One Identity Manager 8.1.5

Administration Guide for Connecting to Exchange Online

One Identity Manager Administration Guide for Connecting to Exchange Online
Updated - 09 July 2021, 12:50
Version - 8.1.5

Contents

1

Managing Exchange Online environments

The key aspects of administrating an Exchange Online system with One Identity Manager are local mapping of mailboxes, email users, email contacts, mail-enabled distribution groups, and Office 365 groups from a cloud environment.

The system information for the Exchange 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 Exchange Online structure, see the Exchange Online documentation from Microsoft.

Related topics

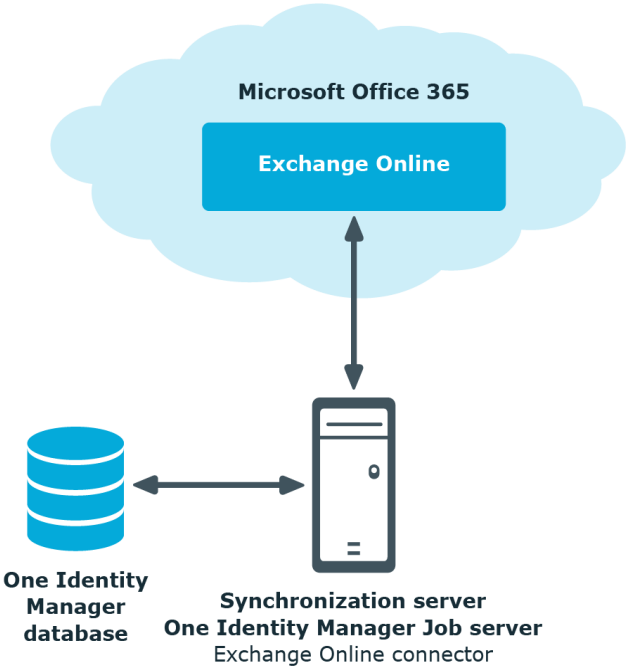
- Editing system objects

Architecture overview

To access Exchange Online organizational data, the Exchange Online connector is installed on a synchronization server. The synchronization server ensures data is compared between the One Identity Manager database and Exchange Online. The Exchange Online connector is part of the Exchange Online Module and responsible for communicating with the Microsoft Office 365 subscriptions of Exchange Online in the cloud. The Exchange Online PowerShell V2 module is used to access Exchange Online data.

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

Figure 1: Architecture for synchronization



One Identity Manager users for managing Exchange Online

The following users are used for setting up and administration of Exchange 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 if required. • Specify which application roles for target system managers are mutually exclusive. • Authorize other employees to be target system

User	Tasks
	administrators. • Do not assume any administrative tasks within the target system.
Target system managers	Target system managers must be assigned to the **Target systems | Exchange 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.

2

Setting up Exchange Online synchronization

One Identity Manager supports synchronization with Exchange Online.

The One Identity Manager Service is responsible for synchronizing data between the One Identity Manager database and Exchange Online. Synchronization prerequisites are:

- Synchronization of the Azure Active Directory system is carried out regularly.
- The Azure Active Directory tenant is declared in One Identity Manager.

To load Exchange 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.
2. One Identity Manager parts for managing Exchange Online systems are available if the **TargetSystem | AzureAD | ExchangeOnline** 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 Exchange Online on page 9
- Installing the Exchange Online PowerShell V2 module on page 11
- Setting up the synchronization server on page 11
- Preparing the administrative workstation for accessing Exchange Online on page 15
- Preparing a remote connection server for accessing Exchange Online on page 15

- Creating a synchronization project for initial synchronization of an Exchange Online environment on page 16
- Disabling synchronization on page 34
- Exchange Online synchronization features on page 24
- Customizing the synchronization configuration on page 26
- Configuration parameters for managing an Exchange Online environment on page 57
- Default project template for Exchange Online on page 58

Users and permissions for synchronizing with Exchange Online

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

Table 2: Users for synchronization

User	Permissions
User for accessing Exchange Online	You must provide a user account with the following authorizations for full synchronization of Exchange Online objects with the supplied One Identity Manager default configuration. • Member of the **Organization Management** role group • Member of the **Recipient management** role group NOTE: • Take into account the password expiry date of the user account for synchronization. Expired passwords will cause synchronization issues. You can disable password expiration for the user account in One Identity Manager. For more information, see the *One Identity Manager Administration Guide for Connecting to Azure Active Directory*. • User accounts for accessing Exchange Online are not allowed to use multifactor authentication.
One Identity Manager Service user account	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.

