One Identity Manager 8.2.1

Administration Guide for Connecting to Microsoft Teams

One Identity Manager Administration Guide for Connecting to Microsoft Teams
Updated - 27 April 2022, 02:59
Version - 8.2.1

Contents

1

About this guide

The *One Identity Manager Administration Guide for Connecting to Microsoft Teams-Umgebung* describes how you set up synchronization of Microsoft Teams with One Identity Manager. You will learn how teams and channels in Microsoft Teams are mapped in One Identity Manager.

For more information about Microsoft Teams, see the *Microsoft Teams documentation* from Microsoft. For more information about synchronizing an Azure Active Directory tenant, see the *One Identity Manager Administration Guide for Connecting to Azure Active Directory*. For more information about synchronizing an Exchange Online organization, see the *One Identity Manager Administration Guide for Connecting to Exchange Online*.

This guide is intended for end users, system administrators, consultants, analysts, and any other IT professionals using the product.

NOTE: This guide describes One Identity Manager functionality available to the default user. It is possible that not all the functions described here are available to you. This depends on your system configuration and permissions.

Available documentation

You can access One Identity Manager documentation in the Manager and in the Designer by selecting the **Help** > **Search** menu item. The online version of One Identity Manager documentation is available in the Support portal under Technical Documentation. You will find videos with additional information at www.YouTube.com/OneIdentity.

2

Managing Microsoft Teams environments

Microsoft Teams teams and channels are mapped in One Identity Manager. A team groups Microsoft Teams users together. A team is linked to an Exchange Online Office 365 group. All members of the Office 365 group are members of the team. The members of a team cab use the team's channels. Standard channels are available to all the team's members. Private channels are only available to certain team members. Team members that are not invited to join a private channel cannot see the channel.

In order for users to use Microsoft Teams, you need a Microsoft Teams service plan. For more information about Microsoft Teams, see the *Microsoft Teams documentation* from Microsoft.

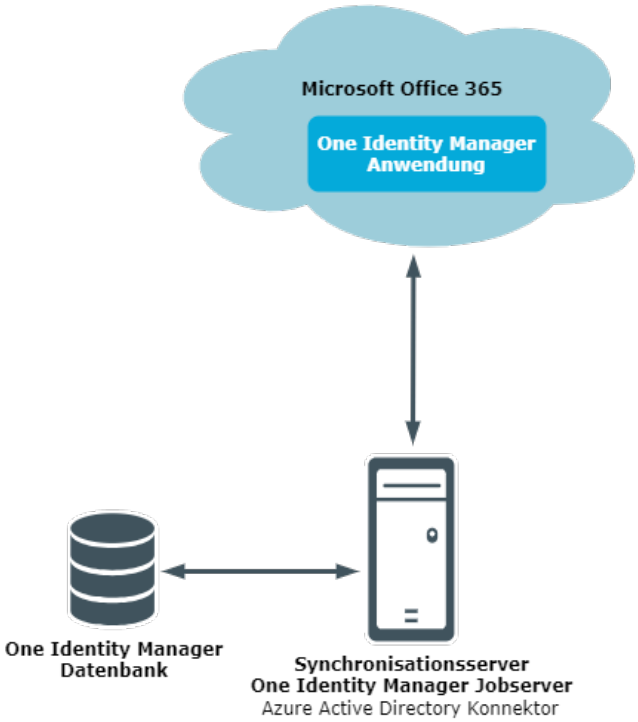
NOTE: The Microsoft Teams Module module must be installed as a prerequisite for managing Microsoft Teams in One Identity Manager For more information about installing, see the *One Identity Manager Installation Guide*.

Architecture overview

The Azure Active Directory connector has the task of synchronizing Microsoft Teams. The Azure Active Directory connector is installed on a synchronization server. The synchronization server ensures the comparison of data between the One Identity Manager database and Microsoft Teams.

The Azure Active Directory is part of the Azure Active Directory Module. Installing the Microsoft Teams Module provide synchronization templates for Microsoft Teams. The Azure Active Directory connector uses the Microsoft Graph API for accessing Microsoft Teams.

Figure 1: Architecture for synchronization



NOTE: To access Microsoft Teams data, the Azure Active Directory tenant and the Exchange Online organization must by synchronized.

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

One Identity Manager users for managing Microsoft Teams

The following users are used for setting up and administration of Microsoft Teams.

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

User	Tasks
	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 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. • Edit password policies for the target system. • Can add employees who have another identity than the **Primary identity**. • Configure synchronization in the Synchronization Editor and define the mapping for comparing target systems and One Identity Manager. • Edit the synchronization's target system types and outstanding objects. • Authorize other employees within their area of responsibility as target system managers and create child application roles if required.
One Identity Manager administrators	One Identity Manager administrator and administrative system users Administrative system users are not added to application roles. 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.

User	Tasks
	• 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.

3

Synchronizing a Microsoft Teams environment

The One Identity Manager Service is responsible for synchronizing data between the One Identity Manager database and Microsoft Teams.

This sections explains how to:

- Set up synchronization to import initial data from Microsoft Teams domains into the One Identity Manager database.
- Adjust a synchronization configuration
- Start and deactivate the synchronization.
- Evaluate the synchronization results.

