -

   In the **Remove assignments** pane, remove the entitlements.
5. Save the changes.

Related topics

- Assigning SharePoint Online entitlements to departments, cost centers, and locations on page 74
- Adding SharePoint Online entitlements to system roles on page 77
- Adding SharePoint Online entitlements to the IT Shop on page 77
- Assigning SharePoint Online user accounts directly to an entitlement on page 79
- Assigning SharePoint Online entitlements directly to a user account on page 80
- One Identity Manager users for managing SharePoint Online on page 9

Adding SharePoint Online entitlements to system roles

Installed modules: System Roles Module

Use this task to add an entitlement to system roles. When you assign a system role to an employee, the entitlement is inherited by all user accounts of this employee.

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

   To remove an assignment

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

Related topics

- Assigning SharePoint Online entitlements to departments, cost centers, and locations on page 74
- Assigning SharePoint Online entitlements to business roles on page 75
- Adding SharePoint Online entitlements to the IT Shop on page 77
- Assigning SharePoint Online user accounts directly to an entitlement on page 79
- Assigning SharePoint Online entitlements directly to a user account on page 80

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) category.
   - **SharePoint Online | Groups**
   - **SharePoint Online | Roles**

   - OR -

   In the Manager select one of the following categories (role-based login) category.
   - **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. In the **Add assignments** pane, the entitlement to the IT Shop shelves.
5. 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) category.
   - **SharePoint Online | Groups**
   - **SharePoint Online | Roles**

   - OR -

   In the Manager select one of the following categories (role-based login) category.
   - **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. In the **Remove assignments** pane, the entitlement from the IT Shop shelves.
5. 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) category.
   - **SharePoint Online | Groups**
   - **SharePoint Online | Roles**

   - OR -

   In the Manager select one of the following categories (role-based login) category.
   - **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 detailed information about requesting company resources through the IT Shop, see the *One Identity Manager IT Shop Administration Guide*.

Related topics

- SharePoint Online group master data on page 103
- General master data for SharePoint Online roles on page 117
- Assigning SharePoint Online entitlements to departments, cost centers, and locations on page 74
- Assigning SharePoint Online entitlements to business roles on page 75
- Adding SharePoint Online entitlements to system roles on page 77
- Assigning SharePoint Online user accounts directly to an entitlement on page 79
- Assigning SharePoint Online entitlements directly to a user account on page 80
- 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 group in the result list.

   - OR -

   Select the role in the result list.
3. Select in the **Assign user accounts** task.
4. In the **Add assignments** pane, assign user accounts.

   - OR -

   In the **Remove assignments** pane, remove user accounts.
5. Save the changes.

Related topics

- Assigning SharePoint Online entitlements directly to a user account on page 80
- Assigning SharePoint Online entitlements to departments, cost centers, and locations on page 74
- Assigning SharePoint Online entitlements to business roles on page 75
- Adding SharePoint Online entitlements to system roles on page 77
- Adding SharePoint Online entitlements to the IT Shop on page 77

Assigning SharePoint Online entitlements directly to a user account

To enable a quick response to special requests, you can assign entitlements directly to a user account.

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.

   - OR -

In the **Remove assignments** pane, remove the entitlements.

5. Save the changes.

Related topics

- Assigning SharePoint Online user accounts directly to an entitlement on page 79
- Assigning SharePoint Online entitlements to departments, cost centers, and locations on page 74
- Assigning SharePoint Online entitlements to business roles on page 75
- Adding SharePoint Online entitlements to system roles on page 77
- Adding SharePoint Online entitlements to the IT Shop on page 77

Assigning SharePoint Online roles to SharePoint Online groups

In order for SharePoint Online user groups 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 enabled 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 roles.

   - OR -

   In the **Remove assignments** pane, remove the roles.
5. Save the changes.

