One Identity Manager 8.1.2

Administration Guide for Connecting to Azure Active Directory

Copyright 2020 One Identity LLC.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of One Identity LLC .

The information in this document is provided in connection with One Identity products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of One Identity LLC products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, ONE IDENTITY ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ONE IDENTITY BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ONE IDENTITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. One Identity makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. One Identity does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

One Identity LLC.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (http://www.OneIdentity.com) for regional and international office information.

Patents

One Identity is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at http://www.OneIdentity.com/legal/patents.aspx.

Trademarks

One Identity and the One Identity logo are trademarks and registered trademarks of One Identity LLC. in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at www.OneIdentity.com/legal. All other trademarks are the property of their respective owners.

Legend

WARNING: A WARNING icon highlights a potential risk of bodily injury or property damage, for which industry-standard safety precautions are advised. This icon is often associated with electrical hazards related to hardware.

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

One Identity Manager Administration Guide for Connecting to Azure Active Directory
Updated - March 2020
Version - 8.1.2

Contents

Managing Azure Active Directory environments **8**
Architecture overview 8
One Identity Manager users for managing an Azure Active Directory environment 9

Setting up synchronization with an Azure Active Directory tenant **12**
Users and permissions for synchronizing with Azure Active Directory 13
Integrating One Identity Manager as enterprise application in Azure Active Directory 14
Setting up the synchronization server 15
Creating a synchronization project for initial synchronization of an Azure Active Directory tenant 18
Displaying synchronization results 24
Customizing the synchronization configuration 25
Configuring synchronization with Azure Active Directory tenants 26
Configuring synchronization of different Azure Active Directory tenants 27
Updating schemas 27
Post-processing outstanding objects 28
Configuring the provisioning of memberships 31
Accelerating provisioning and single object synchronization 32
Help for the analysis of synchronization issues 33
Deactivating synchronization 33

Basic data for managing an Azure Active Directory environment **35**
Account definitions for Azure Active Directory user accounts 36
Creating account definitions 37
Master data for an account definition 37
Creating manage levels 40
Master data for manage levels 41
Creating mapping rules for IT operating data 42
Entering IT operating data 44
Modify IT operating data 45
Assigning account definitions to employees 46
Assigning account definitions to departments, cost centers, and locations 47
Assigning an account definition to business roles 48

Assigning account definitions to all employees 49
Assigning account definitions directly to employees 49
Assigning account definitions to system roles 50
Adding account definitions to the IT Shop 51
Assigning account definitions to a target system 52
Deleting account definitions 53
Password policies for Azure Active Directory user accounts 55
Predefined password policies 55
Using password policies 57
Editing password policies 59
General master data for password policies 59
Policy settings 60
Character classes for passwords 61
Custom scripts for password requirements 62
Script for checking passwords 62
Script for generating a password 63
Password exclusion list 65
Checking passwords 65
Testing password generation 65
Initial password for new Azure Active Directory user accounts 66
Email notifications about login data 66
Target system managers 67
Editing a server 70
Master data for a Job server 71
Specifying server functions 73
Azure Active Directory core directories 75
Azure Active Directory tenant 75
General master data for Azure Active Directory tenants 76
Information about local Active Directory 78
Defining categories for the inheritance of entitlements 78
How to edit a synchronization project 79
Azure Active Directory domains 79
Azure Active Directory user accounts 81
Linking user accounts to employees 81

Supported user account types 82
Default user accounts 84
Administrative user accounts 85
Providing administrative user accounts for one employee 85
Providing administrative user accounts for several employees 86
Privileged user accounts 87
Editing master data for Azure Active Directory user accounts 88
General master data of Azure Active Directory user accounts 90
Contact data for an Azure Active Directory user account 92
Organizational data for an Azure Active Directory user account 93
Information about the local Active Directory user account 94
Additional tasks for managing Azure Active Directory user accounts 94
The Azure Active Directory user accounts overview 95
Changing the manage level of Azure Active Directory user accounts 95
Assigning Azure Active Directory groups directly to Azure Active Directory user accounts 96
Assigning Azure Active Directory administrator roles directly to Azure Active Directory user accounts 96
Assigning Azure Active Directory subscriptions directly to Azure Active Directory user accounts 97
Assigning disabled Azure Active Directory service plans directly to Azure Active Directory user accounts 98
Assigning extended properties to Azure Active Directory user accounts 98
Automatic assignment of employees to Azure Active Directory user accounts 99
Editing search criteria for automatic employee assignment 101
Disabling Azure Active Directory user accounts 103
Deleting and restoring Azure Active Directory user accounts 104

Azure Active Directory groups 106

Editing master data for Azure Active Directory groups 107
General master data for an Azure Active Directory group 107
Information about local Active Directory groups 109
Assigning Azure Active Directory groups to Azure Active Directory user accounts 109
Assigning Azure Active Directory groups to departments, cost centers, and locations 110
Assigning Azure Active Directory groups to business roles 111
Assigning Azure Active Directory user accounts directly to Azure Active Directory 112

groups
Adding Azure Active Directory groups to system roles 113
Adding Azure Active Directory groups to the IT Shop 114
Additional tasks for managing Azure Active Directory groups 116
The Azure Active Directory group overview 116
Adding Azure Active Directory groups to Azure Active Directory groups 116
Effectiveness of group memberships 117
Azure Active Directory group inheritance based on categories 119
Assigning owners to Azure Active Directory groups 121
Assigning extended properties to Azure Active Directory groups 121
Deleting Azure Active Directory groups 122
Azure Active Directory administrator roles 123
Editing master data of Azure Active Directory administrator roles 123
Assigning Azure Active Directory administrator roles to Azure Active Directory user accounts 125
Assigning Azure Active Directory administrator roles to departments, cost centers, and locations 125
Assigning Azure Active Directory administrator roles to business roles 127
Assigning Azure Active Directory user accounts directly to Azure Active Directory administrator roles 128
Adding Azure Active Directory administrator roles to system roles 128
Adding Azure Active Directory administrator roles in the IT Shop 129
Additional tasks for managing Azure Active Directory administrator roles 131
The Azure Active Directory administrator roles overview 131
Azure Active Directory administrator role inheritance based on categories 131
Assigning extended properties to an Azure Active Directory administrator role 132
Azure Active Directory subscriptions and service plans 133
Azure Active Directory subscriptions 133
Editing Azure Active Directory subscription master data 134
Assigning Azure Active Directory subscriptions to Azure Active Directory user accounts 135
Assigning Azure Active Directory subscriptions to departments, cost centers, and locations 136
Assigning Azure Active Directory subscriptions to business roles 137
Assigning Azure Active Directory user accounts directly to an Azure Active Directory subscription 138

Adding Azure Active Directory subscriptions to system roles 139
Adding Azure Active Directory subscriptions to the IT Shop 140
Additional tasks for managing Azure Active Directory subscriptions 141
The Azure Active Directory subscriptions overview 141
Effectiveness of subscription assignments 142
Inheriting Azure Active Directory subscriptions based on categories 142
Assigning additional properties to an Azure Active Directory subscription 143
Disabled Azure Active Directory service plans 143
Editing master data of disabled Azure Active Directory service plans 144
Assigning disabled Azure Active Directory service plans to Azure Active Directory user accounts 145
Assigning disabled Azure Active Directory service plans directly to departments, cost centers, and locations 145
Assigning disabled Azure Active Directory service plans to business roles 147
Assigning Azure Active Directory user accounts directly to Azure Active Directory service plans 148
Adding disabled Azure Active Directory service plans to system roles 149
Adding disabled Azure Active Directory service plans to the IT Shop 149
Additional tasks for managing disabled Azure Active Directory service plans 151
The disabled Azure Active Directory service plans overview 151
Effectiveness of assignments of disabled service plans 151
Inheritance of disabled Azure Active Directory service plans based on categories 152
Assigning extended properties to a disabled Azure Active Directory service plan .152

Reports about Azure Active Directory objects 154
Overview of all assignments 155

Appendix: Configuration parameters for managing an Azure Active Directory environment 157

Appendix: Default project template for Azure Active Directory 160

About us 161
Contacting us 161
Technical support resources 161

Index 162

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, One Identity Manager maps subscriptions, service plans, groups, and administration roles. This makes it possible to use Identity and Access Governance processes, including attestation, Identity Audit, user account management and system entitlements, IT Shop, or report subscriptions for Azure Active Directory tenants.

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

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

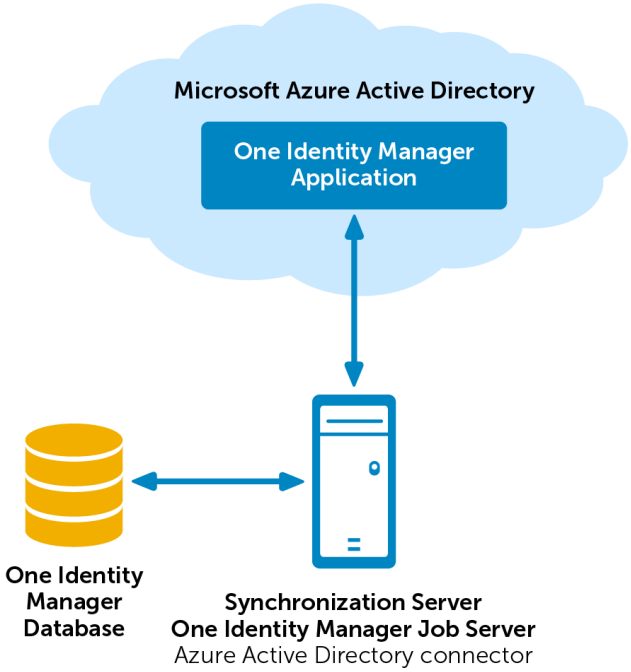
For more information about the Azure Active Directory structure, see the *Azure Active Directory documentation* from Microsoft.

