One Identity Manager 8.0.5

Administration Guide for Connecting to Azure Active Directory

Legend

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

One Identity Manager Administration Guide for Connecting to Azure Active Directory
Updated - May 2020
Version - 8.0.5

Contents

1

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, subscriptions, service plans, groups and administration roles are mapped in One Identity Manager. This makes it possible to use Identity and Access Governance processes such as attesting, 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 necessary user accounts. For this, you can use different mechanisms to connect 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 like tenants and verified domains is loaded into the One Identity Manager database by data synchronization. There are only limited possibilities for customizing this information in the One Identity Manager due to the complex dependencies and far reaching effects of changes.

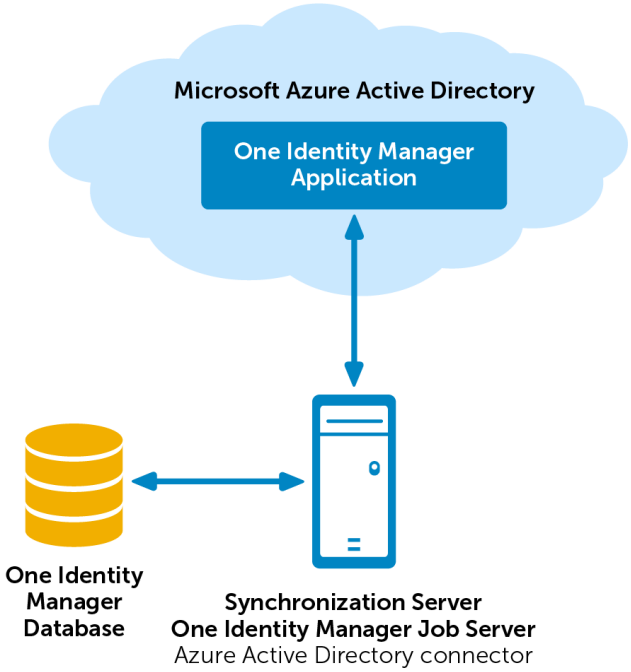
For more detailed information about the Azure Active Directory structure, see the Azure Active Directory documentation from Microsoft.

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

Figure 1: Architecture for synchronization



One Identity Manager Users for Managing an Azure Active Directory System

The following users are used in Azure Active Directory system administration.

Table 1: Users

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

User	Task
	• Authorize other employee 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 application role **Target systems | Azure Active Directory** or a sub application role. Users with this application role: • Assume administrative tasks for the target system. • Create, change or delete target system objects, like user accounts or groups. • Edit password policies for the target system. • Prepare groups for adding to the IT Shop. • Configure synchronization in the Synchronization Editor and defines the mapping for comparing target systems and One Identity Manager. • Edit the synchronization's target system types and outstanding objects. • Authorize other employees within their area of responsibility as target system managers and create child application roles if required.
One Identity Manager administrators	• Create customized permissions groups for application roles for role-based login to administration tools in the Designer, as required. • Create system users and permissions groups for non-role based login to administration tools, as required. • Enable or disable additional configuration parameters in the Designer, as required. • Create custom processes in the Designer, as required. • Create and configures schedules, as required. • Create and configure password policies, as required.
Administrators for the IT Shop	Administrators must be assigned to the application role **Request & Fulfillment | IT Shop | Administrators**. Users with this application role: • Assign to IT Shop structures.
Product owner for the	The product owners must be assigned to the application roles

User	Task
IT Shop	**Request & Fulfillment | IT Shop | Product owners** or an application role below that. 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 application role **Identity Management | Organizations | Administrators**. Users with this application role: • Assign to departments, cost centers and locations.
Business roles administrators	Administrators must be assigned to the application role **Identity Management | Business roles | Administrators**. Users with this application role: • Assign to business roles.

Setting Up Synchronization with an Azure Active Directory Tenant

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

1. Prepare a user account in the Azure Active Directory tenant with sufficient permissions for synchronization.
2. Integrate One Identity Manager in Azure Active Directory as an application for your tenants.
3. The One Identity Manager components for managing Azure Active Directory tenants are available if the configuration parameter "TargetSystem\AzureADS" is set.
    - Check whether the configuration parameter is set in the Designer. Otherwise, set the configuration parameter and compile the database.
    - Other configuration parameters are installed when the module is installed. Check the configuration parameters and modify them as necessary to suit your requirements.
4. Install and configure a synchronization server and declare the server as Job server in One Identity Manager.
5. Create a synchronization project with the Synchronization Editor.

Detailed information about this topic

- Users and Permissions for Synchronizing with Azure Active Directory on page 13
- Integrating One Identity Manager into Azure Active Directory as an Application on page 14
- Setting Up the Synchronization Server on page 15
- Creating a Synchronization Project for initial Synchronization of an Azure Active Directory Tenant on page 19
- Deactivating Synchronization on page 33
- Customizing Synchronization Configuration on page 26

- Appendix: Configuration Parameters for Managing Azure Active Directory on page 151
- Appendix: Default Project Template for Azure Active Directory on page 154

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	You must provide a user account with the following authorizations for full synchronization of Azure Active Directory tenant objects with the supplied One Identity Manager default configuration. • Member in the organization role "Global administrator".
One Identity Manager Service user account	The user account for the One Identity Manager Service requires access rights to carry out operations at file level (issuing user rights, adding directories and files to be edited). The user account must belong to the group "Domain Users". The user account must have the extended access right "Log on as a service". The user account requires access rights to the internal web service. NOTE: If the One Identity Manager Service runs under the network service (NT Authority\NetworkService), you can issue access rights for the internal web service with the following command line call: `netsh http add urlacl url=http://<IP address>:<port number>/ user="NT AUTHORITY\NETWORKSERVICE"` The user account needs full access to the One Identity Manager Service installation directory in order to automatically update the One Identity Manager. In the default installation the One Identity Manager is installed under: • `%ProgramFiles(x86)%\One Identity` (on 32-bit operating systems)

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

Integrating One Identity Manager into Azure Active Directory as an Application

To synchronize data between One Identity Manager and Azure Active Directory, you must integrate One Identity Manager as an application in the Azure Active Directory tenants. The Azure Active Directory connector authenticates itself in Azure Active Directory tenants using the One Identity Manager application.

NOTE: A client ID is created when you add One Identity Manager as an application in Azure Active Directory. You need this client ID for setting up synchronization.

For more detailed information about integrating applications into Azure Active Directory, see the Azure Active Directory documentation from Microsoft.

To configure the One Identity Manager as an application in Azure Active Directory

1. Log on to the Microsoft Azure Management Portal (https://manage.windowsazure.com) and create a new application for One Identity Manager for your directory.

   The following settings are recommended:

   - Select the **Add an application my organization is developing** link.
   - Set One Identity Manager to be a **Public client/native (mobile & desktop)** application.
2. For this application, configure the following permissions for **Microsoft Graph**.
   - Permissions of **Delegated** type:
     - User.Read (Sign in and read user profile)
     - User.ReadWrite (Read and write access to user profile)
     - User.ReadWrite.All (Read and write all users' full profile)
     - Group.ReadWrite.All (Read and write all groups)
     - Directory.ReadWrite.All (Read and write directory data)
     - Directory.AccessAsUser.All (Access directory as the signed in user)
     - openid (Sign users in)

It is not recommended to configure One Identity Manager as the web application because it can lead to limitations in functionality. For example, resetting passwords or administration role assignments would not be supported. If, however, you still want to register One Identity Manager as the web application, configure the following web application permissions for **Windows Azure Active Directory**.

- Permissions of **Application** type:
  - Device.ReadWrite.All (Read and write devices)
  - Directory.Read.All (Read directory data)
  - Member.Read.Hidden (Read all hidden memberships)
  - Directory.ReadWrite.All (Read and write directory data)
  - Domain.ReadWrite.All (Read and write domains)
  - Application.ReadWrite.OwnedBy (Manage apps that this app creates or owns)
  - Application.ReadWrite.All (Read and write all applications)

Related Topics

- Creating a Synchronization Project for initial Synchronization of an Azure Active Directory Tenant on page 19

Setting Up the 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

  Following versions are supported:
  - Windows Server 2008 (non-Itanium based 64-bit) Service Pack 2 or later
  - Windows Server 2008 R2 (non-Itanium based 64-bit) Service Pack 1 or later
  - Windows Server 2012
  - Windows Server 2012 R2
  - Windows Server 2016
- Microsoft .NET Framework Version 4.5.2 or later

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

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

- One Identity Manager Service, Azure Active Directory connector
    - Install One Identity Manager components with the installation wizard.
        1. Select the option **Select installation modules with existing database**.
        2. Select the machine role **Server | Job server | Azure Active Directory**.

All One Identity Manager Service actions are executed against the target system environment on the synchronization server. Data entries required for synchronization and administration with the One Identity Manager database, are processed by the synchronization server. The synchronization server must be declared as a Job server in One Identity Manager.

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

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

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

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

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

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

    - OR -

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

b. Enter the following data for the Job server.

Table 3: Job Servers Properties

Property	Description
Server	Name of the Job servers.
Queue	Name of queue to handle the process steps. Each One Identity Manager Service within the network must have a unique queue identifier. The process steps are requested by the job queue using exactly this queue name. The queue identifier is entered in the One Identity Manager Service configuration file.
Full server name	Full name of the server in DNS syntax. Example: `<name of server>.<fully qualified domain name>`

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

4. Specify which job server roles to include in One Identity Manager on the **Machine role** page. Installation packages to be installed on the Job server are found depending on the selected machine role.
   - Azure Active Directory
5. Specify the server's functions in One Identity Manager on the **Server functions** page. One Identity Manager processes are handled depending on the server function.

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

   Select the following server functions:
   - Azure Active Directory connector (via Microsoft Graph)
6. Check the One Identity Manager Service configuration on the **Service settings** page.

   NOTE: The initial service configuration is already predefined. If further changes need to be made to the configuration, you can do this later with the Designer. For more detailed information about configuring the service, see One Identity Manager Configuration Guide.
7. To configure remote installations, click **Next**.
8. Confirm the security prompt with **Yes**.
9. Select the directory with the install files on the **Select installation source** page.
10. Select the file with the private key on the page **Select private key file**.

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

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

Table 4: Installation Data

Data	Description
Computer	Server on which to install and start the service from. ***To select a server*** • Enter the server name. - OR - • Select a entry from the list.
Service account	One Identity Manager Service user account data. ***To enter a user account for the One Identity Manager Service*** • Set the option **Local system account**. This starts the One Identity Manager Service under the account "NT AUTHORITY\SYSTEM". - OR - • Enter user account, password and password confirmation.
Installation account	Data for the administrative user account to install the service. ***To enter an administrative user account for installation*** • Enable **Advanced**. • Enable the option **Current user**. This uses the user account of the current user. - OR - • Enter user account, password and password confirmation.

12. Click **Next** to start installing the service.

    Installation of the service occurs automatically and may take some time.

13. Click **Finish** on the last page of the Server Installer.

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

Creating a Synchronization Project for initial Synchronization of 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 detailed 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.

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

Table 5: Information Required for Setting up a Synchronization Project

Data	Explanation
Client ID	Client ID created when One Identity Manager is added as the tenant's application.
Login domain	Name of the domain for logging into Azure Active Directory. You can use the base domain or your tenant's verified domain.
User account and password for logging in	User account and password for authentication on Azure Active Directory using the One Identity Manager application. Make a user account available with sufficient permissions. For more information, see Users and Permissions for Synchronizing with Azure Active Directory on page 13.
Key for authenticating as a web application	If you have registered One Identity Manager as a web application in your tenant, you required the key that is created. NOTE: The key is only valid for a limited period and must be renewed when it expired.
Synchronization server for Azure Active Directory	All One Identity Manager Service actions are executed against the target system environment on the synchronization server. Data entries required for synchronization and administration with the One Identity Manager database, are processed by the synchronization server. The One Identity Manager Service with the 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.

<table>
<tr><th>Data</th><th>Explanation</th></tr>
<tr><td></td><td>Table 6: Additional Properties for the Job Server<table><tr><th>Property</th><th>Value</th></tr><tr><td>Server Function</td><td>Azure Active Directory connector (using Microsoft Graph)</td></tr><tr><td>Machine role</td><td>Server/Job server/Azure Active Directory</td></tr></table>
For more information, see Setting Up the Synchronization Server on page 15.</td></tr>
<tr><td>One Identity Manager Database Connection Data</td><td>SQL Server:
Database server
Database
Database user and password
Specifies whether Windows authentication is used.
This type of authentication is not recommended. If you decide to use it anyway, ensure that your environment supports Windows authentication.
Oracle:
Species whether access is direct or through the Oracle client
Which connection data is required, depends on how this option is set.
Database server
Oracle instance port
Service name
Oracle database user and password
Data source (TNS alias name from <code>TNSNames.ora</code>)</td></tr>
<tr><td>Remote connection server</td><td>To configure synchronization with a target system, One Identity Manager must load the data from the target system. One Identity Manager communicates directly with target system to do this. Sometimes direct access from the workstation on which the Synchronization Editor is installed is not possible, because of the firewall configuration, for example, or because the workstation does not fulfill the necessary hardware and software requirements. If direct access to the workstation is not possible, you can set up a remote connection.
The remote connection server and the workstation must be in the same Active Directory domain.</td></tr>
</table>

Data	Explanation
	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 (with respect to the installed software) as the synchronization server. Use the synchronization as remote connection server at the same time, by simply installing the `RemoteConnectPlugin` as well. For more detailed information about setting up a remote connection, see the One Identity Manager Target System Synchronization Reference Guide.

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

- In default mode
- Started from the launchpad

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

To set up initial synchronization project for an Azure Active Directory tenant.

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

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

2. Select the entry **Azure Active Directory target system type**. Click **Run**.

   This starts the Synchronization Editor's project wizard.

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

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

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

4. Enter the basic data for you tenants on the **Azure Active Directory tenant** page.
    - Enter the client ID that was created when the One Identity Manager was added to the tenant's application in **Client ID**.
    - Enter the base domain or one of your tenant's verified domains in **Login domain**.
5. Select the type of login on the **Authentication** page and enter the required login data.
    a. If you have integrated One Identity Manager as a native tenant application in your tenant, select the option **Authenticate as native tenant application** and enter the user account and password for logging into the target system,
    b. If you have integrated One Identity Manager as a web application in your tenant, select the option **Authenticate as web application** and enter the key that was created when One Identity Manager was added as the tenant's application.
6. Verify the One Identity Manager database connection data on the **One Identity Manager connection** page. The data is loaded from the connected database. Reenter the password.

    NOTE: Reenter all the connection data if you are not working with an encrypted One Identity Manager database and no synchronization project has been saved yet in the database. This page is not shown if a synchronization project already exists.

7. The wizard loads the target system schema. This may take a few minutes depending on the type of target system access and the size of the target system.
8. Specify how system access should work on the page **Restrict target system access**. You have the following options:

Table 7: Specifying Target System Access

Option	Meaning
Read-only access to target system.	Specifies whether a synchronization workflow should be set up to initially load the target system into the One Identity Manager database. 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 in synchronization direction "One Identity Manager".
Changes are also	Specifies whether a provisioning workflow should be set up in

Option	Meaning
made to the target system.	addition to the synchronization workflow to initially load the target system. The provisioning workflow displays the following characteristics: • Synchronization in the direction of the "target system" • Processing methods are only defined in the synchronization steps in synchronization direction "target system". • Synchronization steps are only created for such schema classes whose schema types have write access.

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

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

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

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

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

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

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

    The synchronization project is created, saved and enabled immediately.

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

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

    NOTE: The target system connection data is saved in a variable set, which you can change in the Synchronization Editor under **Configuration | Variables** if necessary.

To configure the content of the synchronization log

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

   NOTE: Certain content create a lot of log data.

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

To synchronize on a regular basis

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

To start initial synchronization manually

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

NOTE: Following synchronization, employees are automatically created for user accounts in the default installation. If there are no account definitions for the tenant at the time of synchronization, user accounts are linked to employees. However, account definitions are not assigned. The user accounts are, therefore, in a "Linked" state.

To select user accounts through account definitions

1. Create an account definition.
2. Assign an account definition to the tenant.
3. Assign the account definition and manage level to the user accounts in a "linked" state.
   a. Select the category **Azure Active Directory | User accounts | Linked but not configured | <client>**.
   b. Select the task **Assign account definition to linked accounts**.

Related Topics

- Integrating One Identity Manager into Azure Active Directory as an Application on page 14
- Setting Up the Synchronization Server on page 15
- Users and Permissions for Synchronizing with Azure Active Directory on page 13
- Show Synchronization Results on page 25
- Customizing Synchronization Configuration on page 26
- Appendix: Default Project Template for Azure Active Directory on page 154
- Setting Up Account Definitions on page 35
- Automatic Assignment of Employees to Azure Active Directory User Accounts on page 94

Show Synchronization Results

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

To display a synchronization log

1. Open the synchronization project in the Synchronization Editor.
2. Select the category **Logs**.
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 on it.