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

Detailed information about this topic

- Setting up the initial synchronization with Microsoft Teams on page 11
- Customizing the synchronization configuration for Microsoft Teams on page 23
- Running synchronization on page 29
- Tasks following synchronization on page 33
- Troubleshooting on page 35
- Ignoring data error in synchronization on page 36
- Editing Microsoft Teams system objects on page 55

Setting up the initial synchronization with Microsoft Teams

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

Prerequisites for synchronizing Microsoft Teams are:

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

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

To load Microsoft Teams objects into the One Identity Manager database for the first time

1. Extend the registered One Identity Manager application in the Azure Active Directory tenant by additional permissions.
2. One Identity Manager components for managing Microsoft Teams 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.

      NOTE: If you disable the configuration parameter at a later date, model components and scripts that are not longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*.
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

- Extending permissions for the One Identity Manager application in the Azure Active Directory tenant on page 12
- Users and permissions for synchronizing with Microsoft Teams on page 12
- Setting up the synchronization server for Microsoft Teams on page 14

- Creating a synchronization project for initial synchronization of Microsoft Teams on page 17
- Configuring the synchronization log on page 22
- Default project template for Microsoft Teams on page 54

Extending permissions for the One Identity Manager application in the Azure Active Directory tenant

You can extend the permissions for the One Identity Manager application in the Microsoft Azure Portal (https://portal.azure.com/) or in the Azure Active Directory Admin Center (https://admin.microsoft.com/).

You have already registered a One Identity Manager application in the Azure Active Directory tenant in order to synchronize between One Identity Manager and Azure Active Directory. To be able to synchronize with Microsoft Teams, you must extend the permissions to include this application.

- If you use authentication in a directory user context (delegated permissions), assign the **ChannelMember.Read.All** delegated permissions (Read the members of channels) as well.
- If you use authentication in an application context (application permissions), assign the **ChannelMember.Read.All** (Read the members of channels) application permissions as well.

For more information on how to register an enterprise application for One Identity Manager in the Azure Active Directory tenant and assign permissions, see the *One Identity Manager Administration Guide for Connecting to Azure Active Directory*.

Related topics

- Users and permissions for synchronizing with Microsoft Teams on page 12

Users and permissions for synchronizing with Microsoft Teams

The following users are involved in synchronizing One Identity Manager with an Azure Active Directory tenant.

Table 2: Users for synchronization

Users	Permissions
User for accessing Azure Active Directory or The secret's value	Depending on how the One Identity Manager application is registered in the Azure Active Directory tenant, either a user account with sufficient permissions or the secret is required. • If you use authentication in the context of a directory user (delegated permissions), you require a user account that is a member in the **Global administrator** Azure Active Directory administration role when you set up the synchronization project. Use the Azure Active Directory Admin Center to assign the Azure Active Directory administrator role to the user account. For more information on managing permissions in Azure Active Directory, see the *Microsoft documentation*. NOTE: The user account used to access Azure Active Directory must not use multifactor authentication to allow automated logins in a user context. In addition, the user account must have a license for **Teams**. • If you use authentication in the context of an application (application entitlements), you need the value of the secret when you set up the synchronization project. The secret is generated when the One Identity Manager application is registered with the Azure Active Directory tenant. NOTE: The key is only valid for a limited period and must be renewed when it expires.
One Identity Manager Service user account	The user account for the One Identity Manager Service requires user permissions to carry out operations at file level (adding and editing directories and files). The user account must belong to the **Domain users** group. The user account must have the **Login as a service** extended user permissions. The user account requires permissions for the internal web service. NOTE: If the One Identity Manager Service runs under the network service (**NT Authority\NetworkService**), you can grant permissions for the internal web service with the following command line call: `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)

Users	Permissions
	• `%ProgramFiles%\One Identity` (on 64-bit operating systems)
User for accessing the One Identity Manager database	The **Synchronization** default system user is provided to run synchronization using an application server.

Related topics

- Extending permissions for the One Identity Manager application in the Azure Active Directory tenant on page 12

Setting up the synchronization server for Microsoft Teams

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

The One Identity Manager Service with the Azure Active Directory connector must be installed on the synchronization server.

Detailed information about this topic

- System requirements for the synchronization server for Microsoft Teams on page 14
- Installing the One Identity Manager Service for synchronizing Microsoft Teams on page 15

System requirements for the synchronization server for Microsoft Teams

To set up synchronization with Microsoft Teams, a server has to be available that has the following software installed on it:

- Windows operating system

  The following versions are supported:

  - Windows Server 2022
  - Windows Server 2019

    - Windows Server 2016
    - Windows Server 2012 R2
    - Windows Server 2012
- Microsoft .NET Framework Version 4.7.2 or later

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

Installing the One Identity Manager Service for synchronizing Microsoft Teams

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

Table 3: Properties of the Job server

Property	Value
Server function	Azure Active Directory connector
Machine role	Server | Job server | Azure Active Directory

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 runs 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: The program performs a remote installation of the One Identity Manager Service. Local installation of the service is not possible with this program.

To remotely install the One Identity Manager Service, you must have an administrative workstation on which the One Identity Manager components are installed.

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*.