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 environment

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

Table 1: Users

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

User	Tasks
	• Authorize other employees to be target system administrators. • Do not assume any administrative tasks within the target system.
Target system managers	Target system managers must be assigned to the **Target systems | Azure Active Directory** application role or a child application role. Users with this application role: • Assume administrative tasks for the target system. • Create, change, or delete target system objects like user accounts or groups. • Edit password policies for the target system. • Prepare groups to add to the IT Shop. • Can add employees who have an other identity than the **Primary identity**. • Configure synchronization in the Synchronization Editor and define the mapping for comparing target systems and One Identity Manager. • Edit the synchronization's target system types and outstanding objects. • Authorize other employees within their area of responsibility as target system managers and create child application roles if required.
One Identity Manager administrators	• Create customized permissions groups for application roles for role-based login to administration tools in the Designer as required. • Create system users and permissions groups for non role-based login to administration tools in the Designer as required. • Enable or disable additional configuration parameters in the Designer as required. • Create custom processes in the Designer as required. • Create and configure schedules as required. • Create and configure password policies as required.
Administrators for the IT Shop	Administrators must be assigned to the **Request & Fulfillment | IT Shop | Administrators** application role. Users with this application role:

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

Setting up synchronization with an Azure Active Directory tenant

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

1. Prepare a user account in the Azure Active Directory tenant with sufficient permissions for synchronization.
2. 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 **TargetSystem | AzureAD** configuration parameter is set.
    - In the Designer, check if the configuration parameter is set. Otherwise, set the configuration parameter and compile the database.
    - Other configuration parameters are installed when the module is installed. Check the configuration parameters and modify them as necessary to suit your requirements.
4. Install and configure a synchronization server and declare the server as a Job server in One Identity Manager.
5. Create a synchronization project with the Synchronization Editor.

NOTE: There is no support for synchronizing Microsoft Azure China using the Azure Active Directory connector.

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

Detailed information about this topic

- Users and permissions for synchronizing with Azure Active Directory on page 13
- Integrating One Identity Manager as enterprise application in Azure Active Directory 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 18
- Deactivating synchronization on page 33

- Customizing the synchronization configuration on page 25
- Configuration parameters for managing an Azure Active Directory environment on page 157
- Default project template for Azure Active Directory on page 160

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 **Global administrator** organization role
One Identity Manager Service user account	The user account for One Identity Manager Service requires permissions to carry out operations at file level. For example, assigning permissions and creating and editing directories and files. The user account must belong to the **Domain users** group. The user account must have the **Login as a service** extended user permissions. The user account requires access permissions to the internal web service. NOTE: If One Identity Manager Service runs under the network service (**NT Authority\NetworkService**), you can issue access permissions for the internal web service with the following command line call: `netsh http add urlacl url=http://<IP address>:<port number>/ user="NT AUTHORITY\NETWORKSERVICE"` The user account needs full access to the One Identity Manager Service installation directory in order to automatically update One Identity Manager. In the default installation, One Identity Manager is installed under: • `%ProgramFiles(x86)%\One Identity` (on 32-bit operating

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

Integrating One Identity Manager as enterprise application in Azure Active Directory

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 One Identity Manager tenants using the Azure Active Directory application.

NOTE: An application ID is created when you add One Identity Manager as an application in Azure Active Directory. You need this application 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 One Identity Manager as an application in Azure Active Directory

1. Log in to the Microsoft Azure Management Portal (https://manage.windowsazure.com) and create a new One Identity Manager application 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 18

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

  The following versions are supported:
  - Windows Server 2008 R2 (non-Itanium based 64-bit) service pack 1 or later
  - Windows Server 2012
  - Windows Server 2012 R2
  - Windows Server 2016
  - Windows Server 2019
- Microsoft .NET Framework Version 4.7.2 or later

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

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

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

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

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

- Sets up a Job server.
- Specifies machine roles and server function for the Job server.
- Remotely installs One Identity Manager Service components corresponding to the machine roles.
- Configures the One Identity Manager Service.
- Starts the One Identity Manager Service.

NOTE: To generate processes for the Job server, you need the provider, connection parameters, and the authentication data. By default, this information is determined from the database connection data. If the Job server runs through an application server, you must configure extra connection data in the Designer. For detailed information about setting up Job servers, see the *One Identity Manager Configuration Guide*.

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

To remotely install the One Identity Manager Service, you must have an administrative workstation on which the One Identity Manager components are installed. For detailed information about installing a workstation, see the *One Identity Manager Installation Guide*.

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

1. Start the Server Installer program on your administrative workstation.
2. On the **Database connection** page, enter the valid connection credentials for the One Identity Manager database.
3. On the **Server properties** page, specify the server on which you want to install the

One Identity Manager Service.

a. Select a Job server from the **Server** menu.

   - OR -

   To create a new Job server, click **Add**.

b. Enter the following data for the Job server.

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

     Syntax:

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

   NOTE: You can use the **Extended** option to make changes to other properties for the Job server. You can also edit the properties later with the Designer.

4. On the **Machine roles** page, select **Azure Active Directory**.
5. On the **Server functions** page, select **Azure Active Directory connector (via Microsoft Graph)**.
6. On the **Service Settings** page, enter the connection data and check the One Identity Manager Service configuration.

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

   - For a direct connection to the database:
     a. Select **Process collection | sqlprovider**.
     b. Click the **Connection parameter** entry, then click the **Edit** button.
     c. Enter the connection data for the One Identity Manager database.
   - For a connection to the application server:
     a. Select **Process collection**, click the **Insert** button and select **AppServerJobProvider**.
     b. Click the **Connection parameter** entry, then click the **Edit** button.
     c. Enter the connection data for the application server.
     d. Click the **Authentication data** entry and click the **Edit** button.
     e. Select the authentication module. Depending on the authentication module, other data may be required, such as user and password. For

detailed information about the One Identity Manager authentication modules, see the *One Identity Manager Authorization and Authentication Guide*.

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

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

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

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

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 3: Information required to set up a synchronization project

Data	Explanation
Application ID	Application ID created when One Identity Manager is added as the tenant's application.
Login domain	Name of the domain for logging in to 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 require the generated key. NOTE: The key is only valid for a limited period and must be renewed when it expires.
Synchronization server for Azure Active Directory	All One Identity Manager Service actions are 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 4: Additional properties for the Job server

Property	Value
Server function	Azure Active Directory connector (using Microsoft Graph)
Machine role	Server | Job server | Azure Active Directory

For more information, see Setting up the synchronization server on page 15.

Data	Explanation
One Identity Manager database connection data	• Database server • Database • SQL Server login and password • Specifies whether integrated Windows authentication is used. This type of authentication is not recommended. If you decide to use it anyway, ensure that your environment supports Windows authentication.
Remote connection server	To configure synchronization with a target system, One Identity Manager must load the data from the target system. One Identity Manager communicates directly with the target system to do this. Sometimes direct access from the workstation, on which the Synchronization Editor is installed, is not possible. For example, because of the firewall configuration or the workstation does not fulfill the necessary hardware and software requirements. If direct access is not possible from the workstation, you can set up a remote connection. The remote connection server and the workstation must be in the same Active Directory domain. Remote connection server configuration: • One Identity Manager Service is started • **RemoteConnectPlugin** is installed • Azure Active Directory connector is installed The remote connection server must be declared as a Job server in One Identity Manager. The Job server name is required. TIP: The remote connection server requires the same configuration as the synchronization server (with regard to the installed software and entitlements). Use the synchronization as remote connection server at the same time, by simply installing the `RemoteConnectPlugin` as well. For more detailed information about setting up a remote connection, see the *One Identity Manager Target System Synchronization Reference Guide*.

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

- Executed in default mode
- Started from the Launchpad

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

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

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

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

2. Select the **Target system type Azure Active Directory** entry and click **Start**.

   This starts the Synchronization Editor's project wizard.

3. On the **System access** page, specify how One Identity Manager can access the target system.

   - If access is possible from the workstation on which you started the Synchronization Editor, do not change any settings.
   - If access is not possible from the workstation on which you started the Synchronization Editor, you can set up a remote connection.

     Enable the **Connect using remote connection server** option and select the server to be used for the connection under **Job server**.

4. On the **Azure Active Directory tenant** page, enter the basic data for your tenant.

   - Under **Client ID**, enter the application ID that was generated in the integration of One Identity Manager as an application of the tenant.
   - Under **Login domain**, enter the base domain or a verified domain of your tenant.

5. On the **Authentication** page, select the type of login and enter the required login data.

   a. If you have integrated One Identity Manager as a native client application in your tenant, select **Authenticate as a native client application** and enter the user account and password for logging in to the target system.

   b. If you have integrated One Identity Manager as a web application in your tenant, select the **Authenticate as a web application** option and enter the key that was generated during registration of One Identity Manager as an application of the tenant.

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

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

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

Table 5: Specify target system access

Option	Meaning
Read-only access to target system.	Specifies that a synchronization workflow is only to be set up for the initial loading of the target system into the One Identity Manager database. The synchronization workflow has the following characteristics: • Synchronization is in the direction of **One Identity Manager**. • Processing methods in the synchronization steps are only defined for synchronization in the direction of **One Identity Manager**.
Read/write access to target system. Provisioning available.	Specifies whether a provisioning workflow is to be set up in addition to the synchronization workflow for the initial loading of the target system. The provisioning workflow displays the following characteristics: • Synchronization is in the direction of the **Target system**. • Processing methods are only defined in the synchronization steps for synchronization in the direction of the **Target system**. • Synchronization steps are only created for such schema classes whose schema types have write access.

9. On the **Synchronization server** page, select a synchronization server to execute synchronization.

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

   a. Click to add a new Job server.

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

   c. Click **OK**.

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

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

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

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

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

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

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

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

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

NOTE:

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

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

To select user accounts through account definitions

1. Create an account definition.
2. Assign an account definition to the tenant.
3. Assign a user account in the **Linked** state to the account definition. The account definition's default manage level is applied to the user account.
    a. In the Manager, select the **Azure Active Directory | User accounts | Linked but not configured | <Tenant>** category.
    b. Select the **Assign account definition to linked accounts** task.
    c. In the **Account definition** menu, select the account definition.
    d. Select the user accounts that contain the account definition.
    e. Save the changes.

Related topics

- Integrating One Identity Manager as enterprise application in Azure Active Directory on page 14
- Setting up the synchronization server on page 15
- Users and permissions for synchronizing with Azure Active Directory on page 13
- Displaying synchronization results on page 24
- Customizing the synchronization configuration on page 25

- Default project template for Azure Active Directory on page 160
- Account definitions for Azure Active Directory user accounts on page 36
- Automatic assignment of employees to Azure Active Directory user accounts on page 99

Displaying synchronization results

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

To display a synchronization log

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

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

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

To display a provisioning log

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

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

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

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

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

Synchronization logs are stored for a fixed length of time.

To modify the retention period for synchronization logs

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

Customizing the synchronization configuration

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

You must customize the synchronization configuration to be able to regularly compare the database with the Azure Active Directory environment and to synchronize changes.

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

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

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

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

Detailed information about this topic

- Configuring synchronization with Azure Active Directory tenants on page 26
- Configuring synchronization of different Azure Active Directory tenants on page 27
- Updating schemas on page 27

Configuring synchronization with Azure Active Directory tenants

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

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

Related topics

- Configuring synchronization of different Azure Active Directory tenants on page 27

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 tenant. Use the wizard to attach a base object.
    - In the wizard, select the Azure Active Directory connector and declare the connection parameters. The connection parameters are saved in a special variable set.