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: `netsh http add urlacl url=http://<IP address>:<port number>/ user="NT AUTHORITY\NETWORKSERVICE"` 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: • `%ProgramFiles(x86)%\One Identity` (on 32-bit operating systems) • `%ProgramFiles%\One Identity` (on 64-bit operating systems)
User for accessing the One Identity Manager database	The **Synchronization** default system user is provided to execute synchronization with an application server.

Necessary access permissions explained

The user account used for synchronizing required the following roles:

- Organization management

  Administrators, who are members of the Organization Management role group, have administrative access to the entire Exchange Online organization and can perform almost any task against any Exchange Online object. However, some exceptions apply, such as **Discovery Management**.

- Recipient management

  Administrators who are members of the Recipient Management role group have administrative access to create or modify Exchange Online recipients within the Exchange Online organization.

To assign permissions through the Microsoft Online Portal

NOTE: This method requires assigning an Office 365 license to the user account for synchronization.

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 Admin Center portal.

3. Select **Admin Center > Exchange** from the menu on the left-hand side.
   This takes you to the Exchange Admin Center.

4. In the menu on the left, click **Permissions**.
5. Select **Recipient Management** and click edit.
6. Add the user account for synchronization to the **Members** list.
7. Repeat steps 5 and 6 for the **Organization Management** role.

NOTE: If the synchronization user account does not appear in the list of members, you can allocate the permissions through Windows PowerShell as described below.

Installing the Exchange Online PowerShell V2 module

The Exchange Online connector uses Exchange Online PowerShell V2 module to access data in Exchange Online.

For more information about prerequisites and installation of the Exchange Online PowerShell V2 module, see the Exchange Online PowerShell V2 module documentation from Microsoft.

- The Exchange Online PowerShell V2 module must be installed on the synchronization server.
- If Exchange Online is accessed directly from the workstation on which Synchronization Editor is installed, the Exchange Online PowerShell V2 module must also be installed on this workstation.
- If direct access from the workstation to Exchange Online is not possible, you can set up a remote connection server. The Exchange Online PowerShell V2 module must be installed on the remote connection server.

Related topics

- Setting up the synchronization server on page 11
- Preparing the administrative workstation for accessing Exchange Online on page 15
- Preparing a remote connection server for accessing Exchange Online on page 15

Setting up the synchronization server

To set up synchronization with an Exchange 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 4.7.2 or later

  NOTE: Take the target system manufacturer's recommendations into account.
- Windows Management Framework 4.0
- One Identity Manager Service, Exchange Online connector
    - Install One Identity Manager components with the installation wizard.
        1. Select the **Select installation modules with existing database** option.
        2. Select the **Server | Job server | Exchange Online** machine role.

IMPORTANT: The Exchange Online connector uses Exchange Online PowerShell V2 module to access data in Exchange Online. The Exchange Online PowerShell V2 module must be installed on the 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 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 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 **Exchange Online**.
5. On the **Server functions** page, select **Exchange Online connector (via Windows PowerShell)**.
6. On the **Service Settings** page, enter the connection data and check the One Identity Manager Service configuration.

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

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

a. Select **Process collection**, click the **Insert** button and select **AppServerJobProvider**.

b. Click the **Connection parameter** entry, then click the **Edit** button.

c. Enter the connection data for the application server.

d. Click the **Authentication data** entry and click the **Edit** button.

e. Select the authentication module. Depending on the authentication module, other data may be required, such as user and password. For detailed information about the One Identity Manager authentication modules, see the *One Identity Manager Authorization and Authentication Guide*.