Related topics

- General master data for SharePoint Online permission levels on page 108
- Assigning SharePoint Online groups to SharePoint Online roles on page 82
- Assigning SharePoint Online entitlements to departments, cost centers, and locations on page 74
- Assigning SharePoint Online entitlements to business roles on page 75
- Adding SharePoint Online entitlements to system roles on page 77
- Adding SharePoint Online entitlements to the IT Shop on page 77

- Assigning SharePoint Online user accounts directly to an entitlement on page 79
- Assigning SharePoint Online entitlements directly to a user account on page 80

Assigning SharePoint Online groups to SharePoint Online roles

In order for SharePoint Online user groups 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 enabled that reference permission levels, cannot be assigned to groups.

To assign groups to a SharePoint Online role

1. In the Manager, select the **SharePoint Online | Roles** category.
2. Select the role in the result list.
3. Select the **Assign groups** task.
4. In the **Add assignments** pane, assign groups.

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

   To remove an assignment

   - Select the group and double-click ✅.
5. Save the changes.

Related topics

- General master data for SharePoint Online permission levels on page 108
- Assigning SharePoint Online roles to SharePoint Online groups on page 81
- Assigning SharePoint Online entitlements to departments, cost centers, and locations on page 74
- Assigning SharePoint Online entitlements to business roles on page 75
- Adding SharePoint Online entitlements to the IT Shop on page 77
- Assigning SharePoint Online user accounts directly to an entitlement on page 79
- Assigning SharePoint Online entitlements directly to a user account on page 80

Effectiveness of SharePoint Online entitlement assignments

Table 15: Configuration parameters for conditional inheritance

Configuration parameter	Effect when set
QER | Structures | Inherite | GroupExclusion	Preprocessor relevant configuration parameter for controlling effectiveness of group memberships. If the parameter is set, memberships can be reduced on the basis of exclusion definitions. Changes to this parameter require the database to be recompiled.

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 `O3SUserInO3SGroup` and `O3SBaseTreeHasGroup` tables by the `XIsInEffect` column.

Example of 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.

Clara Harris has a user account in this site collection. She primarily belongs to the "Marketing" department. The "Control group" business role and the "Finance" department are assigned to her 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 16: Specifying excluded groups (`O3SGroupExclusion` table)

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

Table 17: Effective assignments

Employee	Member in role	Effective group
Ben King	Marketing	Group A
Jan Bloggs	Marketing, finance	Group B
Clara Harris	Marketing, finance, control group	Group C
Jenny Basset	Marketing, control group	Group A, Group C

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

The groups A and C are in effect for Jenny Basset because the groups are not defined as mutually exclusive. If this should not be allowed, define further exclusion for group C.

Table 18: Excluded groups and effective assignments

<table>
<tr><th>Employee</th><th>Member in role</th><th>Assigned group</th><th>Excluded group</th><th>Effective group</th></tr>
<tr><td rowspan="2">Jenny Basset</td><td>Marketing</td><td>Group A</td><td></td><td rowspan="2">Group C</td></tr>
<tr><td>Control group</td><td>Group C</td><td>Group B
Group A</td></tr>
</table>

Prerequisites

- The **QER | Structures | Inherite | GroupExclusion** configuration parameter is set.
- 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 not longer mutually exclusive.
5. Save the changes.

SharePoint Online group inheritance based on categories

In One Identity Manager, groups can be selectively inherited by user accounts. For this purpose, the groups and the 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 **Position 1** to **Position 31** category positions.

