One Identity Manager 8.2

Administration Guide for Connecting
to Azure Active Directory

One Identity Manager Administration Guide for Connecting to Azure Active Directory
Updated - 02 December 2021, 16:27
Version - 8.2

Contents

Managing Azure Active Directory environments

One Identity Manager offers simplified user account administration for Azure Active Directory. One Identity Manager concentrates on setting up and editing user accounts and providing the required permissions. To equip users with the required permissions, One Identity Manager maps subscriptions, service plans, groups, and administration roles. This makes it possible to use Identity and Access Governance processes, including attestation, Identity Audit, user account management and system entitlements, IT Shop, or report subscriptions for Azure Active Directory tenants.

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

Additional information about the Azure Active Directory core directory, such as tenants and verified domains, is loaded into the One Identity Manager database by data synchronization. There are limited options for customizing this information in One Identity Manager due to the complex dependencies and far-reaching effects of any changes.

For more information about the Azure Active Directory structure, see the *Azure Active Directory documentation* from Microsoft.

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

Architecture overview

To access Azure Active Directory tenant data, the Azure Active Directory connector is installed on a synchronization server. The synchronization server ensures data is compared between the One Identity Manager database and Azure Active Directory. The Azure Active Directory connector uses the Microsoft Graph API for accessing Azure Active Directory data.

The Azure Active Directory connector must authenticate itself on the Azure Active Directory tenant to access Azure Active Directory tenant data. Authentication is carried out by an

application for One Identity Manager that is integrated in the Azure Active Directory tenant and equipped with the respective access permissions.

Figure 1: Architecture for synchronization
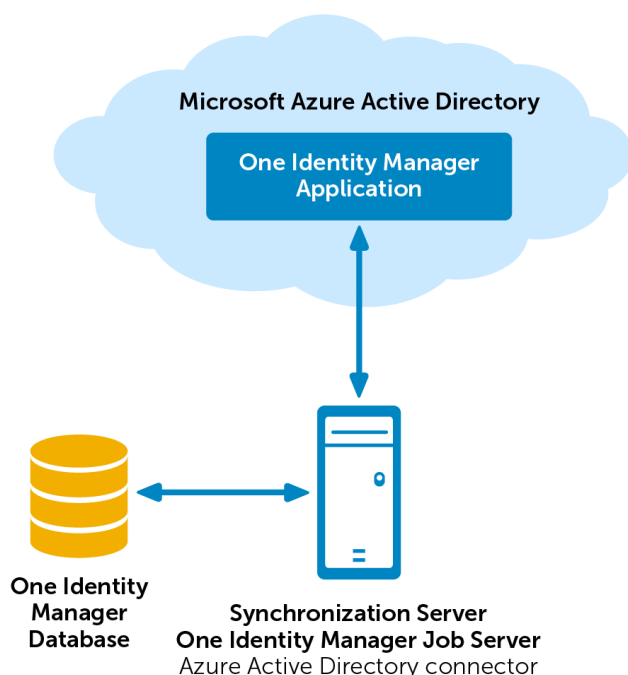
One Identity Manager users for managing an Azure Active Directory environment

The following users are involved in the administration of Azure Active Directory.

Table 1: Users

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

User	Tasks
	if required.
	• Specify which application roles for target system managers are mutually exclusive.
	• Authorize other employees to be target system administrators.
	• Do not assume any administrative tasks within the target system.
Target system managers	Target system managers must be assigned to the **Target systems | Azure Active Directory** 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.
	• Prepare groups to add to the IT Shop.
	• Can add employees who have another identity than the **Primary identity**.
	• Configure synchronization in the Synchronization Editor and define the mapping for comparing target systems and One Identity Manager.
	• Edit the synchronization's target system types and outstanding objects.
	• Authorize other employees within their area of responsibility as target system managers and create child application roles if required.
One Identity Manager administrators	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.
	• Enable or disable additional configuration parameters in the Designer as required.

User	Tasks
	• Create custom processes in the Designer as required. • Create and configure schedules as required. • Create and configure password policies as required.
Administrators for the IT Shop	Administrators must be assigned to the **Request & Fulfillment | IT Shop | Administrators** application role. Users with this application role: • Assign groups to IT Shop structures.
Product owners for the IT Shop	Product owners must be assigned to the **Request & Fulfillment | IT Shop | Product owners** application role or a child application role. Users with this application role: • Approve through requests. • Edit service items and service categories under their management.
Administrators for organizations	Administrators must be assigned to the **Identity Management | Organizations | Administrators** application role. Users with this application role: • Assign groups to departments, cost centers, and locations.
Business roles administrators	Administrators must be assigned to the **Identity Management | Business roles | Administrators** application role. Users with this application role: • Assign groups to business roles.

Configuration parameters for managing an Azure Active Directory environment

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 Azure Active Directory environment on page 226.

Synchronizing an Azure Active Directory environment

NOTE: Synchronization of the following national cloud deployments with the Azure Active Directory connector is not supported.

- Microsoft Cloud for US Government (L5)
- Microsoft Cloud Germany
- Azure Active Directory and Office 365 operated by 21Vianet in China

For more information, see https://support.oneidentity.com/KB/312379.

The One Identity Manager Service is responsible for synchronizing data between the One Identity Manager database and the Azure Active Directory tenant.

This sections explains how to:

- Set up synchronization to import initial data from Azure Active Directory tenant to the One Identity Manager database.
- Adjust a synchronization configuration to synchronize different Azure Active Directory tenants with the same synchronization project, for example.
- Start and deactivate the synchronization.
- Analyze synchronization results.

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

Detailed information about this topic

Setting up initial synchronization with an Azure Active Directory tenant

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

To load Azure Active Directory tenant objects into the One Identity Manager database for the first time

1. Ensure the Azure Active Directory tenant has a license for the **SharePoint Online** service.

   NOTE: If no such license is available, an error will occur when loading the Azure Active Directory user accounts. For more information, see Possible errors when synchronizing an Azure Active Directory tenant on page 224.

2. Register an One Identity Manager application in your Azure Active Directory tenant.

   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 key is required.

3. The One Identity Manager components for managing Azure Active Directory tenants are available if the **TargetSystem | AzureAD** configuration parameter is set.

   - In the Designer, check if the configuration parameter is set. Otherwise, set the configuration parameter and compile the database.

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

   - Other configuration parameters are installed when the module is installed. Check the configuration parameters and modify them as necessary to suit your requirements.

4. Install and configure a synchronization server and declare the server as a Job server in One Identity Manager.

5. Create a synchronization project with the Synchronization Editor.

Detailed information about this topic

Registering an enterprise application for One Identity Manager in the Azure Active Directory tenant

To synchronize data between One Identity Manager and Azure Active Directory, you must register an application in the Azure Active Directory tenants. The Azure Active Directory connector uses the One Identity Manager application to authenticate itself to the Azure Active Directory tenant.

- Register 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/).

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

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

- There are two different ways to authenticate the application.

  - Authentication in the directory user context (delegated permissions)

    Authentication in the context of a directory user is recommended, as this is the only way to reset user passwords.

    If you use authentication in the directory user context, you need a user account with sufficient permissions when setting up the synchronization project.

  - Authentication in the application context (application entitlements)

    If you use authentication in the context of an application, you need the value of the secret when setting 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.

To configure authentication in the directory user context (delegated permissions)

1. In the Microsoft Azure portal, select your app under **App registrations**.

2. Configure the following settings under **Manage > Authentication**.

    a. In the **Platform configurations** section, click **Add a platform** and, under **Configure platforms**, select the **Mobile and desktop applications** tile.

        i. Under **Custom redirect URIs**, you can specify any URI.

        ii. Click **Configure**.

    b. In the **Supported account types** section, select **Accounts in this organization directory only (single tenant)**.

    c. In the **Advanced settings** section, enable the **Allow public client flows** option.

3. Configure the permissions under **Manage > API permissions**.

    a. In the **Configured permissions** section, click **Add a permission**.

        i. Under **Request API permissions > Microsoft APIs**, select the tile **Microsoft Graph**.

        ii. Select **Delegated permissions** and select the following permissions:

            • **Directory.AccessAsUser.All** (Access directory as the signed in user)

            • **Directory.ReadWrite.All** (Read and write directory data)

            • **User.ReadWrite.All** (Read and write all users' full profile)

            • **Group.ReadWrite.All** (Read and write all groups)

            • **openid** (Sign users in)

        iii. Click **Add permissions**.

    b. In the **Configured permissions** section, click **Grant admin consent for ...** and confirm the security prompt with **Yes**.

        This enables the configured permissions.

To configure authentication in the application context (application entitlements)

1. In the Microsoft Azure portal, select your app under **App registrations**.

2. Configure the following settings under **Manage > Authentication**.

    a. In the **Platform configurations** section, click **Add platform**, and under **Configure platforms**, select the **Web** tile.

      i. Under **Redirect URIs**, you can specify any URI.

      ii. Click **Configure**.

  b. In the **Supported account types** section, select **Accounts in this organization directory only (single tenant)**.

  c. In the **Advanced settings** section, enable the **Allow public client flows** option.

3. Configure the permissions under **Manage > API permissions**.

  a. In the **Configured Permissions** section, click **Add a permission**.

      i. Under **Request API permissions > Microsoft APIs**, select the tile **Microsoft Graph**.

      ii. Select **Application entitlements** and select the following permissions:

- **Application.ReadWrite.All** (Read and write all applications)
- **Directory.ReadWrite.All** (Read directory data)
- **Group.ReadWrite.All** (Read and write all groups)
- **Policy.Read.All** (Read your organization's policies)
- **RoleManagement.ReadWrite.Directory** (Read and write all directory RBAC settings)
- **User.ReadWrite.All** (Read and write all users' full profile)

      iii. Click **Add permissions**.

  b. In the **Configured permissions** section, click **Grant admin consent for ...** and confirm the security prompt with **Yes**.

  This enables the configured permissions.

4. Create a secret under **Manage > Certificates & secrets**.

  a. In the **Client secrets** section, click **New client secret**.

      i. Enter a description and the validity period for the secret.

      ii. Click **Add**.

  b. The secret is generated and displayed in the **Client secrets** section.

Related topics

- Users and permissions for synchronizing with Azure Active Directory on page 20
- Creating a synchronization project for initial synchronization of an Azure Active Directory tenant on page 25

Users and permissions for synchronizing with Azure Active Directory

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

Table 2: Users for synchronization

User	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. • 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"`

User	Permissions
	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 run synchronization using an application server.

Related topics

- Registering an enterprise application for One Identity Manager in the Azure Active Directory tenant on page 17

Setting up the Azure Active Directory synchronization server

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

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

Detailed information about this topic

- System requirements for the Azure Active Directory synchronization server on page 21
- Installing One Identity Manager Service with an Azure Active Directory connector on page 22

System requirements for the Azure Active Directory synchronization server

To set up synchronization with an Azure Active Directory tenant, a server must be available with the following software installed on it:

- Windows operating system

  The following versions are supported:
  - Windows Server 2022
  - Windows Server 2019
  - Windows Server 2016
  - Windows Server 2012 R2
  - Windows Server 2012

- Microsoft .NET Framework Version 4.7.2 or later

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

Installing One Identity Manager Service with an Azure Active Directory connector

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. For detailed information about installing a workstation, see the *One Identity Manager Installation Guide*.

> 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. You can also edit the properties later with the Designer.

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 an Azure Active Directory tenant

Use the Synchronization Editor to configure synchronization between the One Identity Manager database and Azure Active Directory. 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.

Related topics

- Information required for Azure Active Directory synchronization projects on page 25
- Creating an initial synchronization project for an Azure Active Directory tenant on page 27
- Customizing synchronization projects to invite guest users on page 34

Information required for Azure Active Directory synchronization projects

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

Table 4: Information required to set up a synchronization project

Data	Explanation
Application ID	The application ID is generated when registering the One Identity Manager application in the Azure Active Directory tenant.
Login domain	Azure Active Directory name of the domain for logging in to Azure Active Directory. You can use the base domain or your Azure Active Directory tenant's verified domain.
User account and password for logging in 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

Data	Explanation
	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.
	• 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.
Synchronization server for Azure Active Directory	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.
	The synchronization server must be declared as a Job server in One Identity Manager. Use the following properties when you set up the Job server.
	• Server function: **Azure Active Directory connector (via Microsoft Graph)**
	• Machine role: **Server | Jobserver | Azure Active Directory**
One Identity Manager database connection data	• Database server
	• Database name
	• SQL Server login and password
	• Specifies whether integrated Windows authentication is used
	Use of the integrated Windows authentication is not recommended. If you decide to use it anyway, ensure that your environment supports Windows authentication.
Remote connection server	To configure synchronization with a target system, One Identity Manager must load the data from the target system. One Identity Manager communicates directly with the target system to do this. Sometimes direct access from the workstation, on which the

Data	Explanation
	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
- Azure Active Directory 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

- Registering an enterprise application for One Identity Manager in the Azure Active Directory tenant on page 17
- Users and permissions for synchronizing with Azure Active Directory on page 20
- Setting up the Azure Active Directory synchronization server on page 21

Creating an initial synchronization project for an Azure Active Directory tenant

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 an Azure Active Directory tenant

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

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

2. Select the **Target system type 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 **Azure Active Directory Synchronization** template.

10. On the **Restrict target system access** page, specify how system access should work. You have the following options:

Table 5: 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 synchronization steps for synchronization in the direction of the **Target system**.

Option	Meaning
	• 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 Azure Active Directory on page 20
- Information required for Azure Active Directory synchronization projects on page 25

Configuring the synchronization log

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

To configure the content of the synchronization log

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

-

Adjusting the synchronization configuration for Azure Active Directory environments

Having used the Synchronization Editor to set up a synchronization project for initial synchronization of an Azure Active Directory tenant, you can use the synchronization project to load Azure Active Directory objects into the One Identity Manager database. If you manage user accounts and their authorizations with One Identity Manager, changes are provisioned in the Azure Active Directory environment.

You must customize the synchronization configuration to be able to regularly compare the database with the Azure Active Directory 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 methods, for example.

- Use variables to set up a synchronization project for synchronizing different clients. Store a connection parameter as a variable for logging in to the clients.

- To specify which Azure Active Directory 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

-
-
-

Configuring synchronization with Azure Active Directory tenants

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

To create a synchronization configuration for synchronizing in Azure Active Directory tenants

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.

Related topics

Configuring synchronization of different Azure Active Directory tenants

If you want to customize a synchronization project to synchronize another Azure Active Directory tenant, make sure that you use the same type of authentication on the application when registering it in the Azure Active Directory tenant.

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 key is required. For more information, see Registering an enterprise application for One Identity Manager in the Azure Active Directory tenant on page 17.

To customize a synchronization project for synchronizing another Azure Active Directory tenant

1. In the Synchronization Editor, open the synchronization project.

2. Create a new base object for every other client.

   - Use the wizard to attach a base object.

   - In the wizard, select the Azure Active Directory connector.

   - Declare the connection parameters. The connection parameters are saved in a special variable set.

   A start up configuration is created that uses the newly created variable set.

3. Change other elements of the synchronization configuration as required.

4. Save the changes.

5. Run a consistency check.

Related topics

- Configuring synchronization with Azure Active Directory tenants on page 33
- Registering an enterprise application for One Identity Manager in the Azure Active Directory tenant on page 17

Customizing synchronization projects to invite guest users

For detailed information about guest users in Azure Active Directory, see the *Azure Active Directory documentation* from Microsoft.

In One Identity Manager you can set up user account with the following user types:

- **Member**: Normal Azure Active Directory user account.
- **Guest**: User account for guest users. The Azure Active Directory connector creates a user account for guest users and ensures that an invitation is sent by email to the given email address.

To send guest user invitations, you must alter the variables in the synchronization project.

Variable	Description
GuestInviteSendMail	Specifies whether the guest user invitation will be sent.

Variable	Description
	Default: **True**
GuestInviteLanguage	Language to use for sending the guest user invitation.
	Default: **en-us**
GuestInviteCustomMessage	Personal welcome greeting for the guest user.
GuestInviteRedirectUrl	URL to reroute guest users after they have accepted the invitation and registered.
	Default: **http://www.office.com**

To edit a variable

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Configuration > Variables** category.
3. Select the variable and edit its value.
4. Save the changes.

Related topics

- General main data of Azure Active Directory user accounts on page 172
- Editing connection parameters in the variable set on page 36

Supporting custom Azure Active Directory extensions

In Azure Active Directory, you can add schema extensions for Azure Active Directory applications that are registered in the company. Schema extensions in Azure Active Directory have the format extension_<appId>_<propertyName>. For more information about schema extensions, see the Microsoft Graph API under https://docs.microsoft.com/en-us/graph/extensibility-overview.

The Azure Active Directory connector can read and write Azure Active Directory schema extensions.

To map and synchronize Azure Active Directory schema extensions in One Identity Manager

1. Extend the One Identity Manager schema by the custom columns. Use the Schema Extension program to do this.

   For more information about extending the One Identity Manager schema, see the *One Identity Manager Configuration Guide*.

2. Use the Synchronization Editor to update the target system schema in your synchronization project and the One Identity Manager connection's schema.

   For more information about updating schema in the Synchronization Editor, see the *One Identity Manager Target System Synchronization Reference Guide*.

3. In the Synchronization Editor, extend the mappings in your synchronization project by the respective property mapping rules for schema extensions.

   For more information about editing property mapping rules in the Synchronization Editor, see the *One Identity Manager Target System Synchronization Reference Guide*.

Changing system connection settings of Azure Active Directory tenants

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

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

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

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

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

Detailed information about this topic

- Editing connection parameters in the variable set on page 36
- Editing target system connection properties on page 37
- Customizing synchronization projects to invite guest users on page 34
- Azure Active Directory connector settings on page 233

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. This especially applies if a synchronization project for synchronization uses different Azure Active Directory tenants.

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 37

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 36

Updating schemas

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

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

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

- A schema was changed by:

  - Changes to a target system schema

  - Customizations to the One Identity Manager schema

- A One Identity Manager update migration
- A schema in the synchronization project was shrunk by:
  - Enabling the synchronization project
  - Saving the synchronization project for the first time
  - Compressing a schema

To update a system connection schema

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Configuration > Target system** category.

   - OR -

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

   This reloads the schema data.

To edit a mapping

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

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

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

Speeding up synchronization

The Azure Active Directory connector supports delta synchronization to speed up Azure Active Directory synchronization. The method is based on the delta query function from Microsoft Graph. It supports the schema types **User** (user account), **Group** (group), and **DirectoryRole** (administrator role). Delta synchronization is not enabled by default. It is a custom setup.

Implementing delta synchronization

1. Set up a regular Azure Active Directory synchronization project.
2. Run initial synchronization.
3. Modify the **TargetSystem | AzureAD | DeltaTokenDirectory** configuration parameter.

The configuration parameter contains the directory where the delta token files are stored. In the Designer, modify the value of the configuration parameter. Ensure that the One Identity Manager Service user account has write access to the directory.

4. (Optional) Modify the `AAD_Organization_DeltaSync` process.

The process is made up of three process steps. Each process step handles on of the three supported schema types. Each process step is configured such that it synchronizes all supported delta properties of the schema types. Furthermore, each of these process step adds its own delta token file. The order of process steps is as follows:

- Synchronize user accounts (`Synchronize User` process step)
- Synchronize groups (`Synchronize Group` process step)
- Synchronize administration roles (`Synchronize DirectoryRole` process step)

If customized, ensure that the process is only generated if there is no other similar process is in the Job queue. In the same way, the process may not start during a regular synchronization.

5. (Optional) Customize processing scripts for supporting schema types.

- Process user accounts (`AAD_ProcessDeltaQueryUser` script)
- Process groups (`AAD_ProcessDeltaQueryGroup` script)
- PRocess administration roles (`AAD_ProcessDeltaQueryDirectoryRole` script)

The `AAD_ProcessDeltaQueryGroup` script has had comments added to it to simplify editing and custom development.

6. Adjust and enable the **Azure Active Directory delta synchronization** schedule

The schedule ensures regular delta synchronization of the Azure Active Directory tenants. The schedule is run by default at **15** minute intervals. You can change this interval in the Designer if necessary. Enable the schedule.

The delta synchronization sequence

1. An initial query is run for a schema type (user account, group, administrator role). The initial query returns a complete list for the schema type, such as all user accounts, including the queried properties. This also returns a state token. This token represents the state of the data at the time of the query in Azure Active Directory.

The state token and the queried properties are written to a delta token file. By default, there is no initial processing of the data.

Delta token file storage structure

`<Directory in TargetSystem | AzureAD | DeltaTokenDirectory configuration parameter>\<UID_AADOrganization>_<SchemaTyp>Query.token`

Example:

`C:\Temp\OneIM\DeltaToken\2da43fd4-ce7b-48af-9a00-686e5e3fb8a5_UserQuery.token`

2. The rest of the queries use the state token of the previous query. Apart from the new state token, they only return the objects that have changed since the last query.

- Tries to add new objects if all mandatory properties have been queried.
- Objects deleted in the target system are generally marked as **Outstanding**.

Objects that fail during processing are logged in the process step's messages.

The new state token is written in the delta token file.

Restrictions

With respect to the stability of repetitions, the difference query method has certain limitations. If a state token has been used once, it is generally invalid and the query cannot be run again. If an error occurs processing the return date, the respective change cannot be loaded until the next time synchronization is scheduled to run. For example, this happens to new group memberships if the member themselves has not been loaded yet.

Another disadvantage is the runtime of the initial query and initial data processing. This process is not recommended. However, because initial processing is meant to be carried out during scheduled synchronization, it is recommended to set the `DoNotProcessOffset` parameter in the process steps to **True** (default).

You should also take into account that not all properties can be queried using the Microsoft Graph API delta query.

If the data in the delta token file does not match the calling parameters of a query, the existing file is renamed to `<alterName>.backup` in order not to lose the state token and a new file is created. In this case, a new initial query is run. This also happens if the file does not exist or is empty.

Supported schema types

The following tables contain the supported schema types and their supported properties. As long as new objects are imported into the database, the mandatory properties in the delta synchronization must be queried.

Table 6: Supported properties for user accounts (schema type: User)

Property	Mandatory	Remark
AccountEnabled		
AgeGroup		
BusinessPhones		
City		
CompanyName		
ConsentProvidedForMinor		
Country		
Department		

Property	Mandatory	Remark
DisplayName	X	
ExternalUserState		
ExternalUserStateChangeDateTime		
GivenName		
ID	X	
JobTitle		
LastPasswordChangeDateTime		
LegalAgeGroupClassification		
Licenses		When this property is queried, another query runs about the user account's assignment status (`LicenseAssignmentStates`). This increases the runtime massively.
		Contains a list of objects with the `DisabledPlans`, `SkuId`, `AssignedByGroup`, `State`, and `Error` properties.
Mail		
MailNickname		
Manager		
MobilePhone		
OfficeLocation		
OnPremisesDistinguishedName		
OnPremisesDomainName		
OnPremisesImmutableId		
OnPremisesLastSyncDateTime		
OnPremisesSamAccountName		
OnPremisesSecurityIdentifier		
OnPremisesSyncEnabled		
OnPremisesUserPrincipalName		
PostalCode		

Property	Mandatory	Remark
PreferredLanguage		
ProxyAddresses		
State		
StreetAddress		
Surname		
UsageLocation		
UserDomain	x	
UserPrincipalName	x	
UserType	x	

Table 7: Unterstützte Eigenschaften für Gruppen (Schematyp: Group)

Property	Mandatory	Remark
Description		
DisplayName	x	
GroupTypes	x	
ID	x	
Licenses		Contains a list of objects with the `DisabledPlans` and `SkuId` properties.
Mail		
MailEnabled	x	
MailNickName	x	
Members		The property is not available in an initial query. The result contains the schema type and the ID.
OnPremisesSecurityIdentifier		
OnPremisesSyncEnabled		
Owners		The property is not available in an initial query. The result contains the schema type and the ID.
ProxyAddresses		
SecurityEnabled	x	

Table 8: Support properties for administration role (schema type: DirectoryRole)

Property	Mandatory	Remark
Description		
DisplayName	x	
ID	x	
Members		The property is not available in an initial query. The result contains the schema type and the ID.

Configuring the provisioning of memberships

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

- Memberships are saved as an object property in list form in the target system.

    Example: List of user accounts in the `Member` property of an Azure Active Directory group (`Group`)

- Memberships can be modified in either of the connected systems.

- A provisioning workflow and provisioning processes are set up.

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

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

To allow separate provisioning of memberships

1. In the Manager, select the **Azure Active Directory > Basic configuration data > Target system types** category.

2. In the result list, select the **Azure Active Directory** target system type.

3. Select the **Configure tables for publishing** task.

4. Select the assignment tables that you want to set up for single provisioning. Multi-select is possible.

5. Click **Merge mode**.

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

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 original condition

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

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

Configuring single object synchronization

Changes made to individual objects in the target system can be immediately applied in the One Identity Manager database without having to start a full synchronization of the target system environment. Individual objects can only be synchronized if the object is already present in the One Identity Manager database. The changes are applied to the mapped object properties. If a membership list belongs to one of these properties, the entries in the assignment table will also be updated. If the object is no longer present in the target system, then it is deleted from the One Identity Manager database.

Prerequisites

- A synchronization step exists that can import the changes to the changed object into One Identity Manager.

- The path to the base object of the synchronization is defined for the table that contains the changed object.

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

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

1. In the Manager, select the **Azure Active Directory > Basic configuration data > Target system types** category.

2. In the result list, select the **Azure Active Directory** 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 50
- Post-processing outstanding objects on page 51

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.

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

To use the synchronization server without load balancing.

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

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

Detailed information about this topic

- Job server for Azure Active Directory-specific process handling on page 219

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

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 an Azure Active Directory tenant on page 25

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 31
- Troubleshooting on page 55

Synchronizing single objects

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

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

To synchronize a single object

1. In the Manager, select the **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.

Features of synchronizing memberships

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

> **Example:**
>
> Base object for assigning user accounts to groups is the group.
>
> In the target system, a user account was assigned to a group. To synchronize this assignment, in the Manager, select the group that the user account was assigned to and run single object synchronization. In the process, all of the group's memberships are synchronized.
>
> The user account must already exist as an object in the One Identity Manager database for the assignment to be made.

NOTE: To load changes to the assignment of subscriptions to user accounts, run single object synchronization on the user account.

Detailed information about this topic

- Configuring single object synchronization on page 45

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 51
- Adding custom tables to the target system synchronization on page 53
- Managing Azure Active Directory user accounts through account definitions on page 54

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: Azure Active Directory** category.

   The navigation view lists all the synchronization tables assigned to the **Azure Active Directory** 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 9: 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. 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. That means, the **Connection is read-only** option must not be set for the target system connection.

Adding custom tables to the target system synchronization

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

To add custom tables to target system synchronization

1. In the Manager, select the **Azure Active Directory > Basic configuration data > Target system types** category.

2. In the result list, select the **Azure Active Directory** 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 51

Managing Azure Active Directory user accounts through account definitions

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

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

To manage user accounts through account definitions

1. Create an account definition.

2. Assign an account definition to the tenant.

3. Assign a user account in the **Linked** state to the account definition. The account definition's default manage level is applied to the user account.

   a. In the Manager, select the **Azure Active Directory > User accounts > Linked but not configured > Client>** category.

   b. Select the **Assign account definition to linked accounts** task.

   c. In the **Account definition** menu, select the account definition.

   d. Select the user accounts that contain the account definition.

   e. Save the changes.

Related topics

- Account definitions for Azure Active Directory user accounts on page 58

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 49

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.

Managing Azure Active Directory user accounts and employees

The main feature of One Identity Manager is to map employees together with the main data and permissions available to them in different target systems. To achieve this, information about user accounts and permissions can be read from the target system into the One Identity Manager database and linked to employees. This provides an overview of the permissions for each employee in all of the connected target systems. One Identity Manager offers the option of managing user accounts and their permissions. You can provision modifications in the target systems. Employees are supplied with the necessary permissions in the connected target systems according to their function in the company. Regular synchronization keeps data consistent between target systems and the One Identity Manager database.

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

- Employees can automatically obtain their account definitions using user account resources. If an employee does not yet have a user account in a tenant, a new user account is created. This is done by assigning account definitions to an employee using the integrated inheritance mechanism and subsequent process handling.