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

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

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

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

Related topics

- Installing the Exchange Online PowerShell V2 module on page 11

Preparing the administrative workstation for accessing Exchange Online

To configure synchronization with a Synchronization Editor appliance in Exchange Online, One Identity Manager must load the data directly from Exchange Online. If Exchange Online is accessed directly from the workstation on which the Synchronization Editor is installed, the following software must also be installed on this workstation:

- Windows PowerShell version 5 or later
- Exchange Online PowerShell V2 module

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

Related topics

- Installing the Exchange Online PowerShell V2 module on page 11
- Users and permissions for synchronizing with Exchange Online on page 9
- Preparing a remote connection server for accessing Exchange Online on page 15

Preparing a remote connection server for accessing Exchange Online

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
- Windows PowerShell version 5.1 or above is installed
- Exchange Online PowerShell V2 module is installed.
- Exchange 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 synchronization server on page 11
- Installing the Exchange Online PowerShell V2 module on page 11
- Users and permissions for synchronizing with Exchange Online on page 9
- Preparing the administrative workstation for accessing Exchange Online on page 15

Creating a synchronization project for initial synchronization of an Exchange Online environment

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

NOTE: When setting up the synchronization, note the recommendations described under Exchange Online synchronization features on page 24.

IMPORTANT: Each Exchange Online environment should have its own 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.

IMPORTANT: It must be possible to reach Exchange Online servers by DNS query for successful authentication. If the DNS cannot be resolved, the target system connection is refused.

Prerequisites for setting up a synchronization project

- Synchronization of the Azure Active Directory system is carried out regularly.
- The Azure Active Directory tenant is declared in One Identity Manager.

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

Table 3: 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 Exchange Online.
	Example:
	`<user>@<domain.com>`
	`<user name of the synchronization user>@yourorganization.onmicrosoft.com`
	Make a user account available with sufficient permissions. For more information, see Users and permissions for synchronizing with Exchange Online on page 9.

Synchronization server for Exchange Online	The One Identity Manager Service with the Exchange Online connector must be installed on the synchronization server. **Table 4: Additional properties for the Job server** **Property** / **Value** Server function: Exchange Online connector Machine role: Server/Jobserver/Azure Active Directory/ExchangeOnline For more information, see Setting up the synchronization server on page 11.
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 accessing Exchange Online on page 15.

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

- Executed in default mode
- Started from the Launchpad

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

To set up initial synchronization project for Exchange Online

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 Exchange 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. On the **Connection parameters** page, enter the login data for connecting to Exchange Online.

   Table 5: Connection parameters for the Exchange Online

Property	Description

User name (user@-domain)	Fully qualified name (FQDN) of the user account for log on.
	Example:
	`<user>@<domain.com>`
	`sync.user@yourorganisation.onmicrosoft.com`

Password	Password for the user account.

   User **Add set** to enter more connection parameters. This allows you to add more synchronization users. These are queried cyclically by the Exchange Online connector when queries are sent to Exchange Online. By using multiple synchronization users, it takes longer to reach the throttling limit.

   For more detailed information about throttling limits in Exchange Online, see the Exchange Online documentation from Microsoft.

   To test the connection parameters separately, click in the set. Click **Check all sets** to check all sets at once.

   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. 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.

8. 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.

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

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

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

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

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

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

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

To configure the content of the synchronization log

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

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

To synchronize on a regular basis

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

To start initial synchronization manually

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

Related topics

- Setting up the synchronization server on page 11
- Advanced settings for the Exchange Online connector
- Users and permissions for synchronizing with Exchange Online on page 9
- Displaying synchronization results on page 23
- Exchange Online synchronization features on page 24
- Customizing the synchronization configuration on page 26
- Default project template for Exchange Online on page 58

Advanced settings for the Exchange Online connector

You can specify whether want to set advanced options in the Synchronization Editor project wizard on the **Connect Exchange Online** page. These settings allow you to change the following options for communicating with Exchange Online:

- The number of concurrent connections per connection parameter set
- The definition of Windows PowerShell commands

Number of concurrent connections per connection parameter set

IMPORTANT: You should only make changes to this option with the help of support desk staff. Changes to this setting will have wide ranging effects on synchronization and must be made carefully.