      A start up configuration is created that uses the newly created variable set.
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 26

Updating schemas

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

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

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

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

To update a system connection schema

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

   - OR -

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

   This reloads the schema data.

To edit a mapping

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

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

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

Post-processing outstanding objects

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

Outstanding objects:

- Cannot be edited in One Identity Manager.
- Are ignored by subsequent synchronizations.
- Are ignored by inheritance calculations.

This means, all memberships and assignments remain intact until the outstanding objects have been processed.

Start target system synchronization to do this.

To post-process outstanding objects

1. In the Manager, select the **Azure Active Directory | Target system synchronization: Azure Active Directory** category.

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

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

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

   - The synchronization log has already been deleted.

     - OR -

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

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

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

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

   TIP:

   To display object properties of an outstanding object

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

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

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

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

Table 6: Methods for handling outstanding objects

Icon	Method	Description
	Delete	The object is immediately deleted from the One Identity Manager database. Deferred deletion is not taken into account. The **Outstanding** label is removed from the object.

Icon	Method	Description
		Indirect memberships cannot be deleted.
	Publish	The object is added to the target system. The **Outstanding** label is removed from the object. The method triggers the `HandleOutstanding` event. This runs a target system specific process that triggers the provisioning process for the object. Prerequisites: • The table containing the object can be published. • The target system connector has write access to the target system.
	Reset	The **Outstanding** label is removed for the object.

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

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

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

To disable bulk processing

- In the form's toolbar, click to disable bulk processing.

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

To add custom tables to target system synchronization

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

NOTE: The target system connector must have write access to the target system in order to publish outstanding objects that are being post-processed. That means, the **Connection is read-only** option must not be set for the target system connection.

Configuring the provisioning of memberships

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

- Memberships are saved in the target system as an object property in list form (Example: List of user accounts in the `Members` property 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 one membership in One Identity Manager changes, by default, the complete list of members is transferred to the target system. Therefore, memberships that were previously added to the target system are removed in the process and previously deleted memberships are added again.

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

To allow separate provisioning of memberships

1. In the Manager, select the **Azure Active Directory | Basic configuration data | Target system types** category.
2. Select **Azure Active Directory** in the result list.
3. Select the **Configure tables for publishing** task.
4. Select the assignment tables that you want to set up for single provisioning. Multi-select is possible.
    - This option can only be enabled for assignment tables that have a base table with `XDateSubItem` or `CCC_XDateSubItem` column.
    - Assignment tables that are grouped together in a virtual schema property in the mapping must be marked 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 One Identity Manager are saved in a separate table. During modification provisioning, the members list in the target system is compared to the entries in this table. This means that only modified memberships are provisioned and not the entire members list.

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

You can restrict single provisioning of memberships with a condition. Once single provisioning has been disabled for a table, the condition is deleted. Tables that have had the condition deleted or edited are marked with the following icon:  . You can restore the original condition at any time.

To restore the default condition

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

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

Accelerating provisioning and single object synchronization

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

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

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

To configure load balancing

1. Configure the server and declare it as a Job server in One Identity Manager.
   - Assign the **Azure Active Directory connector** server function to the Job server.

   All Job servers must access the same Azure Active Directory tenant as the synchronization server for the respective base object.
2. In the Synchronization Editor, assign a custom server function to the base object.

   This server function is used to identify all the Job servers being used for load balancing.

   If there is no custom server function for the base object, create a new one.

   For more information about editing base objects, see the *One Identity Manager Target System Synchronization Reference Guide*.
3. In the Manager, assign this server function to all the Job servers that will be

processing provisioning and single object synchronization for the base object.

Only select those Job servers that have the same configuration as the base object's synchronization server.

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

To use the synchronization server without load balancing.

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

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

Detailed information about this topic

- Editing a server on page 70

Help for the analysis of synchronization issues

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

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

To generate a synchronization analysis report

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

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

Deactivating synchronization

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

To prevent regular synchronization

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

   Now you can only start synchronization manually.

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

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

To deactivate the synchronization project

1. Open the synchronization project in the Synchronization Editor.
2. Select the **General** view on the start page.
3. Click **Deactivate project**.

Related topics

- Creating a synchronization project for initial synchronization of an Azure Active Directory tenant on page 18

3

Basic data for managing an Azure Active Directory environment

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

- Configuration parameter

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

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

  For more information, see Configuration parameters for managing an Azure Active Directory environment on page 157.

- Account definitions

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

  For more information, see Account definitions for Azure Active Directory user accounts on page 36.

- Password policy

  One Identity Manager provides you with support for creating complex password policies, for example, for system user passwords, the employees' central password as well as passwords for individual target systems. Password polices apply not only when the user enters a password but also when random passwords are generated.

  Predefined password policies are supplied with the default installation that you can use or customize if required. You can also define your own password policies.

For more information, see Password policies for Azure Active Directory user accounts on page 55.

- 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 66.

- Email notifications about credentials

  When a new user account is created, the login data are sent 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 66.

- 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 28.

- Target system managers

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

  Define additional application roles if you want to limit the edit permissions for target system managers to individual tenants. The application roles must be added under the default application role.

  For more information, see Target system managers on page 67.

- 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.

  For more information, see Editing a server on page 70.

Account definitions for Azure Active Directory user accounts

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

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

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

The following steps are required to implement an account definition:

- Creating account definitions
- Creating manage levels
- Creating mapping rules for IT operating data
- Entering IT operating data
- Assigning account definitions to employees
- Assigning account definitions to a target system

Creating account definitions

To create a new account definition

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

   -OR-

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

Detailed information about this topic

- Master data for an account definition on page 37

Master data for an account definition

Enter the following data for an account definition:

Table 7: Master data for an account definition

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

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

Creating manage levels

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

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

One Identity Manager supplies a default configuration for manage levels:

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

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

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

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

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

To assign manage levels to an account definition

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

4. In the **Add assignments** pane, assign the manage levels.

   - OR -

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

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

To edit a manage level

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

   - OR -

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

Related topics

- Master data for manage levels on page 41

Master data for manage levels

Enter the following data for a manage level.

Table 8: Master data for manage levels

Property	Description
Manage level	Name of the manage level.
Description	Text field for additional explanation.
IT operating data overwrites	Specifies whether user account data formatted from IT operating data is automatically updated. Permitted values are: • **Never**: Data is not updated. • **Always**: Data is always updated. • **Only initially**: Data is only determined at the start.
Retain groups if temporarily disabled	Specifies whether user accounts of temporarily disabled employees retain their group memberships.
Lock user accounts if temporarily disabled	Specifies whether user accounts of temporarily disabled employees are locked.

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

Creating mapping rules for IT operating data

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

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

- Groups can be inherited
- Identity
- Privileged user account
- Change password at next login

To create a mapping rule for IT operating data

1. In the Manager, select the **Azure Active Directory | Basic configuration data | Account definitions | Account definitions** category.
2. Select an account definition in the result list.

3. Select the **Edit IT operating data mapping** task and enter the following data.

Table 9: Mapping rule for IT operating data

Property	Description
Column	User account property for which the value is set. In the menu, you can select the columns that use the `TSB_ITDataFromOrg` script in their template. For detailed information, see the *One Identity Manager Target System Base Module Administration Guide*.
Source	Specifies which roles to use in order to find the user account properties. You have the following options: • Primary department • Primary location • Primary cost center • Primary business roles NOTE: Only use the primary business role if the Business Roles Module is installed. • Empty If you select a role, you must specify a default value and set the **Always use default value** option.
Default value	Default value of the property for an employee's user account if the value is not determined dynamically from the IT operating data.
Always use default value	Specifies whether user account properties are always filled with the default value. IT operating data is not determined dynamically from a role.
Notify when applying the standard	Specifies whether email notification to a defined mailbox is sent when the default value is used. The **Employee - new user account with default properties created** mail template is used. To change the mail template, adjust the **TargetSystem | AzureAD | Accounts | MailTemplateDefaultValues** configuration parameter.

4. Save the changes.

Related topics

- Entering IT operating data on page 44

Entering IT operating data

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

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

Example

Normally, each employee in department A obtains a default user account in the 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 "Department" property in the IT operating data formatting rule for the account definitions A and B in order to determine the valid IT operating data.

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

To define IT operating data

1. In the Manager, select the role in the **Organizations** or **Business roles** category.
2. Select the **Edit IT operating data** task.

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

Table 10: IT operating data

Property	Description
Effects on	IT operating data application scope. The IT operating data can be used for a target system or a defined account definition. To specify an application scope a. Click → next to the field. b. Under **Table**, select the table that maps the target system for select the `TSBAccountDef` table or an account definition. c. Select the specific target system or account definition under **Effects on**. d. Click **OK**.
Column	User account property for which the value is set. In the menu, you can select the columns that use the `TSB_ITDataFromOrg` script in their template. For detailed information, see the *One Identity Manager Target System Base Module Administration Guide*.
Value	Concrete value which is assigned to the user account property.

4. Save the changes.

Related topics

- Creating mapping rules for IT operating data on page 42

Modify IT operating data

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

Prerequisites

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

  - OR -

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

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

To execute the template

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

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

Old value:	Current value of the object property.
New value:	Value that the object property would have following modification of the IT operating data.
Selection:	Specifies whether or not the new value is transferred to the user account.

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

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

Assigning account definitions to employees

Account definitions are assigned to company employees.

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

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

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

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

Prerequisites for indirect assignment of account definitions to employees

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

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

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

Detailed information about this topic

- Assigning account definitions to departments, cost centers, and locations on page 47
- Assigning an account definition to business roles on page 48
- Assigning account definitions to all employees on page 49
- Assigning account definitions directly to employees on page 49
- Assigning account definitions to system roles on page 50
- Adding account definitions to the IT Shop on page 51

Assigning account definitions to departments, cost centers, and locations

To add account definitions to hierarchical roles

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

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

To remove an assignment

- Select the organization and double-click ✓.

5. Save the changes.

Related topics

- Assigning an account definition to business roles on page 48
- Assigning account definitions to all employees on page 49
- Assigning account definitions directly to employees on page 49
- Assigning account definitions to system roles on page 50
- Adding account definitions to the IT Shop on page 51

Assigning an account definition to business roles

Installed modules: Business Roles Module

To add account definitions to hierarchical roles

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

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

   To remove an assignment

   - Select the business role and double-click ✓.