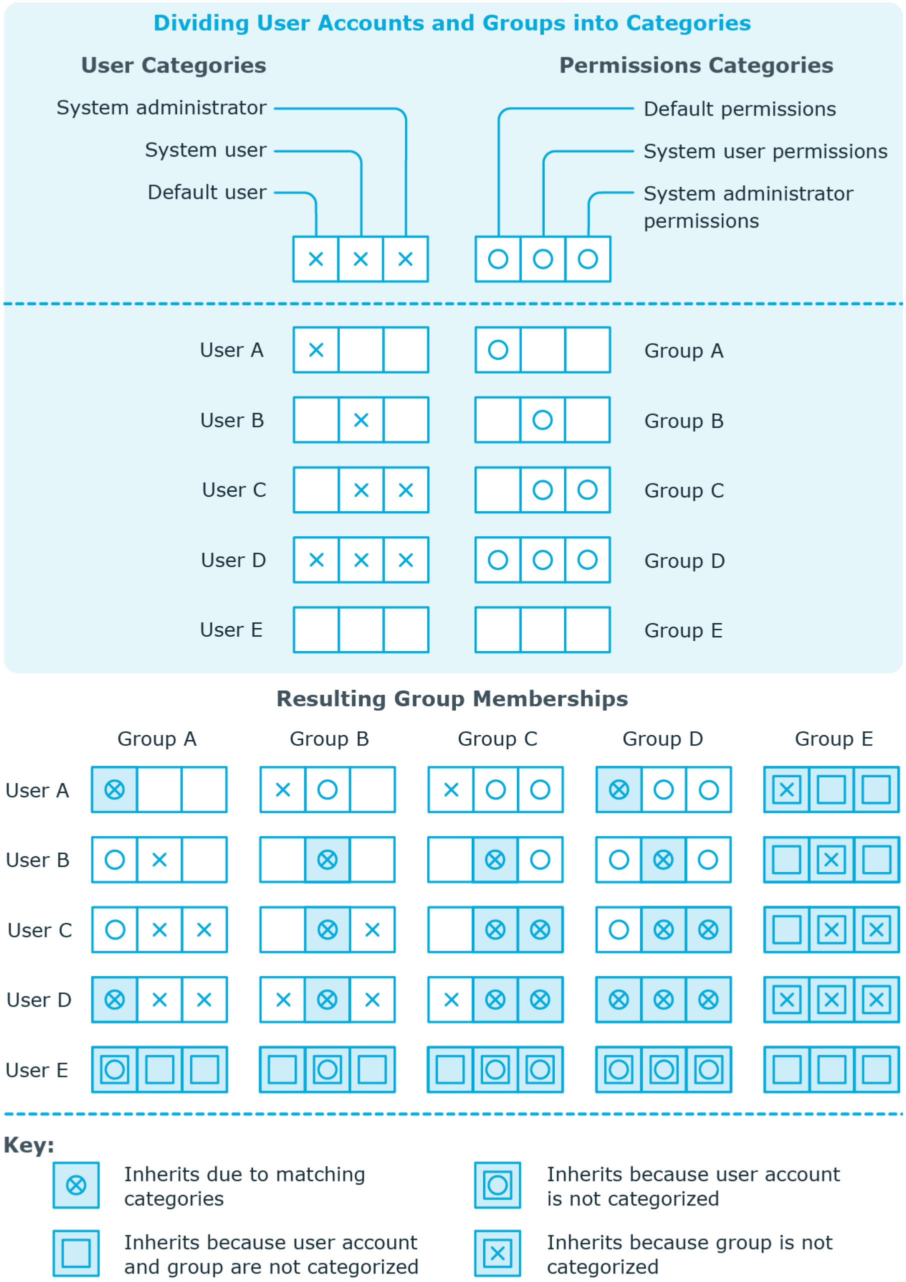
Every user account can be assigned to one or more categories. Each group can also be assigned to one or more categories. The group is inherited by the user account when at least one user account category items matches an assigned group. The group is also inherited by the user account if the group or 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 19: 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

- Define the categories in the site collection.
- Assign categories to user accounts through their master data.
- Assign categories to groups through their master data.

Related topics

- Specifying categories for inheriting SharePoint Online groups on page 111
- Group authenticated user account master data on page 97
- User authenticated user account master data on page 95
- SharePoint Online group master data on page 103

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 20: 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.

5

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 89
- SharePoint Online groups on page 102
- SharePoint Online user accounts on page 92
- SharePoint Online permission levels on page 107
- SharePoint Online site collections on page 109
- SharePoint Online sites on page 112
- SharePoint Online roles on page 116

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 required for the configuration of provisioning processes, the automatic assignment of employees to user accounts, and the inheritance of groups by 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

- General master data for SharePoint Online tenants on page 90
- Synchronizing a SharePoint Online environment on page 12
- Editing system objects on page 134

General master data for SharePoint Online tenants

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

Table 21: General master data for 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 which they are assigned. A different target system manager can be assigned to each tenant. 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.
Synchronized by	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. When creating a tenant using Synchronization Editor, **One Identity Manager** is used.