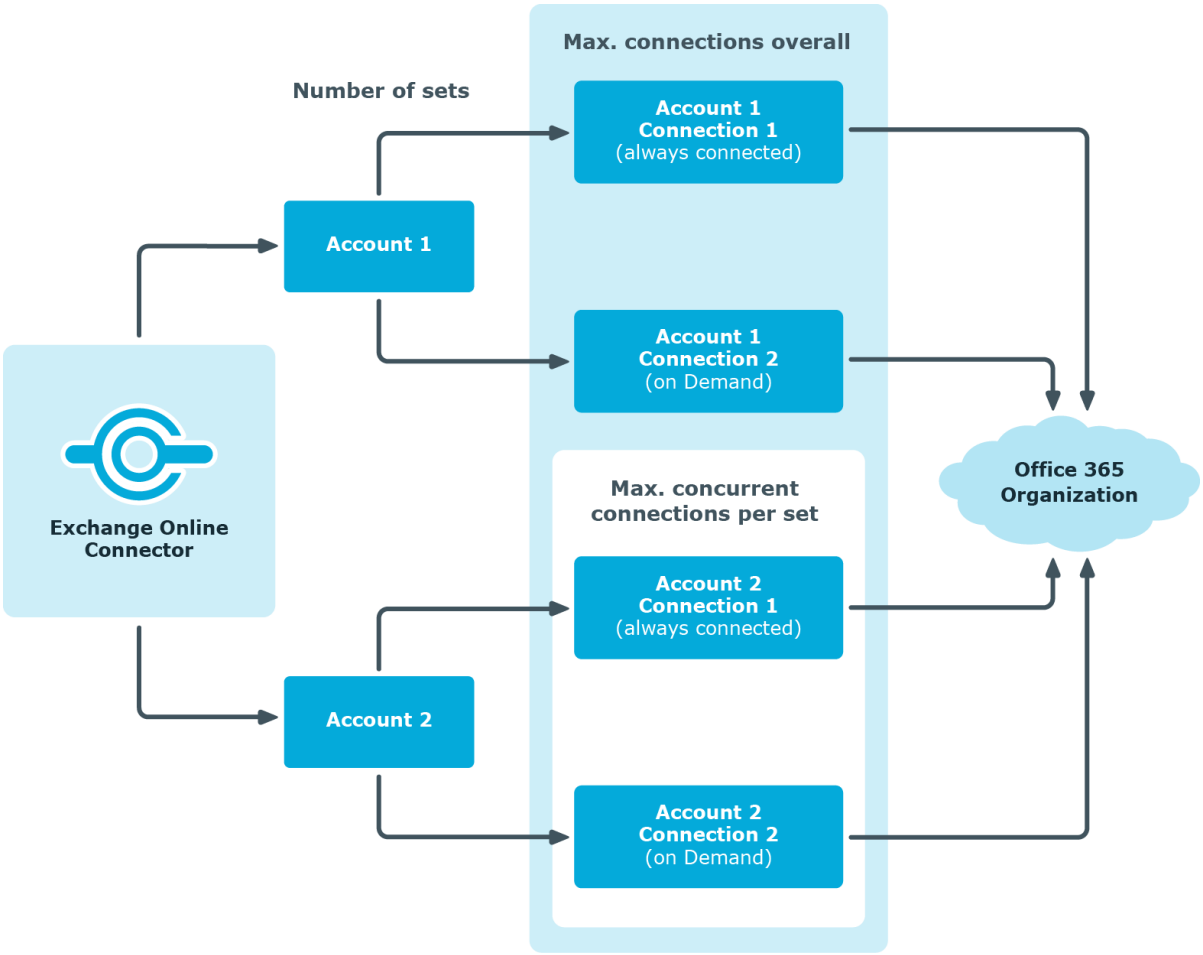
Use this option to set the number of concurrent connections for each connection parameter set or for each user account for synchronization. The setting specifies how many concurrent connections will be created for each user account. The default value is 2. Exchange Online currently allows three connections per user account on the server side.

When the Exchange Online connector creates the connection, it creates one Windows PowerShell session per connection parameter set regardless of the number of queries that follow. Further connections are created on demand, for example, when loading multiple objects during the synchronization.

