One Identity Manager 8.0.4

# Administration Guide for Connecting to SharePoint Online

One Identity Manager Administration Guide for Connecting to SharePoint Online
Updated - September 2019
Version - 8.0.4

# Contents

# 1

# Managing SharePoint Online Environments

Management of SharePoint Online with the One Identity Manager concentrates on mapping site collections, sites and groups in a cloud environment.

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

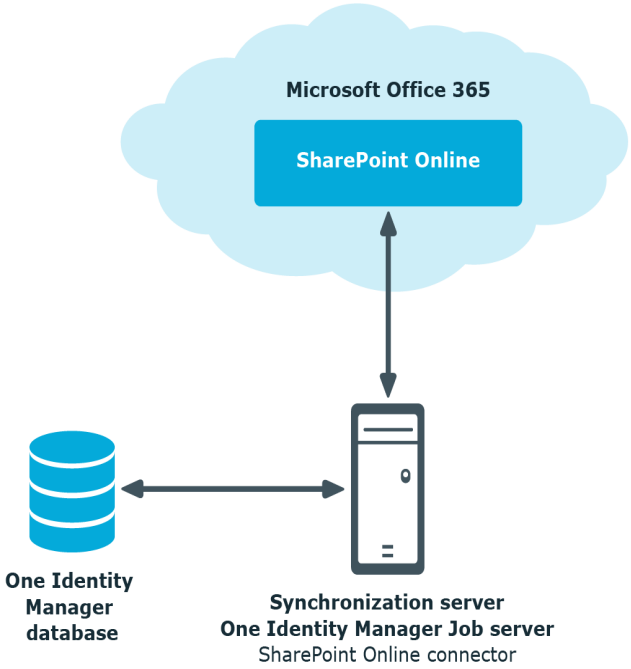
- Appendix: Editing System Objects

# Architecture Overview

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

To access the data in a SharePoint Online organization, the Azure Active Directory target system containing the organization must be synchronized.

**Figure 1: Architecture for synchronization**




# One Identity Manager Users for Managing a SharePoint Online System

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

**Table 1: Users**

| User | Task |
|---|---|
| Target system administrators | Target system administrators must be assigned to the application role **Target system \| Administrators**.<br>Users with this application role:<br>• Administrate application roles for individual target systems types.<br>• Specify the target system manager.<br>• Set up other application roles for target system managers if required.<br>• Specify which application roles are conflicting for target system managers |

| User | Task |
| --- | --- |
| | • Authorize other employee to be target system administrators.<br>• Do not assume any administrative tasks within the target system. |
| Target System Managers | Target system managers must be assigned to the application role **Target systems \| SharePoint Online** or a sub application role.<br>Users with this application role:<br>• Assume administrative tasks for the target system.<br>• Create, change or delete target system objects, like user accounts or groups.<br>• Edit password policies for the target system.<br>• Prepare for adding to the IT Shop.<br>• Configure synchronization in the Synchronization Editor and defines the mapping for comparing target systems and One Identity Manager.<br>• Edit the synchronization's target system types and outstanding objects.<br>• Authorize other employees within their area of responsibility as target system managers and create child application roles if required. |
| One Identity Manager administrator | • Create customized permissions groups for application roles for role-based login to administration tools in the Designer, as required.<br>• Create system users and permissions groups for non-role based login to administration tools, as required.<br>• Enable or disable additional configuration parameters in the Designer, as required.<br>• Create custom processes in the Designer, as required.<br>• Create and configures schedules, as required.<br>• Create and configure password policies, as required. |

# Setting up SharePoint Online Synchronization

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. Synchronization prerequisites are:

- Regular synchronization with the Azure Active Directory system
- The Azure Active Directory tenant is declared in One Identity Manager.
- Administrators for the site collections to be managed are set correctly in the synchronization project.

***To load SharePoint Online objects into the One Identity Manager database***

1. Prepare a user account in the Azure Active Directory tenant with sufficient permissions for synchronization.
2. The One Identity Manager components for managing SharePoint Online systems are available if the configuration parameter "TargetSystem\SharePoint Online" is set.
    - Check whether the configuration parameter is set in the Designer. 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 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 10
- Setting Up the Synchronization Server on page 11
- Creating a Synchronization Project for initial Synchronization of a SharePoint Online Environment on page 14
- Deactivating Synchronization on page 27

- SharePoint Online Synchronization Features on page 21
- Advice for Synchronizing SharePoint Online Site Collections
- Customizing Synchronization Configuration on page 21
- Appendix: Configuration Parameters for Managing SharePoint Online on page 49
- Appendix: Default Project Template for SharePoint Online on page 51

# Advice for Synchronizing SharePoint Online Site Collections

Take the following into account when synchronizing SharePoint Online site collections:

- The mapping for SharePoint Online site collections is part of the SharePoint Online project template. SharePoint Online site collections are synchronized using the SharePoint Online connector.
- You require an administrative user account of the associated Azure Active Directory organization.

  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.

  ***To find the name of the Azure Active Directory organization***

  1. Log in to the Office 365 Admin Portal.
  2. Select **Domains** in the menu on the left, under the category **Setup**.
  3. The organization name is part of the domain name. For example: "<organization name>.onmicrosoft.com".