Table 22: Permitted values

Value	Synchronization by	Provisioned by
One Identity Manager	SharePoint Online connector	SharePoint Online connector
No synchronization	none	none

NOTE: If you select **No synchronization**, you can define custom processes to exchange data between One Identity Manager and the

Property	Description
	target system.
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"	Enables the administrator to hide the **Everyone except external users** group in the person selection.

Related topics

- Target system managers on page 128

Additional tasks for managing SharePoint Online tenant

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

Task	Topic
Overview of SharePoint Online tenants	Overview of a SharePoint Online tenant on page 92
Define search criteria for employee assignment	Editing search criteria for automatic employee assignment on page 59
Edit synchronization project	Editing the synchronization project for a SharePoint Online tenant on page 92

Task	Topic
Synchronize this object	Synchronizing single objects on page 34

Overview of a SharePoint Online tenant

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 a 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. Select the **Change master data** task.
3. Select the **Edit synchronization project...** task.

Related topics

- Customizing the synchronization configuration on page 25

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 Onlineer 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 master data described in the following is mapped through templates from employee master data.

> NOTE:

Related topics

- Application cases for SharePoint Online user account on page 64
- Managing SharePoint Online user accounts and employees on page 39
- Account definitions for SharePoint Online user accounts on page 40
- Default project template for SharePoint Online on page 133
- Editing master data for SharePoint Online user accounts on page 94
- Deleting and restoring SharePoint Online user accounts on page 101
- Managing the assignments of SharePoint Online groups and roles on page 72

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 master data form, edit the master data for the user account.
4. Save the changes.

Detailed information about this topic

- SharePoint Online user accounts on page 92
- Entering master data for SharePoint Online user accounts on page 95

Related topics

- Editing master data for SharePoint Online user accounts on page 94
- Deleting and restoring SharePoint Online user accounts on page 101

Editing master data for SharePoint Online user accounts

To edit master data 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 and run the **Change master data** task.
3. Edit the user account's resource data.
4. Save the changes.

Detailed information about this topic

- Entering master data for SharePoint Online user accounts on page 95

Related topics

- Creating SharePoint Online user accounts on page 93
- Deleting and restoring SharePoint Online user accounts on page 101

Entering master data for SharePoint Online user accounts

Each SharePoint Online user account represents an object from an authentication system. This object can be a group or a user. The group authentication and user authenticated user accounts are select separately in the navigation system.

Detailed information about this topic

- Group authenticated user account master data on page 97
- User authenticated user account master data on page 95

User authenticated user account master data

Enter the following master data for a user authenticated user account.

Table 23: User authenticated user account master data

Property	Description
Employee	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. 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 master data. Which login data is required depends on the selected identity type.
Account definition	Account definition through which the user account was created. Use the account definition to automatically fill user account master 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. NOTE: The account definition cannot be changed once the user account has been saved. NOTE: If employees receive their SharePoint Online user accounts through account definitions, the employees must have user accounts in the corresponding Azure Active Directory tenant that is defined on the

Property	Description
	SharePoint Online tenant
Manage level	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.
Site collection	Site collection the user account is used in.
Principal type	Type of the principal (user, domain 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	Authentication object referencing the user account. 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. The following authentication objects can be assigned to a user-authenticated user account: • Azure Active Directory user accounts from the tenant that is assigned to the SharePoint Online tenant NOTE: The SharePoint Online user account is also created if the user account that is used as the authentication object is disabled or locked.
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 detailed information, see the *One Identity Manager Risk Assessment Administration Guide*.
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.

Property	Description
Identity	User account's identity type Permitted values are: • **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 that is used for a specific purpose, such as training. • **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	Specifies whether the user account can inherit SharePoint Online roles and groups through the employee. If this option is set, the user account inherits SharePoint Online roles and groups through hierarchical roles or IT Shop requests. • 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.
Administrator	Specifies whether the user account is a site collection administrator.
Hidden	Specifies if the user account is displayed in the user interface.

Detailed information about this topic

- Account definitions for SharePoint Online user accounts on page 40
- Specifying categories for inheriting SharePoint Online groups on page 111
- Automatic assignment of employees to SharePoint Online user accounts on page 58
- Supported user account types on page 65

Group authenticated user account master data

Enter the following master data for a group authenticated user account.