The maximum number of sessions established to Exchange Online can be calculated with the following formula:

`Maximum number of Windows PowerShell sessions = Number of parameter sets * Value of concurrent connection per connection parameter set`

The minimum number of sessions established to Exchange Online is the same as the number of connection parameter sets.



To change the number of concurrent connections

1. On the **Connect to Exchange Online** page in the Synchronization Editor connection wizard, select **Show advanced options** and click **Next**.
2. Enter a value between 1 and 3 in **concurrent connections per connection parameter set**.
3. On the **Connection parameters** page, enter the login data for connecting to Exchange Online. For more information, see Creating a synchronization project for initial synchronization of an Exchange Online environment.
4. Click **Finish** to complete.

Customizing the connection definition

You can use this setting to adjust the definition used by the connector in order to convert inputs and outputs between the Exchange Online Cmdlets and the schema of the Synchronization Engine.

IMPORTANT: You should only make changes to the connector definition with the help of support desk staff. Changes to this setting will have wide ranging effects on synchronization and must be made carefully.

NOTE: A customized connection definition is not overwritten by default and must be made with careful consideration.

To customize the connector definition

1. Open the synchronization project in the Synchronization Editor.
2. Select **Configuration | Target system**.
3. Click **Edit connection**.

   This starts the system connection wizard.
4. Enable **Show advanced options** on the system connection wizard's start page.
5. Customize the connector definition as required on the **Advanced options** page.
   a. Select **Customize connector definition**.
   b. Edit the definition according to the instructions given by the support desk staff. You take the following action:
      - Choose to load the definition from a file.
      - Use to test the definition for errors.
      - Choose to display the differences to the standard version.
6. Save the changes.

Displaying synchronization results

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

To display a synchronization log

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

   Logs for all completed synchronization runs are displayed in the navigation view.

4. Select a log by double-clicking it.

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

To display a provisioning log

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

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

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

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

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

Synchronization logs are stored for a fixed length of time.

To modify the retention period for synchronization logs

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

Exchange Online synchronization features

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

Dependency resolution

By default, automatic synchronization step dependency resolution is turned off in the synchronization workflow. This reduces the number of calls required to Exchange Online. This can lead to unresolved references during synchronization that are handled in the maintenance phase at the end of synchronization.

Multiple organizations are not supported

Due to the dynamic number of used login accounts, variable sets cannot be used to parametrize the connection. For this reason, creating more base objects in one synchronization project is not supported.

Changing mailbox types in the Exchange Online portal

The default template for Exchange Online supports conversion of mailbox types as follows:

- Shared mailbox to user mailbox
- User mailbox to share mailbox
- Equipment mailbox to room mailbox
- Room mailbox to equipment mailbox

NOTE: In performing an unsupported change, for example, a room mailbox to a shared mailbox, the synchronization will mark the room mailbox as "missing" and fail to create the shared mailbox due to naming violations. This scenario can only be resolved manually.

NOTE: One Identity Manager does not support handling of mailbox types.

Synchronization of mailbox usage information

Synchronization of mailbox usage information is done in a separate synchronization step. Loading this information from Exchange Online is potentially very time consuming. Therefore, it make sense to create a separate workflow that includes a synchronization step for loading this data. You can run this workflow at longer intervals than the workflow without usage data.

The following usage information is synchronized:

Schema property in the Target System	Description
AssociatedItemCount	Number of elements assigned to this mailbox.
DeletedItemCount	Number of deleted elements.
DumpsterMessagesPerFolderCountReceiveQuota	Maximum number of messages allowed in a folder in the "Recoverable items" folder.
DumpsterMessagesPerFolderCountWarningQuota	Number of item a folder in the "Recoverable items" folder can contain before a warning is sent to the user.
ItemCount	Number of messages in this mailbox (for example, email, calendar, or contacts) that are visible to the user.
LastLoggedOnUserAccount	Name of the last logged on user.
LastLogOffTime	Last log off time
LastLogonTime	Last log on time
StorageLimitStatus	Information about the current storage state with respect to the specified

Schema property in the Target System	Description
	limits.
TotalDeletedItemSize	Size of items in the "Recoverable Items" mailbox.
TotalItemSize	Size of items in mailbox in KB.