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

- When user accounts are inserted, they can be automatically assigned to an existing employee or a new employee can be created if necessary. In the process, the employee main data is created on the basis of existing user account main data. This mechanism can be implemented if a new user account is created manually or by synchronization. However, this is not the One Identity Manager default method. You must define criteria for finding employees for automatic employee assignment.

- Employees and user accounts can be entered manually and assigned to each other.

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

Related topics

Account definitions for Azure Active Directory user accounts

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

The data for the user accounts in the respective target system comes from the basic employee data. The employees must have a central 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.

Specify the manage level for an account definition for managing user accounts. The user account's manage level specifies the extent of the employee's properties that are inherited by the user account. This allows an employee to have several user accounts in one target system, for example:

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

For more detailed information about the principles of account definitions, manage levels, and determining the valid IT operating data, see the *One Identity Manager Target System Base Module Administration Guide*.

The following steps are required to implement an account definition:

- Creating account definitions
- Configuring manage levels
- Creating the formatting rules for IT operating data
- Collecting IT operating data
- Assigning account definitions to employees and target systems

Detailed information about this topic

Creating account definitions

To create a new account definition

1. In the Manager, select the **Azure Active Directory > Basic configuration data > Account definitions > Account definitions** category.
2. Click ⬛ in the result list.
3. On the main data form, enter the main data of the account definition.
4. Save the changes.

Related topics

Editing account definitions

To edit 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 **Change main data** task.

4. Enter the account definition's main data.

5. Save the changes.

Related topics

Main data for an account definition

Enter the following data for an account definition:

Table 10: Main data for an account definition

Property	Description
Account definition	Account definition name.
User account table	Table in the One Identity Manager schema that maps user accounts. For Azure Active Directory user accounts, select **AADUser**.
Target system	Target system to which the account definition applies.
Required account definition	Specifies the required account definition. Define the dependencies between account definitions. When this account definition is requested or assigned, the required account definition is assigned automatically. Leave empty for Azure Active Directory tenants.
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 assigning the account definition to employees. Set a value in the range **0** to **1**. This input field is only visible if the **QER	CalculateRiskIndex** configuration parameter is set. For detailed information, see the *One Identity Manager Risk Assessment Administration Guide*.
Service item	Service item through which you can request the account definition resource in the IT Shop. Assign an existing service item or add a new one.

Property	Description
IT Shop	Specifies whether the account definition can be requested through the IT Shop. The account definition can be requested by an employee through the Web Portal and distributed using a defined approval process. The resource can also be assigned directly to employees and roles outside the IT Shop.
Only for use in IT Shop	Specifies whether the account definition can only be requested through the IT Shop. The account definition can be requested by an employee through the Web Portal and distributed using a defined approval process. The account definition cannot be directly assigned to roles outside the IT Shop.
Automatic assignment to employees	Specifies whether the account definition is automatically assigned to all internal employees. To automatically assign the account definition to all internal employee, use the **Enable automatic assignment to employees** The account definition is assigned to every employee that is not marked as external. Once a new internal employee is created, they automatically obtain this account definition.
	To automatically remove the account definition assignment from all employees, use the **Disable automatic assignment to employees**. The account definition cannot be reassigned to employees from this point on. Existing account definition assignments remain intact.
Retain account definition if permanently disabled	Specifies the account definition assignment to permanently deactivated employees.
	Option set: The account definition assignment remains in effect. The user account remains intact.
	Option not set (default): 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 deactivated employees.
	Option set: The account definition assignment remains in effect. The user account remains intact.
	Option not set (default): 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 remains intact.
	Option not set (default): The account definition assignment is

Property	Description
	not in effect. The associated user account is deleted.
Retain account definition on security risk	Specifies the account definition assignment to employees posing a security risk.
	Option set: The account definition assignment remains in effect. The user account remains intact.
	Option not set (default): 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.
Groups can be inherited	Specifies whether the user account can inherit groups through the linked employee. If the option is set, the user account inherits groups through hierarchical roles, in which the employee is a member, or through IT Shop requests.
	• If you add an employee with a user account to a department, for example, and you have assigned groups to this department, the user account inherits these groups.
	• If an employee has requested group membership in the IT Shop and the request is granted approval, the employee's user account only inherits the group if the option is set.
Subscriptions can be inherited	Specifies whether the user account can inherit Azure Active Directory subscriptions through the employee. If this option is set, the user account inherits Azure Active Directory subscriptions through hierarchical roles or IT Shop requests.
	• If you add an employee with a user account to a department, for example, and you have assigned Azure Active Directory subscriptions to this department, the user account inherits these Azure Active Directory subscriptions.
	• If an employee has requested an Azure Active Directory subscription in the IT Shop and the request is granted approval, the employee's user account only inherits the Azure Active Directory subscription if the option is set.
Administrator roles can be inherited	Specifies whether the user account can inherit Azure Active Directory administrator roles through the employee If this option is set, the user account inherits administrator roles

Property	Description
	through hierarchical roles or IT Shop requests. • If you add an employee with a user account to a department, for example, and you have assigned administrator roles to this department, the user account inherits these administrator roles. • If an employee has requested an administrator role in the IT Shop and the request is granted approval, the employee's user account only inherits the administrator role if the option is set.
Disabled service plans can be inherited	Specifies whether the user account can inherit disabled Azure Active Directory service plans through the employee. If this option is set, the user account inherits disabled service plans through hierarchical roles or IT Shop requests. • If you add an employee with a user account to a department, for example, and you have assigned disabled service plans to this department, the user account inherits these disabled service plans. • If an employee has requested a disabled service plan in the IT Shop and the request is granted approval, the employee's user account only inherits the disabled service plan if the option is set.
Office 365 groups can be inherited	NOTE: This property is only available if the Exchange Online Module is installed. Specifies whether the user account can inherit Office 365 groups through the linked employee. If the option is set, the user account inherits Office 365 groups through hierarchical roles, in which the employee is a member, or through IT Shop requests. • If you add an employee with a user account to a department, for example, and you have assigned Office 365 groups to this department, the Azure Active Directory user account inherits these Office 365 groups. • If an employee has requested group membership in the IT Shop and the request is granted approval, the employee's Azure Active Directory user account only inherits the Office 365 group if the option is set. For more information about Office 365 groups, see the *One Identity Manager Administration Guide for Connecting to Exchange Online*.

Editing manage levels

One Identity Manager supplies a default configuration for manage levels:

- **Unmanaged**: User accounts with the **Unmanaged** manage level are linked to the employee but they do no inherit any further properties. When a new user account is added with this manage level and an employee is assigned, some of the employee's properties are transferred initially. If the employee properties are changed at a later date, the changes are not passed onto the user account.

- **Full managed**: User accounts with the **Full managed** manage level inherit defined properties of the assigned employee. When a new user account is created with this manage level and an employee is assigned, the employee's properties are transferred in an initial state. If the employee properties are changed at a later date, the changes are passed onto the user account.

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 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.
3. Select the **Change main data** task.
4. Edit the manage level's main data.
5. Save the changes.

Related topics

- Main data for manage levels on page 66
- Creating manage levels on page 65
- Assigning manage levels to account definitions on page 65

Creating manage levels

One Identity Manager supplies a default configuration for the **Unmanaged** and **Full managed** manage levels. You can define other manage levels depending on your requirements.

IMPORTANT: In the Designer, extend the templates by adding the procedure for the additional manage levels. For detailed information about templates, see the *One Identity Manager Configuration Guide*.

To create a manage level

1. In the Manager, select the **Azure Active Directory > Basic configuration data > Account definitions > Manage levels** category.

2. Click ⊞ in the result list.

3. On the main data form, edit the main data of the manage level.

4. Save the changes.

Related topics

- Main data for manage levels on page 66
- Editing account definitions on page 59
- Assigning manage levels to account definitions on page 65

Assigning manage levels to account definitions

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

To assign manage levels to an account definition

1. In the Manager, select the **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 level.

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

   To remove an assignment

   - Select the manage level and double-click ⊘.

5. Save the changes.

Main data for manage levels

Enter the following data for a manage level.

Table 11: Main data for manage levels

Property	Description
Manage level	Name of the manage level.
Description	Text field for additional explanation.
IT operating data overwrites	Specifies whether user account data formatted from IT operating data is automatically updated. Permitted values are: • **Never**: Data is not updated. (Default) • **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 deactivated retain their group memberships.
Lock user accounts if temporarily disabled	Specifies whether user accounts of temporarily deactivated employees are locked.
Retain groups if permanently disabled	Specifies whether user accounts of permanently deactivated employees retain group memberships.
Lock user accounts if permanently disabled	Specifies whether user accounts of permanently deactivated employees are locked.
Retain groups on deferred deletion	Specifies whether user accounts of employees marked for deletion retain their group memberships.
Lock user accounts if deletion is deferred	Specifies whether user accounts of employees marked for deletion are locked.
Retain groups on security risk	Specifies whether user accounts of employees posing a security risk retain their group memberships.
Lock user accounts if security is at risk	Specifies whether user accounts of employees posing a security risk are locked.
Retain groups if user account disabled	Specifies whether disabled user accounts retain their group memberships.

Creating mapping rules for IT operating data

An account definition specifies which rules are used to form the IT operating data and which default values will be used if no IT operating data can be found through the employee's primary roles.

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

- Groups can be inherited
- Administrator roles can be inherited
- Subscriptions can be inherited
- Disabled service plans can be inherited
- Change password at next login
- Identity
- Privileged user account.

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.

4. Click **Add** and enter the following information:

    - **Column**: User account property for which the value is set. In the menu, you can select the columns that use the `TSB_ITDataFromOrg` script in their template. For more information about this, 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: The business role can only be used if the Business Roles Module is available.

        - Empty

If you select a role, you must specify a default value and set the **Always use default value** option.

- **Default value**: Default value of the property for an employee's user account if the value is not determined dynamically from the IT operating data.

- **Always use default value**: Specifies whether the user account property is always set with the default value. IT operating data is not determined dynamically from a role.

- **Notify when applying the default**: Specifies whether an email is sent to a specific mailbox when the default value is used. The **Employee - new user account with default properties created** mail template is used.

  To change the mail template, in the Designer, adjust the **TargetSystem | AzureAD | Accounts | MailTemplateDefaultValues** configuration parameter.

  To change the mail template, in the Designer, adjust the **TargetSystem | AzureAD | ExchangeOnline | Accounts | MailTemplateDefaultValues** configuration parameter.

5. Save the changes.

Related topics

- Entering IT operating data on page 68

Entering IT operating data

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

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

Example:

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

Create an account definition A for the default user account of the tenant A and an account definition B for the administrative user account of tenant A.In the IT

ONE IDENTITY
by Quest

operating data mapping rule for the account definitions A and B, specify the **Department** property in order to determine the valid IT operating data.

Specify the effective IT operating data of department A for the tenant A. This IT operating data is used for standard user accounts. In addition, for department A, specify the effective IT operating data of account definition B. This IT operating data is used for administrative user accounts.

To define IT operating data

1. In the Manager, select the role in the **Organizations** or **Business roles** category.

2. Select the **Edit IT operating data** task.

3. Click **Add** and enter the following data.

    - **Effects on**: Specify an IT operating data application scope. The IT operating data can be used for a target system or a defined account definition.

        ### *To specify an application scope*

        a. Click ➜ next to the field.

        b. Under **Table**, select the table that maps the target system for select the `TSBAccountDef` table or an account definition.

        c. Select the specific target system or account definition under **Effects on**.

        d. Click **OK**.

    - **Column**: Select the user account property for which the value is set.

        In the menu, you can select the columns that use the `TSB_ITDataFromOrg` script in their template. For more information about this, see the *One Identity Manager Target System Base Module Administration Guide*.

    - **Value**: Enter a fixed value to assign to the user account's property.

4. Save the changes.

Related topics

- Creating mapping rules for IT operating data on page 67

Modify IT operating data

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

Prerequisites

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

  - OR -

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

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

To run the template

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

2. Select an account definition in the result list.

3. Select the **Run templates** task.

   This displays a list of all user accounts that were created with the selected account definition and whose properties were changed by modifying the IT operating data. That means:

   - **Old value**: Value of the object property before changing the IT operating data.
   - **New value**: Value of the object property after changing the IT operating data.
   - **Selection**: Specifies whether the new value is copied to the user account.

4. Mark all the object properties in the **selection** column that will be given the new value.

5. Click **Apply**.

   The templates are applied to all selected user accounts and properties.

Assigning account definitions to employees

Account definitions are assigned to company employees.

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

You can automatically assign special account definitions to all company employees. It is possible to assign account definitions to the IT Shop as requestable products. Department managers can then request user accounts from the Web Portal for their staff. It is also possible to add account definitions to system roles. These system roles can be assigned to employees through hierarchical roles or added directly to the IT Shop as products.

In the One Identity Manager default installation, the processes are checked at the start to see if the employee already has a user account in the target system that has an account definition. If no user account exists, a new user account is created with the account definition's default manage level.

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

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

Prerequisites for indirect assignment of account definitions to employees

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

To configure assignments to roles of a role class

1. In the Manager, select role classes in the **Organizations > Basic configuration data > Role classes** category.

   - OR -

   In the Manager, select role classes in the **Business roles > Basic configuration data > Role classes** category.

2. Select the **Configure role assignments** task and configure the permitted assignments.

   - To generally allow an assignment, enable the **Assignments allowed** column.
   - To allow direct assignment, enable the **Direct assignments permitted** column.

3. Save the changes.

For 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 72
- Assigning account definitions to business roles on page 72
- Assigning account definitions to all employees on page 73
- Assigning account definitions directly to employees on page 74
- Assigning account definitions to system roles on page 74
- Adding account definitions in the IT Shop on page 75

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 account definitions to business roles

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

To add account definitions to hierarchical roles

1. In the Manager, select the **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, select the role class and assign business roles.

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

To remove an assignment

- Select the business role and double-click ✓.

5. Save the changes.

Related topics

- Assigning account definitions to departments, cost centers, and locations on page 72
- Assigning account definitions to all employees on page 73
- Assigning account definitions directly to employees on page 74
- Assigning account definitions to system roles on page 74
- Adding account definitions in the IT Shop on page 75

Assigning account definitions to all employees

Use this task to assign the account definition to all internal employees. Employees that are marked as external do not obtain this account definition. Once a new internal employee is created, they automatically obtain this account definition. The assignment is calculated by the DBQueue Processor.

IMPORTANT: Only run this task if you can ensure that all current internal employees in the database and all pending newly added internal employees obtain a user account in this target system.

To assign an account definition to all employees

1. In the Manager, select the **Azure Active Directory > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Change main data** task.
4. Select the **Disable automatic assignment to employees** task.
5. Confirm the security prompt with **Yes**.
6. Save the changes.

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

Related topics

- Assigning account definitions to departments, cost centers, and locations on page 72
- Assigning account definitions to business roles on page 72
- Assigning account definitions directly to employees on page 74

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 system roles

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

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

To add account definitions to a system role

1. In the Manager, select the **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.

Related topics

- Assigning account definitions to departments, cost centers, and locations on page 72
- Assigning account definitions to business roles on page 72
- Assigning account definitions to all employees on page 73
- Assigning account definitions directly to employees on page 74
- Adding account definitions in the IT Shop on page 75

Adding account definitions in the IT Shop

An account definition can be requested by shop customers when it is assigned to an IT Shop shelf. To ensure it can be requested, further prerequisites need to be guaranteed.

- The account definition must be labeled with the **IT Shop** option.
- The account definition must be assigned to a service item.

> TIP: In the Web Portal, all products that can be requested are grouped together by service category. To make the account definition easier to find in the Web Portal, assign a service category to the service item.

- If the account definition is only assigned to employees using IT Shop assignments, you must also set the **Only for use in IT Shop** option. Direct assignment to hierarchical roles may not be possible.

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

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

1. In the Manager, select the **Entitlements > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Add to IT Shop** task.
4. In the **Add assignments** pane, assign the account definitions to the IT Shop shelves.
5. Save the changes.

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

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

2. Select an account definition in the result list.

3. Select the **Add to IT Shop** task.

4. In the **Add assignments** pane, assign the account definitions to the IT Shop shelves.

5. Save the changes.

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

1. In the Manager, select the **Entitlements > Account definitions** category.

2. Select an account definition in the result list.

3. Select the **Add to IT Shop** task.

4. In the **Remove assignments** pane, remove the account definitions from the IT Shop shelves.

5. Save the changes.

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

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

2. Select an account definition in the result list.

3. Select the **Add to IT Shop** task.

4. In the **Remove assignments** pane, remove the account definitions from the IT Shop shelves.

5. Save the changes.

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

1. In the Manager, select the **Entitlements > Account definitions** category.

2. Select an account definition in the result list.

3. Select the **Remove from all shelves (IT Shop)** task.

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

5. Click **OK**.

   The account definition is removed from all shelves by the One Identity Manager Service. At the same time, any requests and assignment requests with this account definition are canceled.

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

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

2. Select an account definition in the result list.

3. Select the **Remove from all shelves (IT Shop)** task.

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

5. Click **OK**.

   The account definition is removed from all shelves by the One Identity Manager Service. At the same time, any requests and assignment requests with this account definition are canceled.

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

Related topics

- Main data for an account definition on page 60
- Assigning account definitions to departments, cost centers, and locations on page 72
- Assigning account definitions to business roles on page 72
- Assigning account definitions to all employees on page 73
- Assigning account definitions directly to employees on page 74
- Assigning account definitions to system roles on page 74

Assigning account definitions to Azure Active Directory tenants

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 Azure Active Directory tenant in the **Azure Active Directory > Tenants** category.

2. Select the **Change main data** task.

3. From the **Account definition (initial)** menu, select the account definition for user accounts.

4. Save the changes.

Detailed information about this topic

- Assigning employees automatically to Azure Active Directory user accounts on page 80

Deleting account definitions

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

To delete an account definition

1. Remove automatic assignments of the account definition from all employees.

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

    b. Select an account definition in the result list.

    c. Select the **Change main data** task.

    d. Select the **Disable automatic assignment to employees** task.

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

    f. Save the changes.

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

    a. In the Manager, select the **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 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.

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

  e. 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 Designer Web Portal User Guide*.

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

  a. In the Manager, select the **Entitlements > Account definitions** category.

  b. Select an account definition in the result list.

  c. Select the **Remove from all shelves (IT Shop)** task.

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

  e. Click **OK**.

The account definition is removed from all shelves by the One Identity Manager Service. At the same time, any requests and assignment requests with this account definition are canceled.

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

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

  b. Select an account definition in the result list.

  c. Select the **Remove from all shelves (IT Shop)** task.

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

  e. Click **OK**.

The account definition is removed from all shelves by the One Identity Manager Service. At the same time, any requests and assignment requests with this account definition are canceled.

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 main 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 Azure Active Directory tenant in the **Azure Active Directory > Tenants** category.

   b. Select the **Change main 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.

Assigning employees automatically to Azure Active Directory user accounts

When you add a user account, an existing employee can automatically be assigned to it. If necessary, a new employee can be created. The identity's main data is created on the basis of existing user account main data. This mechanism can be triggered after a new user account is created either manually or through synchronization.When you add a user account, an existing identity can automatically be assigned to it. If necessary, a new identity can be created. The identity's main data is created on the basis of existing user account main data. This mechanism can follow on after a new user account has been created manually or through synchronization.

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

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

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

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

Run the following tasks to assign employees automatically:

- If you want employees to be assigned during the synchronization of user accounts, in the Designer, set the **TargetSystem | AzureAD | PersonAutoFullsync** configuration parameter and select the required mode.

- If you want employees to be assigned outside synchronization in the Designer, set the **TargetSystem | AzureAD | PersonAutoDefault** configuration parameter and select the required mode.

- In the **TargetSystem | AzureAD | PersonExcludeList** configuration parameter, define the user accounts for which no automatic assignment to employees is to take place.

  Example:

  ADMINISTRATOR|GUEST

  TIP: You can edit the value of the configuration parameter in the **Exclude list for automatic employee assignment** dialog.

  To edit the exclude list for automatic employee assignment

  1. In the Designer, edit the **PersonExcludeList** configuration parameter.

  2. Click **...** next to the **Value** field.

     This opens the **Exclude list for automatic employee assignment** dialog.

  3. To add a new entry, click ⊞ **Add**.

     To edit an entry, select it and click ✎ **Edit**.

  4. Enter the name of the user account that does not allow employees to be assigned automatically.

     Each entry in the list is handled as part of a regular expression. You are allowed to use the usual special characters for regular expressions.

  5. To delete an entry, select it and click ✖ **Delete**.

  6. Click **OK**.

- Use the **TargetSystem | AzureAD | PersonAutoDisabledAccounts** configuration parameter to specify whether employees can be automatically assigned to disabled user accounts. User accounts do not obtain an account definition.

- Assign an account definition to the tenant. Ensure that the manage level to be used is entered as the default manage level.

- Define the search criteria for employee assignment in the tenant.

NOTE:

The following applies for synchronization:

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

The following applies outside synchronization:

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

NOTE:

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

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

For more information, see Managing Azure Active Directory user accounts through account definitions on page 54.

Related topics

- Creating account definitions on page 59
- Assigning account definitions to Azure Active Directory tenants on page 77
- Changing manage levels for Azure Active Directory user accounts on page 85
- Editing search criteria for automatic employee assignment on page 82
- Finding employees and directly assigning them to user accounts on page 83

Editing search criteria for automatic employee assignment

NOTE: One Identity Manager supplies a default mapping for employee assignment. Only carry out the following steps when you want to customize the default mapping.

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

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

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

NOTE: Object definitions for user accounts that can have search criteria applied to them are predefined. For example, if you require other objects definitions that limit a preselection of user accounts, set up the respective custom object definitions in the Designer. For

more information, see the *One Identity Manager Configuration Guide*.

To specify criteria for employee assignment

1. In the Manager, select the **Azure Active Directory > Tenants** category.

2. Select the tenant in the result list.

3. Select the **Define search criteria for employee assignment** task.

4. Specify which user account properties must match with which employee so that the employee is linked to the user account.

Table 12: Default search criteria for user accounts and contacts

Apply to	Column for employee	Column for user account
Azure Active Directory user accounts	Central user account (`CentralAccount`)	Alias (`MailNickName`)

5. Save the changes.

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

Related topics

- Assigning employees automatically to Azure Active Directory user accounts on page 80
- Finding employees and directly assigning them to user accounts on page 83

Finding employees and directly assigning them to user accounts

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

Table 13: Manual assignment view

View	Description
Suggested assignments	This view lists all user accounts to which One Identity Manager can assign an employee. All employees are shown who were found using the search criteria and can be assigned.
Assigned user accounts	This view lists all user accounts to which an employee is assigned.

View	Description
Without employee assignment	This view lists all user accounts to which no employee is assigned and for which no employee was found using the search criteria.

To apply search criteria to user accounts

1. In the Manager, select the **Azure Active Directory > Tenants** category.

2. Select the tenant in the result list.

3. Select the **Define search criteria for employee assignment** task.

4. At the bottom of the form, click **Reload**.

   All possible assignments based on the search criteria are found in the target system for all user accounts. The three views are updated.

TIP: By double-clicking on an entry in the view, you can view the user account and employee main data.

The assignment of employees to user accounts creates connected user accounts (**Linked** state). To create managed user accounts (**Linked configured** state), you can assign an account definition at the same time.

To assign employees directly over a suggestion list

- Click **Suggested assignments**.

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

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

  3. Click **Assign selected**.

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

     The employees determined using the search criteria are assigned to the selected user accounts. If an account definition was selected, this is assigned to all selected user accounts.

  - OR -

- Click **No employee assignment**.

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

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

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

  4. Click **Assign selected**.

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

   The employees displayed in the **Employee** column are assigned to the selected user accounts. If an account definition was selected, this is assigned to all selected user accounts.

To remove assignments

- Click **Assigned user accounts**.

  1. Click the **Selection** box of all the user accounts you want to delete the employee assignment from. Multi-select is possible.

  2. Click **Remove selected**.

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

     The assigned employees are removed from the selected user accounts.

Changing manage levels for Azure Active Directory user accounts

The default manage level is applied if you create user accounts using automatic employee assignment. You can change a user account manage level later.

To change the manage level for a user account

1. In the Manager, select the **Azure Active Directory > User accounts** category.

2. Select the user account in the result list.

3. Select the **Change main data** task.

4. Select the manage level in the **Manage level** list on the **General** tab.

5. Save the changes.

Related topics

- Creating and editing Azure Active Directory user accounts on page 171

Supported user account types

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

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

- Identity

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

  Table 14: Identities of user accounts

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

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

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

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

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

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

- Privileged user account

  Privileged user accounts are used to provide employees with additional privileges. This includes administrative user accounts or service accounts, for example. The user

accounts are labeled with the **Privileged user account** property
(`IsPrivilegedAccount` column).

Detailed information about this topic

Default user accounts

Normally, each employee obtains a default user account, which has the permissions they require for their regular work. The user accounts are linked to the employee. The effect of the link and the scope of the employee's inherited properties on the user accounts can be configured through an account definition and its manage levels.

To create default user accounts through account definitions

1. Create an account definition and assign the **Unmanaged** and **Full managed** manage levels.

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

3. Create a formatting rule for IT operating data.

   You use the mapping rule to define which rules are used to map IT operating data for user accounts and which default values are used if no IT operating data can be determined through a person's primary roles.

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

   - In the mapping rules for the `IsGroupAccount_Group`, `IsGroupAccount_SubSku`, and `IsGroupAccount_DeniedService` columns, use the default value **1** and set the **Always use default value** option.

   - In the mapping rule for the `IdentityType` column, use the default value **Primary** and enable **Always use default value**.

4. Enter the effective IT operating data for the target system. Select the concrete target system under **Effects on**.

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

5. Assign the account definition to employees.

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

Related topics

- Account definitions for Azure Active Directory user accounts on page 58

Administrative user accounts

An administrative user account must be used for certain administrative tasks. Administrative user accounts are usually predefined by the target system and have fixed names and login names, such as **Administrator**.

Administrative user accounts are imported into One Identity Manager during synchronization.

NOTE: Some administrative user accounts can be automatically identified as privileged user accounts. To do this, in the Designer, enable the **Mark selected user accounts as privileged** schedule.

Related topics

- Providing administrative user accounts for one employee on page 88
- Providing administrative user accounts for several employees on page 89

Providing administrative user accounts for one employee

Prerequisites

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

To prepare an administrative user account for a person

1. Label the user account as a personalized admin identity.

    a. In the Manager, select the **Azure Active Directory > User accounts** category.

    b. Select the user account in the result list.

    c. Select the **Change main data** task.

d. On the **General** tab, in the **Identity** selection list, select **Personalized administrator identity**.

2. Link the user account to the employee who will be using this administrative user account.

   a. In the Manager, select the **Azure Active Directory > User accounts** category.

   b. Select the user account in the result list.

   c. Select the **Change main data** task.

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

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

Related topics

- Providing administrative user accounts for several employees on page 89
- For more information about mapping employee identities, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Providing administrative user accounts for several employees

Prerequisite

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

To prepare an administrative user account for multiple employees

1. Label the user account as a shared identity.

   a. In the Manager, select the **Azure Active Directory > User accounts** category.

   b. Select the user account in the result list.

   c. Select the **Change main data** task.

   d. On the **General** tab, in the **Identity** menu, select **Shared identity**.

2. Link the user account to a pseudo employee.

a. In the Manager, select the **Azure Active Directory > User accounts** category.

b. Select the user account in the result list.

c. Select the **Change main data** task.

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

> TIP: If you are the target system manager, you can choose ⊞ to create a new pseudo employee.

3. Assign the employees who will use this administrative user account to the user account.

a. In the Manager, select the **Azure Active Directory > User accounts** category.

b. Select the user account in the result list.

c. Select the **Assign employees authorized to use** task.

d. In the **Add assignments** pane, add employees.

> TIP: In the **Remove assignments** pane, you can remove assigned employees.
>
> *To remove an assignment*
>
> • Select the employee and double-click ✓.