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

        Syntax:

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

   NOTE: You can use the **Extended** option to make changes to other properties for the Job server.
4. On the **Machine roles** page, select **Azure Active Directory**.
5. On the **Server functions** page, select **Azure Active Directory connector (via Microsoft Graph)**.
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:
     1. Select **Process collection > sqlprovider**.
     2. Click the **Connection parameter** entry, then click the **Edit** button.
     3. Enter the connection data for the One Identity Manager database.
   - For a connection to the application server:

1. Select **Process collection**, click the **Insert** button and select **AppServerJobProvider**.
2. Click the **Connection parameter** entry, then click the **Edit** button.
3. Enter the connection data for the application server.
4. Click the **Authentication data** entry and click the **Edit** button.
5. Select the authentication module. Depending on the authentication module, other data may be required, such as user and password. For detailed information about 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. Change the directory if necessary.
10. If the database is encrypted, on the **Select private key file** page, select the file with the private key.
11. On the **Service access** page, enter the service's installation data.
    - **Computer**: Enter the name or IP address of the server that the service is installed and started on.
    - **Service account**: Enter the details of the user account that the One Identity Manager Service is running under. Enter the user account, the user account's password and password confirmation.

    The service is installed using the user account with which you are logged in to the administrative workstation. If you want to use another user account for installing the service, you can enter it in the advanced options. You can also change the One Identity Manager Service details, such as the installation directory, name, display name, and the One Identity Manager Service description, using the advanced options.
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**.

Creating a synchronization project for initial synchronization of Microsoft Teams

Use the Synchronization Editor to configure synchronization between the One Identity Manager database and Azure Active Directory environment. The following describes the steps for initial configuration of a synchronization project. For more information about

setting up synchronization, see the *One Identity Manager Target System Synchronization Reference Guide*.

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

Prerequisites for setting up a synchronization project

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

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

Related topics

- Information required for Microsoft Teams synchronization projects on page 18
- Creating an initial synchronization project for synchronizing Microsoft Teams on page 18

Information required for Microsoft Teams synchronization projects

(missing or bad snippet)

Related topics

- Users and permissions for synchronizing with Microsoft Teams on page 12
- Setting up the synchronization server for Microsoft Teams on page 14

Creating an initial synchronization project for synchronizing Microsoft Teams

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

- Run in default mode
- Started from the Launchpad

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

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

To set up an initial synchronization project for Microsoft Teams

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

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

2. Select the **Target system type Azure Active Directory** 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 **Azure Active Directory tenant** page, enter the following information:
   - **Deployment**: Select your cloud deployment. Select from **Microsoft Graph global service** or **Microsoft Cloud for US Government (L4)** .
   - **Application ID**: Enter the application ID. The application ID was generated when registering the One Identity Manager application in the Azure Active Directory tenant.
   - **Login domain**: Enter the base domain or a verified domain of your Azure Active Directory tenant.

5. On the **Authentication** page, select the type of login and enter the required login data. The information is required depends on how the One Identity Manager application is registered with the Azure Active Directory tenant.
   - If you have integrated One Identity Manager as a mobile device and desktop application in your Azure Active Directory tenant, select **Authenticate as mobile device or desktop application** and enter the user account and password for logging in.
   - If you have integrated One Identity Manager as a web application in your Azure Active Directory tenant, select the option **Authenticate as web application** and enter the value in the secret.

     The secret was generated when the One Identity Manager application was registered with the Azure Active Directory tenant.

6. On the last page of the system connection wizard, you can save the connection data.

- Set the **Save connection locally** option to save the connection data. This can be reused when you set up other synchronization projects.
- Click **Finish**, to end the system connection wizard and return to the project wizard.

7. On the **One Identity Manager Connection** tab, test the data for connecting to the One Identity Manager database. The data is loaded from the connected database. Reenter the password.

   NOTE:
   - If you use an unencrypted One Identity Manager database and have not yet saved any synchronization projects to the database, you need to enter all connection data again.
   - This page is not shown if a synchronization project already exists.

8. 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.
9. On the **Select project template** page, select the **Microsoft Teams (via Azure Active Directory)** template.
10. On the **Restrict target system access** page, specify how system access should work. You have the following options:

Table 4: Specify target system access

Option	Meaning
	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 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

Option	Meaning
	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.

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

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

    a. Click to add a new Job server.

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

    c. Click **OK**.

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

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

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

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

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

    NOTE:

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

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

Related topics

- Users and permissions for synchronizing with Microsoft Teams on page 12
- Information required for Microsoft Teams synchronization projects on page 18
- Setting up the synchronization server for Microsoft Teams on page 14
- Configuring the synchronization log on page 22
- Customizing the synchronization configuration for Microsoft Teams on page 23
- Running synchronization on page 29
- Tasks following synchronization on page 33
- Default project template for Microsoft Teams on page 54

Configuring the synchronization log

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

To configure the content of the synchronization log

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

   - OR -

   To configure the synchronization log for the database connection, select the **Configuration > One Identity Manager connection** category in the Synchronization Editor.
2. Select the **General** view and click **Configure**.
3. Select the **Synchronization log** view and set **Create synchronization log**.
4. Enable the data to be logged.

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

Synchronization logs are stored for a fixed length of time.