NOTE: The mailbox usage information is only available for users or shared mailboxes.

Number of external slots for the Job server configuration

Since the number of concurrent connections for Exchange Online is limited to three, you should use a dedicated Job server with a reduced number of external execution slots (not more then two). You will get an error message if to many connections are open at the same time.

You can set the number of connections for each connection parameter set and customize the connector definition. For more information, see Advanced settings for the Exchange Online connector on page 21.

Customizing the synchronization configuration

Having used the Synchronization Editor to set up a synchronization project for initial synchronization of Exchange Online, you can use the synchronization project to load Exchange Online objects into the One Identity Manager database. When you manage mailboxes, email users, email contacts, mail-enabled distribution groups, and Office 365 groups with One Identity Manager, modifications are provisioned in the Exchange Online system.

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

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

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

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

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

Detailed information about this topic

- How to configure Exchange Online synchronization on page 27
- Updating schemas on page 28

How to configure Exchange Online synchronization

The synchronization project for initial synchronization provides a workflow for initial loading of target system objects (initial synchronization) and one for provisioning object modifications from the One Identity Manager database to the target system (provisioning). To use One Identity Manager as the 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 Exchange 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. Open the synchronization project in the Synchronization Editor.
2. Select the **Configuration | Target system** category.

   - OR -

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

   This reloads the schema data.

To edit a mapping

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

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

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

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 **Azure Active Directory | Target system synchronization: Exchange Online** category.

   All the synchronization tables assigned to the **Exchange 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.

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 **Azure Active Directory | Basic configuration data | Target system types** category.
2. In the result list, select the **Exchange 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.

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.

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.
- 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 **Azure Active Directory | Basic configuration data | Target system types** category.
2. In the result list, select the **Exchange Online** target system type.
3. Select the **Configure tables for publishing** task.
4. Select the assignment tables that you want to set up for single provisioning. Multi-select is possible.
    - This option can only be enabled for assignment tables that have a base table with an `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.

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 **Exchange Online connector** server function to the Job server.

   All Job servers must access the same Azure Active Directory 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.

   For more detailed information about editing server, see the *One Identity Manager Administration Guide for Connecting to Azure Active Directory*.

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*.

Help for the analysis of synchronization issues

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

- Consistency check results
- Revision filter settings

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

To generate a synchronization analysis report

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

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

Disabling synchronization

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

To prevent regular synchronization

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

   Now you can only start synchronization manually.

An activated synchronization project can only be edited to a limited 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**.

Related topics

- Creating a synchronization project for initial synchronization of an Exchange Online environment on page 16

3

Basic data for managing an Exchange Online environment

To manage an Exchange Online environment in One Identity Manager, the following basic 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. 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 an Exchange Online environment on page 57.

- 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 Setting up account definitions on page 36.

- 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 29.

- 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 Exchange Online objects 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 Exchange Online objects. The application roles must be added under the default application role.

For more information, see Target system managers on page 54.

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 yet have a user account in a target system, a new user account is created. This is done by assigning account definitions to an employee.

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

For detailed information about account definitions, see the *One Identity Manager Target System Base Module Administration Guide*.

The following steps are required to implement an account definition:

- Creating an account definition
- Creating manage levels
- Creating a formatting rule for IT operating data
- Collecting 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. In the Manager, select the **Azure Active Directory | Basic configuration data | Account definitions | Account definitions** category.
2. Select an account definition in the result list. Select the **Change master data** task.

   -OR-

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

NOTE: Exchange Online mailboxes are generated or deleted through the assignment or removal of licenses through Azure Active Directory subscriptions in the Azure Active Directory Module. For more information, see the One Identity Manager Administration Guide for Connecting to Azure Active Directory.

Detailed information about this topic

- Master data for an account definition on page 37

Related topics

Editing system objects

Master data for an account definition

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 system	Target system to which the account definition applies.
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. Leave empty for Exchange Online.
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 account definition 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

Property	Description
	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 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 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.

Property	Description
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 account definitions.
Spare field 01 - spare field 10	Additional company-specific information. Use the Designer to customize display names, formats, and templates for the input fields.

Creating 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.

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.