Related topics

- Providing administrative user accounts for one employee on page 88
- For detailed information about mapping employee identities, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Privileged user accounts

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

NOTE: The criteria according to which user accounts are automatically identified as privileged are defined as extensions to the view definition (ViewAddOn) in the `TSBVAccountIsPrivDetectRule` table (which is a table of the **Union** type). The evaluation is done in the `TSB_SetIsPrivilegedAccount` script.

To create privileged users through account definitions

1. Create an account definition. Create a new manage level for privileged user accounts and assign this manage level to the account definition.

2. If you want to prevent the properties for privileged user accounts from being overwritten, set the **IT operating data overwrites** property for the manage level to **Only initially**. In this case, the properties are populated just once when the user accounts are created.

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

4. Create a formatting rule for the IT operating data.

   You use the mapping rule to define which rules are used to map IT operating data for user accounts and which default values are used if no IT operating data can be determined through a person's primary roles.

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

   - In the mapping rule for the `IsPrivilegedAccount` column, use the default value **1** and set the **Always use default value** option.

   - You can also specify a mapping rule for the `IdentityType` column. The column owns different permitted values that represent user accounts.

   - To prevent privileged user accounts from inheriting the entitlements of the default user, define a mapping rule for the `IsGroupAccount_Group`, `IsGroupAccount_SubSku`, and `IsGroupAccount_DeniedService` columns with a default value of **0** and set the **Always use default value** option.

5. Enter the effective IT operating data for the target system.

   Specify in the departments, cost centers, locations, or business roles which IT operating data should apply when you set up a user account.

6. Assign the account definition directly to employees who work with privileged user accounts.

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

TIP: If customization requires that the login names of privileged user accounts follow a defined naming convention, specify how the login names are formatted in the template.

- To use a prefix for the login name, in the Designer, set the **TargetSystem | AzureAD | Accounts | PrivilegedAccount | AccountName_Prefix** configuration parameter.

- To use a postfix for the login name, in the Designer, set the **TargetSystem | AzureAD | Accounts | PrivilegedAccount | AccountName_Postfix** configuration parameter.

These configuration parameters are evaluated in the default installation, if a user account is marked with the **Privileged user account** property (`IsPrivilegedAccount` column). The user account login names are renamed according to the formatting rules. This also occurs if the user accounts are labeled as privileged using the **Mark selected user accounts as privileged** schedule. If necessary, modify the schedule in the Designer.

Related topics

- Account definitions for Azure Active Directory user accounts on page 58

Specifying deferred deletion for Azure Active Directory user accounts

You can use deferred deletion to specify how long the user accounts remain in the database after deletion is triggered before they are finally removed. By default, user accounts are finally deleted from the database after 30 days. First, the user accounts are disabled or blocked. You can reenable the user accounts up until deferred deletion runs. After deferred deletion is run, the user accounts are deleted from the database and cannot be restored anymore.

You have the following options for configuring deferred deletion.

- Global deferred deletion: Deferred deletion applies to user accounts in all target system. The default value is **30** days.

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

- Object-specific deferred deletion: Deferred deletion can be configured depending on certain properties of the accounts.

  To use object-specific deferred deletion, in the Designer, create a Script (deferred deletion) for the **AADUser** table.

> **Example:**
>
> Deferred deletion of privileged user accounts is 10 days. The following **Script (deferred deletion)** is entered in the table.
>
> ```
> If Not $IsPrivilegedAccount:Bool$ Then
>      Value = 10
> End If
> ```

For detailed information on editing table definitions and configuring deferred deletion in the Designer, see the *One Identity Manager Configuration Guide*.

Managing memberships in Azure Active Directory groups

Azure Active Directory user accounts can be grouped into Azure Active Directory groups that can be used to regulate access to resources.

In One Identity Manager, you can assign Azure Active Directory groups directly to user accounts or they can be inherited through departments, cost centers, locations, or business roles. Users can also request the groups through the Web Portal. To do this, groups are provided in the IT Shop.

NOTE: Assignments to Azure Active Directory groups that are synchronized with the local Active Directory are not allowed in One Identity Manager. These groups cannot be requested through the web portal. You can only manage these groups in your locally. For more information, see the *Azure Active Directory documentation* from Microsoft.

Detailed information about this topic

- Assigning Azure Active Directory groups to Azure Active Directory user accounts on page 93
- Effectiveness of group memberships on page 103
- Azure Active Directory group inheritance based on categories on page 105
- Overview of all assignments on page 107

Assigning Azure Active Directory groups to Azure Active Directory user accounts

Azure Active Directory groups can be assigned directly or indirectly to Azure Active Directory user accounts.

In the case of indirect assignment, employees and Azure Active Directory groups are assigned to hierarchical roles, such as departments, cost centers, locations, or business roles. The Azure Active Directory 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 Azure Active Directory group.

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

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

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

For detailed information see the following guides:

Topic	Guide
Basic principles for assigning and inheriting company resources	*One Identity Manager Identity Management Base Module Administration Guide*
	One Identity Manager Business Roles Administration Guide
Assigning company resources through IT Shop requests	*One Identity Manager IT Shop Administration Guide*
System roles	*One Identity Manager System Roles Administration Guide*

Detailed information about this topic

- Prerequisites for indirect assignment of Azure Active Directory groups to Azure Active Directory user accounts on page 95
- Assigning Azure Active Directory groups to departments, cost centers and locations on page 96
- Assigning Azure Active Directory groups to business roles on page 97
- Adding Azure Active Directory groups to system roles on page 98
- Adding Azure Active Directory groups to the IT Shop on page 99
- Assigning Azure Active Directory user accounts directly to Azure Active Directory groups on page 101
- Assigning Azure Active Directory groups directly to Azure Active Directory user accounts on page 102

Prerequisites for indirect assignment of Azure Active Directory groups to Azure Active Directory user accounts

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

1. Assignment of employees and Azure Active Directory groups is permitted for role classes (departments, cost centers, locations, or business roles).

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

   To configure assignments to roles of a role class

   a. In the Manager, select role classes in the **Organizations > Basic configuration data > Role classes** category.

      - OR -

      In the Manager, select role classes in the **Business roles > Basic configuration data > Role classes** category.

   b. Select the **Configure role assignments** task and configure the permitted assignments.

      - To generally allow an assignment, enable the **Assignments allowed** column.
      - To allow direct assignment, enable the **Direct assignments permitted** column.

   c. Save the changes.

2. Settings for assigning Azure Active Directory groups to Azure Active Directory user accounts.

   - The Azure Active Directory user account is linked to an employee.
   - The Azure Active Directory user account has the **Groups can be inherited** option set.

NOTE: There are other configuration settings that play a role when company resources are inherited through departments, cost centers, locations, and business roles. For example, role inheritance might be blocked or inheritance of employees not allowed. For more detailed information about the basic principles for assigning company resources, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Related topics

Assigning Azure Active Directory groups to departments, cost centers and locations

Assign groups to departments, cost centers, or locations so that the group can be assigned to user accounts through these organizations.

This task is not available for dynamic groups.

To assign a group to departments, cost centers, or locations (non role-based login)

1. In the Manager, select the **Azure Active Directory > Groups** category.
2. Select the group in the result list.
3. Select the **Assign organizations** task.
4. In the **Add assignments** pane, assign the organizations:
   - On the **Departments** tab, assign departments.
   - On the **Locations** tab, assign locations.
   - On the **Cost centers** tab, assign cost centers.

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

   ### To remove an assignment
   - Select the organization and double-click ⊘.
5. Save the changes.

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

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

   - OR -

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

   - OR -

   In the Manager, select the **Organizations > Locations** category.
2. Select the department, cost center, or location in the result list.
3. Select the **Assign Azure Active Directory groups** task.
4. In the **Add assignments** pane, assign groups.

> TIP: In the **Remove assignments** pane, you can remove the assignment of groups.
>
> ***To remove an assignment***
>
> - Select the group and double-click ✅.

5. Save the changes.

Related topics

- Prerequisites for indirect assignment of Azure Active Directory groups to Azure Active Directory user accounts on page 95
- Assigning Azure Active Directory groups to business roles on page 97
- Adding Azure Active Directory groups to system roles on page 98
- Adding Azure Active Directory groups to the IT Shop on page 99
- Assigning Azure Active Directory user accounts directly to Azure Active Directory groups on page 101
- Assigning Azure Active Directory groups directly to Azure Active Directory user accounts on page 102
- One Identity Manager users for managing an Azure Active Directory environment on page 11

Assigning Azure Active Directory groups to business roles

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

Assign the group to business roles so that the group is assigned to user accounts through these business roles.

This task is not available for dynamic groups.

To assign a group to a business role (non role-based login)

1. In the Manager, select the **Azure Active Directory > Groups** category.
2. Select the group in the result list.
3. Select the **Assign business roles** task.
4. In the **Add assignments** pane, select the role class and assign business roles.

   > TIP: In the **Remove assignments** pane, you can remove assigned business roles.
   >
   > ***To remove an assignment***
   >
   > - Select the business role and double-click ✅.

5. Save the changes.

To assign groups to a business role (non role-based login or role-based login)

1. In the Manager, select the **Business roles > <role class>** category.

2. Select the business role in the result list.

3. Select the **Assign Azure Active Directory groups** task.

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

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

   ### *To remove an assignment*

   - Select the group and double-click ⊘.

5. Save the changes.

Related topics

Adding Azure Active Directory groups to system roles

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

Use this task to add a group to system roles.

If you assign a system role to employees, all Azure Active Directory user accounts owned by this employee inherit the group.

This task is not available for dynamic groups.

NOTE: Groups with **Only use in IT Shop** set can only be assigned to system roles that also have this option set. For more information, see the *One Identity Manager System Roles Administration Guide*.

To assign a group to system roles

1. In the Manager, select the **Azure Active Directory > Groups** category.

2. Select the group in the result list.

3. Select the **Assign system roles** task.

4. In the **Add assignments** pane, assign system roles.

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

   ### *To remove an assignment*

   - Select the system role and double-click ⊘.

5. Save the changes.

Related topics

- Prerequisites for indirect assignment of Azure Active Directory groups to Azure Active Directory user accounts on page 95
- Assigning Azure Active Directory groups to departments, cost centers and locations on page 96
- Assigning Azure Active Directory groups to business roles on page 97
- Adding Azure Active Directory groups to the IT Shop on page 99
- Assigning Azure Active Directory user accounts directly to Azure Active Directory groups on page 101
- Assigning Azure Active Directory groups directly to Azure Active Directory user accounts on page 102

Adding Azure Active Directory groups to the IT Shop

When you assign a group to an IT Shop shelf, it can be requested by the shop customers. To ensure it can be requested, further prerequisites need to be guaranteed:

- The group is not a dynamic group.
- The group must be labeled with the **IT Shop** option.
- The group must be assigned a service item.

  TIP: In the Web Portal, all products that can be requested are grouped together by service category. To make the group easier to find in the Web Portal, assign a service category to the service item.

- If you only want the group to be assigned to employees through IT Shop requests, the group must also be labeled with the **Use only in IT Shop** option. Direct assignment to hierarchical roles or user accounts is no longer permitted.

NOTE: With role-based login, the IT Shop administrators can assign groups to IT Shop shelves. Target system administrators are not authorized to add groups to IT Shop.

To add a group to the IT Shop.

1. In the Manager, select the **Azure Active Directory > Groups** category (non role-based login) category.

   - OR -

   In the Manager, select the **Entitlements > Azure Active Directory groups** (role-based login) category.

2. In the result list, select the group.

3. Select the **Add to IT Shop** task.

4. In the **Add assignments** pane, assign the group to the IT Shop shelves.

5. Save the changes.

To remove a group from individual shelves of the IT Shop

1. In the Manager, select the **Azure Active Directory > Groups** category (non role-based login) category.

   - OR -

   In the Manager, select the **Entitlements > Azure Active Directory groups** (role-based login) category.

2. In the result list, select the group.

3. Select the **Add to IT Shop** task.

4. In the **Remove assignments** pane, remove the group from the IT Shop shelves.

5. Save the changes.

To remove a group from all shelves of the IT Shop

1. In the Manager, select the **Azure Active Directory > Groups** (non role-based login) category.

   - OR -

   In the Manager, select the **Entitlements > Azure Active Directory groups** (role-based login) category.

2. In the result list, select the group.

3. Select the **Remove from all shelves (IT Shop)** task.

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

5. Click **OK**.

   The group is removed from all shelves by the One Identity Manager Service. All requests and assignment requests with this group, are canceled.

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

Related topics

Assigning Azure Active Directory user accounts directly to Azure Active Directory groups

To react quickly to special requests, you can assign groups directly to user accounts. You cannot directly assign groups that have the **Only use in IT Shop** option.

NOTE: User accounts cannot be manually added to dynamic groups.

To assign user accounts directly to a group

1. In the Manager, select the **Azure Active Directory > Groups** category.
2. Select the group in the result list.
3. Select the **Assign user accounts** task.
4. In the **Add assignments** pane, assign the user accounts.

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

   To remove an assignment

   - Select the user account and double-click ⊘.
5. Save the changes.

Related topics

Assigning Azure Active Directory groups directly to Azure Active Directory user accounts

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

NOTE: User accounts cannot be manually added to dynamic groups.

To assign groups directly to user accounts

1. In the Manager, select the **Azure Active Directory > User accounts** category.
2. Select the user account in the result list.
3. Select the **Assign groups** task.
4. In the **Add assignments** pane, assign the groups.

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

   To remove an assignment

   - Select the group and double-click ⊘.

5. Save the changes.

Related topics

Effectiveness of group memberships

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

It is possible to assign an excluded group at any time either directly, indirectly, or with an IT Shop request. One Identity Manager determines whether the assignment is effective.

NOTE:

- You cannot define a pair of mutually exclusive groups. That means, the definition "Group A excludes group B" AND "Group B excludes groups A" is not permitted.

- You must declare each group to be excluded from a group separately. Exclusion definitions cannot be inherited.

- One Identity Manager does not check if membership of an excluded group is permitted in another group (table).

The effectiveness of the assignments is mapped in the `AADUserInGroup` and `AADBaseTreeHasGroup` tables by the `XIsInEffect` column.

Example: The effect of group memberships

- Group A is defined with permissions for triggering requests in a tenant. A group B is authorized to make payments. A group C is authorized to check invoices.

- Group A is assigned through the "Marketing" department, group B through "Finance", and group C through the "Control group" business role.

Clara Harris has a user account in this tenant. She primarily belongs to the "Marketing" department. The "Control group" business role and the "Finance" department are assigned to her secondarily. Without an exclusion definition, the user account obtains all the permissions of groups A, B, and C.

By using suitable controls, you want to prevent an employee from being able to trigger a request and to pay invoices. That means, groups A, B, and C are mutually exclusive. An employee that checks invoices may not be able to make invoice payments as well. That means, groups B and C are mutually exclusive.

Table 15: Specifying excluded groups (`AADGroupExclusion` table)

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

Table 16: Effective assignments

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

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

The groups A and C are in effect for Jenny Basset because the groups are not defined as mutually exclusive. That means that the employee is authorized to trigger requests and to check invoices. If this should not be allowed, define further exclusion for group C.

Table 17: Excluded groups and effective assignments

Employee	Member in role	Assigned group	Excluded group	Effective group
Jenny Basset	Marketing	Group A		Group C
	Control group	Group C	Group B Group A	

Prerequisites

- The **QER | Structures | Inherite | GroupExclusion** configuration parameter is set.

  In the Designer, set the configuration parameter and compile the database.

  NOTE: If you disable the configuration parameter at a later date, model components and scripts that are not longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of

preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*.

- Mutually exclusive groups belong to the same tenant.

To exclude a group

1. In the Manager, select the **Azure Active Directory > Groups** category.

2. Select a group in the result list.

3. Select the **Exclude groups** task.

4. In the **Add assignments** pane, assign the groups that are mutually exclusive to the selected group.

   - OR -

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

5. Save the changes.

Azure Active Directory group inheritance based on categories

In One Identity Manager, user accounts can selectively inherit groups, administrator roles, subscriptions, and disabled service plans. To do this, the groups (administrator roles, subscriptions, and disabled service plans) and the user accounts are divided into categories. The categories can be freely selected and are specified using a mapping rule. Each category is given a specific position within the template. The mapping rule contains different tables. Use the user account table to specify categories for target system dependent user accounts. In the other tables, enter your categories for the groups, administrator roles, subscriptions, and disabled service plans. Each table contains the category positions **position 1** to **position 63**.

Every user account can be assigned to one or more categories. Each group can also be assigned to one or more categories. The group is inherited by the user account when at least one user account category items matches an assigned group. The group is also inherited by the user account if the group or the user account is not put into categories.

NOTE: Inheritance through categories is only taken into account when groups are assigned indirectly through hierarchical roles. Categories are not taken into account when groups are directly assigned to user accounts.

Table 18: Category examples

Category item	Categories for user accounts	Categories for groups
1	Default user	Default permissions

Category item	Categories for user accounts	Categories for groups
2	System users	System user permissions
3	System administrator	System administrator permissions

Figure 2: Example of inheriting through categories.
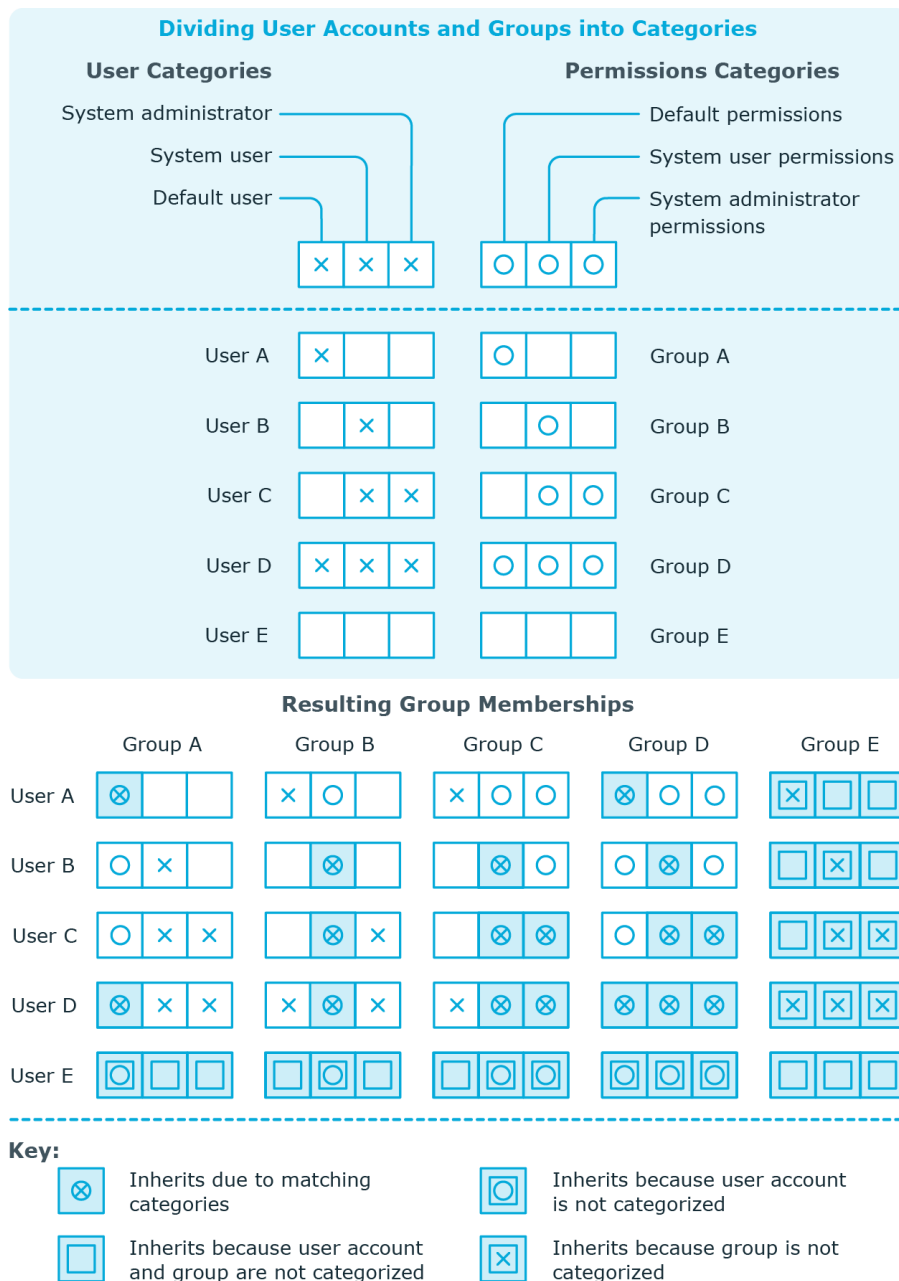
To use inheritance through categories

1. In the Manager, define the categories in the Azure Active Directory tenant.

2. In the Manager, assign categories to user accounts through their main data.

3. In the Manager, assign categories to groups through their main data.

Related topics

Overview of all assignments

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

Examples:

- If the report is created for a resource, all roles are determined in which there are employees with this resource.

- If the report is created for a group or another system entitlement, all roles are determined in which there are employees with this group or system entitlement.

- If the report is created for a compliance rule, all roles are determined in which there are employees who violate this compliance rule.

- If the report is created for a department, all roles are determined in which employees of the selected department are also members.

- If the report is created for a business role, all roles are determined in which employees of the selected business role are also members.

To display detailed information about assignments

- To display the report, select the base object from the navigation or the result list and select the **Overview of all assignments** report.

- Click the ⊞ **Used by** button in the report toolbar to select the role class for which you want to determine whether roles exist that contain employees with the selected base object.

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

- Double-click a control to show all child roles belonging to the selected role.

- By clicking the ⌄ button in a role's control, you display all employees in the role with the base object.

- Use the small arrow next to ⌄ to start a wizard that allows you to bookmark this list of employees for tracking. This creates a new business role to which the employees are assigned.

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

🛈 🖫 | ⊞ Used by ▾ | ▼ | ▶ Department ▶ Dresden
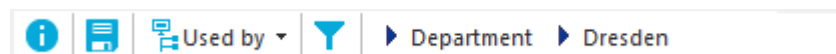
Table 19: Meaning of icons in the report toolbar

Icon	Meaning
🛈	Show the legend with the meaning of the report control elements
🖫	Saves the current report view as a graphic.
⊞	Selects the role class used to generate the report.
▼	Displays all roles or only the affected roles.

Managing Azure Active Directory administrator roles assignments

In One Identity Manager, you can assign the Azure Active Directory administrator roles directly to user accounts or they can be inherited through departments, cost centers, locations, or business roles. Users can also request the administrator roles through the Web Portal. To do this, administrator roles are provided in the IT Shop.

Detailed information about this topic

- Assigning Azure Active Directory administrator roles to Azure Active Directory user accounts on page 109
- Azure Active Directory administrator role inheritance based on categories on page 118
- Overview of all assignments on page 107

Assigning Azure Active Directory administrator roles to Azure Active Directory user accounts

Azure Active Directory administrator roles can be assigned directly or indirectly to Azure Active Directory user accounts.

In the case of indirect assignment, employees and Azure Active Directory administrator roles are assigned to hierarchical roles, such as, departments, cost centers, locations, or business roles. The Azure Active Directory administrator roles 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 Azure Active Directory administrator roles.

You can also request Azure Active Directory administration roles in the Web Portal. To do this, add employees to a shop as customers. All Azure Active Directory administrator roles

assigned as products to this shop, can be requested by the customers. Requested Azure Active Directory administrator roles are assigned to the employees after approval is granted.

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

To react quickly to special requests, you can assign Azure Active Directory administrator roles directly to Azure Active Directory user accounts.

For detailed information see the following guides:

Topic	Guide
Basic principles for assigning and inheriting company resources	*One Identity Manager Identity Management Base Module Administration Guide*
	One Identity Manager Business Roles Administration Guide
Assigning company resources through IT Shop requests	*One Identity Manager IT Shop Administration Guide*
System roles	*One Identity Manager System Roles Administration Guide*

Detailed information about this topic

- Prerequisites for indirect assignment of Azure Active Directory administration roles to Azure Active Directory user accounts on page 111
- Assigning Azure Active Directory administrator roles to departments, cost centers, and locations on page 112
- Assigning Azure Active Directory administrator roles to business roles on page 113
- Adding Azure Active Directory administrator roles to system roles on page 114
- Adding Azure Active Directory administrator roles in the IT Shop on page 115
- Assigning Azure Active Directory user accounts directly to Azure Active Directory administrator roles on page 117
- Assigning Azure Active Directory administrator roles directly to Azure Active Directory user accounts on page 118

Prerequisites for indirect assignment of Azure Active Directory administration roles to Azure Active Directory user accounts

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

1. Assignment of employees and Azure Active Directory administrator roles is permitted for role classes (departments, cost centers, locations, or business roles).

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

   To configure assignments to roles of a role class

   a. In the Manager, select role classes in the **Organizations > Basic configuration data > Role classes** category.

      - OR -

      In the Manager, select role classes in the **Business roles > Basic configuration data > Role classes** category.

   b. Select the **Configure role assignments** task and configure the permitted assignments.

      - To generally allow an assignment, enable the **Assignments allowed** column.

      - To allow direct assignment, enable the **Direct assignments permitted** column.

   c. Save the changes.

2. Settings for assigning Azure Active Directory administrator roles to Azure Active Directory user accounts.

   - The Azure Active Directory user account is linked to an employee.

   - The Azure Active Directory user account has the **Administrator roles can be inherited** option set.

NOTE: There are other configuration settings that play a role when company resources are inherited through departments, cost centers, locations, and business roles. For example, role inheritance might be blocked or inheritance of employees not allowed. For more detailed information about the basic principles for assigning company resources, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Related topics

Assigning Azure Active Directory administrator roles to departments, cost centers, and locations

By assigning administrator roles to departments, cost centers, or locations, you enable the group to be assigned to user accounts through these organizations.

To assign an administrator role to departments, cost centers, or locations (non role-based login)

1. In the Manager, select the **Azure Active Directory > Administrator roles** category.

2. Select the administrator role in the result list.

3. Select the **Assign organizations** task.

4. In the **Add assignments** pane, assign the organizations:

    - On the **Departments** tab, assign departments.

    - On the **Locations** tab, assign locations.

    - On the **Cost centers** tab, assign cost centers.

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

    To remove an assignment

    - Select the organization and double-click ✅.

5. Save the changes.

To assign administrator roles to departments, cost centers or locations (role-based login)

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

    - OR -

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

    - OR -

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

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

3. Select the **Assign Azure Active Directory administrator roles** task.

4. In the **Add assignments** pane, assign administrator roles.

ONE IDENTITY
by Quest

One Identity Manager 8.2 Administration Guide for Connecting to
Azure Active Directory

Managing Azure Active Directory administrator roles assignments

112

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

To remove an assignment

- Select the administrator role and double-click ✅.

5. Save the changes.

Related topics

- Prerequisites for indirect assignment of Azure Active Directory administration roles to Azure Active Directory user accounts on page 111
- Assigning Azure Active Directory administrator roles to business roles on page 113
- Assigning Azure Active Directory user accounts directly to Azure Active Directory administrator roles on page 117
- Adding Azure Active Directory administrator roles to system roles on page 114
- Adding Azure Active Directory administrator roles in the IT Shop on page 115
- One Identity Manager users for managing an Azure Active Directory environment on page 11

Assigning Azure Active Directory administrator roles to business roles

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

By assigning administrator roles to business roles, the administrator role can be assigned to user accounts through these business roles.

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

1. In the Manager, select the **Azure Active Directory > Administrator roles** category.
2. Select the administrator role in the result list.
3. Select the **Assign business roles** task.
4. In the **Add assignments** pane, select the role class and assign business roles.

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

   #### *To remove an assignment*

   - Select the business role and double-click ✅.

5. Save the changes.

To assign administrator roles to a business role (non role-based login)

1. In the Manager, select the **Business roles > <role class>** category.

2. Select the business role in the result list.

3. Select the **Assign Azure Active Directory administrator roles** task.

4. In the **Add assignments** pane, assign administrator roles.

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

   ### *To remove an assignment*

   - Select the administrator role and double-click ⊘.