5. Save the changes.

Related topics

- Assigning account definitions to departments, cost centers, and locations on page 47
- Assigning account definitions to all employees on page 49
- Assigning account definitions directly to employees on page 49
- Assigning account definitions to system roles on page 50
- Adding account definitions to the IT Shop on page 51

Assigning account definitions to all employees

To assign an account definition to all employees

1. In the Manager, select the **Azure Active Directory | Basic configuration data | Account definitions | Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Change master data** task.
4. On the **General** tab, enable the **Automatic assignment to employees** option.

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

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

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

Related topics

- Assigning account definitions to departments, cost centers, and locations on page 47
- Assigning an account definition to business roles on page 48
- Assigning account definitions directly to employees on page 49
- Assigning account definitions to system roles on page 50
- Adding account definitions to the IT Shop on page 51

Assigning account definitions directly to employees

To assign an account definition directly to employees

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

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

To remove an assignment

- Select the employee and double-click .

5. Save the changes.

Related topics

- Assigning account definitions to departments, cost centers, and locations on page 47
- Assigning an account definition to business roles on page 48
- Assigning account definitions to all employees on page 49
- Assigning account definitions to system roles on page 50
- Adding account definitions to the IT Shop on page 51

Assigning account definitions to system roles

Installed modules: System Roles Module

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

To add account definitions to a system role

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

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

   To remove an assignment

   - Select the system role and double-click .

5. Save the changes.

Related topics

- Assigning account definitions to departments, cost centers, and locations on page 47
- Assigning an account definition to business roles on page 48
- Assigning account definitions to all employees on page 49
- Assigning account definitions directly to employees on page 49
- Adding account definitions to the IT Shop on page 51

Adding account definitions to the IT Shop

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

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

  TIP: In the Web Portal, all products that can be requested are grouped together by service category. To make the account definition easier to find in the Web Portal, assign a service category to the service item.
- If the account definition is only assigned to employees using IT Shop assignments, you must also set the **Only for use in IT Shop** option. Direct assignment to hierarchical roles may not be possible.

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

To add an account definition to the IT Shop

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

   - OR -

   In the Manager, select the **Entitlements | Account definitions** (role-based login) category.
2. Select an account definition in the result list.
3. Select the **Add to IT Shop** task.
4. In the **Add assignments** pane, assign the account definitions to the IT Shop shelves.
5. Save the changes.

To remove an account definition from individual IT Shop shelves

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

   - OR -

   In the Manager, select **Entitlements | Account definitions** (role-based login) category.
2. Select an account definition in the result list.
3. Select the **Add to IT Shop** task.
4. In the **Remove assignments** pane, remove the account definitions from the IT Shop shelves.
5. Save the changes.

To remove an account definition from all IT Shop shelves

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

   - OR -

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

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

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

Related topics

- Master data for an account definition on page 37
- Assigning account definitions to departments, cost centers, and locations on page 47
- Assigning an account definition to business roles on page 48
- Assigning account definitions to all employees on page 49
- Assigning account definitions directly to employees on page 49
- Assigning account definitions to system roles on page 50

Assigning account definitions to a target system

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

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

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

To assign the account definition to a target system

1. In the Manager, select the tenant in the **Azure Active Directory | Tenants** category.
2. Select the **Change master data** task.
3. From the **Account definition (initial)** menu, select the account definition for user accounts.
4. Save the changes.

Detailed information about this topic

- Automatic assignment of employees to Azure Active Directory user accounts on page 99

Deleting account definitions

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

To delete an account definition

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

c. Select the **Assign organizations** task.

d. In the **Remove assignments** pane, remove the relevant departments, cost centers, and locations.

e. Save the changes.

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

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

b. Select an account definition in the result list.

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

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

d. Save the changes.

5. If the account definition was requested through the IT Shop, it must be canceled and removed from all IT Shop shelves.

For more detailed information about unsubscribing requests, see the *One Identity Manager Web Portal User Guide*.

To remove an account definition from all IT Shop shelves

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

- OR -

In the Manager, select **Entitlements | Account definitions** (role-based login) category.

b. Select an account definition in the result list.

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

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

e. Click **OK**.

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

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

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

b. Select an account definition in the result list.

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

d. From the **Required account definition** menu, remove the account definition.

e. Save the changes.

7. Remove the account definition's assignments to target systems.
    a. In the Manager, select the tenant in the **Azure Active Directory | Tenants** category.
    b. Select the **Change master data** task.
    c. On the **General** tab, remove the assigned account definitions.
    d. Save the changes.
8. Delete the account definition.
    a. In the Manager, select the **Azure Active Directory | Basic configuration data | Account definitions | Account definitions** category.
    b. Select an account definition in the result list.
    c. Click to delete an account definition.

Password policies for Azure Active Directory user accounts

One Identity Manager provides you with support for creating complex password policies, for example, for system user passwords, the employees' central password as well as passwords for individual target systems. Password polices apply not only when the user enters a password but also when random passwords are generated.

Predefined password policies are supplied with the default installation that you can use or customize if required. You can also define your own password policies.

Detailed information about this topic

- Predefined password policies on page 55
- Using password policies on page 57
- Editing password policies on page 59
- Custom scripts for password requirements on page 62
- Password exclusion list on page 65
- Checking passwords on page 65
- Testing password generation on page 65

Predefined password policies

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

Password for logging in to One Identity Manager

The **One Identity Manager password policy** is applied for logging in to One Identity Manager. This password policy defines the settings for the system user passwords (`DialogUser.Password` and `Person.DialogUserPassword`) as well as the passcode for a one time log in on the Web Portal (`Person.Passcode`).

NOTE: The **One Identity Manager password policy** is marked as the default policy. This password policy is applied if no other password policy can be found for employees, user accounts, or system users.

For detailed information about password policies for employees, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Password policy for forming employees' central passwords

An employee's central password is formed from the target system specific user accounts by respective configuration. The **Employee central password policy** defines the settings for the (`Person.CentralPassword`) central password. Members of the **Identity Management | Employees | Administrators** application role can adjust this password policy.

IMPORTANT: Ensure that the **Employee central password policy** does not violate the target system-specific requirements for passwords.

For detailed information about password policies for employees, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Password policies for user accounts

Predefined password policies are provided, which you can apply to the user account password columns of the user accounts.

IMPORTANT: If you do not use password policies that are specific to the target system, the **One Identity Manager password policy** default policy applies. In this case, ensure that the default policy does not violate the target systems requirements.

NOTE: When you update One Identity Manager version 7.x to One Identity Manager version 8.1.2, the configuration parameter settings for forming passwords are passed on to the target system-specific password policies.

The **Azure Active Directory password policy** is predefined for Azure Active Directory. You can apply this password policy to Azure Active Directory user accounts (`AADUser.Password`) of an Azure Active Directory tenant.

If the tenants' password requirements differ, it is recommended that you set up your own password policies for each tenant.

Furthermore, you can apply password policies based on the account definition of the user accounts or based on the manage level of the user accounts.

Using password policies

The **Azure Active Directory password policy** is predefined for Azure Active Directory. You can apply this password policy to Azure Active Directory user accounts (`AADUser.Password`) of an Azure Active Directory tenant.

If the tenants' password requirements differ, it is recommended that you set up your own password policies for each tenant.

Furthermore, you can apply password policies based on the account definition of the user accounts or based on the manage level of the user accounts.

The password policy that is to be used for a user account is determined in the following sequence:

1. Password policy of the account definition of the user account.
2. Password policy of the manage level of the user account.
3. Password policy for the tenant of the user account.
4. The **One Identity Manager password policy** (default policy).

IMPORTANT: If you do not use password policies that are specific to the target system, the **One Identity Manager password policy** default policy applies. In this case, ensure that the default policy does not violate the target systems requirements.

To reassign a password policy

1. In the Manager, select the **Azure Active Directory | Basic configuration data | Password policies** category.
2. Select the password policy in the result list.
3. Select **Assign objects**.

4. Click **Add** in the **Assignments** section and enter the following data.

Table 11: Assigning a password policy

Property	Description
Apply to	Application scope of the password policy. ***To specify an application scope*** a. Click → next to the field. b. Select one of the following references under **Table**: • The table that contains the base objects of synchronization. • To apply the password policy based on the account definition, select the `TSBAccountDef` table. • To apply the password policy based on the manage level, select the `TSBBehavior` table. c. Under **Apply to**, select the table that contains the base objects. • If you have selected the table containing the base objects of synchronization, next select the specific target system. • If you have selected the `TSBAccountDef` table, next select the specific account definition. • If you have selected the `TSBBehavior` table, next select the specific manage level. 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. In the Manager, select the **Azure Active Directory | Basic configuration data | Password policies** category.
2. Select the password policy in the result list.
3. Select the **Assign objects** task.
4. In the **Assignments** pane, select the assignment you want to change.
5. From the **Password Policies** menu, select the new password policy you want to apply.
6. Save the changes.

Editing password policies

To edit a password policy

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

   - OR -

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

Detailed information about this topic

- General master data for password policies on page 59
- Policy settings on page 60
- Character classes for passwords on page 61
- Custom scripts for password requirements on page 62

General master data for password policies

Enter the following master data for a password policy.

Table 12: Master data for a password policy

Property	Meaning
Display name	Password policy name. Translate the given text using the button.
Description	Text field for additional explanation. Translate the given text using the button.
Error Message	Custom error message generated if the policy is not fulfilled. Translate the given text using the button.
Owner (Application Role)	Application roles whose members can configure the password policies.
Default policy	Mark as default policy for passwords. NOTE: The **One Identity Manager password policy** is marked as the default policy. This password policy is applied if no other password policy can be found for employees, user accounts, or system users.

Policy settings

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

Table 13: Policy settings

Property	Meaning
Initial password	Initial password for newly created user accounts. The initial password is used if a password is not entered when you create a user account or if a random password is not generated.
Password confirmation	Reconfirm password.
Minimum Length	Minimum length of the password. Specify the number of characters a password must have.
Max. length	Maximum length of the password. Specify the number of characters a password can have. The maximum permitted value is **256**.
Max. errors	Maximum number of errors. Set the number of invalid passwords attempts. Only taken into account when logging in to One Identity Manager. This data is only taken into account if the One Identity Manager login was through a system user or employee based authentication module. If a user has reached the number of maximum failed logins, the employee or system user can no longer log in to One Identity Manager. You can use the Password Reset Portal to reset the passwords of employees and system users who have been blocked. For more detailed information, see the *One Identity Manager Web Portal User Guide*.
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, for example, a value of **5** is entered, the user's last five passwords are stored.
Minimum password strength	Specifies how secure the password must be. The higher the password strength, the more secure it is. The value **0** means that the password strength is not tested. The values **1**, **2**, **3** and **4** specify the required complexity of the password. The value **1** represents the lowest requirements in terms of password strength. The value **4** requires the highest level of complexity.
Name properties denied	Specifies whether name properties are permitted in the

Property	Meaning
	password. If this option is set, name properties are not permitted in passwords. The values of these columns are taken into account if the **Contains name properties for password check** option is set. In the Designer, adjust this option in the column definition. For more detailed information, see the *One Identity Manager Configuration Guide*.