  User and password are login data of the Azure Active Directory organization administrator's user account. The user name is, in this case, the email address: <user name>@<organization name>.onmicrosoft.com.
- When you initially set up the system connection for SharePoint Online synchronization using the Synchronization Editor, the synchronization user must be one of the site collections administrators to be managed in SharePoint Online. This must also be an Azure Active Directory administrator.
- Synchronization must take place in the following order:
  1. Azure Active Directory
  2. SharePoint Online

# 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 Online | You must provide a user account with the following permissions for full synchronization of SharePoint Online objects with the supplied One Identity Manager default configuration.<br>• Administrator of all the site collections that need to be managed. |
| One Identity Manager Service user account | The user account for the One Identity Manager Service requires access rights to carry out operations at file level (issuing user rights, adding directories and files to be edited).<br>The user account must belong to the group "Domain Users".<br>The user account must have the extended access right "Log on as a service".<br>The user account requires access rights to the internal web service.<br>NOTE: If the One Identity Manager Service runs under the network service (NT Authority\NetworkService), you can issue access rights for the internal web service with the following command line call:<br>`netsh http add urlacl url=http://<IP address>:<port number>/ user="NT AUTHORITY\NETWORKSERVICE"`<br>The user account needs full access to the One Identity Manager Service installation directory in order to automatically update the One Identity Manager.<br>In the default installation the One Identity Manager is installed under:<br>• `%ProgramFiles(x86)%\One Identity` (on 32-bit operating systems)<br>• `%ProgramFiles%\One Identity` (on 64-bit operating systems) |
| User for accessing the One Identity Manager database | The default system user "Synchronization" is available to run synchronization over an application server. |

### Necessary Access Rights Explained

Site collections in which the synchronization user account should be entered as administrator, are:

- All site collections that are going to be synchronized.

***To assign permissions through the Microsoft Online Portal***

1. Navigate to https://portal.microsoftonline.com and log in as administrator.
   This takes you to the Office 365 welcome page.
2. Click the **Administrator** tile to open the Microsoft Office 365 Admin Center.
3. Select **Admin Center | SharePoint** from the menu on the left.
   This takes you to the SharePoint Admin Center.
4. Click **Site collections** in the menu on the left.
5. Click the check box next to a site collect to select it.
6. Select **Manage Administrators** under the **Owner menu** in the toolbar.
7. Verify that the Azure Active Directory user account is entered as site collection administrator.

   - OR -

   Enter the desired Azure Active Directory user account.

   For more detailed information about Azure Active Directory, see the Azure Active Directory documentation from Microsoft.
8. Repeat steps 5 to 7 on all the site collections that will be managed.

# Setting Up the Synchronization Server

To set up synchronization with a SharePoint Online environment a server has to be available that has the following software installed on it:

- Windows operating system

  Following versions are supported:

  - Windows operating system version 8.1. or later
  - Windows Server 2012
  - Windows Server 2012 R2
  - Windows Server 2016
- Microsoft .NET Framework Version 4.5.2 or later

  NOTE: Microsoft .NET Framework version 4.6.0 is not supported.

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

- Windows Management Framework 4.0
- One Identity Manager Service, SharePoint Online connector
    - Install One Identity Manager components with the installation wizard.
        1. Select the option **Select installation modules with existing database**.
        2. Select the machine role **Server | Job server | 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 synchronization server must be declared as a Job server in One Identity Manager.

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

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

- Setting up a Job server.
- Specifying machine roles and server function for the Job server.
- Remote installation of One Identity Manager Service components corresponding to the machine roles.
- Configures the One Identity Manager Service.
- Starts the One Identity Manager Service.

NOTE: The program executes 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 install and configure the One Identity Manager Service remotely on a server***

1. Start the program Server Installer on your administrative workstation.
2. Enter valid data for connecting to One Identity Manager on the **Database connection** page and click **Next**.
3. Specify on which server you want to install the One Identity Manager Service on the **Server properties** page.
    a. Select a job server in the **Server** menu.

    - OR -

    Click **Add** to add a new job server.

b. Enter the following data for the Job server.

**Table 3: Job Servers Properties**

| Property | Description |
|---|---|
| Server | Name of the Job servers. |
| Queue | Name of 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 exactly this queue name. The queue identifier is entered in the One Identity Manager Service configuration file. |
| Full server name | Full name of the server in DNS syntax.<br>Example:<br>`<name of server>.<fully qualified domain name>` |

NOTE: Use the **Advanced** option to edit other Job server properties. You can use the Designer to change properties at a later date.

4. Specify which job server roles to include in One Identity Manager on the **Machine role** page. Installation packages to be installed on the Job server are found depending on the selected machine role.

   Select at least the following roles:

   - SharePoint Online

5. Specify the server's functions in One Identity Manager on the **Server functions** page. One Identity Manager processes are handled depending on the server function.

   The server's functions depend on which machine roles you have selected. You can limit the server's functionality further here.

   Select the following server functions:

   - SharePoint Online connector

6. Check the One Identity Manager Service configuration on the **Service settings** page.

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

7. To configure remote installations, click **Next**.
8. Confirm the security prompt with **Yes**.
9. Select the directory with the install files on the **Select installation source** page.
10. Select the file with the private key on the page **Select private key file**.