5. Save the changes.

Related topics

- Prerequisites for indirect assignment of Azure Active Directory administration roles to Azure Active Directory user accounts on page 111

- Assigning Azure Active Directory administrator roles to departments, cost centers, and locations on page 112

- Assigning Azure Active Directory user accounts directly to Azure Active Directory administrator roles on page 117

- Adding Azure Active Directory administrator roles to system roles on page 114

- Adding Azure Active Directory administrator roles in the IT Shop on page 115

- One Identity Manager users for managing an Azure Active Directory environment on page 11

Adding Azure Active Directory administrator roles to system roles

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

Use this task to add an administrator role to system roles. When you assign a system role to an employee, the administrator roles are inherited by all user accounts that these employees have.

NOTE: Applications in which the **Only use in IT Shop** option is set can only be assigned to system roles that also have this option set. For more information, see the *One Identity Manager System Roles Administration Guide*.

To assign an administrator role to system roles

1. In the Manager, select the **Azure Active Directory > Administrator roles** category.

2. Select the administrator role in the result list.

3. Select the **Assign system roles** task.

4. In the **Add assignments** pane, assign system roles.

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

   To remove an assignment

   - Select the system role and double-click ⊘.

5. Save the changes.

Related topics

Adding Azure Active Directory administrator roles in the IT Shop

Once an administrator role has been assigned to an IT Shop shelf, it can be requested by the shop customers. To ensure it can be requested, further prerequisites need to be guaranteed:

- The administrator role must be labeled with the **IT Shop** option.
- The administrator role must be assigned to a service item.
- If the administrator role can only be assigned to employees using IT Shop requests, the administrator role must be also labeled with the **Only use in IT Shop** option. Direct assignment to hierarchical roles may not be possible.

NOTE: IT Shop administrators can assign administrator roles to IT Shop shelves in the case of role-based login. Target system administrators are not authorized to add administrator roles in the IT Shop.

To add an administrator role in the IT Shop

1. In the Manager, select the **Azure Active Directory > administrator roles** (non role-based login) category.

   - OR -

In the Manager, select the **Entitlements > Azure Active Directory administrator roles** (role-based login) category.

2. Select the administrator role in the result list.

3. Select the **Add to IT Shop** task.

4. In the **Add assignments** pane, assign the administrator role to the IT Shop shelves.

5. Save the changes.

To remove an administrator role from individual IT Shop shelves

1. In the Manager, select the **Azure Active Directory > administrator roles** (non role-based login) category.

   - OR -

   In the Manager, select the **Entitlements > Azure Active Directory administrator roles** (role-based login) category.

2. Select the administrator role in the result list.

3. Select the **Add to IT Shop** task.

4. In the **Remove assignments** pane, remove the administrator role from the IT Shop shelves.

5. Save the changes.

To remove an administrator role from all IT Shop shelves

1. In the Manager, select the **Azure Active Directory > administrator roles** (non role-based login) category.

   - OR -

   In the Manager, select the **Entitlements > Azure Active Directory administrator roles** (role-based login) category.

2. Select the administrator role 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 administrator role is removed from all shelves by the One Identity Manager Service. All requests and assignment requests with this administrator role are canceled at the same time.

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

Related topics

- Editing main data of Azure Active Directory administrator roles on page 192
- Prerequisites for indirect assignment of Azure Active Directory administration roles to Azure Active Directory user accounts on page 111

Assigning Azure Active Directory user accounts directly to Azure Active Directory administrator roles

To react quickly to special requests, you can assign administrator roles directly to user accounts. You cannot directly assign administration roles that have the **Only use in IT Shop** option set.

To assign a user account directly to an administrator role.

1. In the Manager, select the **Azure Active Directory > Administrator roles** category.

2. Select the administrator role in the result list.

3. Select the **Assign user accounts** task.

4. In the **Add assignments** pane, assign the user accounts.

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

   ### *To remove an assignment*
   - Select the user account and double-click ⊘.

5. Save the changes.

Related topics

- Assigning Azure Active Directory administrator roles directly to Azure Active Directory user accounts on page 118
- Assigning Azure Active Directory administrator roles to departments, cost centers, and locations on page 112
- Assigning Azure Active Directory administrator roles to business roles on page 113
- Adding Azure Active Directory administrator roles to system roles on page 114
- Adding Azure Active Directory administrator roles in the IT Shop on page 115

Assigning Azure Active Directory administrator roles directly to Azure Active Directory user accounts

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

To assign administrator roles directly to user accounts

1. In the Manager, select the **Azure Active Directory > User accounts** category.

2. Select the user account in the result list.

3. Select the **Assign administrator roles** task.

4. In the **Add assignments** pane, assign administrator roles.

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

   To remove an assignment

   - Select the administrator role and double-click ⊘.

5. Save the changes.

Related topics

- Assigning Azure Active Directory administrator roles to Azure Active Directory user accounts on page 109

Azure Active Directory administrator role inheritance based on categories

The procedure described under Azure Active Directory group inheritance based on categories on page 105 can also be applied for administrator roles.

To use inheritance through categories

1. In the Manager, define the categories in the Azure Active Directory tenant.

2. In the Manager, assign categories to user accounts through their main data.

3. In the Manager, assign categories to administrator roles through their main data.

ONE IDENTITY
by Quest

One Identity Manager 8.2 Administration Guide for Connecting to
Azure Active Directory

118

Managing Azure Active Directory administrator roles assignments

Related topics

Managing Azure Active Directory subscription and Azure Active Directory service plan assignments

The user requires an Azure Active Directory subscription to access the service plans in Azure Active Directory. An Azure Active Directory subscription defines the scope of service plans that the user can access. Use of individual service plans by the user can be permitted or not.

Example:

The Azure Active Directory subscription A contains service plan 1, service plan 2, and the service plan 3.

- The subscription A is assigned to the user.
- The user is not permitted service plan 2.

Therefore, the user can use service plans 1 and 3.

In Azure Active Directory, Azure Active Directory subscriptions can be assigned to users and groups. Service plans can be permitted or not depending on the assignment method. The user obtains all the permitted service plans.

Example:

The Azure Active Directory subscription A contains service plan 1, service plan 2, and the service plan 3.

- The Azure Active Directory subscription A is assigned directly to the user.
- The user is not permitted service plan 2.

The Azure Active Directory subscription B contains the service plan 4, service plan 5, and the service plan 6.

- The Azure Active Directory subscription B is assigned to group A.
- The group A is not permitted to user service plan 6.
- The user is in group A.

Therefore, the user can use service plans 1, 3, 4, and 5.

It is possible that a user obtains the same Azure Active Directory subscription directly as well as through one or more groups. If a service plan is permitted by one assignment method and not by another, the user is given the service plan.

Example:

The Azure Active Directory subscription A contains service plan 1, service plan 2, and the service plan 3.

- The Azure Active Directory subscription A is assigned directly to the user.
- The user is not permitted to use service plan 2.
- The Azure Active Directory subscription A is assigned to group A.
- All service plans for the group A are allowed.
- The user is in group A.

Therefore, the user can use service plans 1, 2, and 3.

In One Identity Manager, Azure Active Directory subscriptions and service plans and their assignments to Azure Active Directory user accounts and Azure Active Directory groups are mapped as follows.

Table 20: Azure Active Directory subscription and service plans in the One Identity Manager schema map

Table	Description
AADSubSku	This table contains all Azure Active Directory subscriptions. The information about Azure Active Directory subscriptions within an Azure Active Directory tenant is loaded into One Identity Manager by synchronization. You cannot create new Azure Active Directory subscription in One Identity Manager.
AADServicePlan	This table contains the service plans. The information about service plans within an Azure Active Directory

ONE IDENTITY by Quest

Table	Description
	tenant is loaded into One Identity Manager by synchronization. You cannot create new service plans in One Identity Manager.
AADServicePlanInSubSku	This table contains service plan assignments to Azure Active Directory subscriptions. The assignments are loaded into One Identity Manager by synchronization. You cannot edit the assignments in One Identity Manager.
AADDeniedServicePlan	This table contains service plan assignments to Azure Active Directory subscriptions for mapping service plans that are not permitted. The entries are created automatically in One Identity Manager after synchronizing Azure Active Directory subscriptions.
	Service plans that are not permitted are called "disabled service plans" in One Identity Manager. By assigning a disabled service plans to an Azure Active Directory user account in One Identity Manager, you disable the use of this service plan in Azure Active Directory.
AADUserHasSubSku	This table contains Azure Active Directory subscription assignments to Azure Active Directory user accounts. It maps direct assignments of Azure Active Directory subscriptions to Azure Active Directory user accounts and assignments that an Azure Active Directory user accounts obtains through its Azure Active Directory groups. The assignments are loaded by synchronization.
	You can assign Azure Active Directory subscriptions to Azure Active Directory user accounts in One Identity Manager either directly, though IT Shop requests, or through departments, cost centers, locations and business roles.
	You cannot edit assignments by Azure Active Directory groups in One Identity Manager.
	The Azure Active Directory group that an assignment results from, is mapped in the **Azure Active Directory source group** column (`AADUserHasSubSku.UID_AADGroupSource`). If the column is empty, this assignment of the Azure Active Directory subscription to the Azure Active Directory user account is created either directly, though IT Shop requests, or through departments, cost centers, locations, and business roles. Assignments through Azure Active Directory groups are marked in the **Origin** column with the **Assignment by group** value

Table	Description
	`AADUserHasSubSku.XOrigin=16`).
	The table also contains a list of disabled service plans from its Azure Active Directory subscriptions for each Azure Active Directory user account (`AADUserHasSubSku.DenyList`).
AADUserHasDeniedService	This table contains disabled service plan assignments to Azure Active Directory user accounts. The entries are taken from the list of disabled service plans (`AADUserHasSubSku.DenyList`).
	You can assign disabled service plans to Azure Active Directory user accounts in One Identity Manager either directly, though IT Shop requests, or through departments, cost centers, locations and business roles. By assigning a disabled service plan, you disable the use of this service plan in Azure Active Directory.
	NOTE: A disabled service plan that is assigned to a user account can be permitted if the user accounts obtains the service plan additional through a group and the service plan for the group is allowed. The assignment by group is not mapped in this table.
AADUserHasServicePlan	This table contains the service plan assignments for Azure Active Directory user accounts that are in effect. The assignments are calculated in One Identity Manager from the entries in the `AADUserHasSubSku`, `AADUserHasDeniedService`, `AADGroupHasSubSku`, and `AADGroupHasDeniedService` tables.
AADGroupHasSubSku	This table contains Azure Active Directory subscription assignments to Azure Active Directory groups. This table also contains a list of disabled service plans from its Azure Active Directory subscriptions for each Azure Active Directory group (`AADUserHasSubSku.DenyList`).
	The assignments are loaded into One Identity Manager by synchronization. You cannot edit the assignments in One Identity Manager.
AADGroupHasDeniedService	This table contains disabled service plan assignments to Azure Active Directory groups. The entries are taken from the list of disabled service plans (`AADGroupHasSubSku.DenyList`). You cannot edit the assignments in One Identity Manager.

ONE IDENTITY
by Quest

One Identity Manager 8.2 Administration Guide for Connecting to
Azure Active Directory

Managing Azure Active Directory subscription and Azure Active
Directory service plan assignments

123

Detailed information about this topic

- Displaying enabled and disabled Azure Active Directory service plans forAzure Active Directory user accounts and Azure Active Directory groups on page 124

- Assigning Azure Active Directory subscriptions to Azure Active Directory user accounts on page 126

- Inheriting Azure Active Directory subscriptions based on categories on page 145

- Assigning disabled Azure Active Directory service plans to Azure Active Directory user accounts on page 136

- Inheritance of disabled Azure Active Directory service plans based on categories on page 146

- Overview of all assignments on page 107

Displaying enabled and disabled Azure Active Directory service plans forAzure Active Directory user accounts and Azure Active Directory groups

An Azure Active Directory user account can obtain Azure Active Directory subscriptions and Azure Active Directory service plans directly or through its Azure Active Directory groups.

NOTE: It is possible that an Azure Active Directory user obtains the same Azure Active Directory subscription directly as well as through one or more Azure Active Directory groups. If a service plan is permitted by one assignment method and not by another, the user is given the service plan.

This means:

A disabled service plan that is assigned to a user account can be permitted if the user accounts obtains the service plan additional through a group and the service plan for the group is allowed.

For more information, see Managing Azure Active Directory subscription and Azure Active Directory service plan assignments on page 120.

To display information about Azure Active Directory subscriptions and service plans for a user account

1. In the Manager, select the **Azure Active Directory > User accounts** category.

2. Select the user account in the result list.

3. Select the **Azure Active Directory user account overview** task.

   The following information about Azure Active Directory subscriptions and service plans for a user account is displayed on the overview form.

- **Azure Active Directory subscriptions (owned)**: Azure Active Directory subscriptions assigned to the user account either directly, though IT Shop requests, or through departments, cost centers, locations and business roles.

- **Azure Active Directory subscriptions (inherited)**: Azure Active Directory subscriptions that the user account has obtained through its Azure Active Directory groups.

- **Azure Active Directory service plans**: Azure Active Directory service plans permitted for this user account.

- **Disabled Azure Active Directory service plans from owned subscriptions**: Disabled Azure Active Directory service plans assigned to this user account either directly, through the IT Shop or through departments, cost centers, locations and business roles.

4. Select the **License overview** report.

   The report contains a summary of assigned and effective subscriptions and service plans for an Azure Active Directory user account.

To display information about Azure Active Directory subscriptions and service plans for a group

1. In the Manager, select the **Azure Active Directory > Groups** category.

2. Select the group in the result list.

3. Select the **Azure Active Directory group overview** task.

   The following information about Azure Active Directory subscriptions and service plans for a group is displayed on the overview form.

   - **Azure Active Directory subscriptions**: Azure Active Directory subscriptions assigned to Azure Active Directory groups.

   - **Enabled Azure Active Directory service plans**: Azure Active Directory service plans permitted for this group.

   - **Disabled Azure Active Directory service plans**: Azure Active Directory service plans not permitted for this group.

   - **Azure Active Directory user accounts**: Azure Active Directory user accounts assigned to group and therefore contain subscriptions and service plans.

Related topics

- Assigning Azure Active Directory subscriptions to Azure Active Directory user accounts on page 126
- Assigning disabled Azure Active Directory service plans to Azure Active Directory user accounts on page 136

Assigning Azure Active Directory subscriptions to Azure Active Directory user accounts

Azure Active Directory subscriptions can be assigned directly or indirectly to Azure Active Directory user accounts.

In the case of indirect assignment, employees and Azure Active Directory subscriptions are assigned to hierarchical roles, such as departments, cost centers, locations, or business roles. Azure Active Directory subscriptions assigned to an employee are calculated from the position in the hierarchy and the direction of inheritance. If the employee has a user account in Azure Active Directory, Azure Active Directory role subscriptions are inherited by this Azure Active Directory user account.

Furthermore, Azure Active Directory subscriptions can be assigned to employees through IT Shop requests. Add employees to a shop as customers so that Azure Active Directory subscriptions can be assigned through IT Shop requests. All Azure Active Directory subscriptions assigned to this shop can be requested by the customers. Requested Azure Active Directory subscriptions are assigned to the employees after approval is granted.

TIP: You can combine the account definition for creating the Azure Active Directory user account and the Azure Active Directory subscription that will be used into one system role. In this way, the employee automatically obtains a user account and an Azure Active Directory subscription.

An employee can obtain this system role directly through departments, cost centers, locations, or business roles, or an IT Shop request.

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

NOTE: An Azure Active Directory user account can also obtain Azure Active Directory subscriptions through its Azure Active Directory groups. You cannot edit assignments by Azure Active Directory groups in One Identity Manager.

The AADUserhasSubSku contains the assignments of Azure Active Directory subscription to Azure Active Directory user accounts with their origin. For more information, see Managing Azure Active Directory subscription and Azure Active Directory service plan assignments on page 120.

For detailed information see the following guides:

Topic	Guide
Basic principles for assigning and inheriting company resources	*One Identity Manager Identity Management Base Module Administration Guide*
	One Identity Manager Business Roles Administration Guide
Assigning company resources through	*One Identity Manager IT Shop Administration*

Topic	Guide
IT Shop requests	*Guide*
System roles	*One Identity Manager System Roles Administration Guide*

Detailed information about this topic

Prerequisites for indirect assignment of Azure Active Directory subscriptions to Azure Active Directory user accounts

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

1. Assignment of employees and Azure Active Directory subscriptions is permitted for role classes (departments, cost centers, locations, or business roles).

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

   To configure assignments to roles of a role class

   a. In the Manager, select role classes in the **Organizations > Basic configuration data > Role classes** category.

      - OR -

In the Manager, select role classes in the **Business roles > Basic configuration data > Role classes** category.

b. Select the **Configure role assignments** task and configure the permitted assignments.

- To generally allow an assignment, enable the **Assignments allowed** column.

- To allow direct assignment, enable the **Direct assignments permitted** column.

c. Save the changes.

2. Settings for assigning Azure Active Directory subscriptions to Azure Active Directory user accounts.

- The Azure Active Directory user account is linked to an employee.

- The Azure Active Directory user account has a location.

- The Azure Active Directory user account has the **Subscriptions can be inherited** option set.

NOTE: There are other configuration settings that play a role when company resources are inherited through departments, cost centers, locations, and business roles. For example, role inheritance might be blocked or inheritance of employees not allowed. For more detailed information about the basic principles for assigning company resources, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Related topics

Assigning Azure Active Directory subscriptions to departments, cost centers, and locations

Assign Azure Active Directory subscriptions to departments, cost centers, and locations so that user accounts are assigned to them through these organizations.

To assign an Azure Active Directory subscription to departments, cost centers, or locations (non role-based login)

1. In the Manager, select the **Azure Active Directory > Subscriptions** category.

2. Select an Azure Active Directory subscription in the result list.

3. Select the **Assign organizations** task.

ONE IDENTITY
by Quest

4. In the **Add assignments** pane, assign the organizations:

   - On the **Departments** tab, assign departments.
   - On the **Locations** tab, assign locations.
   - On the **Cost centers** tab, assign cost centers.

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

   To remove an assignment

   - Select the organization and double-click ⊘.

5. Save the changes.

To assign Azure Active Directory subscriptions to a department, cost center, or location (role-based login)

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

   - OR -

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

   - OR -

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

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

3. Select the **Assign Azure Active Directory subscriptions** task.

4. In the **Add assignments** pane, select the Azure Active Directory tenant and assign the Azure Active Directory subscriptions.

   TIP: In the **Remove assignments** pane, you can remove assigned Azure Active Directory subscriptions.

   To remove an assignment

   - Select the ⊘ subscription and double-click Azure Active Directory.

5. Save the changes.

Related topics

- Prerequisites for indirect assignment of Azure Active Directory subscriptions to Azure Active Directory user accounts on page 127
- Assigning Azure Active Directory subscriptions to business roles on page 130
- Assigning Azure Active Directory user account directly to Azure Active Directory subscriptions on page 134
- Adding Azure Active Directory subscriptions to system roles on page 131
- Adding Azure Active Directory subscriptions to the IT Shop on page 132
- One Identity Manager users for managing an Azure Active Directory environment on page 11

Assigning Azure Active Directory subscriptions to business roles

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

Assign Azure Active Directory subscriptions to business roles so that they are assigned to user accounts through these business roles.

To assign an Azure Active Directory subscription to business roles (non role-based login)

1. In the Manager, select the **Azure Active Directory > Subscriptions** category.

2. Select an Azure Active Directory subscription in the result list.

3. Select the **Assign business roles** task.

4. In the **Add assignments** pane, select the role class and assign business roles.

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

   ### To remove an assignment

   - Select the business role and double-click ⊘.

5. Save the changes.

To assign Azure Active Directory subscriptions to a business role (role-based login)

1. In the Manager, select the **Business roles > <role class>** category.

2. Select the business role in the result list.

3. Select the **Assign Azure Active Directory subscriptions** task.

4. In the **Add assignments** pane, select the Azure Active Directory tenant and assign the Azure Active Directory subscriptions.

   TIP: In the **Remove assignments** pane, you can remove assigned Azure Active Directory subscriptions.

   ### To remove an assignment

   - Select the ⊘ subscription and double-click Azure Active Directory.

5. Save the changes.

Related topics

- Prerequisites for indirect assignment of Azure Active Directory subscriptions to Azure Active Directory user accounts on page 127
- Assigning Azure Active Directory subscriptions to departments, cost centers, and locations on page 128

Adding Azure Active Directory subscriptions to system roles

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

Use this task to add an Azure Active Directory subscription to system roles. When you assign a system role to an employee, the Azure Active Directory subscription is inherited by all user accounts owned by these employees.

NOTE: Azure Active Directory subscriptions in which the **Only use in IT Shop** option is set can only be assigned to system roles that also have this option set. For more information, see the *One Identity Manager System Roles Administration Guide*.

TIP: You can combine the account definition for creating the Azure Active Directory user account and the Azure Active Directory subscription that will be used into one system role. In this way, the employee automatically obtains a user account and an Azure Active Directory subscription.

An employee can obtain this system role directly through departments, cost centers, locations, or business roles, or an IT Shop request.

To assign an Azure Active Directory subscription to a system role

1. In the Manager, select the **Azure Active Directory > Subscriptions** category.

2. Select an Azure Active Directory subscription in the result list.

3. Select the **Assign system roles** task.

4. In the **Add assignments** pane, assign system roles.

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

   To remove an assignment

   - Select the system role and double-click ⊘.

5. Save the changes.

Related topics

- Prerequisites for indirect assignment of Azure Active Directory subscriptions to Azure Active Directory user accounts on page 127

Adding Azure Active Directory subscriptions to the IT Shop

Once an Azure Active Directory subscription is assigned to an IT Shop shelf, it can be requested by customers. To ensure it can be requested, further prerequisites need to be guaranteed.

- The Azure Active Directory subscription must be labeled with the **IT Shop** option.
- The Azure Active Directory subscription must be assigned to a service item.
- If the Azure Active Directory subscription is only supposed to be available to employees through IT Shop requests, the Azure Active Directory subscription must also be labeled with the **Only for use in IT Shop** option. Direct assignment to hierarchical roles may not be possible.

NOTE: IT Shop administrators can assign Azure Active Directory subscriptions to IT Shop shelves in the case of role-based login. Target system administrators are not authorized to add Azure Active Directory subscriptions in the IT Shop.

To add an Azure Active Directory subscription to the IT Shop

1. In the Manager, select the **Azure Active Directory > Subscriptions** category (non role-based login) category.

   - OR -

   In the Manager, select the **Entitlements > Azure Active Directory subscriptions** (role-based login) category.

2. Select an Azure Active Directory subscription in the result list.

3. Select **Add to IT Shop**.

4. In the **Add assignments** pane, assign the Azure Active Directory subscription to the IT Shop shelves.

5. Save the changes.

To remove an Azure Active Directory subscription from individual IT Shop shelves

1. In the Manager, select the **Azure Active Directory > Subscriptions** category (non role-based login) category.

   - OR -

   In the Manager, select the **Entitlements > Azure Active Directory subscriptions** (role-based login) category.

2. Select an Azure Active Directory subscription in the result list.

3. Select **Add to IT Shop**.

4. In the **Remove assignments** pane, remove the Azure Active Directory subscription from the IT Shop shelves.

5. Save the changes.

To remove an Azure Active Directory subscription from all IT Shop shelves

1. In the Manager, select the **Azure Active Directory > Subscriptions** category (non role-based login) category.

   - OR -

   In the Manager, select the **Entitlements > Azure Active Directory subscriptions** (role-based login) category.

2. Select an Azure Active Directory subscription 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 Azure Active Directory subscription is removed from all shelves by the One Identity Manager Service. All request and assignment requests for this Azure Active Directory subscription are canceled in the process.

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

Related topics

Assigning Azure Active Directory user account directly to Azure Active Directory subscriptions

To react quickly to special requests, you can assign subscriptions directly to Azure Active Directory user accounts. You cannot directly assign Azure Active Directory subscriptions that have the **Only use in IT Shop** option set.

Special on the assignment form

On the form, assignments of Azure Active Directory subscriptions to Azure Active Directory user accounts are shown with their origin. This means:

- **Azure Active Directory source group**: Azure Active Directory group resulting from an assignment. If the column is empty, this assignment of the Azure Active Directory subscription to the Azure Active Directory user account is created either directly, though IT Shop requests, or through departments, cost centers, locations, and business roles.

- **Origin**: Type of assignment. Assignments through Azure Active Directory groups are marked with the **Assigned by group** value (`AADUserHasSubSku.XOrigin=16`).

NOTE: You cannot delete assignments that are not derived from an Azure Active Directory group.

To assign an Azure Active Directory subscription directly to user accounts

1. In the Manager, select the **Azure Active Directory > Subscriptions** category.
2. Select an Azure Active Directory subscription in the result list.
3. Select in the **Assign user accounts** task.
4. Click **Add** and select the user account in the **Azure Active Directory user account** menu.
5. Save the changes.

To remove direct assignments of Azure Active Directory subscriptions

1. In the Manager, select the **Azure Active Directory > Subscriptions** category.
2. Select an Azure Active Directory subscription in the result list.
3. Select in the **Assign user accounts** task.
4. Select the assignment and click **Remove**.
5. Save the changes.

Related topics

-
-
-
-
-
-

Assigning Azure Active Directory subscriptions directly to Azure Active Directory user accounts

To react quickly to special requests, you can assign subscriptions directly to Azure Active Directory user accounts. You cannot directly assign Azure Active Directory subscriptions that have the **Only use in IT Shop** option set.

Special on the assignment form

On the form, assignments of Azure Active Directory subscriptions to Azure Active Directory user accounts are shown with their origin. This means:

- **Azure Active Directory source group**: Azure Active Directory group resulting from an assignment. If the column is empty, this assignment of the Azure Active Directory subscription to the Azure Active Directory user account is created either directly, though IT Shop requests, or through departments, cost centers, locations, and business roles.

- **Origin**: Type of assignment. Assignments through Azure Active Directory groups are marked with the **Assigned by group** value (AADUserHasSubSku.XOrigin=16).

NOTE: You cannot delete assignments that are not derived from an Azure Active Directory group.

To assign subscriptions directly to Azure Active Directory user accounts

1. In the Manager, select the **Azure Active Directory > User accounts** category.
2. Select the user account in the result list.
3. Select the **Directly assign subscriptions** task.
4. Click **Add** and in the **Azure Active Directory subscription** menu, select an Azure

Active Directory subscription.

5. Save the changes.

To remove direct assignments of Azure Active Directory subscriptions

1. In the Manager, select the **Azure Active Directory > User accounts** category.

2. Select the user account in the result list.

3. Select the **Directly assign subscriptions** task.

4. Select the assignment and click **Remove**.

5. Save the changes.

Related topics

- Displaying enabled and disabled Azure Active Directory service plans forAzure Active Directory user accounts and Azure Active Directory groups on page 124
- Assigning Azure Active Directory subscriptions to Azure Active Directory user accounts on page 126
- Assigning Azure Active Directory subscriptions to departments, cost centers, and locations on page 128
- Assigning Azure Active Directory subscriptions to business roles on page 130
- Adding Azure Active Directory subscriptions to system roles on page 131
- Adding Azure Active Directory subscriptions to the IT Shop on page 132

Assigning disabled Azure Active Directory service plans to Azure Active Directory user accounts

Disabled Azure Active Directory service plans can be assigned directly or indirectly to Azure Active Directory user accounts.

In the case of indirect assignment, employees and disabled service plans are assigned to hierarchical roles, such as departments, cost centers, locations, or business roles. The disabled Azure Active Directory service plans assigned to an employee are calculated from the position in the hierarchy and the direction of inheritance. If the employee has a user account in Azure Active Directory, disabled service plans belonging to roles are inherited by this user account.

Furthermore, disabled service plans can be assigned to employees through IT Shop requests. Add employees to a shop as customers so that disabled service plans can be assigned through IT Shop requests. All disabled service plans are assigned to this shop can be requested by the customers. Requested disabled service plans are assigned to the employees after approval is granted.

ONE IDENTITY
by Quest

One Identity Manager 8.2 Administration Guide for Connecting to
Azure Active Directory

136

Managing Azure Active Directory subscription and Azure Active
Directory service plan assignments

To react quickly to special requests, you can assign disabled service plans directly to Azure Active Directory user accounts.