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

To display a provisioning log.

1. Open the synchronization project in the Synchronization Editor.
2. Select the category **Logs**.
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 on it.

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

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

Synchronization logs are stored for a fixed length of time.

To modify the retention period for synchronization logs

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

Customizing Synchronization Configuration

You have used the Synchronization Editor to set up a synchronization project for initial synchronization of an Azure Active Directory tenant. You can use this 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 in order to compare the Azure Active Directory database with the regularly and to synchronize changes.

- Create a workflow with the direction of synchronization "target system" to use One Identity Manager as the master system for synchronization.
- You can use variables to create generally applicable synchronization configurations which contain the necessary information about the synchronization objects when synchronization starts. Variables can be implemented in base objects, schema classes or processing methods, for example.
- Use variables to set up a synchronization project which can be used for several different domains. Store a connection parameter as a variable for logging in to the domain.
- To specify which Azure Active Directory objects and database object are included in synchronization, edit the scope of the target system connection and the One Identity Manager database connection. To prevent data inconsistencies, define the same scope in both systems. If no scope is defined, all objects will be synchronized.
- Update the schema in the synchronization project, if the One Identity Manager schema or target system schema has changed. Then you can add the changes to the mapping.

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

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

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

Detailed information about this topic

- Configuring Synchronization with Azure Active Directory Tenants on page 27
- Configuring Synchronization of Different Azure Active Directory Tenants on page 28
- Updating Schemas on page 28

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

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

1. Open the synchronization project in the Synchronization Editor.
2. Check whether existing mappings can be used for synchronizing the target system. Create new maps if required.
3. Create a new workflow with the workflow wizard.

   This adds a workflow for synchronizing in the direction of the target system.
4. Create a new start up configuration. Use the new workflow to do this.
5. Save the changes.
6. Run a consistency check.

Related Topics

- Configuring Synchronization of Different Azure Active Directory Tenants on page 28

Configuring Synchronization of Different Azure Active Directory Tenants

To customize a synchronization project for synchronizing another tenant

1. Prepare a user account with sufficient permissions for synchronizing in the other tenant.
2. Open the synchronization project in the Synchronization Editor.
3. Create a new base object for the other tenants. Use the wizards to attach a base object.
    - Select the Azure Active Directory connector in the wizard and enter the connection parameters. The connection parameters are saved in a special variable set.

      A start up configuration is created, which uses the new variable set.
4. Change other elements of the synchronization configuration as required.
5. Save the changes.
6. Run a consistency check.

Related Topics

- Configuring Synchronization with Azure Active Directory Tenants on page 27

Updating Schemas

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

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

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

- A schema was changed by:
    - Changes to a target system schema
    - Customizations to the One Identity Manager schema

    - A One Identity Manager update migration
- A schema in the synchronization project was shrunk by:
    - Activating the synchronization project
    - Synchronization project initial save
    - Compressing a schema

To update a system connection schema

1. Open the synchronization project in the Synchronization Editor.
2. Select the category **Configuration | Target system**.

   - OR -

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

   This reloads the schema data.

To edit a mapping

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

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

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

Post-Processing Outstanding Objects

Objects, which do not exist in the target system, can be marked as outstanding in One Identity Manager by synchronizing. This prevents objects being deleted because of an incorrect data situation or an incorrect synchronization configuration.

Objects marked as outstanding:

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

Start target system synchronization to do this.

To post-process outstanding objects

1. Select the category **Azure Active Directory | Target system synchronization: Azure Active Directory**.

   All tables assigned to the target system type Azure Active Directory as synchronization tables are displayed in the navigation view.

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

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

   TIP:

   To display object properties of an outstanding object

   a. Select the object on the target system synchronization form.

   b. Open the context menu and click **Show object**.

3. Select the objects you want to rework. Multi-select is possible.

4. Click one of the following icons in the form toolbar to execute the respective method.

   Table 8: Methods for handling outstanding objects

Icon	Method	Description
	Delete	The object is immediately deleted in the One Identity Manager. Deferred deletion is not taken into account. The "outstanding" label is removed from the object. Indirect memberships cannot be deleted.
	Publish	The object is added in the target system. The "outstanding" label is removed from the object. The method triggers the event "HandleOutstanding". 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 from the object.

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

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

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

To disable bulk processing

- Deactivate in the form toolbar.

You must customize synchronization to synchronize custom tables.

To add custom tables to the target system synchronization.

1. Select the category **Azure Active Directory | Basic configuration data | Target system types**.
2. Select the target system type Azure Active Directory in the result list.
3. Select **Assign synchronization tables** in the task view.
4. Assign custom tables whose outstanding objects you want to handle in **Add assignments**.
5. Save the changes.
6. Select **Configure tables for publishing**.
7. Select custom tables whose outstanding objects can be published in the target system and set the option **Publishable**.
8. Save the changes.

NOTE: The target system connector must have write access to the target system in order to publish outstanding objects that are being post-processed. That means, the option **Connection is read only** must no be set for the target system connection.

Configuring Memberships Provisioning

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

- Memberships are saved in the target system as an object property in list form (Example: List of users accounts in the property `Members` of an Azure Active Directory `group`).
- Memberships can be modified in either of the connected systems.
- A provisioning workflow and provisioning processes are set up.

If a membership in One Identity Manager changes, the complete list of members is transferred to the target system by default. Memberships, previously added to the target system are removed by this; previously deleted memberships are added again.

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

To allow separate provisioning of memberships

1. Start the Manager.
2. Select the category **Azure Active Directory | Basic configuration data | Target system types**.
3. Select **Configure tables for publishing**.
4. Select the assignment tables for which you want to allow separate provisioning. Multi-select is possible.
    - The option can only be set for assignment tables whose base table has a `XDateSubItem` or a `CCC_XDateSubItem`.
    - Assignment tables, which are grouped together in a virtual schema property in the mapping, must be labeled identically (for example `AADUserInGroup` and `AADGroupInGroup`).
5. Click **Enable merging**.
6. Save the changes.

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

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

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

Help for Analyzing Synchronization Issues

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

- Consistency check results
- Revision filter settings
- Scope applied

- Analysis of the synchronization buffer
- Object access times in the One Identity Manager database and in the target system

To generate a synchronization analysis report

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

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

Deactivating Synchronization

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

To prevent regular synchronization

- Select the start up configuration and deactivate the configured schedule.

  Now you can only start synchronization manually.

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

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

To deactivate the loaded synchronization project

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

Related Topics

- Creating a Synchronization Project for initial Synchronization of an Azure Active Directory Tenant on page 19

3

Base Data for Managing Azure Active Directory

To manage an Azure Active Directory environment in One Identity Manager, the following data is relevant.

- Configuration parameter

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

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

  For more information, see Appendix: Configuration Parameters for Managing Azure Active Directory on page 151.

- Account definitions

  One Identity Manager has account definitions for automatically allocating user accounts to employees during working hours. You can create account definitions for every target system. If an employee does not have a user account in the target system, a new user account is created. This is done by assigning account definitions to an employee using the integrated inheritance mechanism followed by process handling.

  For more information, see Setting Up Account Definitions on page 35.

- Password policies

  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 user or customize if required. You can also define your own password policies.

  For more information, see Password Policies on page 53.

- Initial Password for New User Accounts

  You have the different options for issuing an initial password for user accounts. The central password of the assigned employee can be aligned with the user account password, a predefined, fixed password can be used or a randomly generated initial password can be issued.

  For more information, see Initial Password for New Azure Active Directory User Accounts on page 62.

- Email notifications about login data

  When a new user account is created, the login data are send to a specified recipient. In this case, two messages are sent with the user name and the initial password. Mail templates are used to generate the messages.

  For more information, see Email Notifications about Login Data on page 63.

- Target System Types

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

  For more information, see Post-Processing Outstanding Objects on page 29.

- Target System Managers

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

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

  For more information, see Target System Managers on page 65.

- Servers

  Servers must know your server functionality in order to handle Azure Active Directory specific processes in One Identity Manager. For example, the synchronization server.

  For more information, see Editing a Server on page 67.

Setting Up Account Definitions

One Identity Manager has account definitions for automatically allocating user accounts to employees during working hours. You can create account definitions for every target system. If an employee does not have a user account in the target system, a new user account is created. This is done by assigning account definitions to an employee using the integrated inheritance mechanism followed by process handling.

The data for the user accounts in the respective target system comes from the basic employee data. The assignment of the IT operating data to the employee's user account is controlled through the primary assignment of the employee to a location, a department, a

cost center, or a business role (template processing). Processing is done through templates. There are predefined templates for determining the data required for user accounts included in the default installation. You can customize templates as required.

For more details about the basics, see the One Identity Manager Target System Base Module Administration Guide.

The following steps are required to implement an account definition:

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

Creating an Account Definition

To create a new account definition

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

   - OR -

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

Detailed information about this topic

- Master Data for an Account Definition on page 36

Master Data for an Account Definition

Enter the following data for an account definition:

Table 9: Master Data for an Account Definition

Property	Description
Account definition	Account definition name.

Property	Description
User account table	Table in the One Identity Manager schema which maps user accounts.
Target System	Target system to which the account definition applies.
Required account definition	Required account definitions. Define the dependencies between account definitions. When this account definition is requested or assigned, the required account definition is automatically requested or assigned with it. Leave empty for Azure Active Directory tenants.
Description	Spare text box for additional explanation.
Manage level (initial)	Manage level to use by default when you add new user accounts.
Risk index	Value for evaluating the risk of account definition assignments to employees. Enter a value between 0 and 1. This property is only visible when the configuration parameter QER\CalculateRiskIndex is set. For more detailed information, see the One Identity Manager Risk Assessment Administration Guide.
Service item	Service item through which you can request the account definition in the IT Shop. Assign an existing service item or add a new one.
IT Shop	Specifies whether the account definition can be requested through the IT Shop. The account definition can be ordered by an employee over the Web Portal and distributed using a defined approval process. The account definition can still be directly assigned to employees and roles outside the IT Shop.
Only for use in IT Shop	Specifies whether the account definition can only be requested through the IT Shop. The account definition can be ordered by an employee over the Web Portal and distributed using a defined approval process. This means, the account definition cannot be directly assigned to roles outside the IT Shop.
Automatic assignment to employees	Specifies whether the account definition is assigned automatically to all internal employees. The account definition is assigned to every employee not marked as external, on saving. New employees automatically obtain this account definition as soon as they are added. IMPORTANT: Only set this option if you can ensure that all current internal employees in the database and all pending newly added internal employees obtain a user account in this target system. Disable this option to remove automatic assignment of the account

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

Setting Up Manage Levels

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

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

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

- Unmanaged

  User accounts with a manage level of "Unmanaged" become linked to an employee but do not inherit any other properties. When a new user account is added with this manage level and an employee is assigned, some of the employee's properties are transferred initially. If the employee properties are changed at a later date, the changes are not passed onto the user account.

- Full managed

  User accounts with a manage level of "Full managed" inherit specific properties from the assigned employee.

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

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

Specify the effect of temporarily or permanently disabling, deleting or the security risk of an employee on its user accounts and group memberships for each manage level. For more detailed information about manage levels, see the One Identity Manager Target System Base Module Administration Guide.

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

To assign manage levels to an account definition

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

   - OR -

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

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

To edit a manage level

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

   - OR -

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

Related Topics

- Master Data for a Manage Level on page 40

Master Data for a Manage Level

Enter the following data for a manage level.

Table 10: Master Data for a Manage Level

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

Property	Description
Lock user accounts if deletion is deferred	Specifies whether user accounts of employees marked for deletion are locked.
Retain groups on security risk	Specifies whether user accounts of employees posing a security risk retain their group memberships.
Lock user accounts if security is at risk	Specifies whether user accounts of employees posing a security risk are locked.
Retain groups if user account disabled	Specifies whether locked user accounts retain their group memberships.

Creating a Formatting Rule for IT Operating Data

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

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

- Groups can be inherited
- Identity
- Privileged user account
- Change password the next time you log in

To create a mapping rule for IT operating data

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

Table 11: Mapping rule for IT operating data

Property	Description
Column	User account property for which the value is set.
Source	Specifies which roles to use in order to find the user account properties. You have the following options:

Property	Description
	• Primary department • Primary location • Primary cost center • Primary business roles NOTE: Only use the primary business role if the Business Roles Module is installed. • Empty If you select a role, you must specify a default value and set the option **Always use default value**.
Default value	Default value of the property for an employee's user account if the value is not determined dynamically from the IT operating data.
Always use default value	Specifies whether user account properties are always filled with the default value. IT operating data is not determined dynamically from a role.
Notify when applying the standard	Specifies whether email notification to a defined mailbox is sent when the default value is used. Use the mail template "Employee - new user account with default properties created". To change the mail template, modify the configuration parameter "TargetSystem\AzureAD\Accounts\MailTemplateDefaultValues".

4. Save the changes.

Related Topics

- Determining IT Operating Data on page 42

Determining IT Operating Data

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

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

Example:

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

Create an account definition A for the default user account of the tenant A and an account definition B for the administrative user account of tenant A. Specify the property "Department" in the IT operating data formatting rule for the account definitions A and B in order to determine the valid IT operating data.

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

To specify IT operating data

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

Table 12: IT Operating Data

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

3. Save the changes.

Related Topics

- Creating a Formatting Rule for IT Operating Data on page 41

Modifying IT Operating Data

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

Prerequisites

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

  - OR -

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

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

To execute the template

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

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

Old value	Current value of the object property.
New value	Value applied to the object property after modifying the IT operating data.
Selection	Specifies whether the modification is applied to the user account.

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

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

Assigning Account Definitions to Employees

Account definitions are assigned to company employees. Indirect assignment is the default method for assigning account definitions to employees. Account definitions are assigned to departments, cost centers, locations or roles. The employees are categorized into these departments, cost centers, locations or roles depending on their function in the company and thus obtain their account definitions. To react quickly to special requests, you can assign individual account definitions directly to employees. You can automatically assign special account definitions to all company employees. It is possible to assign account definitions to the IT Shop as requestable products. A department manager can then request user accounts from the Web Portal for his staff. It is also possible to add account definitions to system roles. These system roles can be assigned to employees through hierarchical roles or directly or added as products in the IT Shop.

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

NOTE: If a user account already exists and is disabled, then it is re-enabled. You have to alter the user account manage level afterwards in this case.

Prerequisites for indirect assignment of account definitions to employees

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

For detailed information about preparing role classes to be assigned, see the One Identity Manager Identity Management Base Module Administration Guide.

Detailed information about this topic

Assigning Account Definitions to Departments, Cost Centers and Locations

To add account definitions to hierarchical roles

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

   - OR -

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

Related Topics

- Assigning Account Definitions to Business Roles on page 46
- Assigning Account Definitions to all Employees on page 47
- Assigning Account Definitions Directly to Employees on page 48
- Assigning Account Definitions to System Roles on page 48
- Adding Account Definitions in the IT Shop on page 49

Assigning Account Definitions to Business Roles

Installed Modules: Business Roles Module

To add account definitions to hierarchical roles

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

   - OR -

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

Related Topics

- Assigning Account Definitions to Departments, Cost Centers and Locations on page 46
- Assigning Account Definitions to all Employees on page 47
- Assigning Account Definitions Directly to Employees on page 48
- Assigning Account Definitions to System Roles on page 48
- Adding Account Definitions in the IT Shop on page 49

Assigning Account Definitions to all Employees

To assign an account definition to all employees

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

   IMPORTANT: Only set this option if you can ensure that all current internal employees in the database and all pending newly added internal employees obtain a user account in this target system.
5. Save the changes.

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

NOTE: Disable the option **Automatic assignment to employees** to remove automatic assignment of the account definition to all employees. The account definition cannot be reassigned to employees from this point on. Existing assignments remain intact.

Related Topics

- Assigning Account Definitions to Departments, Cost Centers and Locations on page 46
- Assigning Account Definitions to Business Roles on page 46
- Assigning Account Definitions Directly to Employees on page 48
- Assigning Account Definitions to System Roles on page 48
- Adding Account Definitions in the IT Shop on page 49

Assigning Account Definitions Directly to Employees

To assign an account definition directly to employees

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

   - OR -

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

Related Topics

- Assigning Account Definitions to Departments, Cost Centers and Locations on page 46
- Assigning Account Definitions to Business Roles on page 46
- Assigning Account Definitions to all Employees on page 47
- Assigning Account Definitions to System Roles on page 48
- Adding Account Definitions in the IT Shop on page 49

Assigning Account Definitions to System Roles

Installed Modules: System Roles Module

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

To add account definitions to a system role

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

   - OR -

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

Related Topics

- Assigning Account Definitions to Departments, Cost Centers and Locations on page 46
- Assigning Account Definitions to Business Roles on page 46
- Assigning Account Definitions to all Employees on page 47
- Assigning Account Definitions Directly to Employees on page 48
- Adding Account Definitions in the IT Shop on page 49

Adding Account Definitions in the IT Shop

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

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

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

To add an account definition to the IT Shop

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

   - OR -

   Select the category **Entitlements | Account definitions** (role-based login).
2. Select an account definition in the result list.
3. Select **Add to IT Shop** in the task view.
4. Assign the account definition to the IT Shop shelf in **Add assignments**
5. Save the changes.