Table 24: Group authenticated user account master data

Property	Description
Employee	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. 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 master data. Which login data is required depends on the selected identity type.
Site collection	Site collection the user account is used in.
Group authen-ticated	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	Authentication object referencing the user account. 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. The following authentication objects can be assigned to a group authenticated user account: • Azure Active Directory groups with the **Security group** group type from the tenant that is assigned to the SharePoint Online tenant
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**

Property	Description
	configuration parameter is set. For detailed information, see the *One Identity Manager Risk Assessment Administration Guide*.
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: • **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 that is used for a specific purpose, such as training. • **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 if the user account is displayed in the user interface.

Detailed information about this topic

- Specifying categories for inheriting SharePoint Online groups on page 111
- Supported user account types on page 65

Additional tasks for managing SharePoint Online user accounts

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

Task	Topic
Overview of SharePoint Online user accounts	Overview of SharePoint Online user accounts on page 100
Assigning extended properties	Assigning extended properties on page 100
Assign groups	Assigning SharePoint Online entitlements directly to a user account on page 80
Assign SharePoint Online roles	Assigning SharePoint Online entitlements directly to a user account on page 80
Synchronize object	Synchronizing single objects on page 34

Overview of SharePoint Online user accounts

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

Extended properties are meta objects, such as operating codes, cost codes, or cost accounting areas that cannot be mapped directly in One Identity Manager.

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 the **Assign extended properties** task.
4. In the **Add assignments** pane, assign extended properties.

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

To remove an assignment

- Select the extended property and double-click.

5. Save the changes.

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

Deleting and restoring SharePoint Online user accounts

If a user account is deleted in One Identity Manager, it is initially marked for deletion. The user account is therefore locked. Depending on the deferred deletion setting, the user account is either deleted from the One Identity Manager database immediately, or at a later date.

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 assignment of an account definition is removed, the user account that was created from this account definition is deleted.

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 to delete the user account.
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.

Configuring deferred deletion

By default, user accounts are finally deleted from the database after 30 days.You can reenable the user accounts until deferred deletion is run. After deferred deletion is run, the user accounts are deleted from the database and cannot be restored anymore.In the Designer, you can set an alternative delay on the `O3SUser` table.

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.

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

Detailed information about this topic

- SharePoint Online group master data on page 103
- Specifying categories for inheriting SharePoint Online groups on page 111
- SharePoint Online group inheritance based on categories on page 85

Related topics

- Creating SharePoint Online groups on page 102
- Deleting SharePoint Online groups on page 106

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 master data form, edit the master data for the group.
4. Save the changes.

Detailed information about this topic

- SharePoint Online group master data on page 103
- Additional tasks for managing SharePoint Online groups on page 105

Related topics

- Editing master data for SharePoint Online groups on page 103
- Deleting SharePoint Online groups on page 106

Editing master data for SharePoint Online groups

To edit group master data

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

Detailed information about this topic

- SharePoint Online group master data on page 103
- Additional tasks for managing SharePoint Online groups on page 105

Related topics

- Creating SharePoint Online groups on page 102
- Deleting SharePoint Online groups on page 106

SharePoint Online group master data

Enter the following master data for a group.

Table 25: SharePoint Online group master data

Property	Description
Title	Display name of the group.

Property	Description
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. Enter a value between 0 and 1. This input field is only visible if the **QER | CalculateRiskIndex** configuration parameter is activated.
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 or not the group is displayed 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 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

- Specifying categories for inheriting SharePoint Online groups on page 111
- SharePoint Online group inheritance based on categories on page 85

Additional tasks for managing SharePoint Online groups

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

Task	Theme
Overview of SharePoint Online Groups	Overview of SharePoint Online groups on page 105
Assign user accounts	Assigning SharePoint Online user accounts directly to an entitlement on page 79
Assign SharePoint Online roles	Assigning SharePoint Online roles to SharePoint Online groups on page 81
Assign system roles	Adding SharePoint Online entitlements to system roles on page 77
Assign business roles	Assigning SharePoint Online entitlements to business roles on page 75
Assign organizations	Assigning SharePoint Online entitlements to departments, cost centers, and locations on page 74
Exclude groups	Effectiveness of SharePoint Online entitlement assignments on page 83
Add to IT Shop	Adding SharePoint Online entitlements to the IT Shop on page 77
Assigning extended properties	Assigning extended properties to SharePoint Online groups on page 106
Synchronize object	Synchronizing single objects on page 34

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.