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

11. Enter the service's installation data on the **Service access** page.

**Table 4: Installation Data**

| Data | Description |
|---|---|
| Computer | Server on which to install and start the service from.<br>***To select a server***<br>• Enter the server name.<br>- OR -<br>• Select a entry from the list. |
| Service account | One Identity Manager Service user account data.<br>***To enter a user account for the One Identity Manager Service***<br>• Enter user account, password and password confirmation.<br>The One Identity Manager Service farm's server farm account must be used as user account for SharePoint. |
| Installation account | Data for the administrative user account to install the service.<br>***To enter an administrative user account for installation***<br>• Enable **Advanced**.<br>• Enable the option **Current user**.<br>This uses the user account of the current user.<br>- OR -<br>• Enter user account, password and password confirmation. |

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: The is entered with the name "One Identity Manager Service" in the server's service administration.

# Creating a Synchronization Project for initial Synchronization of a SharePoint Online Environment

Use the Synchronization Editor to configure synchronization between the One Identity Manager database and SharePoint Online. 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.

## Prerequisites for Setting Up a Synchronization Project

- Regular synchronization with the Azure Active Directory system
- The Azure Active Directory tenant is declared in One Identity Manager.
- Administrators for the site collections to be managed are set correctly in the synchronization project.

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

**Table 5: Information Required for Setting up a Synchronization Project**

| Data | Explanation |
|---|---|
| User account and password for logging in | User account and password for logging in to SharePoint Online.<br>Example:<br>`<user name of the synchronization user>@yourorganization.onmicrosoft.com`<br>Make a user account available with sufficient permissions. For more information, see Users and Permissions for Synchronizing with SharePoint Online on page 10. |
| Synchronization server for SharePoint Online | The One Identity Manager Service with the SharePoint Online connector must be installed on the synchronization server.<br>**Table 6: Additional Properties for the Job Server**<br>**Property** / **value**<br>Server function: SharePoint Online connector<br>Machine role: Server/Jobserver/SharePointOnline<br>For more information, see Setting Up the Synchronization Server on page 11. |
| One Identity Manager Database Connection Data | SQL Server:<br>• Database server<br>• Database<br>• Database user and password<br>• Specifies whether Windows authentication is used. |

| Data | Explanation |
| --- | --- |
| | This type of authentication is not recommended. If you decide to use it anyway, ensure that your environment supports Windows authentication.<br><br>Oracle:<br><br>• Species whether access is direct or through the Oracle client<br><br>Which connection data is required, depends on how this option is set.<br><br>• Database server<br>• Oracle instance port<br>• Service name<br>• Oracle database user and password<br>• Data source (TNS alias name from `TNSNames.ora`) |
| Remote connection server | To configure synchronization with a target system, One Identity Manager must load the data from the target system. One Identity Manager communicates directly with target system to do this. Sometimes direct access from the workstation on which the Synchronization Editor is installed is not possible, because of the firewall configuration, for example, or because the workstation does not fulfill the necessary hardware and software requirements. , you can set up a remote connection.<br><br>The remote connection server and the workstation must be in the same Active Directory domain.<br><br>Remote connection server configuration:<br><br>• One Identity Manager Service is started<br>• `RemoteConnectPlugin` is installed<br>• SharePoint Online connector is installed<br><br>The remote connection server must be declared as a Job server in One Identity Manager. The Job server name is required.<br><br>TIP: The remote connection server requires the same configuration (with respect to the installed software) as the synchronization server. Use the synchronization as remote connection server at the same time, by simply installing the `RemoteConnectPlugin` as well.<br><br>For more detailed information about setting up a remote connection, see the One Identity Manager Target System Synchronization Reference Guide. |

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

- In default mode
- Started from the launchpad

Additional settings can be made if the project wizard is run in expert mode or is started directly from the Synchronization Editor. Follow the project wizard instructions through these steps.

### *To set up initial synchronization project for SharePoint Online*

1. Start the Launchpad and log on 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 entry **SharePoint Online target system type**. Click **Run**.

   This starts the Synchronization Editor's project wizard.

3. Specify how the One Identity Manager can access the target system on the **System access** page.

   - If you have access from the workstation from which you started the Synchronization Editor, do not set anything.
   - If you do not have access from the workstation from which you started the Synchronization Editor, you can set up a remote connection.

     In this case, set the option **Connect using remote connection server** and select, under **Job server**, the server you want to use for the connection.

4. Enter login data on the **Enter connection credentials** page to connect to SharePoint Online.

   **Table 7: Connection Parameters for SharePoint Online**

   | Property | Description |
   |---|---|
   | Organization name | Name of the organization. |
   | User name (user@-domain) | Fully qualified name (FQDN) of the user account for logging in.<br>Example:<br>`<user>@<domain.com>`<br>`sync.user@yourorganization.onmicrosoft.com`<br>`The name of your organization is preset.` |
   | Password | User account's password. |

   Click **Next**.

5. Then click **Finished** to return to the project wizard.

6. 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.
7. Specify how system access should work on the page **Restrict target system access**. You have the following options:

**Table 8: Specifying Target System Access**

| Option | Meaning |
|---|---|
| Read-only access to target system. | Specifies whether a synchronization workflow should be set up to initially load the target system into the One Identity Manager database.<br>The synchronization workflow has the following characteristics:<br>• Synchronization is in the direction of "One Identity Manager".<br>• Processing methods in the synchronization steps are only defined in synchronization direction "One Identity Manager". |
| Changes are also made to the target system. | Specifies whether a provisioning workflow should be set up in addition to the synchronization workflow to initially load the target system.<br>The provisioning workflow displays the following characteristics:<br>• Synchronization in the direction of the "target system"<br>• Processing methods are only defined in the synchronization steps in synchronization direction "target system".<br>• Synchronization steps are only created for such schema classes whose schema types have write access. |

8. Select the synchronization server to execute synchronization on the **Synchronization server** page.

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

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

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

     NOTE: Ensure that this server is set up as the synchronization server after saving the synchronization project.