To remove an account definition from individual IT Shop shelves

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

   - OR -

   Select the category **Entitlements | Account definitions** (role-based login).
2. Select an account definition in the result list.
3. Select **Add to IT Shop** in the task view.

4. Remove the account definition from the IT Shop shelves in **Remove assignments**.
5. Save the changes.

To remove an account definition from all IT Shop shelves

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

   - OR -

   Select the category **Entitlements | Account definitions** (role-based login).
2. Select an account definition in the result list.
3. Select **Remove from all shelves (IT Shop)** in the task view.
4. Confirm the security prompt with **Yes**.
5. Click **OK**.

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

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

Related Topics

- Master Data for an Account Definition on page 36
- Assigning Account Definitions to Departments, Cost Centers and Locations on page 46
- Assigning Account Definitions to Business Roles on page 46
- Assigning Account Definitions to all Employees on page 47
- Assigning Account Definitions Directly to Employees on page 48
- Assigning Account Definitions to System Roles on page 48

Assigning Account Definitions to a Target System

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

- The account definition is assigned to the target system.
- The account definition has the default manage level.

User accounts are only linked to the employee (state "Linked") if no account definition is given. This is the case on initial synchronization, for example.

To assign the account definition to a target system

1. Select the tenant in the category **Azure Active Directory | Tenants**.
2. Select **Change master data** in the task view.
3. Select the account definition for user accounts from **Account definition (initial)**.
4. Save the changes.

Detailed information about this topic

- Automatic Assignment of Employees to Azure Active Directory User Accounts on page 94

Deleting an Account Definition

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

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

To delete an account definition

1. Remove automatic assignments of the account definition from all employees.
    a. Select the category **Azure Active Directory | Basic configuration data | Account definitions | Account definitions**.
    b. Select an account definition in the result list.
    c. Select **Change master data** in the task view.
    d. Disable the option **Automatic assignment** to employees on the **General** tab.
    e. Save the changes.
2. Remove direct assignments of the account definition to employees.
    a. Select the category **Azure Active Directory | Basic configuration data | Account definitions | Account definitions**.
    b. Select an account definition in the result list.
    c. Select **Assign to employees** in the task view.
    d. Remove employees from **Remove assignments**.
    e. Save the changes.
3. Remove the account definition's assignments to departments, cost centers and locations.
    a. Select the category **Azure Active Directory | Basic configuration data | Account definitions | Account definitions**.
    b. Select an account definition in the result list.

c. Select **Assign organizations**.

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

e. Save the changes.

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

a. Select the category **Azure Active Directory | Basic configuration data | Account definitions | Account definitions**.

b. Select an account definition in the result list.

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

Remove business roles from **Remove assignments**.

d. Save the changes.

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

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

a. Select the category **Azure Active Directory | Basic configuration data | Account definitions | Account definitions**.

b. Select an account definition in the result list.

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

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

e. Save the changes.

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

a. Select the tenant in the category **Azure Active Directory | Tenants**.

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

c. Remove the assigned account definitions on the **General tab**.

d. Save the changes.

8. Delete the account definition.

a. Select the category **Azure Active Directory | Basic configuration data | Account definitions | Account definitions**.

b. Select an account definition in the result list.

c. Click , to delete the account definition.

Password Policies

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 user or customize if required. You can also define your own password policies.

Detailed information about this topic

Predefined Password Policies

You can customize predefined password policies to meet your own requirements, if necessary.

Password for logging into One Identity Manager

The password policy "One Identity Manager password policy" is used for logging into One Identity Manager. This password policy defined the settings for the system user passwords (`DialogUser.Password` and `Person.DialogUserPassword`) as well as the access code for a one off log in on the Web Portal (`Person.Passcode`).

The password policy "One Identity Manager password policy" is also labeled as the default and is used when no other password policy is found.

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 password policy "Employee central password policy" defines the settings for the central password (`Person.CentralPassword`).

IMPORTANT: Ensure that the password policy "Employee central password policy" does not violate the target system specific password requirements.

Password policies for target systems

A predefined password policy that you can apply to the user account password columns, is provided for every target system.

NOTE: When you update One Identity Manager version 7.x to One Identity Manager version 8.0.5, the configuration parameter settings for forming passwords are passed on to the target system specific password policies.

IMPORTANT: If you are not working with target system specific password policies, the default policy applies. In this case, ensure that the password policy "One Identity Manager password policy" does not violate the target system requirements.

The password policy "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.

Editing Password Policies

To edit a password policy

1. Select the category **Manager | Basic configuration data | Password policies** in the Azure Active Directory.
2. Select the password policy in the result list and select **Change master data** in the task view.

   - OR -

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

Detailed information about this topic

- General Master Data for a Password Policy on page 54
- Policy Settings on page 55
- Character Sets for Passwords on page 56
- Custom Scripts for Password Requirements on page 57

General Master Data for a Password Policy

Enter the following master data for a password policy.

Table 13: Master Data for a Password Policy

Property	Meaning
Display name	Password policy name. Translate the given text using the button.
Description	Spare text box for additional explanation. Translate the given text using the button.
Error Message	Custom error message outputted 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. NOTE: The password policy "One Identity Manager password policy" is marked as the default policy. This password policy is applied if no other password policies can be found.

Policy Settings

Define the following settings for a password policy on the **Password** tab.

Table 14: Policy Settings

Property	Meaning
Initial password	Initial password for new user accounts. If no password is given when the user account is added or a random password is generated, the initial password is used.
Password confirmation	Reconfirm password.
Min. Length	Minimum length of the password. Specify the number of characters a password must have.
Max. length	Maximum length of the password. Specify the number of characters a password can have.
Max. errors	Maximum number of errors. Set the number of invalid passwords. If the user has reached this number the user account is blocked.
Validity period	Maximum age of the password. Enter the length of time a password can be used before it expires.
Password history	Enter the number of passwords to be saved. If the value '5' is entered, for example, the last 5 passwords of the user are

Property	Meaning
	saved.
Min. password strength	Specifies how secure the password must be. The higher the password strength, the more secure it is. The password strength is not tested if the value is '0'. The values '1', '2', '3' and '4' gauge the required complexity of the password. The value '1' demands the least complex password. The value '4' demands the highest complexity.
Name properties denied	Specifies whether name properties are permitted in the password.

Character Sets for Passwords

Use the **Character classes** tab to specify which characters are permitted for a password.

Table 15: Character Classes for Passwords

Property	Meaning
Min. letters	Specifies the minimum number of alphabetical characters the password must contain.
Min. number lower case	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 characters.
Denied special characters	List of characters, which are not permitted.
Max. identical characters in total	Maximum number of identical characters that can be present in the password in total.
Max. identical characters in succession	Maximum number of identical character that can be repeated after each other.

Custom Scripts for Password Requirements

You can implement custom scripts for testing and generating password 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

- Script for Checking a Password on page 57
- Script for Generating a Password on page 58

Script for Checking a Password

You can implement a check script if additional policies need to be used for checking a password, which cannot be mapped with the available settings.

Syntax for 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 test

TIP: To use a base object, take the property `Entity` of the `PasswordPolicy` class.

Example for a script for testing a password

A password cannot have '?' or '!' at the beginning. 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. Create your script in the category **Script Library** in the Designer.
2. Edit the password policy.
    a. Select the category **Manager | Basic configuration data | Password policies** in the Azure Active Directory.
    b. Select the password policy in the result list.
    c. Select **Change master data** in the task view.
    d. Enter the name of the script to test the password in **Check script** on the **Scripts** tab.
    e. Save the changes.

Related Topics

- Script for Generating a Password on page 58

Script for Generating a Password

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 property `Entity` of the `PasswordPolicy` class.