NOTE: It is possible that an Azure Active Directory user obtains the same Azure Active Directory subscription directly as well as through one or more Azure Active Directory groups. If a service plan is permitted by one assignment method and not by another, the user is given the service plan.

This means:

A disabled service plan that is assigned to a user account can be permitted if the user accounts obtains the service plan additional through a group and the service plan for the group is allowed.

For more information, see Managing Azure Active Directory subscription and Azure Active Directory service plan assignments on page 120 and Displaying enabled and disabled Azure Active Directory service plans forAzure Active Directory user accounts and Azure Active Directory groups on page 124.

For detailed information see the following guides:

Topic	Guide
Basic principles for assigning and inheriting company resources	*One Identity Manager Identity Management Base Module Administration Guide*
	One Identity Manager Business Roles Administration Guide
Assigning company resources through IT Shop requests	*One Identity Manager IT Shop Administration Guide*
System roles	*One Identity Manager System Roles Administration Guide*

Detailed information about this topic

- Prerequisites for indirect assignment of disabled Azure Active Directory service plans to Azure Active Directory user accounts on page 138
- Assigning disabled Azure Active Directory service plans directly to departments, cost centers, and locations on page 139
- Assigning disabled Azure Active Directory service plans to business roles on page 140
- Adding disabled Azure Active Directory service plans to system roles on page 141
- Adding disabled Azure Active Directory service plans to the IT Shop on page 142
- Assigning Azure Active Directory user accounts directly to disabled Azure Active Directory service plans on page 144
- Assigning disabled Azure Active Directory service plans directly to Azure Active Directory user accounts on page 145

Prerequisites for indirect assignment of disabled Azure Active Directory service plans to Azure Active Directory user accounts

In the case of indirect assignment, employees and disabled service plans are assigned to hierarchical roles, such as departments, cost centers, locations, or business roles. When assigning disabled Azure Active Directory service plans indirectly, check the following settings and modify them if necessary:

1. Assignment of employees and disabled Azure Active Directory service plans is permitted for role classes (departments, cost centers, locations, or business roles).

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

   To configure assignments to roles of a role class

   a. In the Manager, select role classes in the **Organizations > Basic configuration data > Role classes** category.

      - OR -

      In the Manager, select role classes in the **Business roles > Basic configuration data > Role classes** category.

   b. Select the **Configure role assignments** task and configure the permitted assignments.

      - To generally allow an assignment, enable the **Assignments allowed** column.

      - To allow direct assignment, enable the **Direct assignments permitted** column.

   c. Save the changes.

2. Settings for assigning disabled Azure Active Directory service plans to Azure Active Directory user accounts.

   - The Azure Active Directory user account is linked to an employee.

   - The Azure Active Directory user account has the **Disabled service plans can be inherited** option set.

Related topics

- Creating and editing Azure Active Directory user accounts on page 171
- General main data of Azure Active Directory user accounts on page 172

Assigning disabled Azure Active Directory service plans directly to departments, cost centers, and locations

Assign disabled Azure Active Directory service plans to departments, cost centers, and locations in order to assign user accounts to them through these organizations.

To assign a disabled service plan to departments, cost centers, or locations (non role-based login)

1. In the Manager, select the **Azure Active Directory > Disabled service plans** category.

2. Select the service plan in the result list.

3. Select the **Assign organizations** task.

4. In the **Add assignments** pane, assign the organizations:

   - On the **Departments** tab, assign departments.
   - On the **Locations** tab, assign locations.
   - On the **Cost centers** tab, assign cost centers.

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

   ### To remove an assignment

   - Select the organization and double-click ✅.

5. Save the changes.

To assign disabled service plans to a department, cost center, or location (role-based login)

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

   - OR -

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

   - OR -

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

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

3. Select **Assigning disabled Azure Active Directory service plans**.

4. In the **Add assignments** pane, select the Azure Active Directory subscription and assign the disabled service plans.

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

   ### To remove an assignment

- Select the service plan and double-click ⊘.

5. Save the changes.

Related topics

- [Prerequisites for indirect assignment of disabled Azure Active Directory service plans to Azure Active Directory user accounts](#) on page 138
- [Assigning disabled Azure Active Directory service plans to business roles](#) on page 140
- [Assigning Azure Active Directory user accounts directly to disabled Azure Active Directory service plans](#) on page 144
- [Adding disabled Azure Active Directory service plans to system roles](#) on page 141
- [Adding disabled Azure Active Directory service plans to the IT Shop](#) on page 142
- [One Identity Manager users for managing an Azure Active Directory environment](#) on page 11

Assigning disabled Azure Active Directory service plans to business roles

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

Assign disabled Azure Active Directory service plans to business roles so that they can be assigned to user accounts through these business roles.

To assign a disabled service plan to a business role (non role-based login)

1. In the Manager, select the **Azure Active Directory > Disabled service plans** category.
2. Select the service plan in the result list.
3. Select the **Assign business roles** task.
4. In the **Add assignments** pane, select the role class and assign business roles.

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

    To remove an assignment

    - Select the business role and double-click ⊘.

1. Save the changes.

To assign disabled service plans to a business role (non role-based login)

1. In the Manager, select the **Business roles > <role class>** category.
2. Select the business role in the result list.
3. Select the **Assigning disabled Azure Active Directory service plans** task.

ONE IDENTITY
by Quest

One Identity Manager 8.2 Administration Guide for Connecting to
Azure Active Directory

Managing Azure Active Directory subscription and Azure Active
Directory service plan assignments

140

4. In the **Add assignments** pane, select the Azure Active Directory subscription and assign the disabled service plans.

> TIP: In the **Remove assignments** pane, you can remove assigned service plans.
>
> ***To remove an assignment***
>
> - Select the service plan and double-click ⊘.

5. Save the changes.

Related topics

- Prerequisites for indirect assignment of disabled Azure Active Directory service plans to Azure Active Directory user accounts on page 138
- Assigning disabled Azure Active Directory service plans directly to departments, cost centers, and locations on page 139
- Assigning Azure Active Directory user accounts directly to disabled Azure Active Directory service plans on page 144
- Adding disabled Azure Active Directory service plans to system roles on page 141
- Adding disabled Azure Active Directory service plans to the IT Shop on page 142
- One Identity Manager users for managing an Azure Active Directory environment on page 11

Adding disabled Azure Active Directory service plans to system roles

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

Use this task to add disabled Azure Active Directory service plans to system roles. If you assign a system role to an employee, the disabled service plan is inherited by all user accounts owned by these employees.

> NOTE: Disabled Azure Active Directory service plans in which the **Only use in IT Shop** option is set can only be assigned to system roles that also have this option set. For more information, see the *One Identity Manager System Roles Administration Guide*.

To assign a disabled service plan to system roles

1. In the Manager, select the **Azure Active Directory > Disabled service plans** category.
2. Select the service plan in the result list.
3. Select the **Assign system roles** task.
4. In the **Add assignments** pane, assign system roles.

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

To remove an assignment

- Select the system role and double-click ⊘.

5. Save the changes.

Related topics

- Prerequisites for indirect assignment of disabled Azure Active Directory service plans to Azure Active Directory user accounts on page 138
- Assigning disabled Azure Active Directory service plans directly to departments, cost centers, and locations on page 139
- Assigning disabled Azure Active Directory service plans to business roles on page 140
- Assigning Azure Active Directory user accounts directly to disabled Azure Active Directory service plans on page 144
- Adding disabled Azure Active Directory service plans to the IT Shop on page 142

Adding disabled Azure Active Directory service plans to the IT Shop

A disabled Azure Active Directoryservice plan 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 disabled service plan must be labeled with the **IT Shop** option.
- The disabled service plan must be assigned to a service item.
- If the disabled service plan is only assigned to employees using IT Shop requests, 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 disabled service plans to IT Shop shelves in the case of role-based login. Target system administrators are not authorized to add disabled service plans in the IT Shop.

To add a disabled service plan in the IT Shop

1. In the Manager, select the **Azure Active Directory > Disabled service plans** (non role-based login) category.

    - OR -

    In the Manager, select the **Entitlements > Disabled Azure Active Directory service plans** (role-based login) category.

2. Select the service plan in the result list.

3. Select the **Add to IT Shop** task.

ONE IDENTITY
by Quest

One Identity Manager 8.2 Administration Guide for Connecting to
Azure Active Directory

Managing Azure Active Directory subscription and Azure Active
Directory service plan assignments

142

4. In the **Add assignments** pane, assign the disabled service plan to the IT Shop shelves.

5. Save the changes.

To remove a disabled service plan from individual IT Shop shelves

1. In the Manager, select the **Azure Active Directory > Disabled service plans** (non role-based login) category.

   - OR -

   In the Manager, select the **Entitlements > Disabled Azure Active Directory service plans** (role-based login) category.

2. Select the service plan in the result list.

3. Select the **Add to IT Shop** task.

4. In the **Remove assignments** pane, remove the disabled service plan from the IT Shop shelves.

5. Save the changes.

To remove a disabled service plan from all IT Shop shelves

1. In the Manager, select the **Azure Active Directory > Disabled service plans** (non role-based login) category.

   - OR -

   In the Manager, select the **Entitlements > Disabled Azure Active Directory service plans** (role-based login) category.

2. Select the service plan 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 disabled service plan is removed from all shelves by the One Identity Manager Service. All requests and assignment requests with this disabled service plan are canceled at the same time.

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

Related topics

- Prerequisites for indirect assignment of disabled Azure Active Directory service plans to Azure Active Directory user accounts on page 138
- Assigning disabled Azure Active Directory service plans directly to departments, cost centers, and locations on page 139
- Assigning disabled Azure Active Directory service plans to business roles on page 140
- Assigning Azure Active Directory user accounts directly to disabled Azure Active

-

Assigning Azure Active Directory user accounts directly to disabled Azure Active Directory service plans

To react quickly to special requests, you can assign disabled service plans directly to a user account. You cannot directly assign disabled service plans with the **Only use in IT Shop** option set.

To assign a disabled service plan directly to a user account

1. In the Manager, select the **Azure Active Directory > Disabled service plans** category.

2. Select the service plan in the result list.

3. Select the **Assign user accounts** task.

4. In the **Add assignments** pane, assign the user accounts.

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

   To remove an assignment

   - Select the user account and double-click ⊘.

5. Save the changes.

Related topics

-

-

-

-

-

ONE IDENTITY
by Quest

One Identity Manager 8.2 Administration Guide for Connecting to
Azure Active Directory

Managing Azure Active Directory subscription and Azure Active
Directory service plan assignments

144

Assigning disabled Azure Active Directory service plans directly to Azure Active Directory user accounts

To react quickly to special requests, you can assign disabled service plans directly to a user account. You cannot directly assign disabled service plans with the **Only use in IT Shop** option set.

To assign disabled service plans directly to a user account

1. In the Manager, select the **Azure Active Directory > User accounts** category.

2. Select the user account in the result list.

3. Select the **Assign disabled service plans** task.

4. In the **Add assignments** pane, assign disabled service plans.

   TIP: In the **Remove assignments** pane, you can remove assigned disabled service plans.

   ### *To remove an assignment*

   - Select a disabled service plan and click ⊘.

5. Save the changes.

Related topics

- Assigning disabled Azure Active Directory service plans to Azure Active Directory user accounts on page 136
- Assigning disabled Azure Active Directory service plans directly to departments, cost centers, and locations on page 139
- Assigning disabled Azure Active Directory service plans to business roles on page 140
- Adding disabled Azure Active Directory service plans to system roles on page 141
- Adding disabled Azure Active Directory service plans to the IT Shop on page 142

Inheriting Azure Active Directory subscriptions based on categories

The procedure described under Azure Active Directory group inheritance based on categories on page 105 can also be used for Azure Active Directory subscriptions.

To use inheritance through categories

1. In the Manager, define the categories in the Azure Active Directory tenant.
2. In the Manager, assign categories to user accounts through their main data.
3. In the Manager, assign categories to Azure Active Directory subscriptions through their main data.

Related topics

- Defining categories for the inheritance of entitlements on page 165
- General main data of Azure Active Directory user accounts on page 172
- Editing Azure Active Directory subscription main data on page 195

Inheritance of disabled Azure Active Directory service plans based on categories

The procedure described under Azure Active Directory group inheritance based on categories on page 105 can also be used for disabled service plans.

To use inheritance through categories

1. In the Manager, define the categories in the Azure Active Directory tenant.
2. In the Manager, assign categories to user accounts through their main data.
3. In the Manager, assign categories to disabled service plans through their main data.

Related topics

- Defining categories for the inheritance of entitlements on page 165
- General main data of Azure Active Directory user accounts on page 172
- Editing main data of disabled Azure Active Directory service plans on page 199

Login information for Azure Active Directory user accounts

When new user accounts are created in One Identity Manager, the passwords needed to log in to the target system are created immediately also. Various options are available for assigning the initial password. Predefined password policies are applied to the passwords, and you can adjust these policies to suit your individual requirements if necessary. You can set up email notifications to distribute the login information generated to users.

Detailed information about this topic

Password policies for Azure Active Directory user accounts

One Identity Manager provides you with support for creating complex password policies, for example, for system user passwords, the employees' central password as well as passwords for individual target systems. Password polices apply not only when the user enters a password but also when random passwords are generated.

Predefined password policies are supplied with the default installation that you can use or customize if required. You can also define your own password policies.

Detailed information about this topic

ONE IDENTITY
by Quest

One Identity Manager 8.2 Administration Guide for Connecting to
Azure Active Directory

147

Login information for Azure Active Directory user accounts

Predefined password policies

You can customize predefined password policies to meet your own requirements if necessary.

Password for logging in to One Identity Manager

The **One Identity Manager password policy** is applied for logging in to One Identity Manager. This password policy defines the settings for the system user passwords (`DialogUser.Password` and `Person.DialogUserPassword`) as well as the passcode for a one time log in on the Web Portal (`Person.Passcode`).

NOTE: The **One Identity Manager password policy** is marked as the default policy. This password policy is applied if no other password policy can be found for employees, user accounts, or system users.

For detailed information about password policies for employees, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Password policy for forming employees' central passwords

An employee's central password is formed from the target system specific user accounts by respective configuration. The **Employee central password policy** defines the settings for the (`Person.CentralPassword`) central password. Members of the **Identity Management | Employees | Administrators** application role can adjust this password policy.

IMPORTANT: Ensure that the **Employee central password policy** does not violate the target system-specific requirements for passwords.

For detailed information about password policies for employees, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Password policies for user accounts

Predefined password policies are provided, which you can apply to the user account password columns of the user accounts.

IMPORTANT: If you do not use password policies that are specific to the target system, the **One Identity Manager password policy** default policy applies. In this case, ensure that the default policy does not violate the target systems requirements.

NOTE: When you update One Identity Manager version 7.x to One Identity Manager version 8.2, the configuration parameter settings for forming passwords are passed on to

the target system-specific password policies.

The **Azure Active Directory password policy** is predefined for Azure Active Directory. You can apply this password policy to Azure Active Directory user accounts (AADUser.Password) of an Azure Active Directory tenant.

If the tenants' password requirements differ, it is recommended that you set up your own password policies for each tenant.

Furthermore, you can apply password policies based on the account definition of the user accounts or based on the manage level of the user accounts.

Using password policies

The **Azure Active Directory password policy** is predefined for Azure Active Directory. You can apply this password policy to Azure Active Directory user accounts (AADUser.Password) of an Azure Active Directory tenant.

If the tenants' password requirements differ, it is recommended that you set up your own password policies for each tenant.

Furthermore, you can apply password policies based on the account definition of the user accounts or based on the manage level of the user accounts.

The password policy that is to be used for a user account is determined in the following sequence:

1. Password policy of the user account's account definition.
2. Password policy of the user account's manage level.
3. Password policy of the user account's tenant.
4. The **One Identity Manager password policy** (default policy).

IMPORTANT: If you do not use password policies that are specific to the target system, the **One Identity Manager password policy** default policy applies. In this case, ensure that the default policy does not violate the target systems requirements.

To reassign a password policy

1. In the Manager, select the **Azure Active Directory > Basic configuration data > Password policies** category.
2. Select the password policy in the result list.
3. Select **Assign objects**.
4. Click **Add** in the **Assignments** section and enter the following data.

- **Apply to**: Application scope of the password policy.

  To specify an application scope

  1. Click ➜ next to the field.
  2. Select one of the following references under **Table**:
     - The table that contains the base objects of synchronization.
     - To apply the password policy based on the account definition, select the **TSBAccountDef** table.
     - To apply the password policy based on the manage level, select the **TSBBehavior** table.
  3. Under **Apply to**, select the table that contains the base objects.
     - If you have selected the table containing the base objects of synchronization, next select the specific target system.
     - If you have selected the **TSBAccountDef** table, next select the specific account definition.
     - If you have selected the **TSBBehavior** table, next select the specific manage level.
  4. Click **OK**.
- **Password column**: Name of the password column.
- **Password policy**: Name of the password policy to use.

5. Save the changes.

To change a password policy's assignment

1. In the Manager, select the **Azure Active Directory > Basic configuration data > Password policies** category.
2. Select the password policy in the result list.
3. Select the **Assign objects** task.
4. In the **Assignments** pane, select the assignment you want to change.
5. From the **Password Policies** menu, select the new password policy you want to apply.
6. Save the changes.

Creating password policies

Predefined password policies are supplied with the default installation that you can use or customize if required. You can also define your own password policies.

ONE IDENTITY
by Quest

One Identity Manager 8.2 Administration Guide for Connecting to
Azure Active Directory

Login information for Azure Active Directory user accounts

150

To create a password policy

1. In the Manager, select the **Azure Active Directory > Basic configuration data > Password policies** category.

2. Click in the result list.

3. On the main data form, enter the main data of the password policy.

4. Save the changes.

Detailed information about this topic

Editing password policies

Predefined password policies are supplied with the default installation that you can use or customize if required.

To edit a password policy

1. In the Manager, select the **Azure Active Directory > Basic configuration data > Password policies** category.

2. In the result list, select the password policy.

3. Select the **Change main data** task.

4. Edit the password policy's main data.

5. Save the changes.

Detailed information about this topic

ONE IDENTITY
by Quest

One Identity Manager 8.2 Administration Guide for Connecting to
Azure Active Directory

151

Login information for Azure Active Directory user accounts

General main data of password policies

Enter the following main data of a password policy.

Table 21: main data for a password policy

Property	Meaning
Display name	Password policy name. Translate the given text using the 🌐 button.
Description	Text field for additional explanation. Translate the given text using the 🌐 button.
Error Message	Custom error message generated if the policy is not fulfilled. Translate the given text using the 🌐 button.
Owner (Application Role)	Application roles whose members can configure the password policies.
Default policy	Mark as default policy for passwords. This option cannot be changed.
	NOTE: The **One Identity Manager password policy** is marked as the default policy. This password policy is applied if no other password policy can be found for employees, user accounts, or system users.

Policy settings

Define the following settings for a password policy on the **Password** tab.

Table 22: Policy settings

Property	Meaning
Initial password	Initial password for newly created user accounts. The initial password is used if a password is not entered when you create a user account or if a random password is not generated.
Password confirmation	Reconfirm password.
Minimum Length	Minimum length of the password. Specify the number of characters a password must have. If the value is **0**, no password is required.
Max. length	Maximum length of the password. Specify the number of characters a password can have. The maximum permitted value is **256**.

Property	Meaning
Max. errors	Maximum number of errors. Set the number of invalid passwords attempts. The number of failed logins is only taken into account when logging in to One Identity Manager. If the value is **0**, the number of failed logins is not taken into account.
	This data is only taken into account if the One Identity Manager login was through a system user or employee based authentication module. If a user has exceeded the maximum number of failed logins, the employee or system user will not be able to log in to One Identity Manager.
	You can use the Password Reset Portal to reset the passwords of employees and system users who have been blocked. For more information, see the *One Identity Manager Web Designer Web Portal User Guide*.
Validity period	Maximum age of the password. Enter the length of time a password can be used before it expires. If the value is **0**, then the password does not expire.
Password history	Enter the number of passwords to be saved. If, for example, a value of **5** is entered, the user's last five passwords are stored. If the value is **0**, then no passwords are stored in the password history.
Minimum password strength	Specifies how secure the password must be. The higher the password strength, the more secure it is. The value **0** means that the password strength is not tested. The values **1**, **2**, **3** and **4** specify the required complexity of the password. The value **1** represents the lowest requirements in terms of password strength. The value **4** requires the highest level of complexity.
Name properties denied	Specifies whether name properties are permitted in the password. If this option is set, name properties are not permitted in passwords. The values of these columns are taken into account if the **Contains name properties for password check** option is set. In the Designer, adjust this option in the column definition. For more information, see the *One Identity Manager Configuration Guide*.

Character classes for passwords

Use the **Character classes** tab to specify which characters are permitted for a password.

Table 23: Character classes for passwords

Property	Meaning
Required number of character classes	Number of rules for character classes that must be fulfilled so that a password adheres to the password policy. The following rules are taken into account for **Min. number letters**, **Min. number lowercase**, **Min. number uppercase**, **Min. number digits**, and **Min. number special characters**. That means: • Value **0**: All character class rules must be fulfilled. • Value **>0**: Minimum number of character class rules that must be fulfilled. At most, the value can be the number of rules with a value **>0**. NOTE: Generated passwords are not tested for this.
Min. number letters	Specifies the minimum number of alphabetical characters the password must contain.
Min. number lowercase	Specifies the minimum number of lowercase letters the password must contain.
Min. number uppercase	Specifies the minimum number of uppercase letters the password must contain.
Min. number digits	Specifies the minimum number of digits the password must contain.
Min. number special characters	Specifies the minimum number of special characters the password must contain.
Permitted special characters	List of permitted special characters.
Max. identical characters in total	Specifies the maximum number of identical characters that can be present in the password in total.
Max. identical characters in succession	Specifies the maximum number of identical character that can be repeated after each other.
Denied special characters	List of special characters that are not permitted.

Property	Meaning
Do not generate lowercase letters	Specifies whether a generated password can contain lowercase letters. This setting only applies when passwords are generated.
Do not generate uppercase letters	Specifies whether a generated password can contain uppercase letters. This setting only applies when passwords are generated.
Do not generate digits	Specifies whether a generated password can contain digits. This setting only applies when passwords are generated.
Do not generate special characters	Specifies whether a generated password can contain special characters. If this option is set, only letters, numbers, and spaces are allowed in passwords. This setting only applies when passwords are generated.

Custom scripts for password requirements

You can implement custom scripts for testing and generating passwords if the password requirements cannot be mapped with the existing settings options. Scripts are applied in addition to the other settings.

Detailed information about this topic

- Checking passwords with a script on page 155
- Generating passwords with a script on page 157

Checking passwords with a script

You can implement a script if additional policies need to be used for checking a password that cannot be mapped with the available settings.

Syntax of check scripts

Public Sub CCC_CustomPwdValidate(policy As VI.DB.Passwords.PasswordPolicy, spwd As System.Security.SecureString)

With parameters:

policy = password policy object

spwd = password to check

TIP: To use a base object, take the Entity property of the PasswordPolicy class.

ONE IDENTITY
by Quest

One Identity Manager 8.2 Administration Guide for Connecting to
Azure Active Directory

155

Login information for Azure Active Directory user accounts

> **Example: Script that checks a password**
>
> A password cannot start with **?** or **!** . The password cannot start with three identical characters. The script checks a given password for validity.
>
> ```
> Public Sub CCC_PwdValidate( policy As VI.DB.Passwords.PasswordPolicy, spwd
> As System.Security.SecureString)
>
>     Dim pwd = spwd.ToInsecureArray()
>
>     If pwd.Length>0
>
>         If pwd(0)="?" Or pwd(0)="!"
>
>             Throw New Exception(#LD("Password can't start with '?' or
>             '!'")#)
>
>         End If
>
>     End If
>
>     If pwd.Length>2
>
>         If pwd(0) = pwd(1) AndAlso pwd(1) = pwd(2)
>
>             Throw New Exception(#LD("Invalid character sequence in
>             password")#)
>
>         End If
>
>     End If
>
> End Sub
> ```

To use a custom script for checking a password

1. In the Designer, create your script in the **Script Library** category.
2. Edit the password policy.
   a. In the Manager, select the **Azure Active Directory > Basic configuration data > Password policies** category.
   b. In the result list, select the password policy.
   c. Select the **Change main data** task.
   d. On the **Scripts** tab, enter the name of the script to be used to check a password in the **Check script** field.
   e. Save the changes.

Related topics

- Generating passwords with a script on page 157

ONE IDENTITY
by Quest

One Identity Manager 8.2 Administration Guide for Connecting to
Azure Active Directory

156

Login information for Azure Active Directory user accounts

Generating passwords with a script

You can implement a generating script if additional policies need to be used for generating a random password, which cannot be mapped with the available settings.

Syntax for generating script

```
Public Sub CCC_PwdGenerate( policy As VI.DB.Passwords.PasswordPolicy, spwd As System.Security.SecureString)
```

With parameters:

policy = password policy object

spwd = generated password

TIP: To use a base object, take the `Entity` property of the `PasswordPolicy` class.

Example: Script that generates a password

The script replaces invalid **?** and **!** characters at the beginning of random passwords with **_**.

```
Public Sub CCC_PwdGenerate( policy As VI.DB.Passwords.PasswordPolicy, spwd As System.Security.SecureString)

    Dim pwd = spwd.ToInsecureArray()

    ' replace invalid characters at first position

    If pwd.Length>0

        If pwd(0)="?" Or pwd(0)="!"

            spwd.SetAt(0, CChar("_"))

        End If

    End If

End Sub
```

To use a custom script for generating a password

1. In the Designer, create your script in the **Script Library** category.
2. Edit the password policy.
   a. In the Manager, select the **Azure Active Directory > Basic configuration data > Password policies** category.
   b. In the result list, select the password policy.
   c. Select the **Change main data** task.

d. On the **Scripts** tab, enter the name of the script to be used to generate a password in the **Generating script** field.

e. Save the changes.

Related topics

- Checking passwords with a script on page 155

Password exclusion list

You can add words to a list of restricted terms to prohibit them from being used in passwords.

| NOTE: The restricted list applies globally to all password policies.

To add a term to the restricted list

1. In the Designer, select the **Base data > Security settings > Password policies** category.

2. Create a new entry with the **Object > New** menu item and enter the term you want to exclude from the list.

3. Save the changes.

Checking passwords

When you verify a password, all the password policy settings, custom scripts, and the restricted passwords are taken into account.

To verify if a password conforms to the password policy

1. In the Manager, select the **Azure Active Directory > Basic configuration data > Password policies** category.

2. In the result list, select the password policy.

3. Select the **Change main data** task.

4. Select the **Test** tab.

5. Select the table and object to be tested in **Base object for test**.

6. Enter a password in **Enter password to test**.

    A display next to the password shows whether it is valid or not.

ONE IDENTITY
by Quest

One Identity Manager 8.2 Administration Guide for Connecting to
Azure Active Directory

158

Login information for Azure Active Directory user accounts

Testing password generation

When you generate a password, all the password policy settings, custom scripts and the restricted passwords are taken into account.

To generate a password that conforms to the password policy

1. In the Manager, select the **Azure Active Directory > Basic configuration data > Password policies** category.

2. In the result list, select the password policy.

3. Select the **Change main data** task.

4. Select the **Test** tab.

5. Click **Generate**.

   This generates and displays a password.

Initial password for new Azure Active Directory user accounts

You can issue an initial password for a new Azure Active Directory user account in the following ways:

- When you create the user account, enter a password in the main data.

- Assign a randomly generated initial password to enter when you create user accounts.

  - In the Designer, set the **TargetSystem | AzureAD | Accounts | InitialRandomPassword** configuration parameter.

  - Apply target system specific password policies and define the character sets that the password must contain.

  - Specify which employee will receive the initial password by email.

Related topics

- Password policies for Azure Active Directory user accounts on page 147
- Email notifications about login data on page 159

Email notifications about login data

You can configure the login information for new user accounts to be sent by email to a specified person. In this case, two messages are sent with the user name and the initial

ONE IDENTITY
by Quest

One Identity Manager 8.2 Administration Guide for Connecting to
Azure Active Directory

159

Login information for Azure Active Directory user accounts

password. Mail templates are used to generate the messages. The mail text in a mail template is defined in several languages. This means the recipient's language can be taken into account when the email is generated. Mail templates are supplied in the default installation with which you can configure the notification procedure.