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

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

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

detailed information about manage levels, see the *One Identity Manager Target System Base Module Administration Guide*.

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

To assign manage levels to an account definition

1. In the Manager, select the **Azure Active Directory | Basic configuration data | Account definitions | Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Assign manage level** task.
4. In the **Add assignments** pane, assign the manage levels.

   - OR -

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

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

To edit a manage level

1. In the Manager, select the **Azure Active Directory | Basic configuration data | Account definitions | Manage levels** category.
2. Select the manage level in the result list. Select the **Change master data** task.

   - OR -

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

Related topics

- Master data for manage levels on page 40

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.

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.

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.

- Groups can be inherited

To create a mapping rule for IT operating data

1. In the Manager, select the **Azure Active Directory | 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. For detailed information, see the *One Identity Manager Target System Base Module Administration Guide*.
Source	Specifies which roles to use in order to find the user account properties. You have the following options: • Primary department • Primary location • Primary cost center • Primary business roles NOTE: 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 | AzureAD | ExchangeOnline | Accounts | MailTemplateDefaultValues** configuration parameter.

4. Save the changes.

Related topics

- Collecting IT operating data on page 43

Collecting 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. For detailed information, see the *One Identity Manager Target System Base Module Administration Guide*.
Value	Concrete value which is assigned to the user account property.

4. Save the changes.

Related topics

- Creating a formatting rule for IT operating data on page 41

Modify IT operating data

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

Prerequisites

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

  - OR -

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

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

To execute the template

1. In the Manager, select the **Azure Active Directory | 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 46
- Assigning an account definition to business roles on page 47
- Assigning account definitions to all employees on page 47
- Assigning account definitions directly to employees on page 48
- Assigning account definitions to a target system on page 51

Assigning account definitions to departments, cost centers, and locations

To add account definitions to hierarchical roles

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

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

   To remove an assignment

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

Related topics

- Assigning an account definition to business roles on page 47
- Assigning an account definition to business roles on page 47
- Assigning account definitions directly to employees on page 48

Assigning an account definition to business roles

Installed modules: Business Roles Module

To add account definitions to hierarchical roles

1. In the Manager, select the **Azure Active Directory | 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.

Related topics

- Assigning account definitions to departments, cost centers, and locations on page 46
- Assigning account definitions to all employees on page 47
- Assigning account definitions directly to employees on page 48

Assigning account definitions to all employees

To assign an account definition to all employees

1. In the Manager, select the **Azure Active Directory | 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.

Related topics

- Assigning account definitions to departments, cost centers, and locations on page 46
- Assigning an account definition to business roles on page 47
- Assigning account definitions directly to employees on page 48

Assigning account definitions directly to employees

To assign an account definition directly to employees

1. In the Manager, select the **Azure Active Directory | 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.

Related topics

- Assigning account definitions to departments, cost centers, and locations on page 46
- Assigning an account definition to business roles on page 47
- Assigning account definitions to all employees on page 47

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 **Azure Active Directory | 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 **Azure Active Directory | 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 **Azure Active Directory | Basic configuration data | Account definitions | Account definitions** (non role-based login) category.

   - OR -

   In the Manager, select **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 **Azure Active Directory | Basic configuration data | Account definitions | Account definitions** (non role-based login) category.

   - OR -

   In the Manager, select **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 an account definition on page 37
- Assigning account definitions to departments, cost centers, and locations on page 46

- Assigning an account definition to business roles on page 47
- Assigning account definitions directly to employees on page 48
- Assigning account definitions to system roles on page 49

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 (**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 tenant in the **Azure Active Directory | Tenants** category.
2. Select the **Change master data** task.
3. From the **Account definition (initial)** menu, select the account definition for user accounts.
4. From the **E-mail contact definition (initial)** menu, select the account definition for email contacts.
5. From the **E-mail user definition (initial)** menu, select the account definition for email users.
6. Save the changes.

Related topics

- Assigning account definitions to employees on page 45

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.

To delete an account definition

1. Remove automatic assignments of the account definition from all employees.
    a. In the Manager, select the **Azure Active Directory | 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 **Azure Active Directory | 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 **Azure Active Directory | 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 **Azure Active Directory | 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. 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 **Azure Active Directory | Basic configuration data | Account definitions | Account definitions** (non role-based login) category.