To modify the retention period for synchronization logs

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

Related topics

- Displaying synchronization results on page 32

Customizing the synchronization configuration for Microsoft Teams

Having used the Synchronization Editor to set up a synchronization project for initial synchronization of a Notes domain, you can use the synchronization project to load Microsoft Teams objects into the One Identity Manager database. Changes are provisioned in Microsoft Teams.

You must customize the synchronization configuration to be able to regularly compare the database with the Microsoft Teams environment and to synchronize changes.

- To use One Identity Manager as the primary system during synchronization, create a workflow with synchronization in the direction of the **Target system**.
- You can use variables to create generally applicable synchronization configurations that contain the necessary information about the synchronization objects when synchronization starts. Variables can be implemented in base objects, schema classes, or processing method, for example.
- Use variables to set up a synchronization project for synchronizing different Azure Active Directory tenants. Store a connection parameter as a variable for logging in to the Azure Active Directory tenants.
- To specify which Microsoft Teams 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.
- To synchronize additional schema properties, update the schema in the synchronization project. Include the schema extensions in the mapping.

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

Detailed information about this topic

- How to configure Microsoft Teams synchronization on page 24
- Changing system connection settings of Microsoft Teams on page 24
- Updating schemas on page 26
- Configuring single object synchronization on page 27
- Accelerating provisioning and single object synchronization on page 28

How to configure Microsoft Teams synchronization

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

To create a synchronization configuration for synchronizing Microsoft Teams

1. In the Synchronization Editor, open the synchronization project.
2. Check whether the existing mappings can be used to synchronize into the target system. Create new maps if required.
3. Create a new workflow with the workflow wizard.

   This creates a workflow with **Target system** as its direction of synchronization.
4. Create a new start up configuration. Use the new workflow to do this.
5. Save the changes.
6. Run a consistency check.

Changing system connection settings of Microsoft Teams

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

a. Specify a specialized variable set and change the values of the affected variables.

   The default values remain untouched in the default variable set. The variables can be reset to the default values at any time. (Recommended action).

b. Edit the target system connection with the system connection wizard and change the effected values.

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

For more information about Azure Active Directory connector's settings, see *the One Identity Manager Administration Guide for Connecting to Azure Active Directory*.

Detailed information about this topic

- Editing connection parameters in the variable set on page 25
- Editing target system connection properties on page 26

Editing connection parameters in the variable set

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

NOTE: To guarantee data consistency in the connected target system, ensure that the start-up configuration for synchronization and the base object for provisioning use the same variable set.

To customize connection parameters in a specialized variable set

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

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

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

    - OR -

    To add a new base object, click .
14. Select the specialized variable set in the **Variable set** menu.
15. Save the changes.

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

Related topics

- Editing target system connection properties on page 26

Editing target system connection properties

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

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

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

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

To edit connection parameters using the system connection wizard

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

   NOTE: If the default variable set is selected, the default values are overwritten and cannot be restored at a later time.
3. Select the **Configuration > Target system** category.
4. Click **Edit connection**.

   This starts the system connection wizard.
5. Follow the system connection wizard instructions and change the relevant properties.
6. Save the changes.

Related topics

- Editing connection parameters in the variable set on page 25

Updating schemas

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

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

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

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

To update a system connection schema

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

   - OR -

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

   This reloads the schema data.

To edit a mapping

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

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

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

Configuring single object synchronization

Changes made to individual objects in the target system can be immediately applied in the One Identity Manager database without having to start a full synchronization of the target system environment. Individual objects can only be synchronized if the object is already present in the One Identity Manager database. The changes are applied to the mapped

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

Prerequisites

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

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

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

1. In the Manager, select the **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 the custom table for which you want to use single object synchronization.
5. Save the changes.
6. Select the **Configure tables for publishing** task.
7. Select the custom table and enter the **Root object path**.

   Enter the path to the base object in the ObjectWalker notation of the VI.DB.

   Example: `FK(UID_AADOrganization).XObjectKey`
8. Save the changes.

Related topics

- Synchronizing single objects on page 32
- Post-processing outstanding objects on page 33

Accelerating provisioning and single object synchronization

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

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

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

To configure load balancing

1. Configure the server and declare it as a Job server in One Identity Manager.
   - Job servers that share processing must have the **No process assignment** option enabled.
   - Assign the **Azure Active Directory 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 information about editing Job servers for Azure Active Directory components, 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*.

Running synchronization

Synchronization is started using scheduled process plans. It is possible to start synchronization manually in the Synchronization Editor. You can simulate synchronization

beforehand to estimate synchronization results and discover errors in the synchronization configuration. If synchronization stopped unexpectedly, you must reset the start information to be able to restart synchronization.

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

Detailed information about this topic

- Starting synchronization on page 30
- Deactivating synchronization on page 31
- Displaying synchronization results on page 32
- Synchronizing single objects on page 32

Starting synchronization

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

To synchronize on a regular basis

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

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

To start initial synchronization manually

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

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

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

Deactivating synchronization

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

To prevent regular synchronization

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

   Now you can only start synchronization manually.