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 the **Assign extended properties** task.
4. In the **Add assignments** pane, assign extended properties.

   > TIP: In the **Remove assignments** pane, you can remove assigned extended properties.
   >
   > ***To remove an assignment***
   >
   > - Select the extended property and double-click .

5. Save the changes.

For more detailed information about setting up extended properties, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Deleting SharePoint Online groups

To delete a group

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

The group is deleted completely from the One Identity Manager database and from SharePoint Online.

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 107
- Editing master data for SharePoint Online permission levels on page 107
- General master data for SharePoint Online permission levels on page 108
- Deleting SharePoint Online permission levels on page 108
- Synchronizing single objects on page 34

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 master data form, edit the master data for the permission level.
4. Save the changes.

Related topics

- Editing master data for SharePoint Online permission levels on page 107
- Deleting SharePoint Online permission levels on page 108

Editing master data for SharePoint Online permission levels

To edit master data for 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 master data** task.
3. Edit the master data for the permission level.
4. Save the changes.

Related topics

- General master data for SharePoint Online permission levels on page 108
- Creating SharePoint Online permission levels on page 107

General master data for SharePoint Online permission levels

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

Table 26: General master data for a permission level

Property	Description
Permission level	Name of the permissions 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.
Hidden	Specifies whether a SharePoint Online role with the permission level can be assigned to user accounts or groups.

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 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 the 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 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.

To edit site collection master data

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

Detailed information about this topic

- General master data for a SharePoint Online site collection on page 110
- Specifying categories for inheriting SharePoint Online groups on page 111

General master data for 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 27: General master data for 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 definition's default manage level is applied. 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.
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.
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 40

Address data for a SharePoint Online site collection

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

Table 28: 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.

Specifying categories for inheriting SharePoint Online groups

In One Identity Manager, groups can be selectively inherited by user accounts. For this purpose, the groups and the 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 **Position 1** to **Position 31** category positions.

To define a category

1. In the Manager, select the site collection in the **SharePoint Online | Site collections** category.
2. Select the **Change master 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 85

Additional tasks for managing site collections

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

Task	Theme
Overview of the SharePoint Online site collection	Overview of a SharePoint Online site collection on page 112
Define Search Criteria for Employee Assignment	Editing search criteria for automatic employee assignment on page 59
Synchronize object	Synchronizing single objects on page 34

Overview of a SharePoint Online site collection

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.

To edit site properties

1. In the Manager, select the **SharePoint Online | Sites** category.
2. Select the site in the result list. Select the **Change master data** task.

3. Enter the required data on the master data form.
4. Save the changes.

Detailed information about this topic

- General master data for SharePoint Online sites on page 113
- Address data of SharePoint Online sites on page 114
- Design information of SharePoint Online sites on page 115
- Synchronizing single objects on page 34

General master data for SharePoint Online sites

The following master data is displayed for sites.

Table 29: General master data for 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 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	The owner groups belonging to the site.

Property	Description
group	
Visitor group	The visitor group belonging to the site.
Author	Link to user account that created the site.
Request access email	E-mail 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 the assignments of SharePoint Online groups and roles on page 72

Address data of SharePoint Online sites

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

Table 30: Address data for a site

Properties	Description
URL relative to server	URL of the site relative to the server URL.
URL	Absolute site URL.
Master page URL	URL of the master page used for the site.
Alternative master URL	URL to an alternative master page referenced by the site.

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 115

Design information of SharePoint Online sites

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

Table 31: 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 Manager, select **SharePoint Online | Site collections**.
2. Select the site in the result list.
3. Select **Open URL**.