   - OR -

   In the Manager, select **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.

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

   a. In the Manager, select the **Azure Active Directory | 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.

7. Remove the account definition's assignments to target systems.

   a. In the Manager, select the tenant in the **Azure Active Directory | Tenants** category.

   b. Select the **Change master data** task.

   c. On the **General** tab, remove the assigned account definitions.

   d. Save the changes.

8. Delete the account definition.

   a. In the Manager, select the **Azure Active Directory | Basic configuration data | Account definitions | Account definitions** category.

   b. Select an account definition in the result list.

   c. Click to delete an account definition.

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 Exchange Online objects 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 Exchange Online objects. 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 Exchange Online objects 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 12: Default application roles for target system managers

User	Tasks
Target system managers	Target system managers must be assigned to the **Target systems | Exchange 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.

User	Tasks
	• 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 | Exchange 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 **Azure Active Directory | 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 **Azure Active Directory | Tenants** category.
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 (Exchange Online)** menu.

   - OR -

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

a. Enter the application role name and assign the **Target systems | Exchange 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 Exchange Online on page 6

Appendix A

Configuration parameters for managing an Exchange Online environment

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

Table 13: Configuration parameters for managing an Exchange Online environment

Configuration parameter	Meaning
TargetSystem | AzureAD | ExchangeOnline	Preprocessor relevant configuration parameter for controlling the database model components for the administration of the target system Exchange Online. If the parameter is set, the target system components are available. Changes to this parameter require the database to be recompiled.
TargetSystem | AzureAD | ExchangeOnline | Accounts	This configuration parameter permits configuration of recipient data.
TargetSystem | AzureAD | ExchangeOnline | 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 | AzureAD | ExchangeOnline | DefaultAddress	The configuration parameter contains the recipient's default email address for sending notifications about actions in the target system.
TargetSystem | AzureAD | ExchangeOnline | 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.

Appendix B

Default project template for Exchange 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.

The template uses mappings for the following schema types.

Table 14: Mapping Exchange Online schema types to tables in the One Identity Manager schema

Schema type in Exchange Online	Table in the One Identity Manager Schema
DistributionGroup	O3EDL
DynamicDistributionGroup	O3EDynDL
Mailbox	O3EMailbox
MailContact	O3EMailContact
MailPublicFolder	O3EMailPublicFolder
MailUser	O3EMailUser
MobileDeviceMailboxPolicy	O3EMobileDeviceMBPolicy
OWAMailboxPolicy	O3EOwaMailboxPolicy
PublicFolder	O3EPublicFolder
RetentionPolicy	O3ERetentionPolicy
RoleAssignmentPolicy	O3ERoleAssignmentPolicy
SharingPolicy	O3ESharingPolicy
UnifiedGroup	O3EUnifiedGroup

Appendix C

Editing system objects

The following table describes permitted processing methods of Exchange Online schema types and names restrictions required by system object processing.

Adding and deleting user mailboxes can only be done in One Identity Manager through assignment subscriptions in Azure Active Directory. This creates a mailbox that does not appear in the database until it has been synchronized. Afterward, it can be provisioned automatically in Exchange Online.

Table 15: Methods available for editing schema types

Type	Read	Add	Delete	Refresh
Role assignments policy	Yes	No	No	No
Mobile device mailbox policy	Yes	No	No	No
Sharing policy	Yes	No	No	No
Retention policy	Yes	No	No	No
Outlook Web App mailbox policy	Yes	No	No	No
Public Folder	Yes	No	No	No
Mail-enabled public folder	Yes	No	No	No
Resource mailbox	Yes	Yes	Yes	Yes
Shared mailbox	Yes	Yes	Yes	Yes
User mailbox	Yes	No	No	No
Email contact	Yes	Yes	Yes	Yes
Email user	Yes	Yes	Yes	Yes
Distribution group	Yes	Yes	Yes	Yes
Dynamic distribution	Yes	No	Yes	Yes

Type	Read	Add	Delete	Refresh
group				
Office 365 group	Yes	Yes	Yes	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