Character classes for passwords

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

Table 14: Character classes for passwords

Property	Meaning
Min. number letters	Specifies the minimum number of alphabetical characters the password must contain.
Min. number lowercase	Specifies the minimum number of lowercase letters the password must contain.
Min. number uppercase	Specifies the minimum number of uppercase letters the password must contain.
Min. number digits	Specifies the minimum number of digits the password must contain.
Min. number special characters	Specifies the minimum number of special characters the password must contain.
Permitted special characters	List of permitted special characters.
Max. identical characters in total	Specifies the maximum number of identical characters that can be present in the password in total.
Max. identical characters in succession	Specifies the maximum number of identical character that can be repeated after each other.
Denied special	List of special characters that are not permitted.

Property	Meaning
characters	
Do not generate lowercase letters	Specifies whether or not a generated password can contain lowercase letters. This setting only applies when passwords are generated.
Do not generate uppercase letters	Specifies whether or not a generated password can contain uppercase letters. This setting only applies when passwords are generated.
Do not generate digits	Specifies whether or not a generated password can contain digits. This setting only applies when passwords are generated.
Do not generate special characters	Specifies whether or not a generated password can contain special characters. If this option is set, only letters, numbers, and spaces are allowed in passwords. This setting only applies when passwords are generated.

Custom scripts for password requirements

You can implement custom scripts for testing and generating passwords if the password requirements cannot be mapped with the existing settings options. Scripts are applied in addition to the other settings.

Detailed information about this topic

- Script for checking passwords on page 62
- Script for generating a password on page 63

Script for checking passwords

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

Syntax of check scripts

```
Public Sub CCC_CustomPwdValidate( policy As VI.DB.Passwords.PasswordPolicy, spwd As System.Security.SecureString)
```

With parameters:

policy = password policy object

spwd = password to check

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

Example of a script that checks a password

A password cannot start with **?** or **!** . The password cannot start with three identical characters. The script checks a given password for validity.

```
Public Sub CCC_PwdValidate( policy As VI.DB.Passwords.PasswordPolicy, spwd As
System.Security.SecureString)
    Dim pwd = spwd.ToInsecureArray()
    If pwd.Length>0
        If pwd(0)="?" Or pwd(0)="!"
            Throw New Exception(#LD("Password can't start with '?' or '!'")#)
        End If
    End If
    If pwd.Length>2
        If pwd(0) = pwd(1) AndAlso pwd(1) = pwd(2)
            Throw New Exception(#LD("Invalid character sequence in password")#)
        End If
    End If
End Sub
```

To use a custom script for checking a password

1. In the Designer, create your script in the **Script Library** category.
2. Edit the password policy.
    a. In the Manager, select the **Azure Active Directory | Basic configuration data | Password policies** category.
    b. In the result list, select the password policy.
    c. Select the **Change master data** task.
    d. On the **Scripts** tab, enter the name of the script to be used to check a password in the **Check script** field.
    e. Save the changes.

Related topics

- Script for generating a password on page 63

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 `Entity` property of the `PasswordPolicy` class.

Example for a script to generate a password

The script replaces the **?** and **!** characters at the beginning of random passwords with **_**.

```
Public Sub CCC_PwdGenerate( policy As VI.DB.Passwords.PasswordPolicy, spwd As
System.Security.SecureString)
    Dim pwd = spwd.ToInsecureArray()
    ' replace invalid characters at first position
    If pwd.Length>0
        If pwd(0)="?" Or pwd(0)="!"
            spwd.SetAt(0, CChar("_"))
        End If
    End If
End Sub
```

To use a custom script for generating a password

1. In the Designer, create your script in the **Script Library** category.
2. Edit the password policy.
    a. In the Manager, select the **Azure Active Directory | Basic configuration data | Password policies** category.
    b. In the result list, select the password policy.
    c. Select the **Change master data** task.
    d. On the **Scripts** tab, enter the name of the script to be used to generate a password in the **Generating script** field.
    e. Save the changes.

Related topics

- Script for checking passwords on page 62

Password exclusion list

You can add words to a list of restricted terms to prohibit them from being used in passwords.

NOTE: The restricted list applies globally to all password policies.

To add a term to the restricted list

1. In the Designer, select the **Base Data | Security settings | Restricted passwords** category.
2. Create a new entry with the **Object | New** menu item and enter the term you want to exclude from the list.
3. Save the changes.

Checking passwords

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

To check if a password conforms to the password policy

1. In the Manager, select the **Azure Active Directory | Basic configuration data | Password policies** category.
2. Select the password policy in the result list.
3. Select the **Change master data** task.
4. Select the **Test** tab.
5. Select the table and object to be tested in **Base object for test**.
6. Enter a password in **Enter password to test**.

   A display next to the password shows whether it is valid or not.

Testing password generation

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

To generate a password that conforms to the password policy

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

4. Select the **Test** tab.
5. Click **Generate**.

   This generates and displays a password.

Initial password for new Azure Active Directory user accounts

You can issue an initial password for a new Azure Active Directory user account in the following ways:

- Create user accounts manually and enter a password in their master data.
- Assign a randomly generated initial password to enter when you create user accounts.
  - In the Designer, set the **TargetSystem | AzureAD | Accounts | InitialRandomPassword** configuration parameter.
  - Apply target system specific password policies and define the character sets that the password must contain.
  - Specify which employee will receive the initial password by email.
- Use the employee's central password. The employee's central password is mapped to the user account password. For detailed information about an employee's central password, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Related topics

- Password policies for Azure Active Directory user accounts on page 55
- Email notifications about login data on page 66

Email notifications about login data

You can configure the login information for new user accounts to be sent by email to a specified person. In this case, two messages are sent with the user name and the initial password. Mail templates are used to generate the messages. The mail text in a mail template is defined in several languages. This means the recipient's language can be taken into account when the email is generated. Mail templates are supplied in the default installation with which you can configure the notification procedure.

The following prerequisites must be fulfilled in order to use notifications:

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

   By default, the message sent uses the **Employee - new user account created** mail template. The message contains the name of the user account.
4. In the Designer, set the **TargetSystem | AzureAD | Accounts | InitialRandomPassword | SendTo | MailTemplatePassword** configuration parameter.

   By default, the message sent uses the **Employee - initial password for new user account** mail template. The message contains the initial password for the user account.

TIP: To use custom mail templates for emails of this type, change the value of the configuration parameter.

Target system managers

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

Define additional application roles if you want to limit the edit permissions for target system managers to individual tenants. The application roles must be added under the default application role.

For detailed information about implementing and editing application roles, see the *One Identity Manager Authorization and Authentication Guide*.

Implementing application roles for target system managers

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

   Target system managers with the default application role are authorized to edit all the tenants in One Identity Manager.
3. Target system managers can authorize other employees within their area of responsibility as target system managers and if necessary, create additional child application roles and assign these to individual tenants.

Table 15: Default application roles for target system managers

User	Tasks
Target system managers	Target system managers must be assigned to the **Target systems | Azure Active Directory** application role or a child application role. Users with this application role: • Assume administrative tasks for the target system. • Create, change, or delete target system objects like user accounts or groups. • Edit password policies for the target system. • Prepare groups to add to the IT Shop. • Can add employees who have an other identity than the **Primary identity**. • Configure synchronization in the Synchronization Editor and define the mapping for comparing target systems and One Identity Manager. • Edit the synchronization's target system types and outstanding objects. • Authorize other employees within their area of responsibility as target system managers and create child application roles if required.

To initially specify employees to be target system administrators

1. Log in to the Manager as a One Identity Manager administrator (**Base role \| Administrators** application role)
2. Select the **One Identity Manager Administration \| Target systems \| Administrators** category.

3. Select the **Assign employees** task.
4. Assign the employee you want and save the changes.

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

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

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

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

To specify target system managers for individual tenants

1. Log in to the Manager as a target system manager.
2. Select the **Azure Active Directory | Tenants** category.
3. Select the tenant in the result list.
4. Select the **Change master data** task.
5. On the **General** tab, select the application role in the **Target system manager** menu.

   - OR -

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

   a. Enter the application role name and assign the **Target systems | Azure Active Directory** parent application role.

   b. Click **OK** to add the new application role.
6. Save the changes.
7. Assign employees to this application role who are permitted to edit the tenant in One Identity Manager.

Related topics

- One Identity Manager users for managing an Azure Active Directory environment on page 9
- Azure Active Directory tenant on page 75

Editing a server

Servers must be informed of their server functionality in order to handle Azure Active Directory-specific processes in One Identity Manager. For example, the synchronization server.

You have several options for defining a server's functionality:

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

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

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

To edit a Job server and its functions

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

Detailed information about this topic

- Master data for a Job server on page 71
- Specifying server functions on page 73

Master data for a Job server

NOTE: All editing options are also available in the Designer under **Base Data | Installation | Job server**.

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

Table 16: Job server properties

Property	Meaning
Server	Job server name.
Full server name	Full server name in accordance with DNS syntax. Example: `<Name of server>.<Fully qualified domain name>`
Target system	Computer account target system.
Language	Language of the server.
Server is cluster	Specifies whether the server maps a cluster.
Server belongs to cluster	Cluster to which the server belongs. NOTE: The **Server is cluster** and **Server belongs to cluster** properties are mutually exclusive.
IP address (IPv6)	Internet protocol version 6 (IPv6) server address.
IP address (IPv4)	Internet protocol version 4 (IPv4) server address.
Copy process (source server)	Permitted copying methods that can be used when this server is the source of a copy action. At present, only copy methods that support the `Robocopy` and `rsync` programs are supported. If no method is given, the One Identity Manager Service determines the operating system of the server during runtime. Replication is then performed with the `Robocopy` program between servers with a Windows operating system or with the `rsync` program between servers with a Linux operating system. If the operating systems of the source and destination servers differ, it is important that the right copy method is applied for successful replication. A copy method is chosen that supports both servers.
Copy process (target	Permitted copying methods that can be used when this server is the destination of a copy action.