The following prerequisites must be fulfilled in order to use notifications:

1. Ensure that the email notification system is configured in One Identity Manager. For more information, see the *One Identity Manager Installation Guide*.

2. In the Designer, set the **Common | MailNotification | DefaultSender** configuration parameter and enter the sender address for sending the email notifications.

3. Ensure that all employees have a default email address. Notifications are sent to this address. For more information, see the *One Identity Manager Identity Management Base Module Administration Guide*.

4. Ensure that a language can be determined for all employees. Only then can they receive email notifications in their own language. For more information, see the *One Identity Manager Identity Management Base Module Administration Guide*.

When a randomly generated password is issued for the new user account, the initial login data for a user account is sent by email to a previously specified person.

To send initial login data by email

1. In the Designer, set the **TargetSystem | AzureAD | Accounts | InitialRandomPassword** configuration parameter.

2. In the Designer, set the Designer **TargetSystem | AzureAD | Accounts | InitialRandomPassword | SendTo** configuration parameter and enter the message recipient as a value.

3. In the Designer, set the **TargetSystem | AzureAD | Accounts | InitialRandomPassword | SendTo | MailTemplateAccountName** configuration parameter.

   By default, the message sent uses the mail template **Employee - new user account created**. The message contains the name of the user account.

4. In the Designer, set the **TargetSystem | AzureAD | Accounts | InitialRandomPassword | SendTo | MailTemplatePassword** configuration parameter.

   By default, the message sent uses the mail template **Employee - initial password for new user account**. The message contains the initial password for the user account.

TIP: To use custom mail templates for emails of this type, change the value of the configuration parameter.

Mapping of Azure Active Directory objects in One Identity Manager

In One Identity Manager, you can map user accounts, groups, administrator roles, subscriptions, service plans, applications, service principals, and app roles of an Azure Active Directory tenant. These objects are imported into the One Identity Manager database during synchronization. You cannot display or edit their properties in the Manager.

Detailed information about this topic

Azure Active Directory core directories

For more information about the Azure Active Directory structure, see the *Azure Active Directory documentation* from Microsoft.

You must provide details about your organization the first time you register for a Microsoft cloud service. This detailed information is used to make a new Azure Active Directory directory partition. The organization represents one Azure Active Directory tenant. In One

Identity Manager, you can edit the main data of each tenant. However, you cannot create new tenants in One Identity Manager.

A base domain is linked to the core directory in the cloud. You can also add other user-defined domains in Azure Active Directory, which you can then allocate to Microsoft cloud services. One Identity Manager only loads verified domain data into the database. It is not possible to edit data in One Identity Manager.

Detailed information about this topic

Azure Active Directory tenant

You must provide details about your organization the first time you register for a Microsoft cloud service. This detailed information is used to make a new Azure Active Directory directory partition. The organization represents one Azure Active Directory tenant. In One Identity Manager, you can edit the main data of each Azure Active Directory tenant. However, you cannot create new Azure Active Directory tenants in One Identity Manager.

To edit Azure Active Directory tenant main data

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

Detailed information about this topic

General main data of Azure Active Directory tenants

Enter the following data on the **General** tab.

Table 24: Azure Active Directory tenant main data

Property	Description
Display name	The Azure Active Directory tenant's display name.
Account definition (initial)	Initial account definition for creating Azure Active Directory user accounts. This account definition is used if automatic assignment of employees to user accounts is used for this Azure Active Directory tenant and user accounts should be created which are already managed (**Linked configured** state). The account definition's default manage level is applied.
	User accounts are only linked to the employee (**Linked**) if no account definition is given. This is the case on initial synchronization, for example.
Target system managers	Application role, in which target system managers are specified for the Azure Active Directory tenant. Target system managers only edit the objects from Azure Active Directory tenants to which they are assigned. Each Azure Active Directory tenant can have a different target system manager assigned to it.
	Select the One Identity Manager application role whose members are responsible for administration of this Azure Active Directory tenant. Use the 📘 button to add a new application role.
Location	The Azure Active Directory tenant's location.
Street	Street or road.
City	City.
Zip code	Zip code.
Country	Country.
Synchronized by	Type of synchronization through which the data is synchronized between the Azure Active Directory tenant and One Identity Manager. You can no longer change the synchronization type once objects for this Azure Active Directory tenant are present in One Identity Manager.
	If you create an Azure Active Directory tenant with the Synchronization Editor, **One Identity Manager** is used.

Property	Description

Table 25: Permitted values

Value	Synchronization by	Provisioned by
One Identity Manager	Azure Active Directory connector	Azure Active Directory connector
No synchronization	none	none

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

Property	Description
Recipients (marketing notifications)	List of recipients of marketing notifications.
Recipient (technical notifications)	List of recipients of technical notifications.
Recipients (security notifications)	List of recipients of security notifications.
Phone numbers (security notifications)	Phone numbers for security notifications.

Related topics

- Assigning employees automatically to Azure Active Directory user accounts on page 80
- Target system managers for Azure Active Directory on page 217

Information about local Active Directory

The **Linked** tab shows information about the local Active Directory, which is linked to the Azure Active Directory tenant.

Table 26: Local Active Directory user account data

Property	Description
Synchronization with local	Specifies whether synchronization with a local Active

Property	Description
Active Directory enabled	Directory is enabled.
Last synchronization	Time of the last Azure Active Directory tenant synchronization with the local Active Directory.

Defining categories for the inheritance of entitlements

In One Identity Manager, user accounts can selectively inherit groups, administrator roles, subscriptions, and disabled service plans. To do this, the groups (administrator roles, subscriptions, and disabled service plans) and the user accounts are divided into categories. The categories can be freely selected and are specified using a mapping rule. Each category is given a specific position within the template. The mapping rule contains different tables. Use the user account table to specify categories for target system dependent user accounts. In the other tables, enter your categories for the groups, administrator roles, subscriptions, and disabled service plans. Each table contains the category positions **position 1** to **position 63**.

To define a category

1. In the Manager, select the Azure Active Directory tenant in the **Azure Active Directory > Tenants** category.

2. Select the **Change main data** task.

3. Switch to the **Mapping rule category** tab.

4. Extend the relevant roots of a table.

5. To enable the category, double-click ⊗.

6. Enter a category name of your choice for user accounts and groups (administrator roles, subscriptions, disabled service plans) in the login language that you use.

7. Save the changes.

Related topics

- Azure Active Directory group inheritance based on categories on page 105
- Azure Active Directory administrator role inheritance based on categories on page 118
- Inheriting Azure Active Directory subscriptions based on categories on page 145
- Inheritance of disabled Azure Active Directory service plans based on categories on page 146

Editing the synchronization project for an Azure Active Directory tenant

Synchronization projects in which an Azure Active Directory tenant is already used as a base object can also be opened in the Manager. You can, for example, check the configuration or view the synchronization log in this mode. The Synchronization Editor is not started with its full functionality. You cannot run certain functions, such as, running synchronization or simulation, starting the target system browser and others.

NOTE: The Manager is locked for editing throughout. To edit objects in the Manager, close the Synchronization Editor.

To open an existing synchronization project in the Synchronization Editor

1. In the Manager, select the **Azure Active Directory > Tenants** category.
2. In the result list, select the Azure Active Directory tenant.
3. Select the **Change main data** task.
4. Select the **Edit synchronization project** task.

Related topics

- Adjusting the synchronization configuration for Azure Active Directory environments on page 32

Azure Active Directory domains

A base domain is linked to the core directory in the cloud. You can also add other user-defined domains in Azure Active Directory, which you can then allocate to Microsoft cloud services. One Identity Manager only loads verified domain data into the database. It is not possible to edit data in One Identity Manager.

To obtain an overview of a domain

1. In the Manager, select the **Azure Active Directory > Verified domains** category.
2. Select the domain in the result list.
3. Select the **Azure Active Directory domain overview** task.

Table 27: Domain main data

Property	Description
Domain name	Full domain name.
Tenant	Azure Active Directory tenant entered for this domain.

Property	Description
Type	Type of domain.
Primary domain	Specifies whether this is the primary domain, for example, for creating new Azure Active Directory user accounts.
Initial domain	Specifies whether this is the initial domain. The initial domain is created when a tenant is registered in Azure Active Directory.
Available services	List of the services available in this domain.

Related topics

Azure Active Directory policies for activity-based timeouts

You can use Azure Active Directory activity-based timeout policies to specify the idle time of web sessions for applications. For more information, see the *Azure Active Directory documentation* from Microsoft.

Azure Active Directory activity-based timeout policies are loaded into One Identity Manager during synchronization and cannot be changed.

To display information about an Azure Active Directory policy

1. In the Manager, select the **Azure Active Directory > Tenants > <your tenant> > Policies > Activity-based timeout policies** category.

2. In the result list, select the Azure Active Directory policy.

3. Select one of the following tasks:

    - **Activity-based timeout policy overview**: This shows you an overview of the Azure Active Directory policy and its dependencies.

    - **Change main data**: Shows the Azure Active Directory policy's main data. You cannot edit the main data.

        - **Display name**: The Azure Active Directory policy's display name.

        - **Description**: Description of the Azure Active Directory policy.

        - **Definition**: Definition of the Azure Active Directory in JSON format.

        - **Tenant**: Azure Active Directory tenant that owns the policy.

        - **Default policy**: Specifies whether this is the Azure Active Directory tenant's default policy.

Azure Active Directory policies for home realm discovery

You can use Azure Active Directory home realm discovery policies to accelerate logging users into federated domains. To provide an Azure Active Directory home realm discovery policy for an Azure Active Directory application, you assign the policy to the Azure Active Directory service principal. For more information, see the *Azure Active Directory documentation* from Microsoft.

Azure Active Directory home realm discovery policies are loaded into One Identity Manager during synchronization and cannot be changed.

To display information about an Azure Active Directory policy

1. In the Manager, select the **Azure Active Directory > Tenants > <your tenant> > Policies > Home realm discovery policies** category.

2. In the result list, select the Azure Active Directory policy.

3. Select one of the following tasks:

   - **Home realm discovery policy overview**: This shows you an overview of the Azure Active Directory policy and its dependencies.

   - **Change main data**: Shows the Azure Active Directory policy's main data. You cannot edit the main data.

     - **Display name**: The Azure Active Directory policy's display name.

     - **Description**: Description of the Azure Active Directory policy.

     - **Definition**: Definition of the Azure Active Directory in JSON format.

     - **Tenant**: Azure Active Directory tenant that owns the policy.

     - **Default policy**: Specifies whether this is the Azure Active Directory tenant's default policy.

Related topics

- Displaying Azure Active Directory service principal main data on page 207

Azure Active Directory policies for issuing tokens

You can use Azure Active Directory token issuance policies to specify SAML token properties for logging in. To provide an Azure Active Directory token issuance policy for an Azure Active Directory application, you assign the policy to the Azure Active Directory application. For more information, see the *Azure Active Directory documentation* from Microsoft.

Azure Active Directory token issuance policies are loaded into One Identity Manager during synchronization and cannot be changed.

To display information about an Azure Active Directory policy

1. In the Manager, select the **Azure Active Directory > Tenants > <your tenant> > Policies > Token issuance policies** category.

2. In the result list, select the Azure Active Directory policy.

3. Select one of the following tasks:

   - **Token issuance policy overview**: This shows you an overview of the Azure Active Directory policy and its dependencies.

   - **Change main data**: Shows the Azure Active Directory policy's main data. You cannot edit the main data.

     - **Display name**: The Azure Active Directory policy's display name.

     - **Description**: Description of the Azure Active Directory policy.

     - **Definition**: Definition of the Azure Active Directory in JSON format.

     - **Tenant**: Azure Active Directory tenant that owns the policy.

     - **Default policy**: Specifies whether this is the Azure Active Directory tenant's default policy.

Related topics

- Displaying Azure Active Directory applications on page 203

Azure Active Directory policies for token lifetime

You can use Azure Active Directory token lifetime policies to specify the validity of token for logging in. To provide an Azure Active Directory token lifetime policy for an Azure Active Directory application, you assign the policy to the Azure Active Directory application. For more information, see the *Azure Active Directory documentation* from Microsoft.

Azure Active Directory token lifetime policies are loaded into One Identity Manager during synchronization and cannot be changed.

To display information about an Azure Active Directory policy

1. In the Manager, select the **Azure Active Directory > Tenants > <your tenant> > Policies > Token lifetime policies** category.

2. In the result list, select the Azure Active Directory policy.

3. Select one of the following tasks:

- **Token lifetime policy overview**: This shows you an overview of the Azure Active Directory policy and its dependencies.
- **Change main data**: Shows the Azure Active Directory policy's main data. You cannot edit the main data.
    - **Display name**: The Azure Active Directory policy's display name.
    - **Description**: Description of the Azure Active Directory policy.
    - **Definition**: Definition of the Azure Active Directory in JSON format.
    - **Tenant**: Azure Active Directory tenant that owns the policy.
    - **Default policy**: Specifies whether this is the Azure Active Directory tenant's default policy.

Related topics

Azure Active Directory user accounts

You use One Identity Manager to manage user accounts in Azure Active Directory. The user requires a subscription to access the service plans in Azure Active Directory. Azure Active Directory user accounts obtain the required access permissions to the resources through membership in groups.

Related topics

Creating and editing Azure Active Directory user accounts

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

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

NOTE: If employees are to obtain their user accounts through account definitions, the employees must own a central user account and obtain their IT operating data through assignment to a primary department, a primary location, or a primary cost center.

TIP: You can combine the account definition for creating the user account and the subscription that will be used into one system role. In this way, the employee automatically obtains a user account and a subscription.

An employee can obtain this system role directly through departments, cost centers, locations, or business roles, or an IT Shop request.

To create a user account

1. In the Manager, select the **Azure Active Directory > User accounts** category.
2. Click ￼ in the result list.
3. On the main data form, edit the main data of the user account.
4. Save the changes.

To edit main data of a user account

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

To manually assign a user account for an employee

1. In the Manager, select the **Employees > Employees** category.
2. Select the employee in the result list.
3. Select the **Assign Azure Active Directory user accounts** task.
4. Assign a user account.
5. Save the changes.

Detailed information about this topic

Related topics

General main data of Azure Active Directory user accounts

Enter the following data on the **General** tab.

Table 28: Additional main data of a user account

Property	Description
Employee	Employee that uses this user account. An employee is already entered if the user account was generated by an account definition. If you create the user account manually, you can select an employee in the menu. If you are using automatic employee assignment, an associated employee is found and added to the user account when you save the user account.
	You can create a new employee for a user account with an identity of type **Organizational identity**, **Personalized administrator identity**, **Sponsored identity**, **Shared identity**, or **Service identity**. To do this, click ⬛ next to the input field and enter the required employee main data. Which login data is required depends on the selected identity type.
Account definition	Account definition through which the user account was created.

Property	Description
	Use the account definition to automatically fill user account main data and to specify a manage level for the user account. One Identity Manager finds the IT operating data of the assigned employee and enters it in the corresponding fields in the user account.
	NOTE: The account definition cannot be changed once the user account has been saved.
	NOTE: Use the user account's **Remove account definition** task to reset the user account to **Linked** status. This removes the account definition from both the user account and the employee. The user account remains but is not managed by the account definition anymore. The task only removes account definitions that are directly assigned (XOrigin=1).
Manage level	Manage level of the user account. Select a manage level from the menu. You can only specify the manage level can if you have also entered an account definition. All manage levels of the selected account definition are available in the menu.
Tenant	Azure Active Directory user account's tenant.
User type	Type of user account. Depending on the user type, other mandatory input is required. Permitted values are: • **Member**: Normal Azure Active Directory user account. • **Guest**: User account for guest users. The Azure Active Directory connector creates a user account for guest users and ensures that an invitation is sent by email to the given email address. Further configuration of guest users is required in the synchronization project. For more information, see Customizing synchronization projects to invite guest users on page 34.
Invitation status	(Only for the **Guest** user type) Acceptance status of the guest's invitation. Permitted values are: • **Pending acceptance**: The user has not accepted the invitation yet. • **Accepted**: The user has accepted the invitation. • **Empty**: Guest user without invitation.
Last change	(Only for the **Guest** user type) Time at which the invitation status was changed.
Domain	User account's domain.

Property	Description
Location	Location where this user account is in use. In the One Identity Manager, if you assign Azure Active Directory subscriptions, a location is required.
First name	The user's first name. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
Last name	The user's last name. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
Date of birth	The user's date of birth
Age group	The user's age group. Permitted values are **Minor**, **Teenager**, and **Adult**.
Consent for minors	Specifies whether consent must be given for minors. Permitted values are **Obtained**, **Not obtained**, and **Not required**.
User login name	User account login name. The user's login name is made up of the alias and the domain. User login names that are formatted like this correspond to the User Principal Name (UPN) in Azure Active Directory.
Display name	User account display name.
Alias	Email alias for the user account.
Email address	User account's email address.
Preferred language	User's preferred language, for example, **en-US**.
Password	Password for the user account. The employee's central password can be mapped to the user account password. For detailed information about an employee's central password, see *One Identity Manager Identity Management Base Module Administration Guide*. If you use a random generated initial password for the user accounts, it is automatically entered when a user account is created. The password is deleted from the database after publishing to the target system. NOTE: One Identity Manager password policies are taken into account when a user password is being verified. Ensure that the password policy does not violate the target system's requirements.
Password confirmation	Reconfirm password.
Change password at next login	Specifies whether the user must change their password the next time they log in.
Password	Policies, which only apply to the user account. The available options are:

ONE IDENTITY
by Quest

One Identity Manager 8.2 Administration Guide for Connecting to
Azure Active Directory

174

Mapping of Azure Active Directory objects in One Identity Manager

Property	Description
policy	**No restrictions**, **Password never expires**, and **Allow weak passwords**.
Password last changed	Data of last password change. The date is read in from the Azure Active Directory system and cannot be changed.
Risk index (calculated)	Maximum risk index value of all assigned groups. The property is only visible if the **QER | CalculateRiskIndex** configuration parameter is set. For detailed information, see the *One Identity Manager Risk Assessment Administration Guide*.
Category	Categories for the inheritance of groups by the user account. Groups can be selectively inherited by user accounts. To do this, groups and user accounts or contacts are divided into categories. Select one or more categories from the menu.
Identity	User account's identity type Permitted values are: • **Primary identity**: Employee's default user account. • **Organizational identity**: Secondary user account used for different roles in the organization, for example for subcontracts with other functional areas. • **Personalized administrator identity**: User account with administrative permissions, used by one employee. • **Sponsored identity**: User account to use for a specific purpose. Training, for example. • **Shared identity**: User account with administrative permissions, used by several employees. Assign all employees that use this user account. • **Service identity**: Service account.
Privileged user account.	Specifies whether this is a privileged user account.
Disabled service plans can be inherited	Specifies whether the user account can inherit disabled Azure Active Directory service plans through the employee. If this option is set, the user account inherits disabled service plans through hierarchical roles or IT Shop requests. • If you add an employee with a user account to a department, for example, and you have assigned disabled service plans to this department, the user account inherits these disabled service plans. • If an employee has requested a disabled service plan in the IT Shop and the request is granted approval, the employee's user account only inherits the disabled service plan if the option is set.

Property	Description
Subscriptions can be inherited	Specifies whether the user account can inherit Azure Active Directory subscriptions through the employee. If this option is set, the user account inherits Azure Active Directory subscriptions through hierarchical roles or IT Shop requests. • If you add an employee with a user account to a department, for example, and you have assigned Azure Active Directory subscriptions to this department, the user account inherits these Azure Active Directory subscriptions. • If an employee has requested an Azure Active Directory subscription in the IT Shop and the request is granted approval, the employee's user account only inherits the Azure Active Directory subscription if the option is set.
Administrator roles can be inherited	Specifies whether the user account can inherit Azure Active Directory administrator roles through the employee If this option is set, the user account inherits administrator roles through hierarchical roles or IT Shop requests. • If you add an employee with a user account to a department, for example, and you have assigned administrator roles to this department, the user account inherits these administrator roles. • If an employee has requested an administrator role in the IT Shop and the request is granted approval, the employee's user account only inherits the administrator role if the option is set.
Groups can be inherited	Specifies whether the user account can inherit groups through the linked employee. If the option is set, the user account inherits groups through hierarchical roles, in which the employee is a member, or through IT Shop requests. • If you add an employee with a user account to a department, for example, and you have assigned groups to this department, the user account inherits these groups. • If an employee has requested group membership in the IT Shop and the request is granted approval, the employee's user account only inherits the group if the option is set.
Office 365 groups can be inherited	NOTE: This property is only available if the Exchange Online Module is installed. Specifies whether the user account can inherit Office 365 groups through the linked employee. If the option is set, the user account inherits Office 365 groups through hierarchical roles, in which the employee is a member, or through IT Shop requests. • If you add an employee with a user account to a department, for example, and you have assigned Office 365 groups to this

Property	Description
	department, the Azure Active Directory user account inherits these Office 365 groups. • If an employee has requested group membership in the IT Shop and the request is granted approval, the employee's Azure Active Directory user account only inherits the Office 365 group if the option is set. For detailed information about Office 365 groups, see the *One Identity Manager Administration Guide for Connecting to Exchange Online*.
User account is disabled	Specifies whether the user account is disabled. If a user account is not required for a period of time, you can temporarily disable the user account by using the "User account is disabled" option.
Resource account	Specifies whether this user account is a resource account.

Related topics

- Account definitions for Azure Active Directory user accounts on page 58
- Password policies for Azure Active Directory user accounts on page 147
- Azure Active Directory group inheritance based on categories on page 105
- Managing Azure Active Directory user accounts and employees on page 57
- Supported user account types on page 85
- Disabling Azure Active Directory user accounts on page 181
- Prerequisites for indirect assignment of Azure Active Directory groups to Azure Active Directory user accounts on page 95
- Prerequisites for indirect assignment of Azure Active Directory administration roles to Azure Active Directory user accounts on page 111
- Prerequisites for indirect assignment of Azure Active Directory subscriptions to Azure Active Directory user accounts on page 127
- Prerequisites for indirect assignment of disabled Azure Active Directory service plans to Azure Active Directory user accounts on page 138

Contact data for Azure Active Directory user accounts

Enter the following address data for contacting the employee on the **Contact** tab.

ONE IDENTITY
by Quest

One Identity Manager 8.2 Administration Guide for Connecting to
Azure Active Directory

177

Mapping of Azure Active Directory objects in One Identity Manager

Table 29: Contact data

Property	Description
Street	Street or road. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
State	State. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
City	City. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level. Locations can be automatically generated and employees assigned based on the city.
Zip code	Zip code. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
Country	The country ID.
Business phones	Business telephone numbers.
Mobile phone	Mobile number. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
Fax	Fax number. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
Additional email addresses	User email addresses.
Proxy addresses	Other email addresses for the user. You can also add other mail connectors (for example, CCMail, MS) in addition to the standard address type (SMTP, X400). Use the following syntax to set up other proxy addresses: `Address type: <email address>`

Information about the user profile for Azure Active Directory user accounts

The following information is displayed on the **User profile** tab.

Table 30: User profile

Property	Description
Preferred name	The user's preferred name.
Legal age group	This is used by Enterprise application to determined the legal age groups of users. The property is calculated based on the **Age group**

Property	Description
	and **Consent for minors** properties.
VoIP SIP addresses	The instant message voice over IP (VoIP) session initiation protocol (SIP) addresses for the user.
Personal site	URL for the user's personal website.
About me	Text field to the user to write a description of themselves.
Responsibilities	List of the user's responsibilities.
Schools	List of schools the user has attended.
Skills and expertise	List of the user's qualifications.
Past projects	List of the user's past projects.
Interests	List of the user's interests.

Organizational data for Azure Active Directory user accounts

The following organizational main data is mapped on the **Organizational** tab.

Table 31: Organizational main data

Property	Description
Employee identifier	ID of the user within the organization. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
Date hired	Date on which the user entered the company.
Company	Employee's company. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
Department	Employee's department. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
Office	Office. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
Job description	Job description. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
Account manager	Manager responsible for the user account. ***To specify an account manager*** 1. Click ➜ next to the field.

2. In the **Table** menu, select the table that maps the account manager.

3. In the **Account manager** menu, select the manager.

4. Click **OK**.

Information about the local Active Directory user account

The **Linked** tab shows information about the local Active Directory user account, which is linked to the Azure Active Directory user account.

Table 32: Local Active Directory user account data

Property	Description
Synchronization with local Active Directory enabled	Specifies whether synchronization with a local Active Directory is enabled.
Last synchronization	Time of the last Azure Active Directory user account synchronization with the local Active Directory.
SID of the local account.	Security ID of the local Active Directory user account.
Immutable identifier	Identifier that is used to maintain the relationship between the Active Directory user account and the Azure Active Directory user account. The identifier cannot be changed.
Distinguished name	Active Directory user account's distinguished name.
Full domain name	Full domain name of the user account's Active Directory domain.
Login name (pre Win2000)	Login name of the Active Directory user account for the previous version of Active Directory.
User login name (of local account)	Active Directory user account login name.
Attribute extension 01 - attribute extension 15	Additional company-specific information about the Active Directory user account.

ONE IDENTITY
by Quest

One Identity Manager 8.2 Administration Guide for Connecting to
Azure Active Directory

180

Mapping of Azure Active Directory objects in One Identity Manager

Related topics

Assigning extended properties to Azure Active Directory user accounts

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

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

To specify extended properties for a user account

1. In the Manager, select the **Azure Active Directory > User accounts** category.

2. Select the user account in the result list.

3. Select **Assign extended properties**.

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

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

   To remove an assignment

   - Select the extended property and double-click ✅.

5. Save the changes.

Disabling Azure Active Directory user accounts

The way you disable user accounts depends on how they are managed.

Scenario:

The user account is linked to employees and is managed through account definitions.

User accounts managed through account definitions are disabled when the employee is temporarily or permanently disabled. The behavior depends on the user account manage level. Accounts with the **Full managed** manage level are disabled depending on the account definition settings. For user accounts with a manage level, configure the required behavior using the template in the `AADUser.AccountDisabled` column.

Scenario:

The user accounts are linked to employees. No account definition is applied.

User accounts managed through user account definitions are disabled when the employee is temporarily or permanently disabled. The behavior depends on the **QER | Person | TemporaryDeactivation** configuration parameter

- If the configuration parameter is set, the employee's user accounts are disabled when the employee is permanently or temporarily disabled.

- If the configuration parameter is not set, the employee's properties do not have any effect on the associated user accounts.

To disable the user account when the configuration parameter is disabled

1. In the Manager, select the **Azure Active Directory > User accounts** category.

2. Select the user account in the result list.

3. Select the **Change main data** task.

4. On the **General** tab, set the **Account is disabled** option.

5. Save the changes.

Scenario:

User accounts not linked to employees.

To disable a user account that is no longer linked to an employee

1. In the Manager, select the **Azure Active Directory > User accounts** category.

2. Select the user account in the result list.

3. Select the **Change main data** task.

4. On the **General** tab, set the **Account is disabled** option.

5. Save the changes.

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

Related topics

- Account definitions for Azure Active Directory user accounts on page 58
- Creating manage levels on page 65
- Deleting and restoring Azure Active Directory user accounts on page 183

ONE IDENTITY
by Quest

One Identity Manager 8.2 Administration Guide for Connecting to
Azure Active Directory

182

Mapping of Azure Active Directory objects in One Identity Manager

Deleting and restoring Azure Active Directory user accounts

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

You can delete a user account that was not created using an account definition through the result list or from the menu bar. After you have confirmed the security alert the user account is marked for deletion in the One Identity Manager. The user account is locked in One Identity Manager and permanently deleted from the One Identity Manager database and the target system depending on the deferred deletion setting.

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

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

1. In the Manager, select the **Azure Active Directory > User accounts** category.
2. Select the user account in the result list.
3. Click ⊠ in the result list.
4. Confirm the security prompt with **Yes**.

To restore a user account

1. In the Manager, select the **Azure Active Directory > User accounts** category.
2. Select the user account in the result list.
3. Click ⊡ in the result list.