9. Click **Finish** to complete the project wizard.

   The synchronization project is created, saved and enabled immediately.

   NOTE: If the synchronization project is not going to be executed immediately, disable the option **Activate and save the new synchronization project automatically**.

   In this case, save the synchronization project manually before closing the Synchronization Editor.

***To configure the content of the synchronization log***

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

   NOTE: Certain content create a lot of log data.

   The synchronization log should only contain the data necessary for error analysis and other evaluations.

6. Click **OK**.

***To synchronize on a regular basis***

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

***To start initial synchronization manually***

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

NOTE: Refer to the recommendations for setting up synchronization described in SharePoint Online Synchronization Features on page 21.

## Related Topics

- Setting Up the Synchronization Server on page 11
- Users and Permissions for Synchronizing with SharePoint Online on page 10

# Show 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. Select the category **Logs**.
2. Click ▶ in the navigation view toolbar.

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

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

***To display a provisioning log.***

1. Select the category **Logs**.
2. Click ⚡ in the navigation view toolbar.

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

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

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

Synchronization logs are stored for a fixed length of time.

***To modify the retention period for synchronization logs***

- In the Designer, set the "DPR\Journal\LifeTime" configuration parameter and enter the maximum retention time.

# SharePoint Online Synchronization Features

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

### Multiple organizations are not supported

By default, there is only one Azure Active Directory tenant per synchronization project. This tenant corresponds to the organization for logging in to Microsoft Office 365. The target system schema in One Identity Manager cannot be extended.

### Target system scope settings

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, which have the synchronization user, used in the SharePoint Online administration interface, entered as administrator in the site collections. 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 category **Configuration | Target systems**.
3. Select the **Scope** view.
4. Click **Edit scope**. A list of site collections appears on the right-hand side.
5. Select only those site collections in the list, whose synchronization user corresponds to the administrator in SharePoint Online.

### Related Topics

- Users and Permissions for Synchronizing with SharePoint Online on page 10

# Customizing Synchronization Configuration

You have used the Synchronization Editor to set up a synchronization project for initial synchronization with SharePoint Online. You can use this 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 in SharePoint Online.

You must customize the synchronization configuration in order to compare the One Identity Manager database with the SharePoint Online regularly and to synchronize changes.

- You can use variables to create generally applicable synchronization configurations which contain the necessary information about the synchronization objects when synchronization starts. Variables can be implemented in base objects, schema classes or processing method, for example.
- To specify which SharePoint Online objects and database object are included in synchronization, edit the scope of the target system connection and the One Identity Manager database connection. To prevent data inconsistencies, define the same scope in both systems. If no scope is defined, all objects will be synchronized.
- Update the schema in the synchronization project, if the One Identity Manager schema or target system schema has changed. Then you can add the changes to the mapping.

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

- The moment another synchronization is started with the same start up configuration, the running synchronization process is stopped and given the status, "Frozen". An error message is written to the One Identity Manager Service log file.
- If another synchronization is started with another start up configuration, that addresses same target system, it may lead to synchronization error or loss of data. Specify One Identity Manager behavior in this case, in the start up configuration. Group start up configurations with the same start up behavior.

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

### Detailed information about this topic

- How to Configure SharePoint Online Synchronization on page 22
- Updating Schemas on page 23

# How to Configure SharePoint Online Synchronization

The synchronization project for initial synchronization provides a workflow for initial loading of objects (initial synchronization) and one for provisioning object modifications from the One Identity Manager database to the target system (provisioning). You also

require a workflow with synchronization in the direction of the "target system" to use One Identity Manager as the master system for synchronization.

***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 . Create new maps if required.
3. Create a new workflow with the workflow wizard.

   This adds a workflow for synchronizing in the direction of the target system.
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 loading 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 compressing 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:
  - Activating the synchronization project
  - Synchronization project initial save
  - Compressing a schema

***To update a system connection schema***

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

   - OR -

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

   This reloads the schema data.

***To edit a mapping***

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

   Opens the Mapping Editor. For more detailed information about editing mappings, see 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.

# 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.

Objects marked as outstanding:

- Cannot be edited in One Identity Manager.
- Are ignored by subsequent synchronization.
- Must be post-processed separately in One Identity Manager.

Start target system synchronization to do this.

***To post-process outstanding objects***

1. Select the table whose outstanding objects you want to edit in the navigation view.

   This opens the target system synchronization form. All objects are shown here that are marked as outstanding.

   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**.

2. Select the objects you want to rework. Multi-select is possible.
3. Click one of the following icons in the form toolbar to execute the respective method.

**Table 9: Methods for handling outstanding objects**

| Icon | Method | Description |
|---|---|---|
| | Delete | The object is immediately deleted in the One Identity Manager. Deferred deletion is not taken into account. The "outstanding" label is removed from the object.<br>Indirect memberships cannot be deleted. |
| | Publish | The object is added in the target system. The "outstanding" label is removed from the object.<br>The method triggers the event "HandleOutstanding". This runs a target system specific process that triggers the provisioning process for the object.<br>Prerequisites:<br>• The table containing the object can be published.<br>• The target system connector has write access to the target system. |
| | Reset | The "outstanding" label is removed from the object. |

4. 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***

- Deactivate in the form toolbar.