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

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

To deactivate the synchronization project

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

Related topics

- Creating a synchronization project for initial synchronization of Microsoft Teams on page 17

Displaying synchronization results

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

To display a synchronization log

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

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

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

To display a provisioning log

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

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

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

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

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

Related topics

- Configuring the synchronization log on page 22
- Troubleshooting on page 35

Synchronizing single objects

Individual objects can only be synchronized if the object is already present in the One Identity Manager database. The changes are applied to the mapped object properties.

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

To synchronize a single object

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

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

Detailed information about this topic

- Configuring single object synchronization on page 27

Tasks following synchronization

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

- Post-processing outstanding objects on page 33
- Adding custom tables to the target system synchronization on page 35

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.

   The navigation view lists all the synchronization tables assigned to the **Exchange Online** target system type.

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

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

   - The synchronization log has already been deleted.

     - OR -

   - An assignment from a member list has been deleted from the target system.

     The base object of the assignment was updated during the synchronization. A corresponding entry appears in the synchronization log. The entry in the assignment table is marked as outstanding, but there is no entry in the synchronization log.

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

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

   TIP:

   To display object properties of an outstanding object

   1. Select the object on the target system synchronization form.
   2. Open the context menu and click **Show object**.

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

Table 5: Methods for handling outstanding objects

Icon	Method	Description
	Delete	The object is immediately deleted from the One Identity Manager database. Deferred deletion is not taken into account. Indirect memberships cannot be deleted.
	Publish	The object is added to the target system. The **Outstanding** label is removed from the object. This runs a target system specific process that triggers the provisioning process for the object. Prerequisites: • The table containing the object can be published. • The target system connector has write access to the target system.
	Reset	The **Outstanding** label is removed for the object.

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

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

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

To disable bulk processing

- Disable the icon in the form's toolbar.

NOTE: The target system connector must have write access to the target system in order to publish outstanding objects that are being post-processed.

Adding custom tables to the target system synchronization

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

To add custom tables to target system synchronization

1. In the Manager, select the **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.

Related topics

- Post-processing outstanding objects on page 33

Troubleshooting

Synchronization Editor helps you to analyze and eliminate synchronization errors.

- Simulating synchronization

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

- Analyzing synchronization

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

- Logging messages

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

- Reset start information

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

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

Related topics

- Displaying synchronization results on page 32

Ignoring data error in synchronization

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

To ignoring data errors during synchronization in One Identity Manager

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

   This starts the system connection wizard.
4. On the **Additional options** page, enable **Try to ignore data errors**.

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

   Default columns, such as primary keys, UID columns, or mandatory input columns cannot be ignored.
5. Save the changes.

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

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

Mapping Microsoft Teams objects in One Identity Manager

Microsoft Teams teams and channels are mapped in One Identity Manager. A team groups Microsoft Teams users together. A team is linked to an Exchange Online Office 365 group. All members of the Office 365 group are members of the team. The members of a team cab use the team's channels. Standard channels are available to all the team's members. Private channels are only available to certain team members. Team members that are not invited to join a private channel cannot see the channel.

Microsoft Teams teams and channels are imported into the One Identity Manager database during synchronization. You can edit the main data of the teams individually and create new teams. You can create new standard channels but you cannot create private channels. You cannot edit existing channels.

For more information about Microsoft Teams, see the *Microsoft Teams documentation* from Microsoft.

Detailed information about this topic

- Microsoft Teams teams on page 38
- Microsoft Teams channels on page 46

Microsoft Teams teams

A team groups Microsoft Teams users together. A team is linked to an Exchange Online Office 365 group. All members of the Office 365 group are members of the team.

Teams are imported into One Identity Manager by synchronization. You can edit the main data of the teams individually and create new teams.

For more information about Exchange Online Office 365 groups, see the *One Identity Manager Administration Guide for Connecting to Exchange Online*.

Detailed information about this topic

- Creating Microsoft Teams teams on page 39
- Editing main data of Microsoft Teams teams on page 40
- Archiving Microsoft Teams teams on page 40
- Deleting Microsoft Teams teams on page 40
- Assigning Microsoft Teams teams to Azure Active Directory user accounts on page 41
- Adding Microsoft Teams teams automatically to the IT Shop on page 42
- Displaying members of Microsoft Teams teams on page 43
- Displaying owners of Microsoft Teams teams on page 43
- Displaying the Microsoft Teams team overview on page 44
- Main data for Microsoft Teams teams on page 44

Creating Microsoft Teams teams

In One Identity Manager, you can create new teams.

To create a team

1. In the Manager, select the **Azure Active Directory > Teams** category.
2. Click  in the result list.
3. On the **General** tab, under **Office 365 group**, select the Exchange Online Office 365 group that the team is linked to.

   Members of this Office 365 group become members of the team. The owners of the Office 365 group become owners of the team.
4. Enter the other main data for the team.
5. Save the changes.

Related topics

- Editing main data of Microsoft Teams teams on page 40
- Main data for Microsoft Teams teams on page 44

Editing main data of Microsoft Teams teams

You can edit the main data of existing teams.

To edit the main data of a team

1. In the Manager, select the **Azure Active Directory > Teams** category.
2. Select the team in the result list.
3. Select the **Change main data** task.
4. Edit the team's main data.
5. Save the changes.

Related topics

- Creating Microsoft Teams teams on page 39
- Main data for Microsoft Teams teams on page 44

Archiving Microsoft Teams teams

You can archive teams that are not longer being used.