Related topics

- Address data of SharePoint Online sites on page 114

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 master data for SharePoint Online sites on page 113
- Managing the assignments of SharePoint Online groups and roles on page 72

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 107

Editing master data for SharePoint Online roles

To edit SharePoint Online role master data

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

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

Related topics

- General master data for SharePoint Online roles on page 117
- General master data for SharePoint Online permission levels on page 108

General master data for SharePoint Online roles

The following properties are displayed for SharePoint Online roles.

Table 32: General master data for 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.

Property	Description
Description	Text field for additional explanation.
IT Shop	Specifies whether the SharePoint Online role can 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 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 options **IT Shop** 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

- General master data for SharePoint Online permission levels on page 108

Additional tasks for managing SharePoint Online roles

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

Task	Topic
Overview of SharePoint Online Groups	Overview of SharePoint Online roles on page 119
Assign user accounts	Assigning SharePoint Online user accounts directly to an entitlement on page 79
Assign groups	Assigning SharePoint Online groups to SharePoint Online roles on page 82
Assign system roles	Adding SharePoint Online entitlements to system roles on page 77
Assign business roles	Assigning SharePoint Online entitlements to business roles on page 75
Assign organizations	Assigning SharePoint Online entitlements to departments, cost centers, and locations on page 74

Task	Topic
Exclude SharePoint Online roles	Effectiveness of SharePoint Online roles on page 119
Assigning extended properties	Assigning extended properties to SharePoint Online groups on page 106
Synchronize object	Synchronizing single objects on page 34

Overview of SharePoint Online roles

To obtain an overview of a role

1. In the Manager, select the **SharePoint Online | Roles** category.
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 83 can also be used for SharePoint Online roles.

The effect of the assignments is mapped in the `O3SUserHasO3SRLAssign` and `BaseTreeHasO3SRLAssign` tables through the `XIsInEffect` column.

Prerequisites

- The **QER | Structures | Inherite | GroupExclusion** configuration parameter is set.
- Mutually exclusive SharePoint Online roles belong to the same site collection.

To exclude SharePoint Online roles

1. In the Manager, select the **SharePoint Online | Roles** category.
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 no longer exclude each other.
5. Save the changes.

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 procedure. 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 procedure. 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 attesters 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

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

- *One Identity Manager Web Portal User Guide*
- *One Identity Manager Attestation Administration Guide*
- *One Identity Manager Compliance Rules Administration Guide*
- *One Identity Manager Company Policies Administration Guide*
- *One Identity Manager Risk Assessment Administration Guide*

7

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 123.

- Target system types

  Target system types are required for configuring target system comparisons. Tables containing outstanding objects are maintained on target system types.

  For more information, see Post-processing outstanding objects on page 34.

- Account definitions

  One Identity Manager has account definitions for automatically allocating user accounts to employees during working hours. 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 40.

- Server

  In order to handle SharePoint Online -specific processes in One Identity Manager, the synchronization server and its server functions must be declared.

  For more information, see Job server for SharePoint Online-specific process handling on page 123.

- Target system managers

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

Define additional application roles if you want to limit the edit 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 128.

SharePoint Online authentication modes

The following master data is supplied for the authentication mode.

Table 33: 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 though automatic employee assignment.

Job server for SharePoint Online-specific process handling

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

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

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

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 master data** task.
4. Edit the Job server's master data.
5. Select the **Assign server functions** task and specify server functionality.
6. Save the changes.

Detailed information about this topic

- Master data for a Job server on page 124
- Specifying server functions on page 126

Related topics

- System requirements for the synchronization server on page 15

Editing SharePoint Online Job servers

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 master data** task.
4. Edit the Job server's master data.
5. Select the **Assign server functions** task and specify server functionality.
6. Save the changes.

Detailed information about this topic

- Master data for a Job server on page 124
- Specifying server functions on page 126

Master data for a Job server

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

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

Table 34: Job server properties

Property	Meaning
Server	Job server name.
Full server name	Full server name in accordance with DNS syntax. Example: `<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 executing server. The name of the server that exists physically and where the processes are handled. This input is evaluated when the One Identity Manager Service is automatically updated. If the server is handling several queues, the process steps are not supplied until all the queues that are being processed on the same server have completed their automatic update.
Queue	Name of the queue to handle the process steps. Each One Identity Manager Service within the network must have a unique queue identifier. The process steps are requested by the Job queue using this exact queue name. The queue identifier is entered in the One Identity Manager Service configuration file.
Server operating system	Operating system of the server. This input is required to resolve the path name for replicating software profiles. The values **Win32**, **Windows**, **Linux**, and **Unix** are permitted. If no value is specified, **Win32** is used.