Example for a script to generate a password

The script replaces the invalid characters '?' and '!' in random passwords.

```
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. Create your script in the category **Script Library** in the Designer.
2. Edit the password policy.
    a. Select the category **Manager | Basic configuration data | Password policies** in the Azure Active Directory.
    b. Select the password policy in the result list.
    c. Select **Change master data** in the task view.
    d. Enter the name of the script to generate a password in **Generation script** on the **Scripts** tab.
    e. Save the changes.

Related Topics

- Script for Checking a Password on page 57

Restricted Passwords

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. Select the category **Base Data | Security Settings | Restricted passwords** in the Designer.
2. Create a new entry with the menu item **Object | New** an enter the term to excluded to the list.
3. Save the changes.

Testing a Password

When you test a password, all the password policy settings, custom scripts and the restricted passwords are taken into account.

To test whether a password conforms to the password policy

1. Select the category **Manager | Basic configuration data | Password policies** in the Azure Active Directory.
2. Select the password policy in the result list.
3. Select **Change master data** in the task view.
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.

Testing Generating a Password

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. Select the category **Manager | Basic configuration data | Password policies** in the Azure Active Directory.
2. Select the password policy in the result list.
3. Select **Change master data** in the task view.
4. Select the **Test** tab.
5. Click **Generate**.

   This generates and displays a password.

Assigning a Password Policy

The password policy "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.

IMPORTANT: If you are not working with target system specific password policies, the default policy applies. In this case, ensure that the password policy "One Identity Manager password policy" does not violate the target system requirements.

To reassign a password policy

1. Select the category **Manager | Basic configuration data | Password policies** in the Azure Active Directory.
2. Select the password policy in the result list.
3. Select **Assign objects** in the task view.
4. Click **Add** in the **Assignments** section and enter the following data.

Table 16: Assigning a Password Policy

Property	Description
Apply to	Application scope of the password policy. ***To specify an application scope*** a. Click → next to the text box. b. Select the table which contains the password column under **Table**. c. Select the specific target system under **Apply to**. d. Click **OK**.
Password column	The password column's identifier.
Password policy	The identifier of the password policy to be used.

5. Save the changes.

To change a password policy's assignment

1. Select the category **Manager | Basic configuration data | Password policies** in the Azure Active Directory.
2. Select the password policy in the result list.
3. Select **Assign objects** in the task view.
4. Select the assignment you want to change in **Assignments**.
5. Select the new password policy to apply from the **Password Policies** menu.
6. Save the changes.

Initial Password for New Azure Active Directory User Accounts

Table 17: Configuration Parameters for Formatting Initial Passwords for User Accounts

Configuration parameter	Meaning
QER\Person\UseCentralPassword	This configuration parameter specifies whether the employee's central password is used in the user accounts. The employee's central password is automatically mapped to the employee's user account in all permitted target systems. This excludes privileged user accounts, which are not updated.
QER\Person\UseCentralPassword\PermanentStore	This configuration parameter controls the storage period for central passwords. If the parameter is set, the employee's central password is permanently stored. If the parameter is not set, the central password is only used for publishing to existing target system specific user accounts and is subsequently deleted from the One Identity Manager database.
TargetSystem\AzureAD\Accounts\ InitialRandomPassword	This configuration parameter specifies whether a random generated password is issued when a new user account is added. The password must contain at least those character sets that are defined in the password policy.

You have the following possible options for issuing an initial password for a new Azure Active Directory user account.

- User the employee's central password. The employee's central password is mapped to the user account password.
  - Set the configuration parameter "QER\Person\UseCentralPassword" in the Designer.

    If the configuration parameter "QER\Person\UseCentralPassword" is set, the employee's central password is automatically mapped to an employee's user

account in each of the target systems. This excludes privileged user accounts, which are not updated.

- Use the configuration parameter "QER\Person\UseCentralPassword\PermanentStore" in the Designer to specify whether an employee's central password is permanently saved in the One Identity Manager database or only until the password has been published in the target system.

The password policy "Employee central password policy" is used to format the central password.

IMPORTANT: Ensure that the password policy "Employee central password policy" does not violate the target system specific password requirements.

- Create user accounts manually and enter a password in their master data.
- Specify an initial password to be used when user accounts are created automatically.
  - Apply the target system specific password policies and enter an initial password in the password policies.
- Assign a randomly generated initial password to enter when you create user accounts.
  - Set the configuration parameter "TargetSystem\AzureAD\Accounts\InitialRandomPassword" in the Designer.
  - 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 on page 53
- Email Notifications about Login Data on page 63

Email Notifications about Login Data

Table 18: Configuration Parameters for Notifications about Login Data

Configuration parameter	Meaning
TargetSystem\ AzureAD\Accounts\ InitialRandomPassword\SendTo	This configuration parameter specifies to which employee the email with the random generated password should be sent (manager cost center/department/location/business role, employee's manager or `XUserInserted`). If no recipient can be found, the password is sent to the address stored in the configuration parameter

Configuration parameter	Meaning
	"TargetSystem\AzureAD\DefaultAddress".
TargetSystem\ AzureAD\Accounts\ InitialRandomPassword\SendTo\ MailTemplateAccountName	This configuration parameter contains the name of the mail template sent to inform users about their initial login data (name of the user account). Use the mail template "Employee - new account created".
TargetSystem\ AzureAD\Accounts\ InitialRandomPassword\SendTo\ MailTemplatePassword	This configuration parameter contains the name of the mail template sent to inform users about their initial login data (initial password). Use the mail template "Employee - initial password for new user account".
TargetSystem\ AzureAD\DefaultAddress	The configuration parameter contains the recipient's default email address for sending notifications about actions in the target system.

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 password. Mail templates are used to generate the messages. The mail text in a mail template is defined in several languages, which 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.

To use email notifications about login data

1. Ensure that the email notification system is configured in One Identity Manager. For more detailed information, see the One Identity Manager Configuration Guide.
2. Enable the configuration parameter "Common\MailNotification\DefaultSender" in the Designer and enter the email address for sending the notification.
3. Ensure that all employees have a default email address. Notifications are sent to this address. For more detailed information, see the One Identity Manager Identity Management Base Module Administration Guide.
4. Ensure that a language culture can be determined for all employees. Only then can they receive email notifications in their own language. For more detailed 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. Set the configuration parameter "TargetSystem\AzureAD\Accounts\InitialRandomPassword" in the Designer.
2. Set the configuration parameter "TargetSystem\AzureAD\Accounts\InitialRandomPassword\SendTo" in the Designer and enter the message recipient as the value.

3. Set the configuration parameter "TargetSystem\AzureAD\Accounts\InitialRandomPassword\SendTo\MailTemplateAccountName" in the Designer.

   By default, the message sent uses the mail template "Employee - new account created". The message contains the name of the user account.

4. Set the configuration parameter "TargetSystem\AzureAD\Accounts\InitialRandomPassword\SendTo\MailTemplatePassword" in the Designer.

   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: Change the value of the configuration parameter in order to use custom mail templates for these mails.

Target System Managers

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

Implementing Application Roles for Target System Managers

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

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

Table 19: Default Application Roles for Target System Managers

User	Task
Target System Managers	Target system managers must be assigned to the application role **Target systems | Azure Active Directory** or a sub application role. Users with this application role: • Assume administrative tasks for the target system. • Create, change or delete target system objects, like user accounts

User	Task
	or groups. • Edit password policies for the target system. • Prepare groups for adding to the IT Shop. • Configure synchronization in the Synchronization Editor and defines 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 One Identity Manager administrator (application role **Base role | Administrators**)
2. Select the category **One Identity Manager Administration | Target systems | Administrators**.
3. Select **Assign employees** in the task view.
4. Assign the employee you want and save the changes.

To add the first employees to the default application as target system managers.

1. Log yourself into the Manager as target system administrator (application role **Target systems | Administrator**).
2. Select the category **One Identity Manager Administration | Target systems | Azure Active Directory**.
3. Select **Assign employees** in the task view.
4. Assign the employees you want and save the changes.

To authorize other employees as target system managers when you are a target system manager

1. Login to the Manager as target system manager.
2. Select the application role in the category **Azure Active Directory | Basic configuration data | Target system managers**.
3. Select **Assign employees** in the task view.
4. Assign the employees you want and save the changes.

To define target system managers for individual tenants.

1. Login to the Manager as target system manager.
2. Select the category **Azure Active Directory | Tenants**.
3. Select the tenant from the result list.
4. Select **Change master data** in the task view.
5. Select the application role on the **General** tab in the **Target system manager** menu.

   - OR -

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

   - Enter the application role name and assign the parent application role **Target system | Azure Active Directory**.
   - Click **OK** to add the new application role.
6. Save the changes.
7. Assign the application role to employees, who are authorized to edit the tenant in One Identity Manager.

Related Topics

- One Identity Manager Users for Managing an Azure Active Directory System on page 9
- Azure Active Directory Tenant on page 73

Editing a Server

Servers must know your 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:

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

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

NOTE: One Identity Manager must be installed, configured and started in order for a server to execute its function in the One Identity Manager Service network. Proceed as follows in the One Identity Manager Installation Guide.

To edit a Job server and its functions

1. Select the category **Azure Active Directory | Basic configuration data | Server** in the Manager.
2. Select the Job server entry in the result list.
3. Select **Change master data** in the task view.
4. Edit the Job server's master data.
5. Select **Assign server functions** in the task view and specify server functionality.
6. Save the changes.

Detailed information about this topic

- Master Data for a Job Server on page 68
- Specifying Server Functions on page 70

Master Data for a Job Server

NOTE: All editing options are available to you in the Designer, in the category **Base Data | Installation | Job server**.

Table 20: Job Server Properties

Property	Meaning
Server	Job server name.
Full server name	Full server name in accordance with DNS syntax. Example: `<Name of servers>.<Fully qualified domain name>`
Target System	Computer account target system.
Language culture	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 properties **Server is cluster** and **Server belongs to cluster** are mutually exclusive.
IP address	Internet protocol version 6 (IPv6) server address.

Property	Meaning
(IPv6)	
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. Only the methods "Robocopy" and "Rsync" are currently supported. If no method is given, the One Identity Manager Service determines the operating system of the server during runtime. Replication then takes place between servers with a Windows operating system using "Robocopy" and between servers with the Linux operating system using "rsync". If the operating systems of the source and destination servers differ, it is important that the right copy method is applied for 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 One Identity Manager Service is automatically updated. If the server is handling several queues the process steps are not supplied until all the queues that are being processed on the same server have completed their automatic update.
Queue	Name of the queue to handle the process steps. Each One Identity Manager Service within the network must have a unique queue identifier. The process steps are requested by the job queue using exactly this queue name. The queue identifier is entered in the One Identity Manager Service configuration file.
Server operating system	Operating system of the server. This input is required to resolve the path name for replicating software profiles. Permitted values are "Win32", "Windows", "Linux" and "Unix". If the input is empty, "Win32" is assumed.
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

Property	Meaning
	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 procedure QBM_PJobQueueLoad 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 program "Job Queue Info".
No automatic software update	Specifies whether to exclude the server from automatic software updating. NOTE: Servers must be manually updated if this option is set.
Software update running	Specifies whether a software update is currently being executed.
Server Function	Server functionality in One Identity Manager. One Identity Manager processes are handled depending on the server function.

Related Topics

- Specifying Server Functions on page 70

Specifying Server Functions

NOTE: All editing options are available to you in the Designer, in the category **Base Data | Installation | Job server**.

The server function defines the functionality of a server in One Identity Manager. One Identity Manager processes are handled depending on the server function.

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

Table 21: 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 executes synchronization with the target system Azure Active Directory.
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 controller are considered to be member servers.
Printer server	Server which 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 executes automatic software updating of all other servers. The server requires a direct connection to the database server that the One Identity Manager database is installed on. The server can execute SQL tasks. The server with the installed One Identity Manager database, is labeled with this functionality during initial installation of the schema.
SQL processing server	This server can process SQL tasks. Several SQL processing servers can be set up to spread the load of SQL processes. The system distributes the generated SQL processes throughout all the Job servers with this server function.
Native database connector	The 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 executes synchronization with the target system One Identity Manager.
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	Server for running synchronization with an SMB-based target system.

Server Function	Remark
synchronization Server	
SMTP host	Server from which the One Identity Manager Service sends email notifications. Prerequisite for sending mails using the 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

- Master Data for a Job Server on page 68

4

Azure Active Directory Core Directories

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

You must provide details about for 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. You can edit the master data of each tenant in the One Identity Manager. You cannot create new tenants in the 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 on page 73
- Azure Active Directory Domains on page 77

Azure Active Directory Tenant

You must provide details about for 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. You can edit the master data of each tenant in the One Identity Manager. You cannot create new tenants in the One Identity Manager.

To edit Azure Active Directory tenant master data

1. Select the category **Azure Active Directory | Tenants**.
2. Select the tenant from the result list.
3. Select **Change master data** in the task view.

4. Edit the tenant's master data.
5. Save the changes.

Detailed information about this topic

- General Master Data for an Azure Active Directory Tenant on page 74
- Local Active Directory Data on page 76
- Specifying Categories for Inheriting Permissions on page 76

General Master Data for an Azure Active Directory Tenant

Enter the following data on the **General** tab:

Table 22: Tenant Master Data

Property	Description
Display name	The tenant’s display name.
Account definition (initial)	Initial account definition for creating user accounts. This account definition is used if automatic assignment of employees to user accounts is used for this tenant and user accounts should be created which are already managed (state "linked configured"). The account definition's default manage level is applied. User accounts are only linked to the employee (state "Linked") if no account definition is given. This is the case on initial synchronization, for example.
Target System Managers	Application role in which target system managers are specified for the tenant. Target system managers only edit tenant objects that are assigned to them. Each 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 tenant. Use the button to add a new application role.
Location	The tenant's location.
Street	Street or road.
Town	City.
Zip code	Zip code.

<table>
<tr><th>Property</th><th>Description</th></tr>
<tr><td>Country</td><td>Country.</td></tr>
<tr><td>Synchronized by</td><td>NOTE: You can only specify the synchronization type when adding a new tenant. No changes can be made after saving.
Use "One Identity Manager" when you create a tenant with the Synchronization Editor.
Type of synchronization through which the data is synchronized between the tenant and One Identity Manager.
Table 23: Permitted Values
<table>
<tr><th>Value</th><th>Synchronization by</th><th>Provisioned by</th></tr>
<tr><td>One Identity Manager</td><td>Azure Active Directory connector</td><td>Azure Active Directory connector</td></tr>
<tr><td>No synchronization</td><td>none</td><td>none</td></tr>
</table>
NOTE: If you select "No synchronization" you can define custom processes to exchange data between One Identity Manager and the target system.</td></tr>
<tr><td>Recipients (marketing notifications)</td><td>List of recipients of marketing notifications.</td></tr>
<tr><td>Recipient (technical notifications)</td><td>List of recipients of technical notifications.</td></tr>
<tr><td>Recipients (security notifications)</td><td>List of recipients of security notifications.</td></tr>
<tr><td>Phone numbers (security notifications)</td><td>Phone numbers for security notifications.</td></tr>
</table>

Related Topics

- Automatic Assignment of Employees to Azure Active Directory User Accounts on page 94
- Target System Managers on page 65

Local Active Directory Data

The **Linked** tab shows information about the local Active Directory, which is linked to the Azure Active Directory tenant.

Table 24: 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 tenant synchronization with the local Active Directory.

Specifying Categories for Inheriting Permissions

In One Identity Manager, groups, administrative roles, subscriptions and disabled service plans can be selectively inherited by user accounts. For this, groups(administrative roles, subscriptions and disabled service plans) and user accounts are divided into categories. The categories can be freely selected and are specified by a template. 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. Enter your categories for the structural profiles, administrative roles, subscriptions and disabled service plans in the other tables. Each table contains the category items "Position1" to "Position31".

To define a category

1. Select the category **Azure Active Directory | Tenants**.
2. Select the tenant from the result list.
3. Select **Change master data** in the task view.
4. Switch to the **Mapping rule category** tab.
5. Expand the respective base node of a table.
6. Click to enable category.
7. Enter a name for the user account and group categories (administration roles, subscriptions, disabled service plans) in the current language.
8. Save the changes.

Related Topics

- Azure Active Directory Group Inheritance Based on Categories on page 114
- Azure Active Directory Administrator Role Inheritance Based on Categories on page 126
- Inheriting Azure Active Directory Subscriptions based on Categories on page 137
- Inheritance of Disabled Azure Active Directory Service Plans Based on Categories on page 146

How to Edit a Synchronization Project

Synchronization projects, in which a tenant is already used as a base object, can also be opened using 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. Select the category **Azure Active Directory | Tenants**.
2. Select the tenant from the result list. Select **Change master data** in the task view.
3. Select **Edit synchronization project...** from the task view.

Related Topics

- Customizing Synchronization Configuration on page 26

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. Select the category **Azure Active Directory | Verified domains**.
2. Select the domain in the result list.

3. Select **Azure Active Directory domain overview** in the task view.

Table 25: Domain Master Data

Property	Description
Domain name	Full name of the domain.
Tenant	Tenant entered for this domain.
Type	Domain type.
Primary domain	Specifies whether this is the primary domain for created new user accounts, for example.
Initial domain	Specifies whether this is the initial domain. The initial domain is create when a tenant is registered in Azure Active Directory.
Available services	List of service available in this domain.

5

Azure Active Directory User Accounts