***To add custom tables to the target system synchronization.***

1. Select the category **SharePoint Online | Basic configuration data | Target system types**.
2. Select the target system type SharePoint Online in the result list.
3. Select **Assign synchronization tables** in the task view.
4. Assign custom tables whose outstanding objects you want to handle in **Add assignments**.
5. Save the changes.
6. Select **Configure tables for publishing**.

7. Select custom tables whose outstanding objects can be published in the target system and set the option **Publishable**.
8. Save the changes.

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 option **Connection is read only** must no be set for the target system connection.

# Configuring Memberships Provisioning

Memberships, for example, 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 will probably be overwritten. This behavior can occur under the following conditions:

- Memberships are saved in the target system as an object property in list form.
- Memberships can be modified in either of the connected systems.
- A provisioning workflow and provisioning processes are set up.

If a membership in One Identity Manager changes, the complete list of members is transferred to the target system by default. Memberships, previously added to the target system are removed by this; 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. Start the Manager.
2. Select the category **SharePoint Online | Basic configuration data | Target system types**.
3. Select **Configure tables for publishing**.
4. Select the assignment tables for which you want to allow separate provisioning. Multi-select is possible.
    - The option can only be set for assignment tables whose base table has a `XDateSubItem` or a `CCC_XDateSubItem`.
    - Assignment tables, which are grouped together in a virtual schema property in the mapping, must be labeled identically.
5. Click **Enable merging**.
6. Save the changes.

For each assignment table labeled like this, the changes made in the 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 the members list does not get entirely overwritten.

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.

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

# Help for Analyzing Synchronization Issues

You can generate a report for analyzing problems which occur during synchronization, for example, insufficient performance. The report contains information such as:

- Consistency check results
- Revision filter settings
- Scope applied
- Analysis of the synchronization buffer
- Object access times in the One Identity Manager database and in the target system

***To generate a synchronization analysis report***

1. Select the menu **Help | Generate synchronization analysis report** and answer the security prompt with **Yes**.

   The report may take a few minutes to generate. It is displayed in a separate window.
2. Print the report or save it in one of the available output formats.

# Deactivating Synchronization

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

***To prevent regular synchronization***

- 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 loaded synchronization project***

1. Select **General** on the start page.
2. Click **Deactivate project**.

## Related Topics

- Creating a Synchronization Project for initial Synchronization of a SharePoint Online Environment on page 14

# 3

# Base Data for Managing SharePoint Online

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

- 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. You can find an overview of all configuration parameters in the category **Base data | General | Configuration parameters** in the Designer.

  For more information, see Appendix: Configuration Parameters for Managing SharePoint Online on page 49.

- 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 have a user account in the target system, a new user account is created. This is done by assigning account definitions to an employee using the integrated inheritance mechanism followed by process handling.

  For more information, see Setting Up Account Definitions on page 30.

- 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 24.

- Target System Managers

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

Define other application roles, if you want to limit target system managers' access permissions to individual . The application roles must be added under the default application role.

For more information, see Target System Managers on page 46.

# Setting Up 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 have a user account in the target system, a new user account is created. This is done by assigning account definitions to an employee using the integrated inheritance mechanism followed by process handling.

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

The following steps are required to implement an account definition:

- Creating an Account Definition
- Setting Up Manage Levels
- Creating a Formatting Rule for IT Operating Data
- Determining IT Operating Data
- Assigning Account Definitions to Employees
- Assigning Account Definitions to a Target System

# Creating an Account Definition

***To create a new account definition***

1. Select the category **SharePoint Online | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list. Select **Change master data** in the task view.

   - OR -

   Click  in the result list toolbar.
3. Enter the account definition's master data.
4. Save the changes.

### Detailed information about this topic

- Master Data for an Account Definition on page 31

### Related Topics

Appendix: Editing System Objects

# Master Data for an Account Definition

Enter the following data for an account definition:

**Table 10: Master Data for an Account Definition**

| Property | Description |
|---|---|
| Account definition | Account definition name. |
| User account table | Table in the One Identity Manager schema which maps user accounts. |
| Target System | Target system to which the account definition applies. |
| Required account definition | Required account definitions. Define the dependencies between . When this is requested or assigned, the required is automatically requested or assigned with it.<br>Select an Azure Active Directory account definition from the menu for SharePoint Online. |
| Description | Spare text box 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 property is only visible when the configuration parameter QER\CalculateRiskIndex is set.<br>For more detailed information, see the One Identity Manager Risk Assessment Administration Guide. |
| Service item | Service item through which you can request the in the IT Shop. Assign an existing service item or add a new one. |
| IT Shop | Specifies whether the can be requested through the IT Shop. The can be ordered by an employee over the Web Portal and distributed using a defined approval process. |
| Only for use in IT Shop | Specifies whether the can only be requested through the IT Shop. The can |

| Property | Description |
|---|---|
| | be ordered by an employee over the Web Portal and distributed using a defined approval process. This means, the cannot be directly assigned to roles outside the IT Shop. |
| Automatic assignment to employees | Specifies whether the is assigned automatically to all internal employees. The is assigned to every employee not marked as external, on saving. New employees automatically obtain this as soon as they are added.<br>Disable this option to remove automatic assignment of the to all employees. The cannot be reassigned to employees from this point on. Existing assignments remain intact. |
| Retain account definition if permanently disabled | Specifies the account definition assignment to permanently disabled employees.<br>Option set: the account definition assignment remains in effect. The user account stays the same.<br>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.<br>Option set: the account definition assignment remains in effect. The user account stays the same.<br>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.<br>Option set: the account definition assignment remains in effect. The user account stays the same.<br>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 .<br>Option set: the account definition assignment remains in effect. The user account stays the same.<br>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. |

# Setting Up Manage Levels

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.