Property	Meaning
server)	
Coding	Character set coding that is used to write files to the server.
Parent Job server	Name of the parent Job server.
Executing server	Name of the executing server. The name of the server that exists physically and where the processes are handled. This input is evaluated when the One Identity Manager Service is automatically updated. If the server is handling several queues, the process steps are not supplied until all the queues that are being processed on the same server have completed their automatic update.
Queue	Name of the queue to handle the process steps. Each One Identity Manager Service within the network must have a unique queue identifier. The process steps are requested by the Job queue using this exact 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. The values **Win32**, **Windows**, **Linux**, and **Unix** are permitted. If no value is specified, **Win32** is used.
Service account data	One Identity Manager Service user account information. In order to replicate between non-trusted systems (non-trusted domains, Linux server), the One Identity Manager Service user information has to be declared for the servers in the database. This means that the service account, the service account domain, and the service account password have to be entered for the server.
One Identity Manager Service installed	Specifies whether a One Identity Manager Service is installed on this server. This option is enabled by the `QBM_PJobQueueLoad` procedure the moment the queue is called for the first time. The option is not automatically removed. If necessary, you can reset this option manually for servers whose queue is no longer enabled.
Stop One Identity Manager Service	Specifies whether the One Identity Manager Service has stopped. If this option is set for the Job server, the One Identity Manager Service does not process any more tasks. You can make the service start and stop with the appropriate administrative permissions in the Job Queue Info program. For more detailed information, see the *One Identity Manager Process Monitoring and Troubleshooting Guide*.
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.

Property	Meaning
Software update running	Specifies whether a software update is currently running.
Last fetch time	Last time the process was collected.
Last timeout check	The time of the last check for loaded process steps with a dispatch value that exceeds the one in the **Common | Jobservice | LoadedJobsTimeOut** configuration parameter.
Server function	Server functionality in One Identity Manager. One Identity Manager processes are handled with respect to the server function.

Related topics

- Specifying server functions on page 73

Specifying server functions

NOTE: All editing options are also available in the Designer under **Base Data | Installation | Job server**.

The server function defines the functionality of a server in One Identity Manager. One Identity Manager processes are handled with respect to the server function.

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

Table 17: Permitted server functions

Server function	Remark
Azure Active Directory connector (via Microsoft Graph)	Server on which the Azure Active Directory connector is installed. This server synchronizes the Azure Active Directory target system.
CSV connector	Server on which the CSV connector for synchronization is installed.
Domain controller	The Active Directory domain controller. Servers that are not labeled as domain controllers are considered to be member servers.
Printer server	Server that acts as a print server.
Generic server	Server for generic synchronization with a custom target system.
Home server	Server for adding home directories for user accounts.

Server function	Remark
Update server	This server automatically updates the software on all the other servers. The server requires a direct connection to the database server that One Identity Manager database is installed on. It can run SQL tasks. The server with the One Identity Manager database installed on it is labeled with this functionality during initial installation of the schema.
SQL processing server	This server can run 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.
CSV script server	This server can process CSV files using the `ScriptComponent` process component.
Native database connector	This server can connect to an ADO.Net database.
One Identity Manager database connector	Server on which the One Identity Manager connector is installed. This server synchronizes the One Identity Manager target system.
One Identity Manager Service installed	Server on which a One Identity Manager Service is installed.
Primary domain controller	Primary domain controller.
Profile server	Server for setting up profile directories for user accounts.
SAM synchronization Server	Server for running synchronization with an SMB-based target system.
SMTP host	Server from which One Identity Manager Service sends email notifications. Prerequisite for sending mails using One Identity Manager Service is SMTP host configuration.
Default report server	Server on which reports are generated.
Windows PowerShell connector	The server can run Windows PowerShell version 3.0 or later.

Related topics

- Master data for a Job server on page 71

Azure Active Directory core directories

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

You must provide details about your organization the first time you register for a Microsoft cloud service. This detailed information is used to make a new Azure Active Directory directory partition. The organization represents one Azure Active Directory tenant. In One Identity Manager, you can edit the master data of each tenant. However, you cannot create new tenants in One Identity Manager.

A base domain is linked to the core directory in the cloud. You can also add other user-defined domains in Azure Active Directory, which you can then allocate to Microsoft cloud services. One Identity Manager only loads verified domain data into the database. It is not possible to edit data in One Identity Manager.

Detailed information about this topic

- Azure Active Directory tenant on page 75
- Azure Active Directory domains on page 79

Azure Active Directory tenant

You must provide details about your organization the first time you register for a Microsoft cloud service. This detailed information is used to make a new Azure Active Directory directory partition. The organization represents one Azure Active Directory tenant. In One Identity Manager, you can edit the master data of each tenant. However, you cannot create new tenants in One Identity Manager.

To edit Azure Active Directory tenant master data

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

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

Detailed information about this topic

- General master data for Azure Active Directory tenants on page 76
- Information about local Active Directory on page 78
- Defining categories for the inheritance of entitlements on page 78

General master data for Azure Active Directory tenants

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

Table 18: 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 (**Linked configured** state). The account definition's default manage level is applied. User accounts are only linked to the employee (**Linked**) if no account definition is given. This is the case on initial synchronization, for example.
Target system managers	Application role, in which target system managers are specified for the tenant. Target system managers only edit the objects from tenants to which they are assigned. 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.
City	City.
Zip code	Zip code.
Country	Country.

Property	Description
Synchronized by	Type of synchronization through which the data is synchronized between the tenant and One Identity Manager. You can no longer change the synchronization type once objects for this tenant are present in One Identity Manager. If you create a tenant with the Synchronization Editor, **One Identity Manager** is used. **Table 19: Permitted values** **Value** / **Synchronization by** / **Provisioned by** One Identity Manager / Azure Active Directory connector / Azure Active Directory connector No synchronization / none / none NOTE: If you select **No synchronization**, you can define custom processes to exchange data between One Identity Manager and the target system.
Recipients (marketing notifications)	List of recipients of marketing notifications.
Recipient (technical notifications)	List of recipients of technical notifications.
Recipients (security notifications)	List of recipients of security notifications.
Phone numbers (security notifications)	Phone numbers for security notifications.

Related topics

- Automatic assignment of employees to Azure Active Directory user accounts on page 99
- Target system managers on page 67

Information about local Active Directory

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

Table 20: 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.

Defining categories for the inheritance of entitlements

In One Identity Manager, groups, administrator roles, subscriptions, and disabled services plans can be selectively inherited by user accounts. For this purpose, the groups (administrator roles, subscriptions, disabled service plans) and the user accounts are divided into categories. The categories can be freely selected and are specified using a mapping rule. Each category is given a specific position within the template. The mapping rule contains different tables. Use the user account table to specify categories for target system dependent user accounts. In the other tables enter your categories for the target system-dependent groups, administrator roles, subscriptions, and disabled service plans. Each table contains the **Position 1** to **Position 31** category positions.

To define a category

1. In the Manager, select the tenant in the **Azure Active Directory | Tenants** category.
2. Select the **Change master data** task.
3. Switch to the **Mapping rule category** tab.
4. Extend the relevant roots of a table.
5. To enable the category, double-click .
6. Enter a category name of your choice for user accounts and groups (administrator roles, subscriptions, disabled service plans) in the login language that you use.
7. Save the changes.

Related topics

- Azure Active Directory group inheritance based on categories on page 119
- Azure Active Directory administrator role inheritance based on categories on page 131
- Inheriting Azure Active Directory subscriptions based on categories on page 142
- Inheritance of disabled Azure Active Directory service plans based on categories on page 152

How to edit a synchronization project

Synchronization projects in which a tenant is already used as a base object can also be opened in the Manager. You can, for example, check the configuration or view the synchronization log in this mode. The Synchronization Editor is not started with its full functionality. You cannot run certain functions, such as, running synchronization or simulation, starting the target system browser and others.

NOTE: The Manager is locked for editing throughout. To edit objects in the Manager, close the Synchronization Editor.

To open an existing synchronization project in the Synchronization Editor

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

Related topics

- Customizing the synchronization configuration on page 25

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

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

Table 21: Domain master data

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

5

Azure Active Directory user accounts

You use One Identity Manager to manage user accounts in Azure Active Directory. The user requires a subscription to access the service plans in Azure Active Directory. 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 81
- Supported user account types on page 82
- Editing master data for Azure Active Directory user accounts on page 88

Linking user accounts to employees

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

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

- Employees can automatically obtain their account definitions using user account resources. If an employee does not yet have a user account in a tenant, a new user account is created. This is done by assigning account definitions to an employee

using the integrated inheritance mechanism and subsequent process handling.

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

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

Related topics

- Editing master data for Azure Active Directory user accounts on page 88
- Account definitions for Azure Active Directory user accounts on page 36
- Automatic assignment of employees to Azure Active Directory user accounts on page 99
- 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, service accounts, or privileged user accounts, can be mapped in One Identity Manager.

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

- Identity

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

  Table 22: Identities of user accounts

Identity	Description	Value of the IdentityType column
Primary identity	Employee's default user account.	Primary
Organizational	Secondary user account used for different roles in	Organizational

Identity	Description	Value of the IdentityType column
identity	the organization, for example for subcontracts with other functional areas.	
Personalized admin identity	User account with administrative permissions, used by one employee.	Admin
Sponsored identity	User account that is used for a specific purpose, such as training.	Sponsored
Shared identity	User account with administrative permissions, used by several employees.	Shared
Service identity	Service account.	Service

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

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

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

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

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

- Privileged user account

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

Detailed information about this topic

- Default user accounts on page 84
- Administrative user accounts on page 85
- Providing administrative user accounts for one employee on page 85

- Providing administrative user accounts for several employees on page 86
- Privileged user accounts on page 87

Default user accounts

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

To create default user accounts through account definitions

1. Create an account definition and assign the **Unmanaged** and **Full managed** manage levels.
2. Specify the effect of temporarily or permanently disabling, deleting, or the security risk of an employee on its user accounts and group memberships for each manage level.
3. Create a formatting rule for IT operating data.

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

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

   - In the mapping rule for the `IsGroupAccount` column, use the default value **1** and enable the **Always use default value** option.
   - In the mapping rule for the `IdentityType` column, use the default value **Primary** and enable **Always use default value**.
4. Enter the effective IT operating data for the target system. Select the concrete target system under **Effects on**.

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

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

Related topics

- Account definitions for Azure Active Directory user accounts on page 36

Administrative user accounts

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

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

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

Related topics

- Providing administrative user accounts for one employee on page 85
- Providing administrative user accounts for several employees on page 86

Providing administrative user accounts for one employee

Prerequisites

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

To prepare an administrative user account for a person

1. Label the user account as a personalized admin identity.
    a. In the Manager, select the **Azure Active Directory | User accounts** category.
    b. Select the user account in the result list.
    c. Select the **Change master data** task.
    d. On the **General** tab, in the **Identity** selection list, select **Personalized administrator identity**.
2. Link the user account to the employee who will be using this administrative user account.
    a. In the Manager, select the **Azure Active Directory | User accounts** category.
    b. Select the user account in the result list.
    c. Select the **Change master data** task.