You manage user account in One Identity Manager with Azure Active Directory. The user requires a subscription to access a service plan in Azure Active Directory. User accounts obtain the required access rights to the resources through membership in groups.

Detailed information about this topic

- Linking User Accounts to Employees on page 79
- Supported User Account Types on page 80
- Entering Master Data for Azure Active Directory User Accounts on page 84

Linking User Accounts to Employees

The central component of the One Identity Manager is to map employees and their master data with permissions through which they have control over different target systems. For this purpose, information about user accounts and permissions can be read from the target system into the One Identity Manager database and linked to employees. This gives an overview of the permissions for each employees in all of the connected target systems. One Identity Manager provides the possibility to manage 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, the One Identity Manager offers different methods for supplying user accounts to employees. One Identity Manager supports the following method for linking employees and their user accounts.

- Employees and user accounts can be entered manually and assigned to each other.
- Employees can automatically obtain their account definitions using user account resources. If an employee does not 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 followed by process handling.

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

NOTE: If employees obtain their user accounts through account definitions, they have to have a central user account and obtain their company IT data through assignment to a primary department, primary location or a primary cost center.

- An existing employee is automatically assigned when a user account is added or a new employee is created if necessary. In this case, employee master data is created on the basis of the existing user account master data. This mechanism can be implemented if a new user account is created manually or by synchronization. This method, however, is not the One Identity Manager default method. Define criteria for finding employees for automatic employee assignment.

Related Topics

- Entering Master Data for Azure Active Directory User Accounts on page 84
- Setting Up Account Definitions on page 35
- Automatic Assignment of Employees to Azure Active Directory User Accounts on page 94
- For more detailed information about handling and administration of employees and user accounts, see the One Identity Manager Target System Base Module Administration Guide.

Supported User Account Types

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

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

- Identity (column `IdentityType`)

  The identity describes the type of user account.

Table 26: Identities of User Accounts

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

Identity	Description	Value of the column "IdentityType"
identity		
Organizational identity	Secondary user account used for various roles within the organization, f. ex. In sub-agreements with other functional areas.	Organizational
Personalized admin identity	User account with administration rights used by one person.	Admin
Sponsored identity	User account used for example for training purposes.	Sponsored
Shared identity	User account with administration rights used by several people.	Shared
Service identity	Service account.	Service

- Privileged user account (column `IsPrivilegedAccount`)

  Use this option to flag user accounts with special, privileged permissions. This includes administrative user accounts or service accounts, for example. This option is not used to flag default user accounts.

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 manage level "Unmanaged" or "Full managed" to it.
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.

   An account definition specifies which rules are used to generate the IT operating data for example, whether the container for a user account is made up of the employee's department, cost center, location or business role and which default values will be used if no IT operating data can be found through the employee's primary roles.

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

- Use the default value "1" in the formatting rule for the column `IsGroupAccount` and set the option **Always use default value**.
- Use the default value "primary" in the formatting rule for the column `IdentityType` and set the option **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, which 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.

Administrative User Accounts

An administrative user account must be used for certain administrative tasks. Administrative user accounts are normally predefined in the target system and have fixed identifiers and login names, for example, "Administrator".

Administrative user accounts are loaded through synchronization into the One Identity Manager. To assign a manager to administrative user accounts, assign an employee to the user account in One Identity Manager.

NOTE: You can automatically label administrative user accounts as privileged user accounts. To do this, set the schedule "Mark selected user accounts as privileged" in the Designer.

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 marked with the property **Privileged user account** (`IsPrivilegedAccount`).

NOTE: The criteria used to label user accounts automatically as privileged, are defined as extensions to the view definition (ViewAddOn) on the table `TSBVAccountIsPrivDetectRule` (table type "Union"). The evaluation is done in the script `TSB_SetIsPrivilegedAccount`.

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 properties for privileged user accounts being overwritten, set the property **IT operating data overwrites** for the manage level, to the value "Only initially". In this case, the properties are populated just once when the user accounts is created.

3. 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.
4. Create a formatting rule for IT operating data.

   An account definition specifies which rules are used to generate the IT operating data for example, whether the container for a user account is made up of the employee's department, cost center, location or business role and which default values will be used if no IT operating data can be found through the employee's primary roles.

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

   - Use the default value "1" in the formatting rule for the column `IsPrivilegedAccount` and set the option **Always use default value**.
   - You can also specify a formatting rule for the column `IdentityType`. The column owns different permitted values, which represent user accounts.
   - To prevent privileged user accounts inheriting default user groups, define a template for the column `IsGroupAccount` with the default value "0" and set the option **Always use default value**.
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.

NOTE: Specify a formatting rule for a naming schema if it is required by the company for privileged user account login names.

To use a prefix with a login name, set the configuration parameter "TargetSystem\AzureAD\Accounts\PrivilegedAccount\AccountName_Prefix" in the Designer. To use a postfix with a login name, set the configuration parameter "TargetSystem\AzureAD\Accounts\PrivilegedAccount\AccountName_Postfix" in the Designer.

These configuration parameters are evaluated in the default installation, if a user account is marked with the property **Privileged user account** (`IsPrivilegedAccount`). The user account login names are renamed according to the formatting rules. This also takes place if the user accounts are labeled as privileged by the schedule "Mark selected user accounts as privileged".

Entering Master Data for Azure Active Directory User Accounts

A user account can be linked to an employee in the One Identity Manager. You can also manage user accounts separately from employees.

NOTE: It is recommended to use account definitions to set up user accounts for company employees. In this case, some of the master data described in the following is mapped through templates from employee master data.

NOTE: If employees obtain their user accounts through account definitions, they have to have a central user account and obtain their company IT data through assignment to a primary department, 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, location or business roles or by IT Shop request.

To edit master data for a user account

1. Select the category **Azure Active Directory | User accounts**.
2. Select the user account in the result list and run the task **Change master data**.

   - OR-

   Click in the result list toolbar.
3. Edit the user account's resource data.
4. Save the changes.

To manually assign or create a user account for an employee

1. Select the **Employees | Employees**.
2. Select the employee in the result list and run **Assign Azure Active Directory user accounts** from the task view.
3. Assign a user account.
4. Save the changes.

Detailed information about this topic

- General Master Data for an Azure Active Directory User Account on page 85
- Contact Data for an Azure Active Directory User Account on page 88
- Organizational Data for an Azure Active Directory User Account on page 88
- Active Directory User Account Local Data on page 89

Related Topics

- Setting Up Account Definitions on page 35
- Supported User Account Types on page 80
- Azure Active Directory Subscriptions and Service Plans on page 128

General Master Data for an Azure Active Directory User Account

Enter the following data on the **General** tab:

Table 27: Additional Master Data for 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 use automatic employee assignment, an associated employee is created and entered into the user account when the user account is saved.
Account definition	Account definition through which the user account was created. Use the account definition to automatically fill user account master data and to specify a manage level for the user account. The 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.
Manage level	User account's manage level. 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	User account's tenant.
Domain	User account's user account.
Location	Location where this user account is in use.
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.
User login name	User account login name. The user's login name is made up of the alias

Property	Description
	and the domain. User login names that are formatted like this correspond to the User Principal Name (UPN) in Azure Active Directory.
Alias	Email alias for the user account.
Preferred language	User's preferred language, for example "en-US".
Password	Password for the user account. Depending on the configuration parameter "Person\UseCentralPassword" the employee's central password can be mapped to the user account's password. If you use an initial password for the user accounts, it is automatically entered when a user account is created. 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 the next time you log in	Specifies whether the user must change their password the next time they log in.
Password policies	Policies, which only apply to the user account. The available options are: **No restrictions**, **Password never expires** and **Allow weak passwords**.
Risk index (calculated)	Maximum risk index values for all assigned . This property is only visible if the configuration parameter "QER\CalculateRiskIndex" is set. For more detailed information, see the One Identity Manager Risk Assessment Administration Guide.
Category	Categories for the inheritance of groups by the user account. Select one or more categories from the menu. Groups can be selectively inherited by user accounts. To do this, groups and user accounts or contacts are divided into categories.
Identity	User account's identity type

<table>
<tr><th>Property</th><th>Description</th></tr>
<tr><td></td><td>Table 28: Permitted values for the identity.<table><tr><th>Value</th><th>Description</th></tr><tr><td>Primary identity</td><td>Employee's default user account.</td></tr><tr><td>Organizational identity</td><td>Secondary user account used for different roles in the organization, for example for subcontracts with other functional areas.</td></tr><tr><td>Personalized admin identity</td><td>User account with administrative permissions, used by one employee.</td></tr><tr><td>Sponsored identity</td><td>User account that is used for training purposes, for example.</td></tr><tr><td>Shared identity</td><td>User account with administrative permissions, used by several employees.</td></tr><tr><td>Service identity</td><td>Service account.</td></tr></table></td></tr>
<tr><td>Privileged user account</td><td>Specifies whether this is a privileged user account.</td></tr>
<tr><td>Groups can be inherited</td><td>Specifies whether the user account groups can inherit through the employee. If this option is set, the user account inherits groups through hierarchical roles or IT Shop requests.
If you add an employee with a user account to a department, for example, and you have assigned groups to this department, the user account inherits these groups.
If an employee has requested group membership in the IT Shop and the request is granted approval, the employee's user account only inherits the group if the option is set.</td></tr>
<tr><td>User account is disabled</td><td>Specifies whether the user account is disable. If a user account is not required for a period of time, you can temporarily disable the user account by using the option <User account is deactivated>.</td></tr>
</table>

Related Topics

- Setting Up Account Definitions on page 35
- Password Policies on page 53
- Azure Active Directory Group Inheritance Based on Categories on page 114
- Linking User Accounts to Employees on page 79
- Supported User Account Types on page 80
- Disabling Azure Active Directory User Accounts on page 99

Contact Data for an Azure Active Directory User Account

Enter the following address data for contacting the employee on the **Contact** tab.

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.
Town	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 town.
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.
Email address	User account's email address.
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: new email address`

Organizational Data for an Azure Active Directory User Account

Enter the following organizational master data on the **Organizational** tab.

Table 30: Organizational Master Data

Property	Description
Office	Office. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
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. Departments can be automatically generated and employees assigned based on the department data.
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 text box. 2. Under **Table**, select the table which maps the account manager. 3. Select the manager under **Account manager**. 4. Click **OK**.

Active Directory User Account Local Data

The **Linked** tab shows information about the local Active Directory user account, which is linked to the Azure Active Directory user account.

Table 31: 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	An identifier which cannot be changed to maintain the relation between Active Directory and Azure Active Directory.

Additional Tasks for Managing Azure Active Directory User Accounts

After you have entered the master data, you can apply different tasks to it. The task view contains different forms with which you can run the following tasks.

Overview of Azure Active Directory User Accounts

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. Select the category **Azure Active Directory | User accounts**.
2. Select the user account in the result list.
3. Select **Azure Active Directory user account overview** in the task view.

Related Topics

- Azure Active Directory Subscriptions and Service Plans on page 128

Changing the Manage Level of an Azure Active Directory User Account

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. Select the category **Azure Active Directory | User accounts**.
2. Select the user account in the result list.
3. Select **Change master data** in the task view.
4. Select the manage level in the **Manage level** menu on the tab **General**.
5. Save the changes.

Related Topics

- Entering Master Data for Azure Active Directory User Accounts on page 84

Assigning Azure Active Directory Groups Directly to Azure Active Directory User Accounts

Groups can be assigned directly or indirectly to a user account. Indirect assignment is carried out by allocating the employee and groups in hierarchical roles, like departments, cost centers, locations or business roles. If the employee has a user account in Azure Active Directory, the groups in the role are inherited by this user account.

To react quickly to special requests, you can assign groups directly to the user account.

To assign groups directly to user accounts

1. Select the category **Azure Active Directory | User accounts**.
2. Select the user account in the result list.
3. Select **Assign groups** in the task view.
4. Assign groups in **Add assignments**.

   - OR -

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

Related Topics

- Assigning Azure Active Directory Groups to Azure Active Directory User Accounts on page 105

Assigning Azure Active Directory Administrator Roles directly to Azure Active Directory User Accounts

Administrator roles can be assigned directly or indirectly to a user account. Indirect assignment is carried out by assigning the employee and administrator roles to hierarchical roles, like departments, cost centers, locations or business roles. If the employee has a user account in Azure Active Directory, the administrator roles of the departments, cost centers, locations and business roles are inherited by this user account.

To react quickly to special requests, you can assign administrator roles directly to the user account.

To assign administrator roles directly to user accounts

1. Select the category **Azure Active Directory | User accounts**.
2. Select the user account in the result list.
3. Select **Assign administrator roles** in the task view.
4. Assign administrator roles in **Add assignments**.

   - OR -

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

Related Topics

- Assigning Azure Active Directory Administrator Roles to Azure Active Directory User Accounts on page 120

Assigning Azure Active Directory Subscriptions directly to Azure Active Directory User Accounts

You can assign subscriptions directly or indirectly to a user account. In the case of indirect assignment, employees and subscriptions are assigned to hierarchical roles, such as, departments, cost centers, locations or business roles. If the employee has a user account in Azure Active Directory, role subscriptions are inherited by this user account.

To react quickly to special requests, you can assign subscriptions directly to a user account.

To assign subscriptions directly to user accounts

1. Select the category **Azure Active Directory | User accounts**.
2. Select the user account in the result list.
3. Select **Assign subscriptions** in the task view.
4. Save the changes.

Related Topics

- Assigning Azure Active Directory Subscriptions to Azure Active Directory User Accounts on page 130

Assigning Disabled Azure Active Directory Service Plans directly to Azure Active Directory User Accounts

You can assign disabled service plans directly or indirectly to a user account. 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. If the employee has a user account in Azure Active Directory, disabled service plans belonging to roles are inherited by this user account.

To react quickly to special requests, you can assign disabled service plans directly to a user account.

To assign disabled service plans directly to a user account

1. Select the category **Azure Active Directory | User accounts**.
2. Select the user account in the result list.
3. Select **Assign disabled service plans** in the task view.
4. Save the changes.

Related Topics

- Assigning Disabled Azure Active Directory Service Plans to Azure Active Directory User Accounts on page 139

Assign Extended Properties to an Azure Active Directory User Account

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

To specify extended properties for a user account

1. Select the category **Azure Active Directory | User accounts**.
2. Select the user account in the result list.
3. Select **Assign extended properties** in the task view.
4. Assign extended properties in **Add assignments**.

   - OR -

   Remove assignments to extended properties in **Remove assignments**.
5. Save the changes.

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

Automatic Assignment of Employees to Azure Active Directory User Accounts

Table 32: Configuration Parameters for Automatic Employee Assignment

Configuration parameter	Meaning
TargetSystem\AzureAD\PersonAutoFullsync	This configuration parameter specifies the mode for automatic employee assignment for user accounts added to or updated in the database through synchronization.
TargetSystem\AzureAD\PersonAutoDefault	This configuration parameter specifies the mode for automatic employee assignment for user accounts added to the database outside synchronization.
TargetSystem\AzureAD\PersonExcludeList	List of all user accounts for which automatic employee assignment should not take place. Names given in a pipe (|) delimited list that is handled as a regular search pattern. Example: `Administrator`
TargetSystem\AzureAD\ PersonAutoDisabledAccounts	This configuration parameters specifies whether employees are automatically assigned to disable user accounts. User accounts do not obtain an account definition.

When you add a user account, an existing employee can be assigned automatically or added if necessary. In the process, the employee master data is created based for existing user master 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 assignment to user accounts remain intact.

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

Run the following tasks to assign employees automatically.

- If employees can be assigned by user accounts during synchronization, set the parameter "TargetSystem\AzureAD\PersonAutoFullsync" in the Designer and select the required mode.
- If employees can be assigned by user accounts during synchronization, set the parameter "TargetSystem\AzureAD\PersonAutoDefault" in the Designer and select the mode.
- Specify the user accounts in the configuration parameter "TargetSystem\AzureAD\PersonExcludeList" which must not be assigned automatically to employees.

  Example:

  `ADMINISTRATOR`
- Use the configuration parameter "TargetSystem\AzureAD\PersonAutoDisabledAccounts" 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 the manage level to be used is entered as default automation level.
- Define the search criteria for employees assigned to tenants.

NOTE:

The following applies for synchronization:

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

The following applies outside synchronization:

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

NOTE: Following synchronization, employees are automatically created for user accounts in the default installation. If there are no account definitions for the tenant at the time of synchronization, user accounts are linked to employees. However, account definitions are not assigned. The user accounts are, therefore, in a "Linked" state.

To select user accounts through account definitions

1. Create an account definition.
2. Assign an account definition to the tenant.
3. Assign the account definition and manage level to the user accounts in a "linked" state.
    a. Select the category **Azure Active Directory | User accounts | Linked but not configured | <client>**.
    b. Select the task **Assign account definition to linked accounts**.

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

Related Topics

- Creating an Account Definition on page 36
- Assigning Account Definitions to a Target System on page 50
- Editing Search Criteria for Automatic Employee Assignment on page 96

Editing Search Criteria for Automatic Employee Assignment