Related topics

- Disabling Azure Active Directory user accounts on page 181
- Specifying deferred deletion for Azure Active Directory user accounts on page 92

Displaying the Azure Active Directory user account overview

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

To obtain an overview of a user account

1. In the Manager, select the **Azure Active Directory > User accounts** category.
2. Select the user account in the result list.

3. Select the **Azure Active Directory user account overview** task.

Related topics

-

Displaying Active Directory user accounts for Azure Active Directory user accounts

You can see the Active Directory user account for an Azure Active Directory user account on the overview form.

To display the Active Directory user account for an Azure Active Directory user account

1. In the Manager, select the **Azure Active Directory > User accounts** category.

2. Select the user account in the result list.

3. Select the **Azure Active Directory user account overview** task.

   The **Active Directory user account** form element shows which user account is linked to it.

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

Related topics

-

Azure Active Directory groups

Azure Active Directory recognizes several group types into which you can organize users and groups to regulate access to resources or email distribution, for example.

Azure Active Directory groups are loaded into One Identity Manager by synchronization. You can edit individual main data of the group and you can create new security groups in One Identity Manager. However, you cannot create more group types in One Identity Manager.

To add users to groups, you assign the groups directly to users. This can be assignments of groups to departments, cost centers, locations, business roles, or the IT Shop.

NOTE: Assignments to Azure Active Directory groups that are synchronized with the local Active Directory are not allowed in One Identity Manager. These groups cannot be requested through the web portal. You can only manage these groups in your locally. For

more information, see the *Azure Active Directory documentation* from Microsoft.

The group types supported in One Identity Manager are listed below.

Table 33: Support groups types

Group type	Description
Security group	Resource permissions are distributed through security groups. User accounts and other groups are added to security groups, which makes administration easier.
	Security groups are loaded into One Identity Manager by synchronization. You can edit security groups in One Identity Manager and also create new ones.
Office 365 group	Office 365 groups are loaded into One Identity Manager by synchronization. You can edit Office 365 groups in One Identity Manager but
	you can only create new Office 365 groups in One Identity Manager if the Exchange Online Module in installed. For more information, see the *One Identity Manager Administration Guide for Connecting to Exchange Online*.
Distribution group	Distribution groups are used to send emails to group members. Distribution groups are loaded into One Identity Manager by synchronization. You can edit distribution groups in One Identity Manager but you cannot create them in One Identity Manager.
Mail-enabled security groups	Mail-enabled security groups are security groups that are used as distribution groups.
	Mail-enabled security groups are loaded into One Identity Manager by synchronization. You can edit mail-enabled security groups in One Identity Manager but you can only create new mail-enabled security groups in One Identity Manager if the Exchange Online Module is installed. For more information, see the *One Identity Manager Administration Guide for Connecting to Exchange Online*.
Dynamic group	Members of a dynamic group are not strictly assigned, but determined through defined rules. Dynamic groups are loaded into One Identity Manager by synchronization. You can change dynamic groups in One Identity Manager. You cannot create new dynamic groups in One Identity Manager.

Related topics

- Managing memberships in Azure Active Directory groups on page 93
- Editing main data of Azure Active Directory groups on page 186
- Adding Azure Active Directory groups to Azure Active Directory groups on page 189
- Assigning owners to Azure Active Directory groups on page 189

- Assigning extended properties to Azure Active Directory groups on page 190
- Deleting Azure Active Directory groups on page 191
- Displaying the Azure Active Directory group overview on page 191
- Displaying Active Directory groups for Azure Active Directory groups on page 191
- Synchronizing single objects on page 50
- Displaying enabled and disabled Azure Active Directory service plans forAzure Active Directory user accounts and Azure Active Directory groups on page 124

Editing main data of Azure Active Directory groups

Azure Active Directory groups are loaded into One Identity Manager by synchronization. You can create security groups in One Identity Manager. You cannot create distribution group and dynamic groups in One Identity Manager.

You can only create mail-enabled security groups and Office 365 groups in One Identity Manager if the Exchange Online Module is installed. For more information, see the *One Identity Manager Administration Guide for Connecting to Exchange Online*.

the data you can edit depends on the group type.

To edit group main data

1. In the Manager, select the **Azure Active Directory > Groups** category.
2. Select the group in the result list.
3. Select the **Change main data** task.
4. On the main data form, edit the main data of the group.
5. Save the changes.

Detailed information about this topic

- General main data of Azure Active Directory groups on page 187
- Information about local Active Directory groups on page 188

General main data of Azure Active Directory groups

Enter the following data on the **General** tab.

Table 34: General main data

Property	Description
Display name	The display name is used to display the group in the One Identity Manager tools user interface.
Tenant	The group's Azure Active Directory tenant.
Alias	Email alias for the group.
Email address	Group's email address
Proxy addresses	Other email addresses for the group. You can also add other mail connectors (for example, CCMail, MS) in addition to the standard address type (SMTP, X400). Use the following syntax to set up other proxy addresses: `Address type: new email address`
Group type	The type of group. is empty for security and distribution groups. The value is **Unified** for Office 365 groups and For dynamic groups, the value entered is **DynamicMembership**.
Security group	Specifies whether this group is a security group. Resource permissions are distributed through security groups. User accounts and other groups are added to security groups, which makes administration easier.
Mail-enabled	Specifies whether the email is enabled for the group. If this option is set for a security group, it is a mail-enabled security group. Otherwise, it is a distribution group.
IT Shop	Specifies whether the group can be requested through the IT Shop. If this option is set, the group can be requested by the employees through the Web Portal and distributed with a defined approval process. The group can still be assigned directly to hierarchical roles.
Only for use in IT Shop	Specifies whether the group can only be requested through the IT Shop. If this option is set, the group can be requested by the employees through the Web Portal and distributed with a defined approval process. Direct assignment of the group to hierarchical roles or user accounts is not permitted.
Service item	Service item data for requesting the group through the IT Shop.
Risk index	Value for evaluating the risk of assigning the group to user accounts. Set a

Property	Description
	value in the range **0** to **1**. This input field is only visible if the **QER | CalculateRiskIndex** configuration parameter is activated. For more information about risk assessment, see the *One Identity Manager Risk Assessment Administration Guide*.
Category	Categories for group inheritance. Groups can be selectively inherited by user accounts. To do this, groups and user accounts are divided into categories. Select one or more categories from the menu.
Description	Text field for additional explanation.

Related topics

- Azure Active Directory group inheritance based on categories on page 105
- For more information about preparing groups for requesting through the IT Shop, see the *One Identity Manager IT Shop Administration Guide*.

Information about local Active Directory groups

The **Federation** tab shows information about the local Active Directory user account that is linked to the Azure Active Directory user account.

Assignments to Azure Active Directory groups that are synchronized with the local Active Directory are not allowed in One Identity Manager. These groups cannot be requested through the web portal. You can only manage these groups in your locally. For more information, see the *Azure Active Directory documentation* from Microsoft.

Table 35: Local Active Directory group data

Property	Description
Synchronization with local Active Directory enabled	Specifies whether synchronization with a local Active Directory is enabled.
Last synchronization	Time of the last Azure Active Directory group synchronization with the local Active Directory.
SID of local group	Security ID of the local Active Directory group.

Related topics

- For more information, see Displaying Active Directory groups for Azure Active Directory groups on page 191.

Adding Azure Active Directory groups to Azure Active Directory groups

Use this task to add a group to another group. This means that the groups can be hierarchically structured.

To assign groups directly to a group as members

1. In the Manager, select the **Azure Active Directory > Groups** category.

2. Select the group in the result list.

3. Select the **Assign groups** category.

4. Select the **Has members** tab.

5. Assign child groups in **Add assignments**.

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

   To remove an assignment

   - Select the group and double-click ⊘.

6. Save the changes.

To add a group as a member of other groups

1. In the Manager, select the **Azure Active Directory > Groups** category.

2. Select the group in the result list.

3. Select the **Assign groups** task.

4. Select the **Is member of** tab.

5. In the **Add assignments** pane, assign parent groups.

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

   To remove an assignment

   - Select the group and double-click ⊘.

6. Save the changes.

Assigning owners to Azure Active Directory groups

A group owner can edit group properties.

To assign owners to a group

1. In the Manager, select the **Azure Active Directory > Groups** category.

2. Select the group in the result list.

3. Select the **Assign owner** task.

4. Select the table containing the owner from the **Table** menu at the top of the form. You have the following options:

   - Azure Active Directory user accounts

5. In the **Add assignments** pane, assign owners.

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

   ### To remove an assignment

   - Select the owner and double-click ⊘.

6. Save the changes.

Assigning extended properties to Azure Active Directory groups

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

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

To specify extended properties for a group

1. In the Manager, select the **Azure Active Directory > Groups** category.

2. Select the group in the result list.

3. Select **Assign extended properties**.

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

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

   ### To remove an assignment

   - Select the extended property and double-click ⊘.

5. Save the changes.

ONE IDENTITY
by Quest

One Identity Manager 8.2 Administration Guide for Connecting to
Azure Active Directory

190

Mapping of Azure Active Directory objects in One Identity Manager

Deleting Azure Active Directory groups

Groups are deleted permanently from the One Identity Manager database and from Azure Active Directory.

To delete a group

1. In the Manager, select the **Azure Active Directory > Groups** category.

2. Select the group in the result list.

3. Click in the result list.

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

Displaying the Azure Active Directory group overview

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

To obtain an overview of a group

1. In the Manager, select the **Azure Active Directory > Groups** category.

2. Select the group in the result list.

3. Select the **Azure Active Directory group overview** task.

Related topics

- Displaying enabled and disabled Azure Active Directory service plans forAzure Active Directory user accounts and Azure Active Directory groups on page 124

Displaying Active Directory groups for Azure Active Directory groups

The Active Directory group linked to an Azure Active Directory group is displayed on the overview form.

To display the Active Directory group for an Azure Active Directory group

1. In the Manager, select the **Azure Active Directory > Groups** category.

2. Select the group in the result list.

3. Select the **Azure Active Directory group overview** task.

   The **Active Directory group** form element shows which group is linked to it.

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

Related topics

- Information about local Active Directory groups on page 188

Azure Active Directory administrator roles

By using Azure Active Directory administrator roles, you can assign administrative permissions to users. Azure Active Directory recognizes several administrator roles that fulfill different functions. For more information about administrator roles, see the *Azure Active Directory documentation* from Microsoft.

One Identity Manager administrator roles are loaded into Azure Active Directory by synchronization. You can edit individual main data of Azure Active Directory administrator roles but you cannot create new Azure Active Directory administrator roles in One Identity Manager.

To add users to Azure Active Directory administrator roles, assign the Azure Active Directory administrator roles directly to the user. This may be Azure Active Directory administrator role assignments to departments, cost centers, locations, business roles, or the IT Shop.

Related topics

- Managing Azure Active Directory administrator roles assignments on page 109
- Editing main data of Azure Active Directory administrator roles on page 192
- Assigning extended properties to Azure Active Directory administrator roles on page 194
- Displaying the Azure Active Directory administration role overview on page 194
- Synchronizing single objects on page 50

Editing main data of Azure Active Directory administrator roles

One Identity Manager administrator roles are loaded into Azure Active Directory by synchronization. You can edit individual main data of Azure Active Directory administrator roles but you cannot create new Azure Active Directory administrator roles in One Identity Manager.

To edit the main data of an Azure Active Directory administrator role

1. In the Manager, select the **Azure Active Directory > Administrator roles** category.

2. Select the administrator role in the result list.

3. Select the **Change main data** task.

4. Edit the administrator role's main data.

5. Save the changes.

Table 36: Azure Active Directory administrator role main data

Property	Description
Display name	The display name is used to display the administrator role in the One Identity Manager tools' user interface.
Tenant	The administrator role's Azure Active Directory tenant.
Template ID.	ID of the administrator role template on which this administrator role was based.
IT Shop	Specifies whether the administrator role can be requested through the IT Shop. The administrator role can be ordered by its employees over the Web Portal and distributed using a defined approval process. The administrator role can still be assigned directly to user accounts and hierarchical roles.
Only for use in IT Shop	Specifies whether the administrator role can only be requested through the IT Shop. The administrator role can be ordered by its employees over the Web Portal and distributed using a defined approval process. You cannot assign an administrator role directly to a hierarchical role.
Service item	Specifies a service item for requesting the administrator role through the IT Shop.
Risk index	Value for assessing the risk of assigning administrator roles to user accounts. Set a value in the range **0** to **1**. This input field is only visible if the **QER | CalculateRiskIndex** configuration parameter is set. For more information about risk assessment, see the *One Identity Manager Risk Assessment Administration Guide*.
Category	Categories for inheriting administrator roles. Administrator roles can be selectively inherited by user accounts. To do this, administrator roles and user accounts are divided into categories. Use the menu to allocate one or more categories to the administrator role.
Description	Text field for additional explanation.

Related topics

-
- For more information about preparing administrator roles for requesting through the IT Shop, see the *One Identity Manager IT Shop Administration Guide*.

Assigning extended properties to Azure Active Directory administrator roles

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

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

To specify extended properties for an administrator role

1. In the Manager, select the **Azure Active Directory > Administrator roles** category.
2. Select the administrator role in the result list.
3. Select the **Assign extended properties** task.
4. In the **Add assignments** pane, assign extended properties.

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

   To remove an assignment
   - Select the extended property and double-click ⊘.
5. Save the changes.

Displaying the Azure Active Directory administration role overview

Use this task to obtain an overview of the most important information about an administrator role.

To obtain an overview of a administration role

1. In the Manager, select the **Azure Active Directory > Administrator roles** category.
2. Select the administrator role in the result list.
3. Select the **Azure Active Directory administrator role overview** task.

Azure Active Directory subscriptions and Azure Active Directory service principals

Information about Azure Active Directory subscriptions and Azure Active Directory service plans within an Azure Active Directory tenant is loaded into One Identity Manager during synchronization. In One Identity Manager, you cannot create new Azure Active Directory subscriptions or Azure Active Directory service plans. However, in One Identity Manager, you can edit certain main data of requesting the Azure Active Directory subscription in the IT Shop and for user account assignments.

NOTE: An Azure Active Directory user account can also obtain Azure Active Directory subscriptions through its Azure Active Directory groups. You cannot edit assignments by Azure Active Directory groups in One Identity Manager.

Related topics

Editing Azure Active Directory subscription main data

To edit Azure Active Directory subscription main data

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

Table 37: Azure Active Directory subscription main data

Property	Description
SKU display name	The SKU display name of the Azure Active Directory subscription. For example, AAD_Premium or RMSBASIC.
Tenant	Tenant given for this Azure Active Directory subscription.
Subscription status	The Azure Active Directory subscription status, such as **enabled** (active).
Purchased licenses	The number of licenses purchased.
Assigned licenses	Number of actively used licenses.
Suspended licenses	Number of suspended licenses.
Warning units	Number of licenses with a warn status.
IT Shop	Specifies whether the Azure Active Directory subscription can be requested through the IT Shop. This Azure Active Directory subscription can be requested by staff using the Web Portal and granted through a defined approval process. The Azure Active Directory subscription can still be assigned directly to user accounts and hierarchical roles.
Only for use in IT Shop	Specifies whether the Azure Active Directory subscription can only be requested through the IT Shop. This Azure Active Directory subscription can be requested by staff using the Web Portal and granted through a defined approval process. The Azure Active Directory subscription may not be assigned directly to hierarchical roles.
Service item	Service item data for requesting the Azure Active Directory subscription through the IT Shop.
Risk index	Value for evaluating the risk of assigning the Azure Active Directory subscription to Azure Active Directory user accounts. Set a value in the range **0** to **1**. This field is only visible if the **QER | CalculateRiskIndex** configuration parameter is set. For more information about risk assessment, see the *One Identity Manager Risk Assessment Administration Guide.*
Category	Category for Azure Active Directory subscription inheritance. Azure Active Directory subscriptions can be selectively inherited by Azure Active Directory user accounts. To do this, the Azure Active Directory subscriptions the Azure Active Directory user accounts are divided into categories. Use this menu to allocate one or more categories to the Azure Active Directory subscription.

Related topics

- Azure Active Directory group inheritance based on categories on page 105
- For detailed information about preparing subscriptions for requesting through the IT Shop, see the *One Identity Manager IT Shop Administration Guide*.

Assigning additional properties to Azure Active Directory subscriptions

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

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

To specify extended properties for an Azure Active Directory subscription

1. In the Manager, select the **Azure Active Directory > Subscriptions** category.
2. Select an Azure Active Directory subscription in the result list.
3. Select **Assign extended properties**.
4. In the **Add assignments** pane, assign extended properties.

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

   To remove an assignment
   - Select the extended property and double-click ⊘.
5. Save the changes.

Displaying the Azure Active Directory subscriptions and service plan overview

Use this task to obtain an overview of the most important information about an Azure Active Directory subscription and a service plan.

To obtain an overview of an Azure Active Directory subscription

1. In the Manager, select the **Azure Active Directory > Subscriptions** category.
2. Select an Azure Active Directory subscription in the result list.
3. Select the **Azure Active Directory subscription overview** task.

To obtain an overview of an Azure Active Directory service plan

1. In the Manager, select the **Azure Active Directory > Service plans** category.

2. Select the Azure Active Directory service plan in the result list.

3. Select the **Azure Active Directory service plan overview** task.

Related topics

- Displaying enabled and disabled Azure Active Directory service plans forAzure Active Directory user accounts and Azure Active Directory groups on page 124

Disabled Azure Active Directory service plans

To prevent users from using individual Azure Active Directory service plans, so-called "disabled service plans" are mapped in One Identity Manager. Disabled service plans are created automatically in One Identity Manager after synchronizing Azure Active Directory subscriptions. Disabled service plans are requested through the IT Shop or assigned to users through departments, cost centers, locations, business roles, or system roles.

NOTE: An Azure Active Directory user accounts can also obtain disabled service plans through its Azure Active Directory groups. You cannot edit assignments by Azure Active Directory groups in One Identity Manager.

Related topics

- Managing Azure Active Directory subscription and Azure Active Directory service plan assignments on page 120
- Displaying enabled and disabled Azure Active Directory service plans forAzure Active Directory user accounts and Azure Active Directory groups on page 124
- Editing main data of disabled Azure Active Directory service plans on page 199
- Assigning extended properties to disabled Azure Active Directory service plans on page 200
- Displaying the disabled Azure Active Directory service plan overview on page 200
- Synchronizing single objects on page 50

Editing main data of disabled Azure Active Directory service plans

To edit disabled Azure Active Directory service plan main data

1. In the Manager, select the **Azure Active Directory > Disabled service plans** category.

2. Select the disabled service plan from the result list.

3. Select the **Change main data** task.

4. Edit the disabled service plan's main data.

5. Save the changes.

Table 38: Disabled service plan main data

Property	Description
Subscription	Name of the Azure Active Directory subscription.
Service plan	Name of the Azure Active Directory service plan.
IT Shop	Specifies whether the service plan can be requested through the IT Shop. The disabled service plan can be requested by your staff though the Web Portal and granted through a defined approval process. The disabled service plan can still be assigned directly to hierarchical roles.
Only for use in IT Shop	Specifies whether the disabled service plan can only be requested through the IT Shop. The disabled service plan can be requested by your staff though the Web Portal and granted through a defined approval process. The disabled service plan may not be assigned directly to hierarchical roles.
Service item	Service item data for requesting the disabled service plan through the IT Shop.
Category	Categories for disabled service plan inheritance. User accounts can selectively inherit disabled Azure Active Directory service plans. To do this, disabled service plans and Azure Active Directory user accounts are divided into categories. Use this menu to allocate one or more categories to the disabled service plan.

Related topics

- Azure Active Directory group inheritance based on categories on page 105

- For detailed information about preparing service plans for requesting through the IT Shop, see the *One Identity Manager IT Shop Administration Guide*.

Assigning extended properties to disabled Azure Active Directory service plans

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

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

To specify extended properties for a disabled Azure Active Directory service plan

1. In the Manager, select the **Azure Active Directory > Disabled service plans** category.
2. Select the disabled service plan from the result list.
3. Select **Assign extended properties**.
4. In the **Add assignments** pane, assign extended properties.

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

   ### *To remove an assignment*
   - Select the extended property and double-click ⊘.
5. Save the changes.

Displaying the disabled Azure Active Directory service plan overview

Use this task to obtain an overview of the most important information about a disabled Azure Active Directory service plan.

To obtain an overview of a disabled Azure Active Directory service plan

1. In the Manager, select the **Azure Active Directory > Disabled service plans** category.
2. Select the disabled service plan from the result list.
3. Select the **Disabled Azure Active Directory service plan overview** task.

Related topics

- Displaying enabled and disabled Azure Active Directory service plans forAzure Active Directory user accounts and Azure Active Directory groups on page 124

Azure Active Directory applications and Azure Active Directory service principals

When an application is registered in an Azure Active Directory tenant, it creates an associated Azure Active Directory service principal. There are so-called app roles defined for applications. Azure Active Directory users, Azure Active Directory groups, or Azure Active Directory service principals can use app roles to provide permissions or functions for the application.

For detailed information about integrating applications into Azure Active Directory, see the *Azure Active Directory documentation* from Microsoft.

Information about Azure Active Directory applications, Azure Active Directory service principals, and app roles within an Azure Active Directory tenant is loaded into One Identity Manager during synchronization. You cannot create new Azure Active Directory applications, Azure Active Directory service principals, and app roles in One Identity Manager but you can specify owners of applications and service principals and create or delete app roles in One Identity Manager.

Detailed information about this topic

- Displaying information about Azure Active Directory applications on page 201
- Assigning owners to Azure Active Directory applications on page 202
- Displaying Azure Active Directory applications on page 203
- Displaying information about Azure Active Directory service principals on page 204
- Assigning owner to Azure Active Directory service principals on page 205
- Editing authorizations for Azure Active Directory service principals on page 206
- Displaying Azure Active Directory service principal main data on page 207

Displaying information about Azure Active Directory applications

The information about the Azure Active Directory application is loaded into One Identity Manager during synchronization. All the Azure Active Directory applications with their Azure Active Directory service principals that are registered in this Azure Active Directory tenant are loaded for each Azure Active Directory tenant.

IF an Azure Active Directory application is used in an Azure Active Directory tenant that is registered in another Azure Active Directory tenant, only the Azure Active Directory service principal and not the Azure Active Directory application is loaded into One Identity Manager.

You cannot create Azure Active Directory applications in One Identity Manager.

To display information about an Azure Active Directory application

1. In the Manager, select the **Azure Active Directory > Applications** category.

2. In the result list, select the Azure Active Directory application.

3. Select one of the following tasks:

   - **Azure Active Directory application overview**: This shows you an overview of the Azure Active Directory application and its dependencies.
   - **Change main data**: Shows the Azure Active Directory application's main data.
   - **Assign owners**: Shows the Azure Active Directory application's owners. You can assign owners to an application or remove them again.

Related topics

- Assigning owners to Azure Active Directory applications on page 202
- Displaying Azure Active Directory applications on page 203
- Displaying information about Azure Active Directory service principals on page 204

Assigning owners to Azure Active Directory applications

Use this task to assign owners to an Azure Active Directory application or to remove them from an Azure Active Directory application. Owners of Azure Active Directory application can show the application registration in Azure Active Directory and edit it.

To assign owners to an Azure Active Directory application

1. In the Manager, select the **Azure Active Directory > Applications** category.

2. In the result list, select the Azure Active Directory application.

3. Select the **Assign owner** task.

4. In the **Table** menu, select the **Azure Active Directory user accounts (AADUser)** item.

5. In the **Add assignments** pane, assign owners.

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

   To remove an assignment

   - Select the owner and double-click ⊘.

6. Save the changes.

ONE IDENTITY
by Quest

One Identity Manager 8.2 Administration Guide for Connecting to
Azure Active Directory

202

Mapping of Azure Active Directory objects in One Identity Manager

Displaying Azure Active Directory applications

The information about the Azure Active Directory application is loaded into One Identity Manager during synchronization. You cannot edit Azure Active Directory application main data.

To display an Azure Active Directory application's main data

1. In the Manager, select the **Azure Active Directory > Applications** category.

2. In the result list, select the Azure Active Directory application.

3. Select **Change main data**.

Table 39: Azure Active Directory application main data

Property	Description
Display name	Display name of the application.
Publisher domain	Name of the application's verified publisher domain.
Registration date	Date and time when the application was registered.
Group membership claim	Group membership claim expected by the application. Group types that are included in the access, ID, and SAML tokens. Permitted values are: • **None**: No group types • **All**: All group types • **Security groups**: Security groups with the user as a member.
Logo URL	Link to the application's logo.
Marketing URL	Link to the application's marketing page.
Privacy statement URL	Link to the application's privacy statement.
Service URL	Link to the application's support page.
Terms of service URL	Link to the application's terms of service.
Fallback public client	Specifies whether the fallback application type is a public client, such as an application installed and running on a mobile device. The default value is false meaning the fallback application type is a confidential client such as a web application. If the option is disabled, it means that the fallback

Property	Description
	application type is a confidential client, such as a web application (default).
Supported user accounts	Specifies which Microsoft user accounts for the current application are supported. Permitted values are: - Accounts in this organizational directory only - Accounts in any organizational directory - Accounts in any organizational directory and personal Microsoft accounts - Only personal Microsoft accounts
Token issuance policies	Name of the policy for issuing tokens.
Token lifetime policy	Name of the policy for token lifetimes.
Tags	User-defined string to use for categorizing and identifying the application.

Related topics

Displaying information about Azure Active Directory service principals

When an application is registered in an Azure Active Directory tenant in Microsoft Azure Management Portal, it creates an associated Azure Active Directory service principal.

The information about the Azure Active Directory service principal is loaded into One Identity Manager during synchronization. You cannot create new Azure Active Directory service principals in One Identity Manager.

To display information about anAzure Active Directory service principal

1. In the Manager, select the **Azure Active Directory > Service principals** category.

2. In the result list, select the Azure Active Directory service principal.

3. Select one of the following tasks:

    - **Azure Active Directory service principal overview**: This shows you an overview of the Azure Active Directory service principal and its dependencies.

- **Change main data**: This displays the Azure Active Directory service principal's main data.
- **Assign owners**: This displays the Azure Active Directory service principals owners. You can assign owners to a service principal or remove them.
- **Assign authorizations**: This displays user accounts, groups, and service principals with their assigned app roles. You can create more authorizations or removed them.

Related topics

Assigning owner to Azure Active Directory service principals

Use this task to assign owners to an Azure Active Directory service principal or to remove them from a service principal.

To assign owners to an Azure Active Directory application

1. In the Manager, select the **Azure Active Directory > Service principals** category.
2. In the result list, select the Azure Active Directory service principal.
3. Select the **Assign owner** task.
4. In the **Table** menu, select the **Azure Active Directory user accounts (AADUser)** item.
5. In the **Add assignments** pane, assign owners.

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

   ### *To remove an assignment*
   - Select the owner and double-click ⊘.

6. Save the changes.

Editing authorizations for Azure Active Directory service principals

There are so-called app roles defined for applications. Azure Active Directory users, Azure Active Directory groups, or Azure Active Directory service principals can use app roles to provide permissions or functions for the application.

App roles and their assignments are loaded into One Identity Manager by synchronization. However, you cannot create new app roles in One Identity Manager. In One Identity Manager, you can add or remove authorizations for the service principals and their applications respectively.

To assign authorizations to an Azure Active Directory service principal

1. In the Manager, select the **Azure Active Directory > Service principals** category.

2. In the result list, select the Azure Active Directory service principal.

3. Select the **Assign authorizations** task.

4. In the **Assignments** pane, click **Add** and enter the following data.

    - **Authorized for**: Specify the user account, group, or service principal for the authorization.

        a. Click ➜ next to the field.

        b. Under **Table**, select one of the following tables:

            - To authorize a user account, select **AADUser**.

            - To authorize a group, select **AADGroup**.

            - To authorize a service principal, select **AADServicePrincipal**.

        c. Under **Authorized for**, select the user account, group, or service principal.

        d. Click **OK**.

    - **App role**: Select the app role for the authorization.

        NOTE: If there is no app role defined for a service principal, leave this item empty to authorize the user account, group, or service principal.