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

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

Related topics

- Providing administrative user accounts for several employees on page 86
- For detailed information about mapping employee identities, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Providing administrative user accounts for several employees

Prerequisite

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

To prepare an administrative user account for multiple employees

1. Label the user account as a shared identity.
    a. In the Manager, select the **Azure Active Directory | User accounts** category.
    b. Select the user account in the result list.
    c. Select the **Change master data** task.
    d. On the **General** tab, in the **Identity** menu, select **Shared identity**.
2. Link the user account to a dummy employee.
    a. In the Manager, select the **Azure Active Directory | User accounts** category.
    b. Select the user account in the result list.
    c. Select the **Change master data** task.
    d. On the **General** tab, select the dummy employee from the **Employee** menu.

    TIP: If you are the target system manager, you can choose to create a new dummy employee.
3. Assign the employees who will use this administrative user account to the user account.

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

b. Select the user account in the result list.

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

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

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

To remove an assignment

- Select the employee and double-click ✓.

Related topics

- Providing administrative user accounts for one employee on page 85
- For detailed information about mapping employee identities, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Privileged user accounts

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

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

To create privileged users through account definitions

1. Create an account definition. Create a new manage level for privileged user accounts and assign this manage level to the account definition.
2. If you want to prevent the properties for privileged user accounts from being overwritten, set the **IT operating data overwrites** property for the manage level to **Only initially**. In this case, the properties are populated just once when the user accounts are created.
3. Specify the effect of temporarily or permanently disabling or deleting, or the security risk of an employee on its user accounts and group memberships for each manage level.
4. Create a formatting rule for the IT operating data.

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

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

- In the mapping rule for the `IsPrivilegedAccount` column, use the default value **1** and set the **Always use default value** option.
- You can also specify a mapping rule for the `IdentityType` column. The column owns different permitted values that represent user accounts.
- To prevent privileged user accounts from inheriting the entitlements of the default user, define a mapping rule for the `IsGroupAccount` column with a default value of **0** and set the **Always use default value** option.

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

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

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

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

TIP: If customization requires that the login names of privileged user accounts follow a defined naming convention, create the template according to which the login names are formed.

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

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

Related topics

- Account definitions for Azure Active Directory user accounts on page 36

Editing master data for Azure Active Directory user accounts

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

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

NOTE: If employees are to obtain their user accounts through account definitions, the employees must own a central user account and obtain their IT operating data through assignment to a primary department, a primary location, or a primary cost center.

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

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

To create a user account

1. In the Manager, select the **Azure Active Directory | User accounts** category.
2. Click in the result list.
3. On the master data form, edit the master data for the user account.
4. Save the changes.

To edit master data for a user account

1. In the Manager, select the **Azure Active Directory | User accounts** category.
2. Select the user account in the result list and run the **Change master data** task.
3. Edit the user account's resource data.
4. Save the changes.

To manually assign or create a user account for an employee

1. In the Manager, select the **Employees | Employees** category.
2. Select the employee in the result list and run the **Assign Azure Active Directory user accounts** task.
3. Assign a user account.
4. Save the changes.

Detailed information about this topic

- General master data of Azure Active Directory user accounts on page 90
- Contact data for an Azure Active Directory user account on page 92
- Organizational data for an Azure Active Directory user account on page 93
- Information about the local Active Directory user account on page 94

Related topics

- Account definitions for Azure Active Directory user accounts on page 36
- Supported user account types on page 82

- Azure Active Directory subscriptions and service plans on page 133

General master data of Azure Active Directory user accounts

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

Table 23: General 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 are using automatic employee assignment, an associated employee is found and added to the user account when you save the user account. You can create a new employee for a user account with an identity of type **Organizational identity**, **Personalized administrator identity**, **Sponsored identity**, **Shared identity**, or **Service identity**. To do this, click next to the input field and enter the required employee master data. Which login data is required depends on the selected identity type.
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. 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	Manage level of the user account. Select a manage level from the menu. You can only specify the manage level can if you have also entered an account definition. All manage levels of the selected account definition are available in the menu.
Tenant	User account's tenant.
Domain	User account's domain.
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	User account login name. The user's login name is made up of the alias

Property	Description
name	and the domain. User login names that are formatted like this correspond to the User Principal Name (UPN) in Azure Active Directory.
Display name	User account display name.
Alias	Email alias for the user account.
Preferred language	User's preferred language, for example, **en-US**.
Password	Password for the user account. The employee's central password can be mapped to the user account password. For detailed information about an employee's central password, see *One Identity Manager Identity Management Base Module Administration Guide*. If you use 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 at next login	Specifies whether the user must change their password the next time they log in.
Password policy	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 value of all assigned . The property is only visible if the **QER | CalculateRiskIndex** configuration parameter 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. Groups can be selectively inherited by user accounts. To do this, groups and user accounts or contacts are divided into categories. Select one or more categories from the menu.
Identity	User account's identity type Permitted values are: • **Primary identity**: Employee's default user account. • **Organizational identity**: Secondary user account used for different roles in the organization, for example for subcontracts with other functional areas. • **Personalized administrator identity**: User account with

Property	Description
	administrative permissions, used by one employee. • **Sponsored identity**: User account that is used for a specific purpose, such as training. • **Shared identity**: User account with administrative permissions, used by several employees. Assign all employees that use this user account. • **Service identity**: Service account.
Privileged user account.	Specifies whether this is a privileged user account.
Groups can be inherited	Specifies whether the user account can inherit groups 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.
User account is disabled	Specifies whether the user account is disabled. If a user account is not required for a period of time, you can temporarily disable the user account by using the "User account is disabled" option.

Related topics

- Account definitions for Azure Active Directory user accounts on page 36
- Password policies for Azure Active Directory user accounts on page 55
- Azure Active Directory group inheritance based on categories on page 119
- Linking user accounts to employees on page 81
- Supported user account types on page 82
- Disabling Azure Active Directory user accounts on page 103

Contact data for an Azure Active Directory user account

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

Table 24: Contact data

Property	Description
Street	Street or road. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
State	State. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
City	City. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level. Locations can be automatically generated and employees assigned based on the city.
Zip code	Zip code. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
Country	The country ID.
Business phones	Business telephone numbers.
Mobile phone	Mobile number. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
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 25: 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

Property	Description
	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 field. 2. In the **Table** menu, select the table that maps the account manager. 3. In the **Account manager** menu, select the manager. 4. Click **OK**.

Information about the local Active Directory user account

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

Table 26: 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 that used to maintain the relationship between Active Directory and Azure Active Directory and cannot be changed.

Additional tasks for managing Azure Active Directory user accounts

After you have entered the master data, you can run the following tasks.

The Azure Active Directory user accounts overview

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

To obtain an overview of a user account

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

Related topics

- Azure Active Directory subscriptions and service plans on page 133

Changing the manage level of Azure Active Directory user accounts

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

To change the manage level for a user account

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

Related topics

- Editing master data for Azure Active Directory user accounts on page 88

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

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

   To remove an assignment

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

Related topics

- Assigning Azure Active Directory groups to Azure Active Directory user accounts on page 109

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

   - OR -

   In the **Remove assignments** pane, remove administrator roles.
5. Save the changes.

Related topics

- Assigning Azure Active Directory administrator roles to Azure Active Directory user accounts on page 125

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 **Azure Active Directory | User accounts** category.
2. Select the user account in the result list.
3. Select the **Assign subscriptions** task.
4. In the **Add assignments** pane, add subscriptions.

   TIP: In **Remove assignments**, you can remove the subscription assignments.

   To remove an assignment

   - Select the subscription and double-click ✓.
1. Save the changes.

Related topics

- Assigning Azure Active Directory subscriptions to Azure Active Directory user accounts on page 135

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 **Azure Active Directory | User accounts** category.
2. Select the user account in the result list.
3. Select the **Assign disabled service plans** task.
4. In the **Add assignments** pane, assign disabled service plans.

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

   To remove an assignment

   - Select the service plan and double-click .
5. Save the changes.

Related topics

- Assigning disabled Azure Active Directory service plans to Azure Active Directory user accounts on page 145

Assigning extended properties to Azure Active Directory user accounts

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

To specify extended properties for a user account

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

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

   To remove an assignment

   - Select the extended property and double-click ✓.
5. Save the changes.

For 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

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 on the basis of existing user account master data. This mechanism can be triggered after a new user account is created either manually or through synchronization. Define criteria for finding employees to apply to automatic employee assignment. If a user account is linked to an employee through the current mode, the user account is given, through an internal process, the default manage level of the account definition entered in the user account's target system. You can customize user account properties depending on how the behavior of the manage level is defined.

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

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

Run the following tasks to assign employees automatically:

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

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

  Example:

  ADMINISTRATOR
- Use the **TargetSystem | AzureAD | PersonAutoDisabledAccounts** configuration parameter to specify whether employees can be automatically assigned to disabled user accounts. User accounts do not obtain an account definition.
- Assign an account definition to the tenant. Ensure that the manage level to be used is entered as the default manage level.
- Define the search criteria for employee assignment in the tenant.

NOTE:

The following applies for synchronization:

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

The following applies outside synchronization:

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

NOTE:

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

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

To select user accounts through account definitions

1. Create an account definition.
2. Assign an account definition to the tenant.
3. Assign a user account in the **Linked** state to the account definition. The account definition's default manage level is applied to the user account.
   a. In the Manager, select the **Azure Active Directory | User accounts | Linked but not configured | <Tenant>** category.
   b. Select the **Assign account definition to linked accounts** task.
   c. In the **Account definition** menu, select the account definition.
   d. Select the user accounts that contain the account definition.
   e. Save the changes.

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

Related topics

- Creating account definitions on page 37
- Assigning account definitions to a target system on page 52
- Editing search criteria for automatic employee assignment on page 101

Editing search criteria for automatic employee assignment

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

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

NOTE: 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 assignments to administrative user accounts based on search criteria. Use **Change master data** to assign employees to administrative user accounts 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 **Azure Active Directory | Tenants** category.
2. Select the tenant in the result list.
3. Select the **Define search criteria for employee assignment** task.
4. Specify which user account properties must match with which employee so that the employee is linked to the user account.

Table 27: Standard search criteria for user accounts and contacts

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

5. Save the changes.

Direct assignment of employees to user accounts based on a suggestion list

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

Table 28: 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 using a suggestion list

1. Click **Suggested assignments**.
   a. Check the **Selection** box of all the user accounts to which you want to assign the suggested employees. Multi-select is possible.
   b. Click **Assign selected.**
   c. Confirm the security prompt with **Yes**.