Criteria for employee assignment are defined in the tenant. In this case, you specify which user account properties must match the employee's properties such that the employee can be assigned to the user account. You can limit search criteria further by using format definitions. The search criteria are written in XML notation in the column "Search criteria for automatic employee assignment" (`AccountToPersonMatchingRule`) of 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: When the employees are assigned to user accounts on the basis of search criteria, user accounts are given the default manage level of the account definition entered in the user account's target system. You can customize user account properties depending on how the behavior of the manage level is defined.

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

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.

To specify criteria for employee assignment

1. Select the category **Azure Active Directory | Tenants**.
2. Select the tenant from the result list.
3. Select **Define search criteria for employee assignment** in the task view.
4. Specify which user account properties must match with which employee so that the employee is linked to the user account.

Table 33: Default Search Criteria for User Accounts and Contacts

Apply to	Column on Employee	Column on User Account
Azure Active Directory user accounts	Central user account (`CentralAccount`)	Alias (`MailNickName`)

5. Save the changes.

Direct Assignment of Employees to User Accounts Based on a Suggestion List

You can create a suggestion list in the "Assignments" view for assignments of employees to user accounts based on the search criteria. User accounts are grouped in different views for this.

Table 34: 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.
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.

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

To apply search criteria to user accounts

- 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.

To assign employees directly over a suggestion list

1. Click **Suggested assignments**.
   a. Click **Select** for all user accounts to be assigned to the suggested employee. Multi-select is possible.
   b. Click **Assign selected.**
   c. Confirm the security prompt with **Yes**.

      The selected user accounts are assigned to the employees found using the search criteria.

   – OR –
2. Click **No employee assignment**.
   a. Click **Select employee...** for the user account to which you want to assign the employee. Select an employee from the menu.
   b. Click **Select** for all user accounts to which you want to assign the selected employees. Multi-select is possible.
   c. Click **Assign selected**.
   d. Confirm the security prompt with **Yes**.

      This assigns the selected user accounts to the employees shown in the "Employee" column.

To remove assignments

1. Click **Assigned user accounts**.
   a. Click **Select** for all user accounts whose employee assignment you want to remove. Multi-select is possible.
   b. Click **Delete selected**.
   c. Confirm the security prompt with **Yes**.

      The assigned employees are deleted from the selected user accounts.

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

Related Topics

- Automatic Assignment of Employees to Azure Active Directory User Accounts on page 94

Disabling Azure Active Directory User Accounts

Table 35: Configuration Parameter for User Accounts

Configuration parameter	Meaning
QER\Person\TemporaryDeactivation	This configuration parameter specifies whether user accounts for an employee are locked if the employee is temporarily or permanently disabled.

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. User accounts with the manage level "Full managed" are disabled depending on the account definition settings. For user accounts with another manage level, modify the column template `AADUser.AccountDisabled` accordingly.

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 configuration parameter "QER\Person\TemporaryDeactivation".

- If the configuration parameter is set, the employee's user accounts are disabled if 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 lock a user account when the configuration parameter is disabled

1. Select the category **Azure Active Directory | User accounts**.
2. Select the user account in the result list.
3. Select **Change master data** in the task view.
4. Set the option **Account is disabled** on the **General** tab.
5. Save the changes.

Scenario:

- User accounts not linked to employees.

To lock a user account, which is not linked to an employee

1. Select the category **Azure Active Directory | User accounts**.
2. Select the user account in the result list.
3. Select **Change master data** in the task view.
4. Set the option **Account is disabled** on the **General** tab.
5. Save the changes.

Related Topics

- Setting Up Account Definitions on page 35
- Setting Up Manage Levels on page 38
- Deleting and Restoring Azure Active Directory User Accounts on page 100
- For more detailed information about deactivating and deleting employees and user accounts, see the One Identity Manager Target System Base Module Administration Guide.

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 created through this account definition, is deleted.

To delete a user account

1. Select the category **Azure Active Directory | User accounts**.
2. Select the user account in the result list.
3. Delete the user account.
4. Confirm the security prompt with **Yes**.

To restore user account

1. Select the category **Azure Active Directory | User accounts**.
2. Select the user account in the result list.
3. Click **Undo delete** in the result list toolbar.

Configuring Deferred Deletion

By default, user accounts are finally deleted from the database after 30 days.The user accounts are initially disabled. You can reenable the user accounts until deferred deletion is run. After deferred deletion is run, the user account are deleted from the database and

cannot be restored anymore. You can configure an alternative delay on the table AADAccount in the Designer.

Related Topics

- Disabling Azure Active Directory User Accounts on page 99
- For more detailed information about deactivating and deleting employees and user accounts, see the One Identity Manager Target System Base Module Administration Guide.

Azure Active Directory Groups

Azure Active Directory recognizes several groups types, in which you can gather users and groups to, for example, regulate access to resources or email distribution.

Groups are loaded into One Identity Manager by synchronization. You can edit individual master data of the group and you can create new security groups in One Identity Manager. You cannot create more groups 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, location, business roles or to the IT Shop.

The group types supported in One Identity Manager are listed below.

Table 36: 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 cannot create new them in One Identity Manager.
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 edit mail-enabled security in One Identity Manager but you cannot create new mail-enabled security groups in One Identity Manager.

Editing Azure Active Directory Group Master Data

Groups are loaded into One Identity Manager by synchronization. You can create new security groups in One Identity Manager. You can merely edit the other groups types and which of the data you can edit, depends on the group type.

To edit group master data

1. Select the category **Azure Active Directory | Groups**.
2. Select the group in the result list and run **Change master data** in the task view.

   - OR -

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

Detailed information about this topic

- General Master Data for an Azure Active Directory Group on page 103
- Information about Local Active Directory Groups on page 105

General Master Data for an Azure Active Directory Group

Enter the following data on the **General** tab:

Table 37: General Master 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 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).

Property	Description
	Use the following syntax to set up other proxy addresses: `Address type: new email address`
Group type	Specifies a group's type The value is "unified" for Office 365 group and is empty for security and distribution groups.
Security group	Specifies whether the 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. This group can be requested by staff through the Web Portal and granted through 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. This group can be requested by staff through the Web Portal and granted through a defined approval process. Direct assignment of the group to hierarchical roles or user accounts is no 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. Enter a value between 0 and 1. This property is only visible when the configuration parameter QER\CalculateRiskIndex is set. For more detailed 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. Use this menu to allocate one or more categories to the group.
Description	Spare text box for additional explanation.

Related Topics

- Azure Active Directory Group Inheritance Based on Categories on page 114
- For more detailed 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, which is linked to the Azure Active Directory user account.

Table 38: 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.

Assigning Azure Active Directory Groups to Azure Active Directory User Accounts

Groups can be assigned directly or indirectly to user accounts. In the case of indirect assignment, employees and groups are assigned to hierarchical roles, such as , departments, cost centers, locations or business roles. The 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 a user account, the user account is added to the groups. Prerequisites for indirect assignment of employees to user accounts:

- Assignment of employees and groups is permitted for role classes (department, cost center, location or business role).
- The user accounts are marked with the option **Groups can be inherited**.

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

Detailed information about this topic

- Assigning Azure Active Directory Groups to Departments, Cost Centers and Locations on page 106

- Assigning Azure Active Directory Groups to Business Roles on page 107
- Assigning Azure Active Directory User Accounts directly to an Azure Active Directory Group on page 108
- Adding Azure Active Directory Groups to System Roles on page 109
- Adding Azure Active Directory Groups to the IT Shop on page 109

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.

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

1. Select the category **Azure Active Directory | Groups**.
2. Select the group in the result list.
3. Select **Assign organizations**.
4. Assign organizations in **Add assignments**.
   - Assign departments on the **Departments** tab.
   - Assign locations on the **Locations** tab.
   - Assign cost centers on the **Cost center** tab.

   - OR -

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

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

1. Select the category **Organizations | Departments**.

   - OR -

   Select the category **Organizations | Cost centers**.

   - OR -

   Select the category **Organizations | Locations**.
2. Select the department, cost center or location in the result list.
3. Select **Assign Azure Active Directory groups.**
4. Assign groups in **Add assignments**.

   - OR -

   Remove assignments to groups in **Remove assignments**.
5. Save the changes.

Related Topics

- Assigning Azure Active Directory Groups to Business Roles on page 107
- Assigning Azure Active Directory User Accounts directly to an Azure Active Directory Group on page 108
- Adding Azure Active Directory Groups to System Roles on page 109
- Adding Azure Active Directory Groups to the IT Shop on page 109
- One Identity Manager Users for Managing an Azure Active Directory System on page 9

Assigning Azure Active Directory Groups to Business Roles

Installed Modules: Business Roles Module

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

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

1. Select the category **Azure Active Directory | Groups**.
2. Select the group in the result list.
3. Select **Assign business roles** in the task view.
4. Assign business roles in **Add assignments**.

   - OR -

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

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

1. Select the category **Business roles | <Role class>**.
2. Select the business role in the result list.
3. Select **Assign Azure Active Directory groups.**
4. Assign groups in **Add assignments**.

   - OR -

   Remove assignments to groups in **Remove assignments**.
5. Save the changes.

Related Topics

- Assigning Azure Active Directory Groups to Departments, Cost Centers and Locations on page 106
- Assigning Azure Active Directory User Accounts directly to an Azure Active Directory Group on page 108
- Adding Azure Active Directory Groups to System Roles on page 109
- Adding Azure Active Directory Groups to the IT Shop on page 109
- One Identity Manager Users for Managing an Azure Active Directory System on page 9

Assigning Azure Active Directory User Accounts directly to an Azure Active Directory Group

Groups can be assigned directly or indirectly to user accounts. Indirect assignment is carried out by allocating the employee and groups in company structures, like departments, cost centers, locations or business roles. If the employee has a user account in Azure Active Directory, the groups in the role are inherited by this user account.

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

To assign a group directly to user accounts

1. Select the category **Azure Active Directory | Groups**.
2. Select the group in the result list.
3. Select **Assign user accounts** in the task view.
4. Assign user accounts in **Add assignments**.

   - OR -

   Remove user accounts from **Remove assignments**.
5. Save the changes.

Related Topics

- Assigning Azure Active Directory Groups Directly to Azure Active Directory User Accounts on page 91
- Assigning Azure Active Directory Groups to Departments, Cost Centers and Locations on page 106
- Assigning Azure Active Directory Groups to Business Roles on page 107
- Adding Azure Active Directory Groups to System Roles on page 109
- Adding Azure Active Directory Groups to the IT Shop on page 109

Adding Azure Active Directory Groups to System Roles

Installed Modules: System Roles Module

Use this task to add a group to system roles. If you assign a system role to employees, all the employees' user accounts inherit the group.

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

To assign a group to system roles

1. Select the category **Azure Active Directory | Groups**.
2. Select the group in the result list.
3. Select **Assign system roles in the task view**.
4. Assign system roles in **Add assignments**.

   - OR -

   Remove system roles from **Remove assignments**.
5. Save the changes.

Related Topics

- Assigning Azure Active Directory Groups to Departments, Cost Centers and Locations on page 106
- Assigning Azure Active Directory Groups to Business Roles on page 107
- Assigning Azure Active Directory User Accounts directly to an Azure Active Directory Group on page 108
- Adding Azure Active Directory Groups to the IT Shop on page 109

Adding Azure Active Directory Groups to the IT Shop

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

- The group must be labeled with the option **IT Shop**.
- The group must be assigned to a service item.
- The group must be labeled with the option **Only use in IT Shop** if the group can

only be assigned to employees through IT Shop requests. Direct assignment to hierarchical roles or user accounts is no longer permitted.

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

To add a group to the IT Shop

1. Select the category **Azure Active Directory | Groups** (non role-based login).

   - OR -

   Select the category **Entitlements | Azure Active Directory groups** (role-based login).
2. Select the group in the result list.
3. Select **Add to IT Shop** in the task view.
4. Assign the group to the IT Shop shelves in **Add assignments**.
5. Save the changes.

To remove a group from individual IT Shop shelves.

1. Select the category **Azure Active Directory | Groups** (non role-based login).

   - OR -

   Select the category **Entitlements | Azure Active Directory groups** (role-based login).
2. Select the group in the result list.
3. Select **Add to IT Shop** in the task view.
4. Remove the group from the IT Shop shelves in **Remove assignments**.
5. Save the changes.

To remove a group from all IT Shop shelves.

1. Select the category **Azure Active Directory | Groups** (non role-based login).

   - OR -

   Select the category **Entitlements | Azure Active Directory groups** (role-based login).
2. Select the group in the result list.
3. Select **Remove from all shelves (IT Shop)** in the task view.
4. Confirm the security prompt with **Yes**.
5. Click **OK**.

   This removes the group from all One Identity Manager Service shelves. All requests and assignment requests with this group are canceled in the process.

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

Related Topics

- General Master Data for an Azure Active Directory Group on page 103
- Assigning Azure Active Directory Groups to Departments, Cost Centers and Locations on page 106
- Assigning Azure Active Directory Groups to Business Roles on page 107
- Assigning Azure Active Directory User Accounts directly to an Azure Active Directory Group on page 108
- Adding Azure Active Directory Groups to System Roles on page 109

Additional Tasks for Managing Azure Active Directory Groups

After you have entered the master data, you can apply different tasks to it. The task view contains different forms with which you can run the following tasks.

Overview of Azure Active Directory Groups

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

To obtain an overview of a group

1. Select the category **Azure Active Directory | Groups**.
2. Select the group in the result list.
3. Select **Azure Active Directory group overview** in the task view.

Adding Azure Active Directory Groups to Azure Active Directory Groups

Use this task to add a group to another group.

To assign groups directly to a group

1. Select the category **Azure Active Directory | Groups**.
2. Select the group in the result list.
3. Select **Assign groups** in the task view.

4. Assign child groups of the selected group in **Add assignments**.

   - OR -

   Remove assignments to groups in **Remove assignments**.
5. Save the changes.

Effectiveness of Group Memberships

Table 39: Configuration Parameter for Conditional Inheritance

Configuration parameter	Active Meaning
QER\Structures\Inherite\GroupExclusion	Preprocessor relevant configuration parameter for controlling effectiveness of group memberships. If the parameter is set, memberships can be reduced on the basis of exclusion definitions. The database has to be recompiled after changes have been made to the parameter.

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 directly, indirectly or by IT Shop request at any time. 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 whether membership of an excluded group is permitted in another group.

The effect of the assignments is mapped in the tables `AADUserInGroup` and `AADBaseTreeHasGroup` through the column `XIsInEffect`.

Example of 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 department "Marketing", group B through "Finance" and group C through the business role "Control group".

Clara Harris has a user account in this tenant. She primarily belongs to the department "marketing". The business role "Control group" and the department "Finance" 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 40: Specifying excluded groups (table `AADGroupExclusion`)

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

Table 41: 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 business role "control group" 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 request and to check invoices. If this should not be allowed, define further exclusion for group C.

Table 42: 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 configuration parameter "QER\Inherite\GroupExclusion" is enabled.
- Mutually exclusive groups belong to the same tenant.

To exclude a group

1. Select the category **Azure Active Directory | Groups**.
2. Select a group in the result list.
3. Select **Exclude groups** in the task view.
4. Assign the groups that are mutually exclusive to the selected group in **Add assignments**.

   - OR -

   Remove the conflicting groups that are no longer mutually exclusive in **Remove assignments**.
5. Save the changes.

Azure Active Directory Group Inheritance Based on Categories

In One Identity Manager, groups, administrative roles, subscriptions and disabled service plans can be selectively inherited by user accounts. For this, groups(administrative roles, subscriptions and disabled service plans) and user accounts are divided into categories. The categories can be freely selected and are specified by a template. 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. Enter your categories for the structural profiles, administrative roles, subscriptions and disabled service plans in the other tables. Each table contains the category items "Position1" to "Position31".

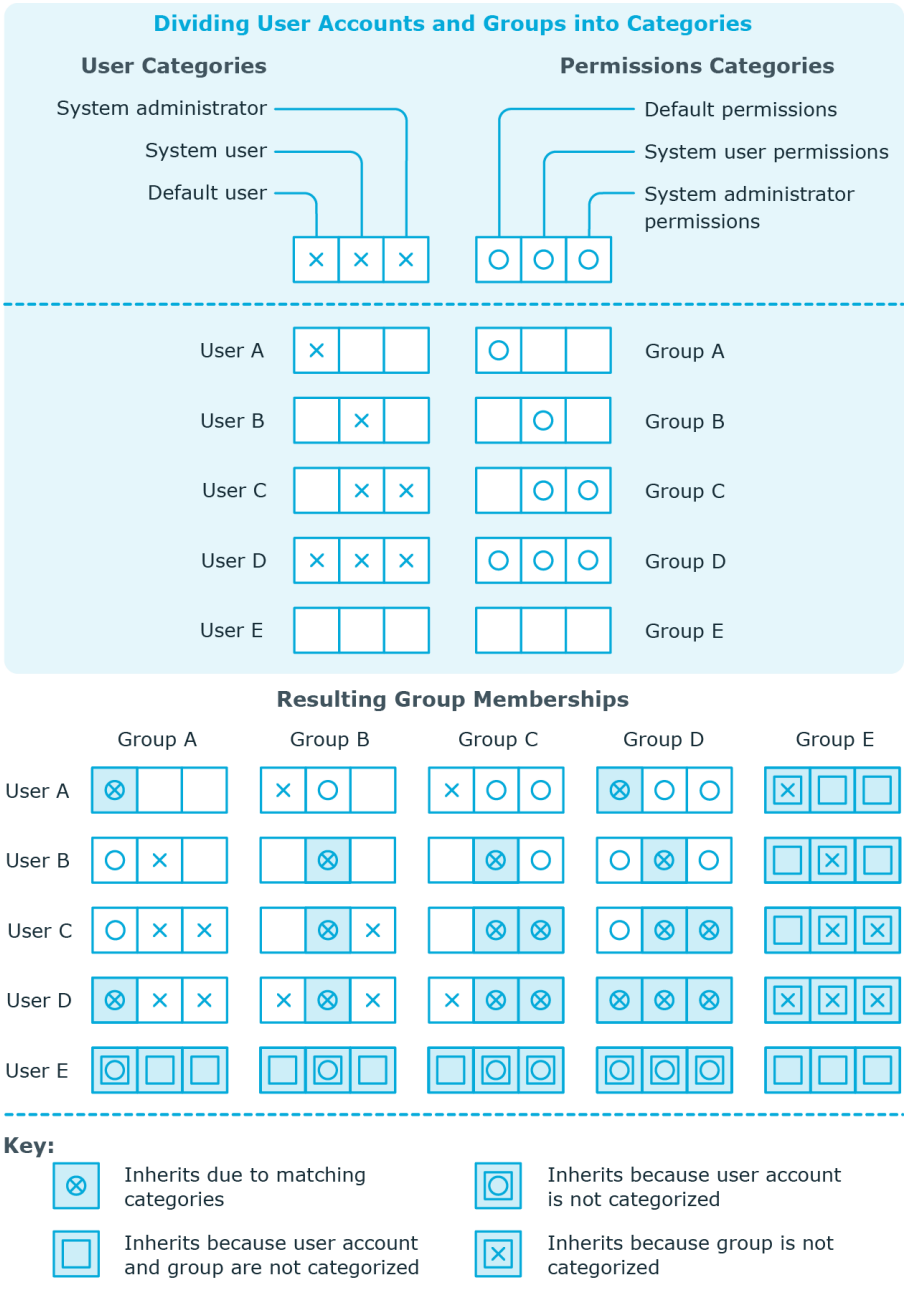
Every user account can be assigned to one or more categories. Each group can also be assigned to one or more categories. The group is inherited by the user account when at least one user account category item matches an assigned group. The group is also inherited by the user account if the group or the 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 43: Category Examples

Category Position	Categories for User Accounts	Categories for Groups
1	Default user	Default permissions
2	System user	System user permissions
3	System administrator	System administrator permissions

Figure 2: Example of inheriting through categories.



To use inheritance through categories

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

Related Topics

- Specifying Categories for Inheriting Permissions on page 76
- General Master Data for an Azure Active Directory User Account on page 85
- General Master Data for an Azure Active Directory Group on page 103
- For more information, see Editing Azure Active Directory Subscription Master Data on page 128.

Assigning Owners to Azure Active Directory Groups

A group owner can edit group properties.

To assign owners to a group

1. Select the category **Azure Active Directory | Groups**.
2. Select the group in the result list.
3. Select **Assign owner** in the task view.
4. Select the table containing the owner from the menu at the top **of the** form. You have the following options:
    - Azure Active Directory user accounts
5. Assign owners in **Add assignments**.

   - OR -

   Remove owners in **Remove assignments**.
6. Save the changes.

Assigning Extended Properties to an Azure Active Directory Group

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

To specify extended properties for a group

1. Select the category **Azure Active Directory | Groups**.
2. Select the group in the result list.
3. Select **Assign extended properties** in the task view.
4. Assign extended properties in **Add assignments**.

   - OR -

   Remove extended properties from **Remove assignments**.
5. Save the changes.

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

Deleting Azure Active Directory Groups

To delete a group

1. Select the category **Azure Active Directory | Groups**.
2. Select the group in the result list.
3. Delete the group using  .
4. Confirm the security prompt with **Yes**.

The group is deleted completely from the One Identity Manager database and from Azure Active Directory.

Azure Active Directory Administrator Roles

By using administrator roles, you can assign administrative permissions to users. Azure Active Directory recognizes several administrator roles, which fulfill different functions. For more detailed information about administrator roles, see the Azure Active Directory documentation from Microsoft.