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	Specifies whether a One Identity Manager Service is installed on this server. This option is enabled by the `QBM_PJobQueueLoad` procedure the moment the queue is called for the first time. The option is not automatically removed. If necessary, you can reset this option manually for servers whose queue is no longer enabled.
Stop One Identity Manager Service	Specifies whether the One Identity Manager Service has stopped. If this option is set for the Job server, the One Identity Manager Service does not process any more tasks. You can make the service start and stop with the appropriate administrative permissions in the Job Queue Info program. For more detailed information, see the *One Identity Manager Process Monitoring and Troubleshooting Guide*.
No automatic software update	Specifies whether to exclude the server from automatic software updating. NOTE: Servers must be manually updated if this option is set.
Software update running	Specifies whether a software update is currently running.
Last fetch time	Last time the process was collected.
Last timeout check	The time of the last check for loaded process steps with a dispatch value that exceeds the one in the **Common | Jobservice | LoadedJobsTimeOut** configuration parameter.
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 126

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 35: 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	This server automatically updates the software on all the other servers. The server requires a direct connection to the database server that One Identity Manager database is installed on. It can run SQL tasks. The server with the One Identity Manager database installed on it is labeled with this functionality during initial installation of the schema.
SQL processing server	This server can run SQL tasks. Several SQL processing servers can be set up to spread the load of SQL processes. The system distributes the generated SQL processes throughout all the Job servers with this server function.
CSV script server	This server can process CSV files using the `ScriptComponent` process component.
Native 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.
One Identity Manager Service installed	Server on which a One Identity Manager Service is installed.
Primary domain	Primary domain controller.

Server function	Remark
controller	
Profile server	Server for setting up profile directories for user accounts.
SAM synchronization Server	Server for running synchronization with 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

- Master data for a Job server on page 124

Target system managers

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

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

For detailed 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 36: Default application roles for target system managers

User	Tasks
Target system managers	Target system managers must be assigned to the **Target systems | SharePoint Online** application role or a child application role. Users with this application role: • Assume administrative tasks for the target system. • Create, change, or delete target system objects like user accounts or groups. • Edit password policies for the target system. • Prepare groups to add to the IT Shop. • Can add employees who have an other 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**.
3. Select the tenant in the result list.
4. Select the **Change master 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

Appendix A

Configuration parameters for managing SharePoint Online

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

Table 37: Configuration parameter

Configuration parameter	Meaning
TargetSystem | SharePointOnline	Preprocessor relevant configuration parameter for controlling the database model components for the administration of the SharePoint Online target system. If the parameter is set, the target system components are available. Changes to this parameter require the database to be recompiled.
TargetSystem | SharePointOnline | Accounts	Parameter for configuring SharePoint Online user account data.
TargetSystem | SharePointOnline | Accounts | MailTemplateDefaultValues	This configuration parameter contains the mail template used to send notifications if 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	The configuration parameter contains the recipient's default email address for sending notifications about actions in the target system.
TargetSystem | SharePointOnline | MaxFullsyncDuration	This configuration parameter contains the maximum runtime for synchronization. No recalculation of group memberships by the DBQueue Processor can take place during this time. If the maximum runtime is exceeded, group membership are recalculated.
TargetSystem |	This configuration parameter specifies the mode for

Configuration parameter	Meaning
SharePointOnline | PersonAutoDefault	automatic employee assignment for user accounts added to the database outside synchronization.
TargetSystem | SharePointOnline | PersonAutoFullsync	This configuration parameter specifies the mode for automatic employee assignment for user accounts added to or updated in the database through synchronization.

Appendix B

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.

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

Table 38: 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

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

Appendix C

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 39: Methods available for editing objects types

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

About us

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

Contacting us

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

Technical support resources

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

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

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

Index

T

U