To archive a team

1. In the Manager, select the **Azure Active Directory > Teams** category.
2. Select the team in the result list.
3. Select the **Change main data** task.
4. On the **General**, enable the **Archived** option.
5. Save the changes.

Related topics

- Deleting Microsoft Teams teams on page 40

Deleting Microsoft Teams teams

To delete a Microsoft Teams team, delete the Exchange Online Office 365 group linked to the team. When you delete an Office 365 group, the team is deleted as well. When you delete an Office 365 group, the Azure Active Directory group associated with the Office 365 group is also deleted.

To delete an Office 365 group

1. In the Manager, select the **Azure Active Directory > Office 365 groups** category.
2. Select the Office 365 group in the result list.
3. Click in the result list.
4. Confirm the security prompt with **Yes**.

For more information about Exchange Online Office 365 groups, see the *One Identity Manager Administration Guide for Connecting to Exchange Online*.

Related topics

- Archiving Microsoft Teams teams on page 40

Assigning Microsoft Teams teams to Azure Active Directory user accounts

Teams can be directly or indirectly assigned to Azure Active Directory user accounts through Office 365 groups. All members of the Office 365 group are members of the team.

In the case of indirect assignment, employees and Office 365 groups are assigned to hierarchical roles, such as departments, cost centers, locations, or business roles. The Office 365 groups assigned to an employee are calculated from the position in the hierarchy and the direction of inheritance. If you add an employee to roles and that employee owns an Azure Active Directory user account, the Azure Active Directory user account is added to the Office 365 group.

Furthermore, Office 365 groups can be requested through the Web Portal. To do this, add employees to a shop as customers. All Office 365 groups are assigned to this shop can be requested by the customers. Requested Office 365 groups are assigned to the employees after approval is granted.

Through system roles, Office 365 groups can be grouped together and assigned to employees and workdesks as a package. You can create system roles that contain only Office 365 groups. You can also group any number of company resources into a system role.

To react quickly to special requests, you can assign Office 365 groups directly to Azure Active Directory user accounts.

For more information about Exchange Online Office 365 groups, see the *One Identity Manager Administration Guide for Connecting to Exchange Online*.

Related topics

- Adding Microsoft Teams teams automatically to the IT Shop on page 42
- Displaying members of Microsoft Teams teams on page 43

Adding Microsoft Teams teams automatically to the IT Shop

The following steps can be used to automatically add Microsoft Teams teams to the IT Shop. Synchronization ensures that the teams are added to the IT Shop through their Office 365 groups.

For more information about Exchange Online Office 365 groups, see the *One Identity Manager Administration Guide for Connecting to Exchange Online*.

To add Microsoft Teams teams automatically to the IT Shop

1. In the Designer, set the **QER | ITShop | AutoPublish | O3TTeam** configuration parameter.
2. In order not to add teams to the IT Shop automatically, in the Designer, set the **QER | ITShop | AutoPublish | O3TTeam | ExcludeList** configuration parameter.

   This configuration parameter contains a listing of all teams that should not be allocated to the IT Shop automatically. You can extend this list if required. To do this, enter the name of the groups in the configuration parameter. Names are listed in a pipe (|) delimited list. Regular expressions are supported.
3. Compile the database.

The teams and their Office 365 groups are added automatically to the IT Shop from now on.

The following steps are run to add a group to the IT Shop.

1. A service item is determined for the teams' Office 365 group.
2. The service item is assigned to the **Azure Active Directory groups | Office 365 groups in Microsoft Teams** default service category.
3. An application role for product owners is determined and assigned to the service item.

   Product owners can approve requests for membership in these teams and their Office 365 groups. The default product owner is the Office 365 group's owner.
4. The Office 365 group is labeled with the **IT Shop** option and assigned to the **Microsoft Teams groups** or **Office 365 groups** IT Shop shelf in the **Identity & Access Lifecycle** shop.

Then the shop customers can use the Web Portal to request memberships in the teams and their Office 365 groups.

NOTE: When a team is irrevocably deleted from the One Identity Manager database, the associated service item is also deleted.

For more information about configuring the One Identity Manager IT Shop Administration Guide, see the *IT Shop*. For more information about requesting access requests in the Web Portal, see the *One Identity Manager Web Portal User Guide*.

Related topics

- Assigning Microsoft Teams teams to Azure Active Directory user accounts on page 41
- Displaying members of Microsoft Teams teams on page 43
- Deleting Microsoft Teams teams on page 40

Displaying members of Microsoft Teams teams

A team is linked to an Exchange Online Office 365 group. All members of the Office 365 group are members of the team. In order for users to use Microsoft Teams, you need a Microsoft Teams service plan. For more information about Microsoft Teams, see the *Microsoft Teams documentation* from Microsoft.

To display the members of a team

1. In the Manager, select the **Azure Active Directory > Teams** category.
2. Select the team in the result list.
3. Select the **Microsoft Teams team overview** task.

   The overview form displays the following information about the members of a team:

   - **Members**: Displays the team members that own a Microsoft Teams service plan. These members can use Microsoft Teams.
   - **Members without service plan 'Teams'**: Displays the team members that do not have a Microsoft Teams service plan. These members cannot use Microsoft Teams.