The One Identity Manager supplies a default configuration for manage levels:

- Unmanaged

  User accounts with a manage level of "Unmanaged" become linked to an employee but do not inherit any other 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 a manage level of "Full managed" inherit specific properties from the assigned employee.

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

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

Specify the effect of temporarily or permanently disabling, deleting or the security risk of an employee on its user accounts and group memberships for each manage level.

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

***To assign manage levels to an account definition***

1. Select the category **SharePoint Online | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list.
3. Select **Assign manage level** in the task view.

4. Assign manage levels in **Add assignments**.

   - OR -

   Remove assignments to manage levels in **Remove assignments**.
5. Save the changes.

IMPORTANT: The manage level "Unmanaged" is assigned automatically when an account definition is assigned and cannot be removed.

***To edit a manage level***

1. Select the category **SharePoint Online | Basic configuration data | Account definitions | Manage levels**.
2. Select the manage level in the result list. Select **Change master data**.

   - OR -

   Click in the result list toolbar.
3. Edit the manage level's master data.
4. Save the changes.

### Related Topics

- Master Data for a Manage Level on page 34

# Master Data for a Manage Level

Enter the following data for a manage level.

**Table 11: Master Data for a Manage Level**

| Property | Description |
|---|---|
| Manage level | Name of the manage level. |
| Description | Spare text box for additional explanation. |
| IT operating data overwrites | Specifies whether user account data formatted from IT operating data is automatically updated. Permitted values are:<br>Never: Data is not updated<br>always: Data is always updated<br>Only initially: Data is only initially determined. |
| Retain groups if temporarily disabled | Specifies whether user accounts of temporarily disabled employees retain their group memberships. |

| Property | Description |
|---|---|
| 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 locked user accounts retain their group memberships. |

# Creating a Formatting Rule 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.

***To create a mapping rule for IT operating data***

1. Select the category **SharePoint Online | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list.
3. Select **Edit IT operating data mapping** in the task view and enter the following data.

**Table 12: Mapping rule for IT operating data**

| Property | Description |
|---|---|
| Column | User account property for which the value is set. |
| Source | Specifies which roles to use in order to find the user account properties. |

| Property | Description |
|---|---|
| | You have the following options:<br>• Primary department<br>• Primary location<br>• Primary cost center<br>• Primary business roles<br>NOTE: Only use the primary business role if the Business Roles Module is installed.<br>• Empty<br>If you select a role, you must specify a default value and set the option **Always use default value**. |
| 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. Use the mail template "Employee - new user account with default properties created". To change the mail template, modify the configuration parameter "TargetSystem\SharePointOnline\Accounts\MailTemplateDefaultValues". |

4. Save the changes.

### Related Topics

- Determining IT Operating Data on page 36

# Determining IT Operating Data

In order for an employee to create user accounts with the manage level "Full managed", the necessary IT operating data must be determined. The operating data required to automatically supply an employee with IT resources is shown in the departments, locations, cost centers, and business roles. An employee is assigned to one primary location, one primary department, one primary cost center or one primary business role. 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 A. In addition, certain employees in department A obtain administrative user accounts in the 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 A. Specify the property "Department" 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 A. This IT operating data is used for standard user accounts. In addition, specify the effective account definition B IT operating data for department A. This IT operating data is used for administrative user accounts.

***To specify IT operating data***

1. Select the role in the category **Organizations** or **Business roles**.
2. Select **Edit IT operating data** in the task view and enter the following data.

**Table 13: IT Operating Data**

| Property | Description |
|---|---|
| Organization/Business role | Department, cost center, location or business role for which the IT operating data is valid. |
| Effects on | IT operating data application scope. The IT operating data can be used for a target system or a defined account definition.<br>***To specify an application scope***<br>a. Click → next to the text box.<br>b. Select the table under **Table**, which maps the target system or the table `TSBAccountDef` for an account definition.<br>c. Select the concrete target system or concrete account definition under **Effects on**.<br>d. Click **OK**. |
| Column | User account property for which the value is set.<br>Columns using the script template `TSB_ITDataFromOrg` in their template are listed. |
| Value | Concrete value which is assigned to the user account property. |

3. Save the changes.

### Related Topics

- Creating a Formatting Rule for IT Operating Data on page 35

# Modifying IT Operating Data

If IT operating data changes, you must transfer these 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 the effect of a change to the IT operating data has on the existing user accounts. You can decide whether the change is transferred to the database in the case of each affected column in each affected database.

***Prerequisites***

- The IT operating data of a department, cost center, business role or a location was changed.

  - OR -

- The default values in the IT operating data template were modified for an account definition.