5. Save the changes.

To remove authorizations from an Azure Active Directory service principal

1. In the Manager, select the **Azure Active Directory > Service principals** category.

2. In the result list, select the Azure Active Directory service principal.

3. Select the **Assign authorizations** task.

4. In the **Assignments** pane, select the authorization you want to remove.

5. Click **Remove**.

6. Save the changes.

Displaying Azure Active Directory service principal main data

The information about the Azure Active Directory service principal is loaded into One Identity Manager during synchronization. You cannot edit Azure Active Directory service principal main data.

To display an Azure Active Directory service principal's main data

1. In the Manager, select the **Azure Active Directory > Service principals** category.

2. In the result list, select the Azure Active Directory service principal.

3. Select the **Change main data** task.

Table 40: General main data for an Azure Active Directory service principal

Property	Description
Display name	Name for displaying the service principal.
Alternative names	Alternative names for the service principal. This is used to call service principals by subscription, to identify resource groups and full resource IDs for managing identities.
Web page	Home page of the Azure Active Directory application.
Enabled	Specifies whether the service principal is enabled.
Application display name.	Display name of the associated Azure Active Directory application.
App role assignment required	Specifies whether users or other service principals must be assigned an app role for this service principal before they can login or obtain application tokens.
Logo URL	Link to the application's logo.
Marketing URL	Link to the application's marketing page.
Privacy statement URL	Link to the application's privacy statement.
Service URL	Link to the application's support page.
Terms of service URL	Link to the application's terms of service.
Login URL	URL that the identity provider uses to reroute the user to Azure Active Directory for authentication.

Property	Description
Logout URL	URL that the Microsoft authorization service uses to log out a user using OPENID Connect front channel, OpenID Connect back-channel, or SAML logout protocols.
Notification mail addresses	List of email addresses that Azure Active Directory sends a notification to if the active certificate is nearing the expiration date.
Preferred single sign-on mode	Single sign-on mode configured for this Azure Active Directory application.
Reply URLs	URLs that user tokens are sent to for logging in with the associated application, or the redirect URIs that OAuth 2.0 authorization codes and access tokens are sent to for the associated application.
Service principal names	Contains the list of URIs that identify the associated Azure Active Directory application within its Azure Active Directory tenant, or within a verified custom domain, if the Azure Active Directory application is an Azure Active Directory multi-tenant.
Service principal type	Specifies whether the service principal represents an application or a managed identity. This is set by Azure Active Directory internally. Permitted values are: • **Application**: The service principal represents an application. • **ManagedIdentity**: The service principal represents a managed identity
Encryption key ID	ID of the public key for logging in using certificates.
Home realm discovery policy	Name of the home realm discovery policy.
Delete date	Time at which the service principal was deleted.
Tags	User-defined string to use for categorizing and identifying the application.

Related topics

- Azure Active Directory policies for home realm discovery on page 168

Reports about Azure Active Directory objects

One Identity Manager makes various reports available containing information about the selected base object and its relations to other One Identity Manager database objects. The following reports are available for Azure Active Directory.

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

Table 41: Data quality target system report

Report	Published for	Description
Show overview	User account	This report shows an overview of the user account and the assigned permissions.
Show overview including origin	User account	This report shows an overview of the user account and origin of the assigned permissions.
Show overview including history	User account	This report shows an overview of the user accounts including its history. Select the end date for displaying the history (**Min. date**). Older changes and assignments that were removed before this date, are not shown in the report.
License overview	User account	The report contains a summary of assigned and effective subscriptions and service plans for a user account.
License overview	Subscription	The report shows an overview of a subscription license. It shows to which groups and user accounts the subscription is assigned and which service plans effectively apply to the groups and the user accounts.
Overview of all assignments	group Subscription Administrator role	This report finds all roles containing employees who have the selected system entitlement.
Show overview	group	This report shows an overview of the system entitlement and its assignments.
Show overview including origin	group	This report shows an overview of the system entitlement and origin of the assigned user accounts.
Show overview including history	group	This report shows an overview of the system entitlement and including its history.

Report	Published for	Description
		Select the end date for displaying the history (**Min. date**). Older changes and assignments that were removed before this date, are not shown in the report.
Show entitlement drifts	Tenant	This report shows all system entitlements that are the result of manual operations in the target system rather than provisioned by One Identity Manager.
Show user accounts overview (incl. history)	Tenant	This report returns all the user accounts with their permissions including a history. Select the end date for displaying the history (**Min. date**). Older changes and assignments that were removed before this date, are not shown in the report.
Show user accounts with an above average number of system entitle- ments	Tenant	This report contains all user accounts with an above average number of system entitlements.
Show employees with multiple user accounts	Tenant	This report shows all the employees that have multiple user accounts. The report contains a risk assessment.
Show system entitlements overview (incl. history)	Tenant	This report shows the system entitlements with the assigned user accounts including a history. Select the end date for displaying the history (**Min. date**). Older changes and assignments that were removed before this date, are not shown in the report.
Overview of all assignments	Tenant	This report finds all roles containing employees with at least one user account in the selected target system.
Show unused user accounts	Tenant	This report contains all user accounts, which have not been used in the last few months.
Show orphaned user accounts	Tenant	This report shows all user accounts to which no employee is assigned.

Table 42: Additional reports for the target system

Report	Description
Azure Active Directory user account and group	This report contains a summary of user account and group distribution in all tenants. You can find this report in the **My**

Report	Description
administration	**One Identity Manager** category.
Data quality summary for Azure Active Directory user accounts	This report contains different evaluations of user account data quality in all tenants. You can find this report in the **My One Identity Manager** category.

Handling of Azure Active Directory objects in the Web Portal

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

- Managing user accounts and employees

  An account definition can be requested by shop customers in the Web Portal if it is assigned to an IT Shop shelf. The request undergoes a defined approval process. The user account is not created until it has been agreed by an authorized person, such as a manager.

- Managing assignments of groups, administrator roles, subscriptions, and disabled service plans

  In the Web Portal, by assigning groups, administrator roles, subscriptions, and disabled service plans to an IT Shop shelf, you can request these products from shop customers. The request undergoes a defined approval process. The group, administrator role, subscription, or disabled service plan is not assigned until it has been approved by an authorized person.

  In the Web Portal, managers and administrators of organizations can assign groups, administrator roles, subscriptions, and disabled service plans to the departments, cost centers, or locations for which they are responsible. The groups, administrator roles, subscriptions, and disabled service plans are inherited by all employees who are members of these departments, cost centers, or locations.

  If the Business Roles Module is available, in the Web Portal, managers and administrators of business roles can assign groups, administrator roles, subscriptions, and disabled service plans to the business roles for which they are responsible. The groups, administrator roles, subscriptions, and disabled service plans are inherited by all employees who are members of these business roles.

  If the System Roles Module is available, in the Web Portal, supervisors of system roles can assign groups, administrator roles, subscriptions, and disabled service plans to the system roles. The groups, administrator roles, subscriptions, and disabled service plans are inherited by all employees that have these system roles assigned to them.

- Attestation

    If the Attestation Module is available, the correctness of the properties of target system objects and of entitlement assignments can be verified on request. To enable this, attestation policies are configured in the Manager. The attestors use the Web Portal to approve attestation cases.

- Governance administration

    If the Compliance Rules Module is available, you can define rules that identify the invalid entitlement assignments and evaluate their risks. The rules are checked regularly, and if changes are made to the objects in One Identity Manager. Compliance rules are defined in the Manager. Supervisors use the Web Portal to check and resolve rule violations and to grant exception approvals.

    If the Company Policies Module is available, company policies can be defined for the target system objects mapped in One Identity Manager and their risks evaluated. Company policies are defined in the Manager. Supervisors use the Web Portal to check policy violations and to grant exception approvals.

- Risk assessment

    You can use the risk index of groups, administrator roles, subscriptions and disabled service plans to evaluate the risk of entitlement assignments for the company. One Identity Manager provides default calculation functions for this. The calculation functions can be modified in the Web Portal.

- Reports and statistics

    The Web Portal provides a range of reports and statistics about the employees, user accounts, and their entitlements and risks.

For detailed information about the named topics, see Managing Azure Active Directory user accounts and employees on page 57, Managing memberships in Azure Active Directory groups on page 93, Managing Azure Active Directory administrator roles assignments on page 109, Managing Azure Active Directory subscription and Azure Active Directory service plan assignments on page 120 and in refer to the following guides:

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

ONE IDENTITY
by Quest

One Identity Manager 8.2 Administration Guide for Connecting to
Azure Active Directory

213

Handling of Azure Active Directory objects in the Web Portal

Recommendations for federations

NOTE: The following modules must be installed to support federations in One Identity Manager:

- Active Directory Module
- Azure Active Directory Module

In a federation, the local Active Directory user accounts are connected to Azure Active Directory user accounts. The connection is established by using the `ms-ds-consistencyGUID` property in the Active Directory user account and the `immutable` property in the Azure Active Directory user account. Synchronization of Active Directory and Azure Active Directory user accounts is carried out in the federation by Azure AD Connect. For more information about Azure AD Connect, see the *Azure Active Directory documentation* from Microsoft.

One Identity Manager maps the connection using the Active Directory user account's Azure AD Connect anchor ID (`ADSAccount.MSDsConsistencyGuid`) and the Azure Active Directory user account's immutable identifier (`AADUser.OnPremImmutableId`).

Some of the target system relevant properties of Azure Active Directory user accounts that are linked to local Active Directory user account cannot be changed in One Identity Manager. However, assignment of permissions to Azure Active Directory user accounts in One Identity Manager is possible.

Assignments to Azure Active Directory groups that are synchronized with the local Active Directory are not allowed in One Identity Manager. These groups cannot be requested through the web portal. You can only manage these groups in your locally. For more information, see the *Azure Active Directory documentation* from Microsoft.

The One Identity Manager supports the following scenarios for federations.

Scenario 1

1. Active Directory user accounts are created in One Identity Manager and provisioned the local Active Directory environment.

2. Azure AD Connect creates the Azure Active Directory user accounts in Azure Active Directory tenants.

3. Azure Active Directory synchronization loads the Azure Active Directory user accounts in to One Identity Manager.

This is the recommended procedure. Creating Azure Active Directory user accounts through Azure AD Connect and then loading them into One Identity Manager normally takes a while. Azure Active Directory user accounts are not immediately available in One Identity Manager.

Scenario 2

1. Active Directory user accounts and Azure Active Directory user accounts are created in One Identity Manager.

   In this case, the connection is established by using the `ADSAccount.MSDsConsistencyGuid` and `AADUser.OnPremImmutableId` columns. This can be carried using custom scripts or custom templates.

2. Active Directory and Azure Active Directory user accounts are provisioned independently in their own target systems.

3. Azure AD Connect detects the connection between the user accounts, establishes the connection in the federation and updates the required properties.

4. The next Azure Active Directory synchronization updates the Azure Active Directory user accounts in One Identity Manager.

With this scenario, the Azure Active Directory user accounts are immediately available in One Identity Manager and can be issued their permissions.

NOTE: Do not post-process Azure Active Directory user accounts using templates because certain target system relevant properties cannot be edited and the following errors may occur:

    [Exception]: ServiceException occured

    Code: Request_BadRequest

    Message: Unable to update the specified properties for on-premises mastered Directory Sync objects or objects currently undergoing migration.

    [ServiceException]: Code: Request_BadRequest - Message: Unable to update the specified properties for on-premises mastered Directory Sync objects or objects currently undergoing migration.

If you are working with account definitions, you can apply the **IT operating data overwrites** property with the value **Only initially** in the manage level. Then the data is only determined in the initial case.

Related topics

- Information about the local Active Directory user account on page 180

Basic configuration data for managing an Azure Active Directory environment

To manage an Azure Active Directory 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 51.

- Target system managers

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

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

  For more information, see Target system managers for Azure Active Directory on page 217.

- Servers

  Servers must be informed of your server functionality in order to handle Azure Active Directory-specific processes in One Identity Manager. For example, the 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*.

Target system managers for Azure Active Directory

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

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

For detailed information about implementing and editing application roles, see the *One Identity Manager Authorization and Authentication Guide*.

Implementing application roles for target system managers

1. The One Identity Manager administrator allocates employees to be target system administrators.

2. These target system administrators add employees to the default application role for target system managers.

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

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

Table 43: Default application roles for target system managers

User	Tasks
Target system managers	Target system managers must be assigned to the **Target systems | Azure Active Directory** 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.
	• Prepare groups to add to the IT Shop.
	• Can add employees who have another identity than the **Primary identity**.
	• Configure synchronization in the Synchronization Editor and define the mapping for comparing target systems and One Identity Manager.
	• Edit the synchronization's target system types and outstanding

objects.

- Authorize other employees within their area of responsibility as target system managers and create child application roles if required.

To initially specify employees to be target system administrators

1. Log in to the Manager as a One Identity Manager administrator (**Base role | Administrators** application role)

2. Select the **One Identity Manager Administration > Target systems > Administrators** category.

3. Select the **Assign employees** task.

4. Assign the employee you want and save the changes.

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

1. Log in to the Manager as a target system administrator (**Target systems | Administrators** application role).

2. Select the **One Identity Manager Administration > Target systems > Azure Active Directory** 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 clients

1. Log in to the Manager as a target system manager.

2. Select the **Azure Active Directory > Tenants** category.

3. Select the client in the result list.

4. Select the **Change main data** task.

5. On the **General** tab, select the application role in the **Target system manager** menu.

   - OR -

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

a. Enter the application role name and assign the **Target systems | Azure Active Directory** 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 client in One Identity Manager.

Related topics

- One Identity Manager users for managing an Azure Active Directory environment on page 11
- Azure Active Directory tenant on page 162

Job server for Azure Active Directory-specific process handling

Servers must be informed of their server functionality in order to handle Azure Active Directory-specific processes in One Identity Manager. For example, the synchronization server.

You have several options for defining a server's functionality:

- In the Designer, create an entry for the Job server in the **Base Data > Installation > Job server** category. For more information about this, see the *One Identity Manager Configuration Guide*.

- In the Manager, select an entry for the Job server in the **Azure Active Directory > Basic configuration data > Server** category and edit the Job server main data.

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

NOTE: One Identity Manager must be installed, configured, and started in order for a server to perform its function in the One Identity Manager Service network. Proceed as described in the *One Identity Manager Installation Guide*.

To edit a Job server and its functions

1. In the Manager, select the **Azure Active Directory > Basic configuration data > Server** category.

2. Select the Job server entry in the result list.

3. Select the **Change main data** task.

4. Edit the Job server's main data.

5. Select the **Assign server functions** task and specify server functionality.

6. Save the changes.

Detailed information about this topic

-
-

General main data of Job servers

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

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

Table 44: Job server properties

Property	Meaning
Server	Job server name.
Full server name	Full server name in accordance with DNS syntax. Syntax: `<Name of servers>.<Fully qualified domain name>`
Target system	Computer account target system.
Language	Language of the server.
Server is cluster	Specifies whether the server maps a cluster.
Server belongs to cluster	Cluster to which the server belongs. NOTE: The **Server is cluster** and **Server belongs to cluster** properties are mutually exclusive.
IP address (IPv6)	Internet protocol version 6 (IPv6) server address.
IP address (IPv4)	Internet protocol version 4 (IPv4) server address.
Copy process (source server)	Permitted copying methods that can be used when this server is the source of a copy action. At present, only copy methods that support the `Robocopy` and `rsync` programs are supported. If no method is given, the One Identity Manager Service determines the operating system of the server during runtime. Replication is then performed with the `Robocopy` program between servers with a Windows operating system or with the `rsync` program between servers with a Linux operating system. If the operating systems of the source and destination servers differ, it is important that the right copy method is applied for

Property	Meaning
	successful replication. A copy method is chosen that supports both servers.
Copy process (target server)	Permitted copying methods that can be used when this server is the destination of a copy action.
Coding	Character set coding that is used to write files to the server.
Parent Job server	Name of the parent Job server.
Executing server	Name of the executing server. The name of the server that exists physically and where the processes are handled.
	This input is evaluated when the One Identity Manager Service is automatically updated. If the server is handling several queues, the process steps are not supplied until all the queues that are being processed on the same server have completed their automatic update.
Queue	Name of the queue to handle the process steps. The process steps are requested by the Job queue using this queue identifier. The queue identifier is entered in the One Identity Manager Service configuration file.
Server operating system	Operating system of the server. This input is required to resolve the path name for replicating software profiles. The values **Win32**, **Windows**, **Linux**, and **Unix** are permitted. If no value is specified, **Win32** is used.
Service account data	One Identity Manager Service user account information. In order to replicate between non-trusted systems (non-trusted domains, Linux server), the One Identity Manager Service user information has to be declared for the servers in the database. This means that the service account, the service account domain, and the service account password have to be entered for the server.
One Identity Manager Service installed	Specifies whether a One Identity Manager Service is installed on this server. This option is enabled by the QBM_PJobQueueLoad procedure the moment the queue is called for the first time.
	The option is not automatically removed. If necessary, you can reset this option manually for servers whose queue is no longer enabled.
Stop One Identity Manager Service	Specifies whether the One Identity Manager Service has stopped. If this option is set for the Job server, the One Identity Manager Service does not process any more tasks.
	You can make the service start and stop with the appropriate administrative permissions in the Job Queue Info program. For more information, see the *One Identity Manager Process Monitoring and Troubleshooting Guide*.
No	Specifies whether to exclude the server from automatic software updating.

Property	Meaning
automatic software update	NOTE: Servers must be manually updated if this option is set.
Software update running	Specifies whether a software update is currently running.
Server function	Server functionality in One Identity Manager. One Identity Manager processes are handled with respect to the server function.

Related topics

Specifying server functions

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

The server function defines the functionality of a server in One Identity Manager. One Identity Manager processes are handled with respect to the server function.

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

Table 45: Permitted server functions

Server function	Remark
Azure Active Directory connector (via Microsoft Graph)	Server on which the Azure Active Directory connector is installed. This server synchronizes the Azure Active Directory target system.
CSV connector	Server on which the CSV connector for synchronization is installed.
Domain controller	The Active Directory domain controller. Servers that are not labeled as domain controllers are considered to be member servers.
Printer server	Server that acts as a print server.
Generic server	Server for generic synchronization with a custom target system.
Home server	Server for adding home directories for user accounts.
Update server	This server automatically updates the software on all the other servers. The server requires a direct connection to the database server that One Identity Manager database is installed on. It can run SQL tasks.

Server function	Remark
	The server with the One Identity Manager database installed on it is labeled with this functionality during initial installation of the schema.
SQL processing server	It can run SQL tasks. The server requires a direct connection to the database server that One Identity Manager database is installed on.
	Several SQL processing servers can be set up to spread the load of SQL processes. The system distributes the generated SQL processes throughout all the Job servers with this server function.
CSV script server	This server can process CSV files using the `ScriptComponent` process component.
Generic database connector	This server can connect to an ADO.Net database.
One Identity Manager database connector	Server on which the One Identity Manager connector is installed. This server synchronizes the One Identity Manager target system.
One Identity Manager Service installed	Server on which a One Identity Manager Service is installed.
Primary domain controller	Primary domain controller.
Profile server	Server for setting up profile directories for user accounts.
SAM synchronization Server	Server for running synchronization with an SMB-based target system.
SMTP host	Server from which One Identity Manager Service sends email notifications. Prerequisite for sending mails using One Identity Manager Service is SMTP host configuration.
Default report server	Server on which reports are generated.
Windows PowerShell connector	The server can run Windows PowerShell version 3.0 or later.

Related topics

- General main data of Job servers on page 220

Troubleshooting

Possible errors when synchronizing an Azure Active Directory tenant

Issue

An error occurs when loading the Azure Active Directory user accounts:

[Exception]: ServiceException occured

Code: BadRequest

Message: Tenant does not have a SPO license.

[ServiceException]: Code: BadRequest - Message: Tenant does not have a SPO license.

Cause

An Azure Active Directory tenant is synchronized that does not have a license for the **SharePoint Online** service.

Possible solutions

- Ensure the Azure Active Directory tenant has a license that includes the **SharePoint Online** service. (Recommended)

- If you want to synchronize an Azure Active Directory tenant that does not have a license for the **SharePoint Online** service, change the synchronization project with the Synchronization Editor.

  In **Users** mapping, disable the property mapping rules for the following schema properties. To do this, set the mapping direction to the **Do not map**.

  - BirthDay
  - PreferedName

- Responsibilities

- Schools

- Skills

- PastProjects

- Interests

- HireDate

- EmployeeID

- AboutMe

- MySite

- ImAddresses

- FaxNumber

- OtherMails

For more information about editing property mapping rules in the Synchronization Editor, see the *One Identity Manager Target System Synchronization Reference Guide*.

Configuration parameters for managing an Azure Active Directory environment

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

Table 46: Configuration parameters

Configuration parameter	Description
TargetSystem | AzureAD	Preprocessor relevant configuration parameter for controlling the database model components for the administration of the Azure Active Directory target system. 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*.
TargetSystem | AzureAD | Accounts	Allows configuration of user account data.
TargetSystem | AzureAD | Accounts | InitialRandomPassword	Specifies whether a random password is generated when a new user account is added. The password must contain at least those character sets that are defined in the password policy.
TargetSystem | AzureAD | Accounts | InitialRandomPassword | SendTo	Employee to receive an email with the random generated password (manager cost center/department/location/role, employee's manager or XUserInserted). If no recipient can be found, the password is sent to the address stored in the **TargetSystem | AzureAD | DefaultAddress** configuration parameter.

ONE IDENTITY
by Quest

One Identity Manager 8.2 Administration Guide for Connecting to
Azure Active Directory

Appendix: Configuration parameters for managing an Azure Active
Directory environment

226

Configuration parameter	Description
TargetSystem | AzureAD | Accounts | InitialRandomPassword | SendTo | MailTemplateAccountName	Mail template name that is sent to supply users with the login credentials for the user account. The **Employee - new user account created** mail template is used.
TargetSystem | AzureAD | Accounts | InitialRandomPassword | SendTo | MailTemplatePassword	Mail template name that is sent to supply users with the initial password. The **Employee - initial password for new user account** mail template is used.
TargetSystem | AzureAD | Accounts | MailTemplateDefaultValues	Mail template used to send notifications about whether default IT operating data mapping values are used for automatically creating a user account. The **Employee - new user account with default properties created** mail template is used.
TargetSystem | AzureAD | Accounts | PrivilegedAccount	Allows configuration of privileged Azure Active Directory user account settings.
TargetSystem | AzureAD | Accounts | PrivilegedAccount | AccountName_Postfix	Postfix for formatting the login name of privileged user accounts.
TargetSystem | AzureAD | Accounts | PrivilegedAccount | AccountName_Prefix	Prefix for formatting a login name of privileged user accounts.
TargetSystem | AzureAD | DefaultAddress	Default email address of the recipient for notifications about actions in the target system.
TargetSystem | AzureAD | DeltaTokenDirectory	Directory where the delta token files for the delta synchronization are stored.
TargetSystem | AzureAD | MaxFullsyncDuration	Maximum runtime of a synchronization in minutes. No recalculation of group memberships by the DBQueue Processor can take place during this time. If the maximum runtime is exceeded, group membership are recalculated.
TargetSystem | AzureAD | PersonAutoDefault	Mode for automatic employee assignment for user accounts added to the database outside synchronization.

Configuration parameter	Description
TargetSystem | AzureAD | PersonAutoDisabledAccounts	Specifies whether employees are automatically assigned to disabled user accounts. User accounts are not given an account definition.
TargetSystem | AzureAD | PersonAutoFullSync	Mode for automatic employee assignment for user accounts that are added to or updated in the database by synchronization.

TargetSystem | AzureAD | PersonExcludeList	Listing of all user account without automatic employee assignment. Names are listed in a pipe (|) delimited list that is handled as a regular search pattern.
	
	Example:
	
	`ADMINISTRATOR|GUEST|KRBTGT|TSINTERNETUSER|IUSR_.*|IWAM_.*`
	`|SUPPORT_.*|.* | $`

Default project template for Azure Active Directory

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 47: Azure Active Directory schema type mapping

Schema type in Azure Active Directory	Table in the One Identity Manager Schema
DirectoryRole	AADDirectoryRole
Group	AADGroup
LicenseAssignments	AADUserHasSubSku
GroupLicenseAssignments	AADGroupHasSubSku
Organization	AADOrganization
ServicePlanInfo	AADServicePlan
SubscribedSku	AADSubSku
User	AADUser
VerifiedDomain	AADVerifiedDomain
Application	AADApplication
AppRole	AADAppRole
AppRoleAssignment	AADAppRoleAssignment

Schema type in Azure Active Directory	Table in the One Identity Manager Schema
ServicePrincipal	AADServicePrincipal
ActivityBasedTimeoutPolicy	AADActivityBasedTimeoutPolicy
HomeRealmDiscoveryPolicy	AADHomeRealmDiscoveryPolicy
TokenIssuancePolicy	AADTokenIssuancePolicy
TokenLifetimePolicy	AADTokenLifetimePolicy

Editing Azure Active Directory system objects

The following table describes permitted editing methods of Azure Active Directory schema types and names restrictions required by system object processing.

Table 48: Methods available for editing schema types

Type	Read	Add	Delete	Refresh
Subscriptions (`SubscribedSku`)	Yes	No	No	No
Administrator roles (`DirectoryRole`)	Yes	No	No	Yes
User accounts (`User`)	Yes	Yes	Yes	Yes
Service plans (`ServicePlanInfo`)	Yes	No	No	No
Domains (`VerifiedDomain`)	Yes	No	No	No
Groups (`Group`)	Yes	Yes	Yes	Yes
License assignments to user accounts (`LicenseAssignments`)	Yes	Yes	Yes	Yes
License assignments to groups (`GroupLicenseAssignments`)	Yes	No	No	No
Tenants (`Organization`)	Yes	No	No	Yes
Applications (`Application`)	Yes	No	No	Yes
Service principle (`ServicePrincipal`)	Yes	No	No	Yes
App roles (`AppRole`)	Yes	No	No	No
Assignments to app roles (`AppRoleAssignment`)	Yes	Yes	Yes	Yes
Policies on activity-based timeout (`ActivityBasedTimeoutPolicy`)	Yes	No	No	No
Policies on home realm discovery (`HomeRealmDiscoveryPolicy`)	Yes	No	No	No

ONE IDENTITY
by Quest

One Identity Manager 8.2 Administration Guide for Connecting to
Azure Active Directory

231

Appendix: Editing Azure Active Directory system objects

Type	Read	Add	Delete	Refresh
Policies on token issuance (`TokenIssuancePolicy`)	Yes	No	No	No
Policies on token lifetime (`TokenLifetimePolicy`)	Yes	No	No	No

Azure Active Directory connector settings

The following settings are configured for the system connection with the Azure Active Directory connector.

Table 49: Azure Active Directory connector settings

Setting	Meaning
Client ID	Application ID that was generated during integration of One Identity Manager as an Azure Active Directory tenant application. Variable: `CP_ClientID`
Login domain	Base domain or a verified domain of your Azure Active Directory tenant. Variable: `CP_OrganizationDomain`
User name	User account name for logging in on Azure Active Directory if you have integrated One Identity Manager as a native client application in for Azure Active Directory tenant. Variable: `CP_Username`
Password	The user account's password. Variable: `CP_Password`
Key	Key that was generated during registration of One Identity Manager as an Azure Active Directory web application of the tenant. Variable: `CP_Secret`
Organization ID	The Azure Active Directory tenant ID. Variable: `OrganizationID`
GuestInviteSendMail	Specifies whether the guest user invitation will be sent.

One Identity Manager 8.2 Administration Guide for Connecting to
Azure Active Directory **233**
Appendix: Azure Active Directory connector settings

Setting	Meaning
	Default: **True**
	Variable: `GuestInviteSendMail`
GuestInviteLanguage	Language to use for sending the guest user invitation.
	Default: **en-us**
	Variable: `GuestInviteLanguage`
GuestInviteCustomMessage	Personal welcome greeting for the guest user.
	Variable: `GuestInviteCustomMessage`
GuestInviteRedirectUrl	URL to reroute guest users after they have accepted the invitation and registered.
	Default: **http://www.office.com**
	Variable: `GuestInviteRedirectUrl`

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