Related topics

- Displaying the Microsoft Teams team overview on page 44

Displaying owners of Microsoft Teams teams

A team is linked to an Exchange Online Office 365 group. The owners of the Office 365 group are owners of the team.

The team's owners see the team's channels in Microsoft Teams. Limited information is available for private channels. For more information about Microsoft Teams, see the *Microsoft Teams documentation* from Microsoft.

To show all the owners of a team

1. In the Manager, select the **Azure Active Directory > Teams** category.
2. Select the team in the result list.
3. Select the **Microsoft Teams team overview** task.
4. In the header of the **Office 365 groups** form element, click on the group's name.

   This opens the team's Office 365 group. On the **Office 365 group overview** form, you can see the owners.

Related topics

- Displaying the Microsoft Teams team overview on page 44
- Microsoft Teams channels on page 46

Displaying the Microsoft Teams team overview

Use this task to obtain an overview of the most important information about a team.

To obtain an overview of a user account

1. In the Manager, select the **Azure Active Directory > Teams** category.
2. Select the team in the result list.
3. Select the **Microsoft Teams team overview** task.

Related topics

- Displaying members of Microsoft Teams teams on page 43
- Displaying owners of Microsoft Teams teams on page 43
- Microsoft Teams channels on page 46

Main data for Microsoft Teams teams

Table 6: Team main data

Property	Description
Office 365 group	The team is linked to this Exchange Online Office 365 group. The members of the Office 365 group are members of the team. The owners of the Office 365 group are owners of the team. For more information about Exchange Online Office 365 groups, see the

Property	Description
	One Identity Manager Administration Guide for Connecting to Exchange Online.
Web URL	URL that links directly to the Microsoft Teams team. The web URL is formed by Microsoft Teams.
Archived	Specifies whether the team is in read-only mode.
Allow Giphy	Specifies whether the use of Giphy is allowed.
Giphy content classification	Giphy content classification. Possible values are **Moderate** and **Strict**.
Custom memes are allowed.	Specifies whether users can incorporate custom memes.
Allow stickers and memes	Specifies whether users can incorporate stickers and memes.
Create and update channels (guests)	Specifies whether guests can create and update channels.
Delete channels (guests)	Specifies whether guests can delete channels.
Add and remove apps	Specifies whether members can add and remove apps.
Create and update channels (members)	Specifies whether members can create and update channels.
Delete channels (members)	Specifies whether members can delete channels.
Use of connect-ors	Specifies whether members can create, update, and remove connectors.
Use of tabs	Specifies whether members can create, update, and remove tabs.
Allow edit messages (user)	Specifies whether users can edit their messages.
Allow delete messages	Specifies whether users can delete their messages.

Property	Description
(user)	
Allow delete messages (owner)	Specifies whether owners can delete all messages.
Allow channel mentions	Specifies whether mentions of the channel (@Channel) are allowed.
Allow team mentions	Specifies whether mentions of the team (@Team) are allowed.

Related topics

- Editing main data of Microsoft Teams teams on page 40
- Archiving Microsoft Teams teams on page 40
- Displaying members of Microsoft Teams teams on page 43
- Displaying owners of Microsoft Teams teams on page 43

Microsoft Teams channels

A team is linked to an Exchange Online Office 365 group. All members of the Office 365 group are members of the team. The members of a team cab use the team's channels. Standard channels are available to all the team's members. Private channels are only available to certain team members. Team members that are not invited to join a private channel cannot see the channel.

Channels are imported into One Identity Manager by synchronization. You can create new standard channels but you cannot create private channels. You cannot edit existing channels.

Detailed information about this topic

- Creating Microsoft Teams standard channels on page 47
- Displaying private Microsoft Teams channels on page 47
- Deleting Microsoft Teams channels on page 48
- Displaying the Microsoft Teams channel overview on page 48
- Main data for Microsoft Teams channels on page 49
- Displaying members of Microsoft Teams teams on page 43
- Displaying owners of Microsoft Teams teams on page 43

Creating Microsoft Teams standard channels

You can create new standard channels in One Identity Manager but you cannot create private channels in One Identity Manager.

To create a standard channel

1. In the Manager, select the **Azure Active Directory > Channels** category.
2. Click in the result list.
3. On the General tab, enter the following data:
    - **Display name**: Channel name that the user sees in Microsoft Teams.
    - **Membership type**: When standard channels are created, they have the **Standard** type. This channel is available to all the team's members.
    - **Description**: Detailed description of the channel.
    - **Team**: The channel belongs to the team selected here.
4. Save the changes.

Related topics

- Displaying private Microsoft Teams channels on page 47
- Main data for Microsoft Teams channels on page 49
- Displaying members of Microsoft Teams teams on page 43

Displaying private Microsoft Teams channels

You cannot create private channels in One Identity Manager. You can show the main data and owners of private channels. The members are not shown in One Identity Manager.

To display the main data of a private channel

1. In the Manager, select the **Azure Active Directory > Channels** category.
2. Select the channel in the result list.
3. Select the **Change main data** task.
4. On the General tab, you can see the following information.
    - **Display name**: Channel name that the user sees in Microsoft Teams.
    - **Memberships type**: The value **Private** is shown for private channels. The channel is only available to certain team members.
    - **Description**: Detailed description of the channel.
    - **Team**: The channel belongs to the team selected here.