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

***To execute the template***

1. Select the category **SharePoint Online | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list.
3. Select **Execute templates** in the task view

   This displays a list of all user account, which are created through the selected account definition and whose properties are changed by modifying the IT operating data.

   | | |
   |---|---|
   | Old value | Current value of the object property. |
   | New value | Value applied to the object property after modifying the IT operating data. |
   | Selection | Specifies whether the modification is applied 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. A department manager can then request user accounts from the Web Portal for his staff. It is also possible to add account definitions to system roles. These system roles can be assigned to employees through hierarchical roles or directly or added as products in the IT Shop.

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. You have to alter the user account manage level afterwards in this case.

### Prerequisites for indirect assignment of account definitions to employees

- Assignment of employees and account definitions is permitted for role classes (department, cost center, location or business role).

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 40
- Assigning Account Definitions to Business Roles on page 40
- Assigning Account Definitions to all Employees on page 41
- Assigning Account Definitions Directly to Employees on page 42
- Assigning Account Definitions to a Target System on page 44

# Assigning Account Definitions to Departments, Cost Centers and Locations

***To add account definitions to hierarchical roles***

1. Select the category **SharePoint Online | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list.
3. Select **Assign organizations**.
4. Assign organizations in **Add assignments**.
   - Assign departments on the **Departments** tab.
   - Assign locations on the **Locations** tab.
   - Assign cost centers on the **Cost center** tab.

   - OR -

   Remove the organizations from **Remove assignments**.
5. Save the changes.

## Related Topics

- Assigning Account Definitions to Business Roles on page 40
- Assigning Account Definitions Directly to Employees on page 42

# Assigning Account Definitions to Business Roles

Installed Modules: Business Roles Module

***To add account definitions to hierarchical roles***

1. Select the category **SharePoint Online | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list.
3. Select **Assign business roles** in the task view.
4. Assign business roles in **Add assignments**.

   - OR -

   Remove business roles in **Remove assignments**.
5. Save the changes.

### Related Topics

- Assigning Account Definitions to Departments, Cost Centers and Locations on page 40
- Assigning Account Definitions to all Employees on page 41
- Assigning Account Definitions Directly to Employees on page 42

## Assigning Account Definitions to all Employees

***To assign an account definition to all employees***

1. Select the category **SharePoint Online | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list.
3. Select **Change master data** in the task view.
4. Set the option **Automatic assignment to employees** on the **General** tab.

   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 the option **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.

### Related Topics

- Assigning Account Definitions to Departments, Cost Centers and Locations on page 40
- Assigning Account Definitions to Business Roles on page 40
- Assigning Account Definitions Directly to Employees on page 42

# Assigning Account Definitions Directly to Employees

***To assign an account definition directly to employees***

1. Select the category **SharePoint Online | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list.
3. Select **Assign to employees** in the task view.
4. Assign employees in **Add assignments**.

   - OR -

   Remove employees from **Remove assignments**.
5. Save the changes.

## Related Topics

- Assigning Account Definitions to Departments, Cost Centers and Locations on page 40
- Assigning Account Definitions to Business Roles on page 40
- Assigning Account Definitions to all Employees on page 41

# Assigning Account Definitions to System Roles

Installed Modules: System Roles Module

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

***To add account definitions to a system role***

1. Select the category **SharePoint Online | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list.
3. Select **Assign system roles in the task view**.
4. Assign system roles in **Add assignments**.

   - OR -

   Remove assignments to system roles in **Remove assignments**.
5. Save the changes.

# Adding Account Definitions in the IT Shop

A 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.
- If the account definition is only assigned to employees using IT Shop assignments, you must also set the option **Only for use in IT Shop**. 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. Select an account definition in the result list.
2. Select **Add to IT Shop** in the task view.
3. Assign the account definition to the IT Shop shelf in **Add assignments**
4. Save the changes.

***To remove an account definition from individual IT Shop shelves***

1. Select an account definition in the result list.
2. Select **Add to IT Shop** in the task view.
3. Remove the account definition from the IT Shop shelves in **Remove assignments**.
4. Save the changes.

***To remove an account definition from all IT Shop shelves***

1. Select an account definition in the result list.
2. Select **Remove from all shelves (IT Shop)** in the task view.
3. Confirm the security prompt with **Yes**.
4. Click **OK**.

   The account definition is removed from all shelves by the One Identity Manager Service. All requests and assignment requests with this account definition are canceled in the process.

For more detailed information about request from company resources through the IT Shop, see the One Identity Manager IT Shop Administration Guide.

## Related Topics

- Master Data for an Account Definition on page 31
- Assigning Account Definitions to Departments, Cost Centers and Locations on page 40

- Assigning Account Definitions to Business Roles on page 40
- Assigning Account Definitions Directly to Employees on page 42
- Assigning Account Definitions to System Roles on page 42

# Assigning Account Definitions to a Target System

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

- 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 (state "Linked") 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. Select the site collection in the category **SharePoint Online | Site collections**.
2. Select **Change master data** in the task view.
3. Select the account definition for user accounts from **Account definition (initial)**.
4. Save the changes.

### Related Topics

- Assigning Account Definitions to Employees on page 39

# Deleting an Account Definition

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

NOTE: If an account definition is deleted, the user accounts arising from this account definition are deleted.

***To delete an account definition***

1. Remove automatic assignments of the account definition from all employees.
    a. Select the category **SharePoint Online | Basic configuration data | Account definitions | Account definitions**.
    b. Select an account definition in the result list.

c. Select **Change master data** in the task view.

d. Disable the option **Automatic assignment** to employees on the **General** tab.

e. Save the changes.