Administrator roles are loaded into One Identity Manager by synchronization. You can edit individual master data of administrator roles but cannot create new administrator roles in One Identity Manager.

To add users to administrator roles, assign the administrator roles directly to the user. This may be administrator role assignments to departments, cost centers, location, business roles or to the IT Shop.

Editing Azure Active Directory Administrator Role Master Data

Administrator roles are loaded into One Identity Manager by synchronization. You can edit individual master data of administrator roles but cannot create new administrator roles in One Identity Manager.

To edit the master data of an administrator role

1. Select the category **Azure Active Directory | Administrator roles**.
2. Select the administrator role in the result list and run the task **Change master data**.
3. Edit the administrator role's master data.
4. Save the changes.

Table 44: Administrator Role Master Data

Property	Description
Display name	The display name is used to display the administrator role in the One Identity Manager tool's user interface.
Tenant	The administrator role's 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 administration 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 using to request the administrator role through the IT Shop.
Risk index	Value for assessing the rich of assigning administrator roles to user accounts. Enter a value between 0 and 1. This property is only visible if the configuration parameter "QER\CalculateRiskIndex" is set. For more detailed 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	Spare text box for additional explanation.

Related Topics

- Azure Active Directory Administrator Role Inheritance Based on Categories on page 126
- For more detailed information about preparing administrator roles for requesting through the IT Shop, see the One Identity Manager IT Shop Administration Guide.

Assigning Azure Active Directory Administrator Roles to Azure Active Directory User Accounts

Administrator roles can be assigned directly or indirectly to user accounts. In the case of indirect assignment, employees and administrator roles are assigned to hierarchical roles, such as, departments, cost centers, locations or business roles. The 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 a user account, the user account is added to the administrator roles. Prerequisites for indirect assignment of employees to user accounts:

- Assignment of employees and administrator roles is permitted for role classes (department, cost center, location or business role).
- The user accounts are marked with the option **Groups can be inherited**.

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

Detailed information about this topic

- Assigning Azure Active Directory Administration Roles to Departments, Cost Centers and Locations on page 120
- Assigning Azure Active Directory Administrator Roles to Business Roles on page 122
- Assigning Azure Active Directory User Accounts directly to Azure Active Directory Administrator Roles on page 123
- Adding Azure Active Directory Administrator Roles to System Roles on page 123
- Adding Azure Active Directory Administrator Roles in the IT Shop on page 124

Assigning Azure Active Directory Administration 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. Select the category **Azure Active Directory | Administrator roles**.
2. Select the administrator role in the result list.
3. Select **Assign organizations**.
4. Assign organizations in **Add assignments**.
   - Assign departments on the **Departments** tab.
   - Assign locations on the **Locations** tab.
   - Assign cost centers on the **Cost center** tab.

   - OR -

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

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

1. Select the category **Organizations | Departments**.

   - OR -

   Select the category **Organizations | Cost centers**.

   - OR -

   Select the category **Organizations | Locations**.
2. Select the department, cost center or location in the result list.
3. Select **Assign Azure Active Directory administrator roles** in the task view.
4. Assign administrator roles in **Add assignments**.

   - OR -

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

Related Topics

- Assigning Azure Active Directory Administrator Roles to Business Roles on page 122
- Assigning Azure Active Directory User Accounts directly to Azure Active Directory Administrator Roles on page 123
- Adding Azure Active Directory Administrator Roles to System Roles on page 123
- Adding Azure Active Directory Administrator Roles in the IT Shop on page 124
- One Identity Manager Users for Managing an Azure Active Directory System on page 9

Assigning Azure Active Directory Administrator Roles to Business Roles

Installed Modules: Business Roles Module

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. Select the category **Azure Active Directory | Administrator roles**.
2. Select the administrator role in the result list.
3. Select **Assign business roles** in the task view.
4. Assign business roles in **Add assignments**.

   - OR -

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

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

1. Select the category **Business roles | <Role class>**.
2. Select the business role in the result list.
3. Select **Assign Azure Active Directory administrator roles** in the task view.
4. Assign administrator roles in **Add assignments**.

   - OR -

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

Related Topics

- Assigning Azure Active Directory Administration Roles to Departments, Cost Centers and Locations on page 120
- Assigning Azure Active Directory User Accounts directly to Azure Active Directory Administrator Roles on page 123
- Adding Azure Active Directory Administrator Roles to System Roles on page 123
- Adding Azure Active Directory Administrator Roles in the IT Shop on page 124
- One Identity Manager Users for Managing an Azure Active Directory System on page 9

Assigning Azure Active Directory User Accounts directly to Azure Active Directory Administrator Roles

Administrator roles can be assigned directly or indirectly to user accounts. Indirect assignment is carried out by allocating the employee and administrator roles in company structures, like departments, cost centers, locations or business roles. If the employee has a user account in Azure Active Directory, the administrator roles in the role are inherited by this user account.

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

To assign a user account directly to an administrator role.

1. Select the category **Azure Active Directory | Administrator roles**.
2. Select the administrator role in the result list.
3. Select **Assign user accounts** in the task view.
4. Assign user accounts in **Add assignments**.

   - OR -

   Remove user accounts from **Remove assignments**.
5. Save the changes.

Related Topics

- Assigning Azure Active Directory Administrator Roles directly to Azure Active Directory User Accounts on page 91
- Assigning Azure Active Directory Administration Roles to Departments, Cost Centers and Locations on page 120
- Assigning Azure Active Directory Administrator Roles to Business Roles on page 122
- Adding Azure Active Directory Administrator Roles to System Roles on page 123
- Adding Azure Active Directory Administrator Roles in the IT Shop on page 124

Adding Azure Active Directory Administrator Roles to System Roles

Installed Modules: System Roles Module

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: Administrator roles with the option **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 an administrator role to system roles

1. Select the category **Azure Active Directory | Administrator roles**.
2. Select the administrator role in the result list.
3. Select **Assign system roles in the task view**.
4. Assign system roles in **Add assignments**.

   - OR -

   Remove system roles from **Remove assignments**.
5. Save the changes.

Related Topics

- Assigning Azure Active Directory Administration Roles to Departments, Cost Centers and Locations on page 120
- Assigning Azure Active Directory Administrator Roles to Business Roles on page 122
- Assigning Azure Active Directory User Accounts directly to Azure Active Directory Administrator Roles on page 123
- Adding Azure Active Directory Administrator Roles in the IT Shop on page 124

Adding Azure Active Directory Administrator Roles in the IT Shop

Once an administration 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 option **IT Shop**.
- The administrator role must be assigned to a service item.
- The administrator role must be also labeled with the option **Only use in IT Shop** if the administrator role can only be assigned to employees using IT Shop requests. 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. Select the category **Azure Active Directory | Administrator roles** (non role-based login).

   - OR -

   Select the category **Entitlements | Azure Active Directory administrator roles** (role-based login).
2. Select the administrator role in the result list.
3. Select **Add to IT Shop** in the task view.
4. Assign an administration role to the IT Shop shelf in **Add assignments**.
5. Save the changes.

To remove a role from individual IT Shop shelves

1. Select the category **Azure Active Directory | Administrator roles** (non role-based login).

   - OR -

   Select the category **Entitlements | Azure Active Directory administrator roles** (role-based login).
2. Select the administrator role in the result list.
3. Select **Add to IT Shop** in the task view.
4. Remove the administrator role from IT Shop shelves in **Remove assignments**.
5. Save the changes.

To remove an administrator role from individual IT Shop shelves

1. Select the category **Azure Active Directory | Administrator roles** (non role-based login).

   - OR -

   Select the category **Entitlements | Azure Active Directory administrator roles** (role-based login).
2. Select the administrator role in the result list.
3. Select **Remove from all shelves (IT Shop)** in the task view.
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 in the process.

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

Related Topics

- Editing Azure Active Directory Administrator Role Master Data on page 118
- Assigning Azure Active Directory Administration Roles to Departments, Cost Centers and Locations on page 120
- Assigning Azure Active Directory Administrator Roles to Business Roles on page 122
- Assigning Azure Active Directory User Accounts directly to Azure Active Directory Administrator Roles on page 123
- Adding Azure Active Directory Administrator Roles to System Roles on page 123

Additional Tasks for Managing Azure Active Directory Administrator Roles

After you have entered the master data, you can apply different tasks to it. The task view contains different forms with which you can run the following tasks.

Azure Active Directory Administrator Roles 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. Select the category **Azure Active Directory | Administrator roles**.
2. Select the administrator role in the result list.
3. Select the task **Azure Active Directory administrator role overview**.

Azure Active Directory Administrator Role Inheritance Based on Categories

You can also apply the behavior described under Azure Active Directory Group Inheritance Based on Categories on page 114 for administration roles.

To use inheritance through categories

- Define the categories in the tenant.
- Assign categories to user accounts through their master data.
- Assign categories to administrator roles through their master data.

Related Topics

- Specifying Categories for Inheriting Permissions on page 76
- General Master Data for an Azure Active Directory User Account on page 85
- Editing Azure Active Directory Administrator Role Master Data on page 118

Assigning Extended Properties to an Azure Active Directory Administrator Role

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

To specify extended properties for an administrator role

1. Select the category **Azure Active Directory | Administrator roles**.
2. Select the administrator role in the result list.
3. Select **Assign extended properties** in the task view.
4. Assign extended properties in **Add assignments**.

   - OR -

   Remove extended properties from **Remove assignments**.
5. Save the changes.

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

Azure Active Directory Subscriptions and Service Plans

Users require a subscription to access a service plan in Azure Active Directory. Users obtain all the service plans that are linked to a subscription. By assigning subscriptions directly to users, you make the subscriptions available to them. You can assign subscriptions to departments, cost centers, locations, business roles or the IT Shop.

So called "disabled service plans" are mapped in the One Identity Manager to prevent users from using single service plans. Disabled service plans are created automatically after synchronizing the subscription in the One Identity Manager. Disabled service plans are requested through the IT Shop or assigned to users through departments, cost centers, locations, business roles or system roles.

The actual service plans available to the user in Azure Active Directory result from the user's subscription and the service plans associated with it and the assignment of disabled service plans.

Azure Active Directory Subscriptions

Information about subscriptions and service plans within a tenant is loaded into One Identity Manager during synchronization. You cannot create new subscriptions and service plans in the One Identity Manager. You can edit individual properties of the subscription for requesting in the IT Shop and assigning to user accounts in the One Identity Manager.

Editing Azure Active Directory Subscription Master Data

To edit subscription master data

1. Select the category **Azure Active Directory | Subscriptions**.
2. Select a subscription in the result list.

3. Select **Change master data** in the task view.
4. Edit the subscription's master data.
5. Save the changes.

Table 45: Subscription Master Data

Property	Description
SKU display name	The SKU display name for the subscription, for example "AAD_Premium" or "RMSBASIC".
Tenant	Tenant entered for this subscription.
Subscription status	The subscription status, for example, "Enabled".
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 in a warning status.
IT Shop	Specifies whether the subscription can be requested through the IT Shop. This subscription can be requested by staff through the Web Portal and granted through a defined approval procedure. The subscription can still be assigned directly to user accounts and hierarchical roles.
Only for use in IT Shop	Specifies whether the subscription can only be requested through the IT Shop. This subscription can be requested by staff through the Web Portal and granted through a defined approval procedure. The subscription may not be assigned directly to hierarchical roles.
Service item	Service item data for requesting the subscription through the IT Shop.
Risk index	Value for evaluating the risk of assigning the subscription to user accounts. Enter a value between 0 and 1. This property is only visible if the configuration parameter "QER\CalculateRiskIndex" is set. For more detailed information about risk assessment, see the One Identity Manager Risk Assessment Administration Guide.
Category	Category for subscription inheritance. Subscriptions can be selectively inherited by user accounts. To do this, subscriptions and user accounts are divided into categories. Use this menu to allocate one or more categories to the subscription.

Related Topics

- Azure Active Directory Group Inheritance Based on Categories on page 114
- For more detailed information about preparing subscriptions for requesting through the IT Shop, see the One Identity Manager IT Shop Administration Guide.

Assigning Azure Active Directory Subscriptions to Azure Active Directory User Accounts

You can assign subscriptions directly or indirectly to a user account. In the case of indirect assignment, employees and subscriptions are assigned to hierarchical roles, such as, departments, cost centers, locations or business roles. 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, role subscriptions are inherited by this user account.

Prerequisites for indirect assignment of employees to user accounts:

- Assignment of employees and subscriptions is permitted for role classes (department, cost center, location or business role).
- The user accounts are marked with the option **Groups can be inherited**.

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

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, location or business roles or by IT Shop request.

Detailed information about this topic

- Assigning Azure Active Directory Subscriptions to Departments, Cost Centers and Locations on page 131
- Assigning Azure Active Directory Subscriptions to Business Roles on page 132
- Assigning Azure Active Directory User Accounts directly to an Azure Active Directory Subscription on page 133
- Adding Azure Active Directory Subscriptions to System Roles on page 133
- Adding Azure Active Directory Subscriptions to the IT Shop on page 134

Assigning Azure Active Directory Subscriptions to Departments, Cost Centers and Locations

Assign subscriptions to departments, cost centers and locations in order to assign user accounts to them through these organizations.

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

1. Select the category **Azure Active Directory | Subscriptions**.
2. Select a subscription in the result list.
3. Select **Assign organizations**.
4. Assign organizations in **Add assignments**.
   - Assign departments on the **Departments** tab.
   - Assign locations on the **Locations** tab.
   - Assign cost centers on the **Cost center** tab.

   - OR -

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

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

1. Select the category **Organizations | Departments**.

   - OR -

   Select the category **Organizations | Cost centers**.

   - OR -

   Select the category **Organizations | Locations**.
2. Select the department, cost center or location in the result list.
3. Select **Assign Azure Active Directory subscriptions** in the task view.
4. Assign the subscriptions in **Add assignments**.

   - OR -

   Remove the subscriptions in **Remove assignments**.
5. Save the changes.

Related Topics

- Assigning Azure Active Directory Subscriptions to Business Roles on page 132
- Assigning Azure Active Directory User Accounts directly to an Azure Active Directory Subscription on page 133

- Adding Azure Active Directory Subscriptions to System Roles on page 133
- Adding Azure Active Directory Subscriptions to the IT Shop on page 134
- One Identity Manager Users for Managing an Azure Active Directory System on page 9

Assigning Azure Active Directory Subscriptions to Business Roles

Installed Modules: Business Roles Module

Assign subscriptions to business roles to assign them to user accounts over these business roles.

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

1. Select the category **Azure Active Directory | Subscriptions**.
2. Select a subscription in the result list.
3. Select **Assign business roles** in the task view.
4. Assign business roles in **Add assignments**.

   - OR -

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

To assign subscriptions to a business role (role-based login)

1. Select the category **Business roles | <Role class>**.
2. Select the business role in the result list.
3. Select **Assign Azure Active Directory subscriptions** in the task view.
4. Assign the subscriptions in **Add assignments**.

   - OR -

   Remove the subscriptions in **Remove assignments**.
5. Save the changes.

Related Topics

- Assigning Azure Active Directory Subscriptions to Departments, Cost Centers and Locations on page 131
- Assigning Azure Active Directory User Accounts directly to an Azure Active Directory Subscription on page 133
- Adding Azure Active Directory Subscriptions to System Roles on page 133
- Adding Azure Active Directory Subscriptions to the IT Shop on page 134

- One Identity Manager Users for Managing an Azure Active Directory System on page 9

Assigning Azure Active Directory User Accounts directly to an Azure Active Directory Subscription

You can assign subscriptions directly or indirectly to a user account. In the case of indirect assignment, employees and subscriptions are assigned to hierarchical roles, such as, departments, cost centers, locations or business roles. If the employee has a user account in Azure Active Directory, role subscriptions are inherited by this user account.

To react quickly to special requests, you can assign subscriptions directly to a user account.

To assign a subscription directly to user accounts

1. Select the category **Azure Active Directory | Subscriptions**.
2. Select a subscription in the result list.
3. Select **Assign user accounts** in the task view.
4. Assign user accounts in **Add assignments**.

   - OR -

   Remove user accounts from **Remove assignments**.
5. Save the changes.

Related Topics

- Assigning Azure Active Directory Subscriptions directly to Azure Active Directory User Accounts on page 92
- Assigning Azure Active Directory Subscriptions to Departments, Cost Centers and Locations on page 131
- Assigning Azure Active Directory Subscriptions to Business Roles on page 132
- Adding Azure Active Directory Subscriptions to System Roles on page 133
- Adding Azure Active Directory Subscriptions to the IT Shop on page 134

Adding Azure Active Directory Subscriptions to System Roles

Installed Modules: System Roles Module

Use this task to add a subscription to system roles. When you assign a system role to an employee, the subscription is inherited by all user accounts owned by these employees.

NOTE: Subscriptions with the option **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 subscription to a system role

1. Select the category **Azure Active Directory | Subscriptions**.
2. Select a subscription in the result list.
3. Select **Assign system roles in the task view**.
4. Assign system roles in **Add assignments**.

   - OR -

   Remove system roles from **Remove assignments**.
5. Save the changes.

Related Topics

- Assigning Azure Active Directory Subscriptions to Departments, Cost Centers and Locations on page 131
- Assigning Azure Active Directory Subscriptions to Business Roles on page 132
- Assigning Azure Active Directory User Accounts directly to an Azure Active Directory Subscription on page 133
- Adding Azure Active Directory Subscriptions to the IT Shop on page 134

Adding Azure Active Directory Subscriptions to the IT Shop

Once a 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 subscription must be labeled with the **IT Shop** option.
- The subscription must be assigned to a service item.
- If the subscription is only supposed to be available to employees through IT Shop requests, the subscription must also be labeled with the option **Only for use in IT Shop**. Direct assignment to hierarchical roles may not be possible.

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

To add a subscription in the IT Shop

1. Select the category **Azure Active Directory | Subscriptions** (non role-based login).

   - OR -

   Select the category **Entitlements | Azure Active Directory subscriptions** (role-based subscription).
2. Select a subscription in the result list.
3. Select **Add to IT Shop** in the task view.
4. Assign the subscription to the IT Shop in **Add assignments**.
5. Save the changes.

To remove a subscription from individual IT Shop shelves

1. Select the category **Azure Active Directory | Subscriptions** (non role-based login).

   - OR -

   Select the category **Entitlements | Azure Active Directory subscriptions** (role-based subscription).
2. Select a subscription in the result list.
3. Select **Add to IT Shop** in the task view.