To display the owners of a private channel

1. In the Manager, select the **Azure Active Directory > Channels** category.
2. Select the channel in the result list.
3. Select the **Microsoft Teams channel overview** task.

   The **Microsoft Teams channel owners** form element, displays the owners of the private channel.

Related topics

- Displaying the Microsoft Teams channel overview on page 48
- Creating Microsoft Teams standard channels on page 47
- Main data for Microsoft Teams channels on page 49

Deleting Microsoft Teams channels

Channels are deleted permanently from the One Identity Manager database and from Microsoft Teams.

NOTE: Channels with the name **General** cannot be deleted in One Identity Manager.

To delete a channel

1. In the Manager, select the **Azure Active Directory > Channels** category.
2. Select the channel in the result list.
3. Click in the result list.
4. Confirm the security prompt with **Yes**.

Related topics

- Known issues about connecting Microsoft Teams on page 56

Displaying the Microsoft Teams channel overview

Use this task to obtain an overview of the most important information about a channel.

To obtain an overview of a user account

1. In the Manager, select the **Azure Active Directory > Channels** category.
2. Select the channel in the result list.
3. Select the **Microsoft Teams channel overview** task.

Related topics

- Displaying private Microsoft Teams channels on page 47

Main data for Microsoft Teams channels

Table 7: Channel main data

Property	Description
Display name	Channel name that the user sees in Microsoft Teams.
Description	Detailed description of the channel.
Team	The channel belongs to this team.
Email address	Email address for sending messages to the channel. The email address is formed by Microsoft Teams.
Web URL	URL that links directly to the Microsoft Teams channel. The web URL is formed by Microsoft Teams.
Membership type	Type of channel. You have the following options: • **Standard**: Standard channel. This channel is available to all the team's members. • **Private**: Private channel. The channel is only available to certain team members.

5

Basic data for managing a Microsoft Teams environment

To manage a Microsoft Teams environment in One Identity Manager, the following basic data is relevant.

- Target system types

  Target system types are required for configuring target system comparisons. Tables with outstanding objects are maintained with the target system types and settings are configured for provisioning memberships and single objects synchronization. Target system types also map objects in the Unified Namespace.

  For more information, see Post-processing outstanding objects on page 33.

- Target system managers

  Target system managers for Exchange Online are also responsible for Microsoft Teams objects. Target system managers must be assigned to the **Target systems | Exchange Online** application role or a child application role.

  For more information, see the *One Identity Manager Administration Guide for Connecting to Exchange Online*.

- Servers

  Servers must be informed of your server functionality in order to handle Microsoft Teams-specific processes in One Identity Manager. For example, the synchronization server. The One Identity Manager Service with the Azure Active Directory connector must be installed on the synchronization server. The synchronization server must be declared as a Job server in One Identity Manager.

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

- Configuration parameters

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

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

For more information, see Configuration parameters for managing a Microsoft Teams environment on page 52.

Appendix A

Configuration parameters for managing a Microsoft Teams environment

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

Table 8: Configuration parameters

Configuration parameters	Description
TargetSystem | AzureAD | ExchangeOnline | Teams	Preprocessor relevant configuration parameter for controlling database model components for Microsoft Teams target system administration. If the parameter is set, the target system components are available. Changes to this parameter require the database to be recompiled. If you disable the configuration parameter at a later date, model components and scripts that are not longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*.
QER | ITShop | AutoPublish | O3TTeam	Preprocessor relevant configuration parameter for automatically adding Microsoft Teams teams to the IT Shop. If the parameter is set, all teams are automatically assigned as products to the IT Shop. Changes to this parameter require the database to be recompiled. If you disable the configuration parameter at a later date, model components and scripts that are not longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*.
QER | ITShop | AutoPublish |	List of all Microsoft Teams teams that must not be automatically assigned to the IT Shop. Each entry is part of a regular search pattern

Configuration parameters	Description
O3TTeam | ExcludeList	and supports regular expression notation.

Appendix B

Default project template for Microsoft Teams

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

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

The project template uses mappings for the following schema types.

Table 9: Microsoft Teams schema type mapping

Schema type in Microsoft Teams	Table in the One Identity Manager Schema
Channel	O3TTeamChannel
Team	O3TTeam

Appendix C

Editing Microsoft Teams system objects

The following table describes permitted editing methods of Microsoft Teams schema types and names restrictions required by system object processing.

Table 10: Methods available for editing schema types

Type	Read	Add	Delete	Refresh
Teams (`Team`)	Yes	Yes	No	Yes
Standard channel (`Channel`)	Yes	Yes	Yes	No
Private channel (`Channel`)	Yes	No	No	No

Appendix D

Known issues about connecting Microsoft Teams

Issue

A error occurs when you create a channel: `Channel name is already taken`.

Cause

If you created and deleted a channel in Microsoft Teams, it is not possible to create a new channel with the same name.

Solution

None.

This is the default behavior from Microsoft Teams. For more information about Microsoft Teams, see the *Microsoft Teams documentation* from Microsoft.

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

P

S

T

V