2. Remove direct assignments of the account definition to employees.

a. Select the category **SharePoint Online | Basic configuration data | Account definitions | Account definitions**.

b. Select an account definition in the result list.

c. Select **Assign to employees** in the task view.

d. Remove employees from **Remove assignments**.

e. Save the changes.

3. Remove the account definition's assignments to departments, cost centers and locations.

a. Select the category **SharePoint Online | Basic configuration data | Account definitions | Account definitions**.

b. Select an account definition in the result list.

c. Select **Assign organizations**.

d. Remove the account definition's assignments to departments, cost centers and locations in **Remove assignments**.

e. Save the changes.

4. Remove the account definition's assignments to business roles.

a. Select the category **SharePoint Online | Basic configuration data | Account definitions | Account definitions**.

b. Select an account definition in the result list.

c. Select **Assign business roles** in the task view.

Remove business roles from **Remove assignments**.

d. Save the changes.

5. If the account definition was requested through the IT Shop, it must be canceled and removed from all IT Shop shelves. For more detailed information, see the One Identity Manager IT Shop Administration Guide.

6. Remove the account definition assignment as required account definition for another account definition. As long as the account definition is required for another account definition, it cannot be deleted. Check all the account definitions.

a. Select the category **SharePoint Online | Basic configuration data | Account definitions | Account definitions**.

b. Select an account definition in the result list.

c. Select **Change master data** in the task view.

d. Remove the account definition from the **Required account definition** menu.

e. Save the changes.

7. Remove the account definition's assignments to target systems.
    a. Select **Change master data** in the task view.
    b. Remove the assigned account definitions on the **General tab**.
    c. Save the changes.
8. Delete the account definition.
    a. Select the category **SharePoint Online | Basic configuration data | Account definitions | Account definitions**.
    b. Select an account definition in the result list.
    c. Click , to delete the account definition.

# Target System Managers

For more detailed information about implementing and editing application roles, see the One Identity Manager Application Roles Administration Guide.

### Implementing Application Roles for Target System Managers

1. The One Identity Manager administrator assigns employees to be target system managers.
2. These target system managers add employees to the default application role for target system managers.

   The default application role target system managers are entitled to edit all SharePoint Online site collections in One Identity Manager.
3. Target system managers can authorize more employees as target system managers, within their scope of responsibilities and create other child application roles and assign individual tenants.

**Table 14: Default Application Roles for Target System Managers**

| User | Task |
|---|---|
| Target System Managers | Target system managers must be assigned to the application role **Target systems | SharePoint Online** or a sub application role.<br>Users with this application role:<br>• Assume administrative tasks for the target system.<br>• Create, change or delete target system objects, like user accounts or groups.<br>• Edit password policies for the target system.<br>• Prepare for adding to the IT Shop.<br>• Configure synchronization in the Synchronization Editor and defines |

| User | Task |
| --- | --- |
| | the mapping for comparing target systems and One Identity Manager.<br>• Edit the synchronization's target system types and outstanding objects.<br>• 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 One Identity Manager administrator (application role **Base role | Administrators**)
2. Select the category **One Identity Manager Administration | Target systems | Administrators**.
3. Select **Assign employees** in the task view.
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 yourself into the Manager as target system administrator (application role **Target systems | Administrator**).
2. Select the category **One Identity Manager Administration | Target systems | SharePoint Online**.
3. Select **Assign employees** in the task view.
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. Login to the Manager as target system manager.
2. Select the application role in the category **SharePoint Online | Basic configuration data | Target system managers**.
3. Select **Assign employees** in the task view.
4. Assign the employees you want and save the changes.

***To define target system managers for individual .***

1. Login to the Manager as target system manager.
2. Select the category **SharePoint Online | Tenants**.
3. Select the tenant from the result list.
4. Select **Change master data** in the task view.

5. Select the application role on the **General** tab in the **Target system manager** menu.

   - OR -

   Click next to the **Target system manager** menu to create a new application role.

   - Enter the application role name and assign the parent application role **Target system | SharePoint Online**.
   - Click **OK** to add the new application role.

6. Save the changes.
7. Assign the application role to employees, who are authorized to edit the tenant in One Identity Manager.

## Related Topics

- One Identity Manager Users for Managing a SharePoint Online System on page 6

# Appendix: Configuration Parameters for Managing SharePoint Online

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

**Table 15: Configuration Parameter for Managing a SharePoint Online Environment**

| Configuration Parameter | Meaning |
|---|---|
| TargetSystem\SharePointOnline | Preprocessor relevant configuration parameter for controlling the database model components for the administration of the target system SharePoint Online. If the parameter is set, the target system components are available. Changes to the parameter require recompiling the database. |
| TargetSystem\SharePointOnline\Accounts | This configuration parameter permits configuration of recipient 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. Use the mail template "Employee - new user account with default properties created". |
| 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 |

| Configuration Parameter | Meaning |
| --- | --- |
| | 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\SharePointOnline\ PersonAutoDefault | This configuration parameter specifies the mode for 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: Default Project Template for SharePoint Online

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

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

The template uses mappings for the following schema types.

**Table 16: 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 |
|---|---|
| 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: 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 17: Methods available for editing objects types**

| Type | Read | Insert | 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 or other inquiries, such as licensing, support, and renewals, visit https://www.oneidentity.com/company/contact-us.aspx or call +1-800-306-9329.

## 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

## S



## T



## U