4. Remove the subscription from the IT Shop shelves in **Remove assignments**.
5. Save the changes.

To remove a subscription from all IT Shop shelves

1. Select the category **Azure Active Directory | Subscriptions** (non role-based login).

   - OR -

   Select the category **Entitlements | Azure Active Directory subscriptions** (role-based subscription).
2. Select a subscription in the result list.
3. Select **Remove from all shelves (IT Shop)** in the task view.
4. Confirm the security prompt with **Yes**.
5. Click **OK**.

   The subscription is removed from all shelves by the One Identity Manager Service. All request and assignment requests for this subscription are canceled in the process.

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

Related Topics

- Editing Azure Active Directory Subscription Master Data on page 128
- Assigning Azure Active Directory Subscriptions to Departments, Cost Centers and Locations on page 131
- Assigning Azure Active Directory Subscriptions to Business Roles on page 132
- Assigning Azure Active Directory User Accounts directly to an Azure Active Directory Subscription on page 133
- Adding Azure Active Directory Subscriptions to System Roles on page 133

Additional Tasks for Managing Azure Active Directory Subscriptions

After you have entered the master data, you can apply different tasks to it. The task view contains different forms with which you can run the following tasks.

Overview of Azure Active Directory Subscriptions

To obtain an overview of a subscription

1. Select the category **Azure Active Directory | Subscriptions**.
2. Select a subscription in the result list.
3. Select **Azure Active Directory subscription** overview in the task view.

To obtain an overview of a service plan

1. Select the category **Azure Active Directory | Service plans**.
2. Select the service plan in the result list.
3. Select **Azure Active Directory service plan overview** in the task view.

To obtain an overview of a disabled service plan

1. Select the category **Azure Active Directory | Disabled service plans**.
2. Select the service plan in the result list.
3. Select **Disabled Azure Active Directory service plan overview**.

Effectiveness of Subscription Assignments

You can also apply the behavior described under Effectiveness of Group Memberships on page 112 to subscriptions. The effect of the assignments is mapped in the tables

AADUserHasSubSku and AADBaseTreeHasSubSku through the column XIsInEffect.

Prerequisites

- The configuration parameter "QER\Structures\Inherite\GroupExclusion" is set.
- Mutually exclusive subscriptions belong to the same tenant.

To exclude subscriptions

1. Select the category **Azure Active Directory | Subscriptions**.
2. Select a subscription in the result list.
3. Select **Exclude subscriptions**.
4. Assign subscriptions that are mutually exclusive to the selected one, in **Add assignments**.

   - OR -

   Remove subscriptions that are no longer mutually exclusive, in **Remove assignments**.
5. Save the changes.

Inheriting Azure Active Directory Subscriptions based on Categories

You can also apply the behavior described under Azure Active Directory Group Inheritance Based on Categories on page 114 to subscriptions.

To use inheritance through categories

- Define the categories in the tenant.
- Assign categories to user accounts through their master data.
- Assign categories to subscriptions through their master data.

Related Topics

- Specifying Categories for Inheriting Permissions on page 76
- General Master Data for an Azure Active Directory User Account on page 85
- Editing Azure Active Directory Subscription Master Data on page 128

Assigning Additional Properties to an Azure Active Directory Subscription

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

To specify extended properties for a subscription

1. Select the category **Azure Active Directory | Subscriptions**.
2. Select a subscription in the result list.
3. Select **Assign extended properties** in the task view.
4. Assign extended properties in **Add assignments**.

   - OR -

   Remove extended properties from **Remove assignments**.
5. Save the changes.

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

Disabled Azure Active Directory Service Plan

So called "disabled service plans" are mapped in the One Identity Manager to prevent users from using single service plans. Disabled service plans are created automatically after synchronizing the subscription in the One Identity Manager. Disabled service plans are requested through the IT Shop or assigned to users through departments, cost centers, locations, business roles or system roles.

Editing Master Data of Disabled Azure Active Directory Service Plans

To edit disabled service plan master data

1. Select the category **Azure Active Directory | Disabled service plans**.
2. Select the service plan in the result list.
3. Select **Change master data** in the task view.
4. Edit the service plan's master data.
5. Save the changes.

Table 46: Disabled Service Plan Master Data

Property	Description
Subscription	Name of the subscription.
Service plan	Name of the 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 service plans. To do this, disabled service plans and 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 114
- For more detailed information about preparing disabled service plans for requesting through the IT Shop, see the One Identity Manager IT Shop Administration Guide.

Assigning Disabled Azure Active Directory Service Plans to Azure Active Directory User Accounts

You can assign disabled service plans directly or indirectly to a user account. 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 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.

Prerequisites for indirect assignment of employees to user accounts:

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

- The user accounts are marked with the option **Groups can be inherited**.

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.

Detailed information about this topic

- Assigning Disabled Azure Active Directory Service Plans to Departments, Cost Centers and Locations on page 140
- Assigning Disabled Azure Active Directory Service Plans to Business Roles on page 141
- Assigning Azure Active Directory User Accounts directly to Azure Active Directory Service Plans on page 142
- Adding Disabled Azure Active Directory Service Plans to System Roles on page 143
- Adding Disabled Azure Active Directory Service Plans to the IT Shop on page 144

Assigning Disabled Azure Active Directory Service Plans to Departments, Cost Centers and Locations

Assign disabled 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. Select the category **Azure Active Directory | Disabled service plans**.
2. Select the service plan in the result list.
3. Select **Assign organizations**.
4. Assign organizations in **Add assignments**.
   - Assign departments on the **Departments** tab.
   - Assign locations on the **Locations** tab.
   - Assign cost centers on the **Cost center** tab.

   - OR -

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

To assign disabled service plans to a department, cost center or location (role-based login)

1. Select the category **Organizations | Departments**.

   - OR -

   Select the category **Organizations | Cost centers**.

   - OR -

   Select the category **Organizations | Locations**.
2. Select the department, cost center or location in the result list.
3. Select **Assign disabled Azure Active Directory service plan** in the task view.
4. Assign service plans in **Add assignments**.

   - OR -

   Remove service plans in **Remove assignments**.
5. Save the changes.

Related Topics

- Assigning Disabled Azure Active Directory Service Plans to Business Roles on page 141
- Assigning Azure Active Directory User Accounts directly to Azure Active Directory Service Plans on page 142
- Adding Disabled Azure Active Directory Service Plans to System Roles on page 143
- Adding Disabled Azure Active Directory Service Plans to the IT Shop on page 144
- One Identity Manager Users for Managing an Azure Active Directory System on page 9

Assigning Disabled Azure Active Directory Service Plans to Business Roles

Installed Modules: Business Roles Module

Assign disabled service plans to business roles to assign them to user accounts over these business roles.

To assign a disabled service plan to a business role (non role-based login)

1. Select the category **Azure Active Directory | Disabled service plans**.
2. Select the service plan in the result list.
3. Select **Assign business roles** in the task view.
4. Assign business roles in **Add assignments**.

- OR -

Remove business roles from **Remove assignments**.

5. Save the changes.

To assign disabled service plans to a business role (non role-based login)

1. Select the category **Business roles | <Role class>**.
2. Select the business role in the result list.
3. Select **Assign disabled Azure Active Directory service plan** in the task view.
4. Assign service plans in **Add assignments**.

   - OR -

   Remove service plans in **Remove assignments**.
5. Save the changes.

Related Topics

- Assigning Disabled Azure Active Directory Service Plans to Departments, Cost Centers and Locations on page 140
- Assigning Azure Active Directory User Accounts directly to Azure Active Directory Service Plans on page 142
- Adding Disabled Azure Active Directory Service Plans to System Roles on page 143
- Adding Disabled Azure Active Directory Service Plans to the IT Shop on page 144
- One Identity Manager Users for Managing an Azure Active Directory System on page 9

Assigning Azure Active Directory User Accounts directly to Azure Active Directory Service Plans

You can assign disabled service plans directly or indirectly to a user account. 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. If the employee has a user account in Azure Active Directory, disabled service plans belonging to roles are inherited by this user account.

To react quickly to special requests, you can assign disabled service plans directly to a user account.

To assign a disabled service plan directly to a user account

1. Select the category **Azure Active Directory | Disabled service plans**.
2. Select the service plan in the result list.
3. Select **Assign user accounts** in the task view.

4. Assign user accounts in **Add assignments**.

   - OR -

   Remove user accounts from **Remove assignments**.
5. Save the changes.

Related Topics

- Assigning Azure Active Directory Subscriptions directly to Azure Active Directory User Accounts on page 92
- Assigning Disabled Azure Active Directory Service Plans to Departments, Cost Centers and Locations on page 140
- Assigning Disabled Azure Active Directory Service Plans to Business Roles on page 141
- Adding Disabled Azure Active Directory Service Plans to System Roles on page 143
- Adding Disabled Azure Active Directory Service Plans to the IT Shop on page 144

Adding Disabled Azure Active Directory Service Plans to System Roles

Installed Modules: System Roles Module

Use this task to add disabled 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 service plans with the option **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 disabled service plan to system roles

1. Select the category **Azure Active Directory | Disabled service plans**.
2. Select the service plan in the result list.
3. Select **Assign system roles in the task view**.
4. Assign system roles in **Add assignments**.

   - OR -

   Remove system roles from **Remove assignments**.
5. Save the changes.

Related Topics

- Assigning Disabled Azure Active Directory Service Plans to Departments, Cost Centers and Locations on page 140
- Assigning Disabled Azure Active Directory Service Plans to Business Roles on page 141
- Assigning Azure Active Directory User Accounts directly to Azure Active Directory Service Plans on page 142
- Adding Disabled Azure Active Directory Service Plans to the IT Shop on page 144

Adding Disabled Azure Active Directory Service Plans to the IT Shop

A disabled service 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 option **IT Shop**.
- 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 option **Only for use in IT Shop**. 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. Select the category **Azure Active Directory | Disabled service plan** (non role-based login).

   - OR -

   Select the category **Entitlements | Disabled Azure Active Directory service plans** (role-based subscription).
2. Select the service plan in the result list.
3. Select **Add to IT Shop** in the task view.
4. Assign the disabled service plan to the IT Shop in **Add assignments**.
5. Save the changes.

To remove a disabled service plan from individual IT Shop shelves

1. Select the category **Azure Active Directory | Disabled service plan** (non role-based login).

   - OR -

Select the category **Entitlements | Disabled Azure Active Directory service plans** (role-based subscription).

2. Select the service plan in the result list.
3. Select **Add to IT Shop** in the task view.
4. Remove the disabled service plan from the IT Shop shelves in **Remove assignments**.
5. Save the changes.

To remove a disabled service plan from all IT Shop shelves

1. Select the category **Azure Active Directory | Disabled service plan** (non role-based login).

   - OR -

   Select the category **Entitlements | Disabled Azure Active Directory service plans** (role-based subscription).
2. Select the service plan in the result list.
3. Select **Remove from all shelves (IT Shop)** in the task view.
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 in the process.

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

Related Topics

- Assigning Disabled Azure Active Directory Service Plans to Departments, Cost Centers and Locations on page 140
- Assigning Disabled Azure Active Directory Service Plans to Business Roles on page 141
- Assigning Azure Active Directory User Accounts directly to Azure Active Directory Service Plans on page 142
- Adding Disabled Azure Active Directory Service Plans to System Roles on page 143

Additional Tasks for Managing Disabled Azure Active Directory Service Plans

After you have entered the master data, you can apply different tasks to it. The task view contains different forms with which you can run the following tasks.

Overview of Disabled Azure Active Directory Service Plans

To obtain an overview of a disabled service plan

1. Select the category **Azure Active Directory | Disabled service plans**.
2. Select the service plan in the result list.
3. Select **Disabled Azure Active Directory service plan overview**.

Effectiveness of Assignments of Disabled Service Plans

You can also apply the behavior described under Effectiveness of Group Memberships on page 112 for disabled service plans. The effect of the assignments is mapped in the tables `AADUserHasDeneiedService` and `AADBaseTreeHasDeniedService` through the column `XIsInEffect`.

Prerequisites

- The configuration parameter "QER\Structures\Inherite\GroupExclusion" is set.
- Mutually exclusive groups belong to the same tenant.

To exclude subscriptions

1. Select the category **Azure Active Directory | Disabled service plans**.
2. Select the disabled service plan from the result list.
3. Select **Exclude disabled service plans** in the task view.
4. Assign disabled service plans that are mutually exclusive to the selected one, in **Add assignments**.

   - OR -

   Remove disabled service plans that are no longer mutually exclusive, in **Remove assignments**.
5. Save the changes.

Inheritance of Disabled Azure Active Directory Service Plans Based on Categories

You can also apply the behavior described under Azure Active Directory Group Inheritance Based on Categories on page 114 for disabled service plans.

To use inheritance through categories

- Define the categories in the tenant.
- Assign categories to user accounts through their master data.
- Assign categories to disabled service plans through their master data.

Related Topics

- Specifying Categories for Inheriting Permissions on page 76
- General Master Data for an Azure Active Directory User Account on page 85
- Editing Master Data of Disabled Azure Active Directory Service Plans on page 138

Assigning Extended Properties to a disabled Azure Active Directory Service Plan

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

To specify extended properties for a disabled service plan

1. Select the category **Azure Active Directory | Disabled service plans**.
2. Select the service plan in the result list.
3. Select **Assign extended properties** in the task view.
4. Assign extended properties in **Add assignments**.

   - OR -

   Remove extended properties from **Remove assignments**.
5. Save the changes.

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

9

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 47: Reports for the Target System

Report	Description
Overview of all Assignments	This report finds all roles containing employees with at least one user account in the selected tenant.
Show orphaned user accounts	This report shows all user accounts in the tenant, which are not assigned to an employee. The report contains group memberships and risk assessment.
Show employees with multiple user accounts	This report shows all employees with more than one user account in the tenant. The report is a risk assessment.
Show unused user accounts	This report shows all the tenant's user accounts that have not been used in the last few months. The report contains group memberships and risk assessment.
Show entitlement drifts	This report shows all the groups in the tenant, which are the result of manual operations in the target system rather than provisioned through One Identity Manager.
Show user accounts with an above average number of system entitlements	This report contains all user accounts in the tenant with an above average number of group memberships.
Azure Active Directory user account and group administration	This report contains a summary of user account and group distribution in all tenants. You can find this report in the category **My One Identity Manager**.

Report	Description
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 category **My One Identity Manager**.

Overview of all Assignments

The report "Overview of all Assignments" is displayed for certain objects, for example, permissions, 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 employee who own the selected base object. In this case, direct as well as indirect base object assignments are included.

Example

- 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, all roles are determined in which there are employees with this group.
- If the report is created for a compliance rule, all roles are determined in which there are employees with 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 report **Overview of all assignments**.
- Use the **Used by button** in the report's toolbar to select the role class (department, location, business role or IT Shop structure) for which you determine if roles exist in which there are 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. In the report's toolbar, click to open the legend.
- 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 employee for tracking. This creates a new business role to which the employees are assigned.

Figure 3: Toolbar for Report "Overview of all assignments"

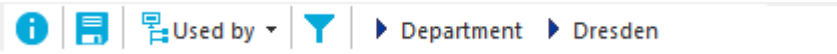


Table 48: Meaning of Icons in the Report Toolbar

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.

Appendix: Configuration Parameters for Managing Azure Active Directory

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

Table 49: Configuration parameter

Configuration parameter	Description
TargetSystem\AzureAD	Preprocessor relevant configuration parameter for controlling the database model components for the administration of the target system Azure Active Directory. If the parameter is set, the target system components are available. Changes to the parameter require recompiling the database.
TargetSystem\AzureAD\Accounts	This configuration parameter permits configuration of user account data.
TargetSystem\AzureAD\Accounts\InitialRandomPassword	This configuration parameter specifies whether a random generated password is issued 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	This configuration parameter specifies to which employee the email with the random generated password should be sent (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 configuration parameter "TargetSystem\AzureAD\DefaultAddress".
TargetSystem\AzureAD\Accounts\InitialRandomPassword\SendTo\MailTemplateAccountName	This configuration parameter contains the name of the mail template sent to inform users about their initial login data (name of the user

Configuration parameter	Description
	account). Use the mail template "Employee - new account created".
TargetSystem\AzureAD\Accounts\ InitialRandomPassword\SendTo\ MailTemplatePassword	This configuration parameter contains the name of the mail template sent to inform users about their initial login data (initial password). Use the mail template "Employee - initial password for new user account".
TargetSystem\AzureAD\Accounts\ MailTemplateDefaultValues	This configuration parameter contains the mail template used to send notifications if default IT operating data mapping values are used for automatically creating a user account. Use the mail template "Employee - new user account with default properties created".
TargetSystem\AzureAD\Accounts\ PrivilegedAccount	This configuration parameter allows configuration of settings for privileged Azure Active Directory user accounts.
TargetSystem\AzureAD\Accounts\ PrivilegedAccount\ AccountName_Postfix	This configuration parameter contains the postfix for formatting login names for privileged user accounts.
TargetSystem\AzureAD\Accounts\ PrivilegedAccount\ AccountName_Prefix	This configuration parameter contains the prefix for formatting login names for privileged user accounts.
TargetSystem\AzureAD\DefaultAddress	The configuration parameter contains the recipient's default email address for sending notifications about actions in the target system.
TargetSystem\AzureAD\ MaxFullsyncDuration	This configuration parameter contains the maximum runtime for synchronization. No recalculation of group memberships by the DBQueue Processor can take place during this time. If the maximum runtime is exceeded, group membership are recalculated.
TargetSystem\AzureAD\ PersonAutoDefault	This configuration parameter specifies the mode for automatic employee assignment for user accounts added to the database outside synchronization.
TargetSystem\AzureAD\ PersonAutoDisabledAccounts	This configuration parameters specifies whether employees are automatically assigned to disable user accounts. User accounts do not obtain an account definition.
TargetSystem\AzureAD\	This configuration parameter specifies the

Configuration parameter	Description
PersonAutoFullSync	mode for automatic employee assignment for user accounts added to or updated in the database through synchronization.
TargetSystem\AzureAD\ PersonExcludeList	List of all user accounts for which automatic employee assignment should not take place. Names given in a pipe (|) delimited list that is handled as a regular search pattern. Example: `ADMINISTRATOR`

Appendix: Default Project Template for Azure Active Directory

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

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

The template uses mappings for the following schema types.

Table 50: Mapping Azure Active Directory schema types to tables in the One Identity Manager schema.

Schema type in Azure Active Directory	Table in the One Identity Manager schema
DirectoryRole	AADDirectoryRole
Group	AADGroup
LicenseAssignments	AADUserHasSubSku
Organization	AADOrganization
ServicePlans	AADServicePlan
SubscribedSku	AADSubSku
User	AADUser
Verified Domain	AADVerifiedDomain

About us

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

Contacting us

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

Technical support resources

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

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

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

Index

A

C

D

E

I

J

L

M

N

O

P

S

T

U