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

   – OR –
2. Click **No employee assignment**.
   a. Click the **Select employee** option of the user account to which you want to assign an employee. Select an employee from the menu.

b. Check the **Selection** box of all the 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**.

The employees displayed in the **Employee** column are assigned to the selected user accounts.

To remove assignments

1. Click **Assigned user accounts**.
   a. Click the **Selection** box of all user accounts you want to delete the employee assignment from. Multi-select is possible.
   b. Click **Remove selected**.
   c. Confirm the security prompt with **Yes**.

   The assigned employees are removed 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 99

Disabling Azure Active Directory user accounts

The way you disable user accounts depends on how they are managed.

Scenario:

- The user account is linked to employees and is managed through account definitions.

User accounts managed through account definitions are disabled when the employee is temporarily or permanently disabled. The behavior depends on the user account manage level. Accounts with the **Full managed** manage level are disabled depending on the account definition settings. For user accounts with a manage level, configure the required behavior using the template in the `AADUser.AccountDisabled` column.

Scenario:

- The user accounts are linked to employees. No account definition is applied.

User accounts managed through user account definitions are disabled when the employee is temporarily or permanently disabled. The behavior depends on the **QER | Person | TemporaryDeactivation** configuration parameter

- If the configuration parameter is set, the employee's user accounts are disabled when the employee is permanently or temporarily disabled.
- If the configuration parameter is not set, the employee's properties do not have any effect on the associated user accounts.

To disable the user account when the configuration parameter is disabled

1. In the Manager, select the **Azure Active Directory | User accounts** category.
2. Select the user account in the result list.
3. Select the **Change master data** task.
4. On the **General** tab, set the **Account is disabled** option.
5. Save the changes.

Scenario:

- User accounts not linked to employees.

To disable a user account that is no longer linked to an employee

1. In the Manager, select the **Azure Active Directory | User accounts** category.
2. Select the user account in the result list.
3. Select the **Change master data** task.
4. On the **General** tab, set the **Account is disabled** option.
5. Save the changes.

Related topics

- Account definitions for Azure Active Directory user accounts on page 36
- Creating manage levels on page 40
- Deleting and restoring Azure Active Directory user accounts on page 104
- 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 assignment of an account definition is removed, the user account that was created from this account definition is deleted.

To delete a user account

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

To restore a user account

1. Select the **Azure Active Directory | User accounts** category.
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 accounts are deleted from the database and cannot be restored anymore.In the Designer, you can set an alternative delay on the `AADUser` table.

Related topics

- Disabling Azure Active Directory user accounts on page 103
- 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 group types into which you can organize users and groups to regulate access to resources or email distribution, for example.

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. However, you cannot create more group types in One Identity Manager.

To add users to groups, you assign the groups directly to users. This can be assignments of groups to departments, cost centers, locations, business roles, or the IT Shop.

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

Table 29: 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 ones 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 can edit mail-enabled security groups in One Identity Manager but you cannot create new mail-enabled security groups in One Identity Manager.

Group type	Description
Dynamic group	Members of a dynamic group are not strictly assigned, but determined through defined rules. Dynamic groups are loaded into One Identity Manager by synchronization. You cannot change dynamic groups in One Identity Manager. You cannot create new dynamic groups in One Identity Manager.

Editing master data for Azure Active Directory groups

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

To edit group master data

1. In the Manager, select the **Azure Active Directory | Groups** category.
2. Select the group in the result list and run the **Change master data** task.
3. On the master data form, edit the master data for the group.
4. Save the changes.

Detailed information about this topic

- General master data for an Azure Active Directory group on page 107
- Information about local Active Directory groups on page 109

General master data for an Azure Active Directory group

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

Table 30: 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.

Property	Description
Alias	Email alias for the group.
Email address	Group's email address
Proxy addresses	Other email addresses for the group. You can also add other mail connectors (for example, CCMail, MS) in addition to the standard address type (SMTP, X400). Use the following syntax to set up other proxy addresses: `Address type: new email address`
Group type	Specifies a group's type. The value is **Unified** for Office 365 groups and is empty for security and distribution groups. For dynamic groups, the value entered is **DynamicMembership**.
Security group	Specifies whether this group is a security group. Resource permissions are distributed through security groups. User accounts and other groups are added to security groups, which makes administration easier.
Mail-enabled	Specifies whether the email is enabled for the group. If this option is set for a security group, it is a mail-enabled security group. Otherwise, it is a distribution group.
IT Shop	Specifies whether the group can be requested through the IT Shop. If this option is set, the group can be requested by the employees through the Web Portal and distributed with a defined approval process. The group can still be assigned directly to hierarchical roles.
Only for use in IT Shop	Specifies whether the group can only be requested through the IT Shop. If this option is set, the group can be requested by the employees through the Web Portal and distributed with a defined approval process. Direct assignment of the group to hierarchical roles or user accounts is not permitted.
Service item	Service item data for requesting the group through the IT Shop.
Risk index	Value for evaluating the risk of assigning the group to user accounts. Enter a value between 0 and 1. This input field is only visible if the **QER | CalculateRiskIndex** configuration parameter is activated. 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. Select one or more categories from the menu.
Description	Text field for additional explanation.

Related topics

- Azure Active Directory group inheritance based on categories on page 119
- 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 that is linked to the Azure Active Directory user account.

Table 31: 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 the indirect assignment of employees to user accounts include:

- Assignment of employees and groups is permitted for role classes (departments, cost centers, locations, or business roles).
- User accounts are marked with the **Groups can be inherited** option.

Groups can also be assigned to persons through IT Shop requests. So that groups can be assigned using IT Shop requests, employees are added to a shop as customers. All groups 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 110
- Assigning Azure Active Directory groups to business roles on page 111
- Assigning Azure Active Directory user accounts directly to Azure Active Directory groups on page 112
- Adding Azure Active Directory groups to system roles on page 113
- Adding Azure Active Directory groups to the IT Shop on page 114

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

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

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

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

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

   - OR -

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

   - OR -

   In the Manager, select the **Organizations | Locations** category.
2. Select the department, cost center, or location in the result list.

3. Select the **Assign Azure Active Directory groups** task.
4. In the **Add assignments** pane, assign groups.

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

   To remove an assignment

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

Related topics

- Assigning Azure Active Directory groups to business roles on page 111
- Assigning Azure Active Directory user accounts directly to Azure Active Directory groups on page 112
- Adding Azure Active Directory groups to system roles on page 113
- Adding Azure Active Directory groups to the IT Shop on page 114
- One Identity Manager users for managing an Azure Active Directory environment 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. In the Manager, select the **Azure Active Directory | Groups** category.
2. Select the group in the result list.
3. Select the **Assign business roles** task.
4. In the **Add assignments** pane, assign business roles.

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

   To remove an assignment

   - Select the business role and double-click ✓.
5. Save the changes.

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

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

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

   To remove an assignment

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

Related topics

- Assigning Azure Active Directory groups to departments, cost centers, and locations on page 110
- Assigning Azure Active Directory user accounts directly to Azure Active Directory groups on page 112
- Adding Azure Active Directory groups to system roles on page 113
- Adding Azure Active Directory groups to the IT Shop on page 114
- One Identity Manager users for managing an Azure Active Directory environment on page 9

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

Groups can be assigned directly or indirectly to user accounts. Indirect assignment is done by allocating the employee and groups into company structures such as 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. In the Manager, select the **Azure Active Directory | Groups** category.
2. Select the group in the result list.
3. Select the **Assign user accounts** task.
4. In **Add assignments** pane, assign user accounts.

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

To remove an assignment

- Select the user account and double-click ✓.

5. Save the changes.

Related topics

- Assigning Azure Active Directory groups directly to Azure Active Directory user accounts on page 96
- Assigning Azure Active Directory groups to departments, cost centers, and locations on page 110
- Assigning Azure Active Directory groups to business roles on page 111
- Adding Azure Active Directory groups to system roles on page 113
- Adding Azure Active Directory groups to the IT Shop on page 114

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 user accounts belonging to these employees inherit the group.

NOTE: Groups with **Only use in IT Shop** set 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. In the Manager, select the **Azure Active Directory | Groups** category.
2. Select the group in the result list.
3. Select the **Assign system roles** task.
4. In the **Add assignments** pane, assign system roles.

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

   To remove an assignment

   - Select the system role and double-click ✓.

5. Save the changes.

Related topics

- Assigning Azure Active Directory groups to departments, cost centers, and locations on page 110
- Assigning Azure Active Directory groups to business roles on page 111
- Assigning Azure Active Directory user accounts directly to Azure Active Directory groups on page 112
- Adding Azure Active Directory groups to the IT Shop on page 114

Adding Azure Active Directory groups to the IT Shop

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

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

  TIP: In the Web Portal, all products that can be requested are grouped together by service category. To make the group easier to find in the Web Portal, assign a service category to the service item.
- If you only want the group to be assigned to employees through IT Shop requests, the group must also be labeled with the **Use only in IT Shop** option. Direct assignment to hierarchical roles or user accounts is no longer permitted.

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

To add a group to the IT Shop.

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

   - OR -

   In the Manager, select the **Entitlements | Azure Active Directory groups** (role-based login) category.
2. In the result list, select the group.
3. Select the **Add to IT Shop** task.
4. In the **Add assignments** pane, assign the group to the IT Shop shelves.
5. Save the changes.

To remove a group from individual shelves of the IT Shop

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

   - OR -

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

To remove a group from all shelves of the IT Shop

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

   - OR -

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

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

For more detailed information about requesting 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 107
- Assigning Azure Active Directory groups to departments, cost centers, and locations on page 110
- Assigning Azure Active Directory groups to business roles on page 111
- Assigning Azure Active Directory user accounts directly to Azure Active Directory groups on page 112
- Adding Azure Active Directory groups to system roles on page 113

Additional tasks for managing Azure Active Directory groups

After you have entered the master data, you can run the following tasks.

The Azure Active Directory group overview

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

To obtain an overview of a group

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

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. In the Manager, select the **Azure Active Directory | Groups** category.
2. Select the group in the result list.
3. Select the **Assign groups** category.
4. In the **Add assignments** pane, assign the groups that are subordinate to the selected group.

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

   To remove an assignment

   - Select the group and double-click .
5. Save the changes.

Effectiveness of group memberships

Table 32: Configuration parameters for conditional inheritance

Configuration parameter	Effect when set
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. Changes to this parameter require the database to be recompiled.

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

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

NOTE:

- You cannot define a pair of mutually exclusive groups. That means, the definition "Group A excludes group B" `AND` "Group B excludes groups A" is not permitted.
- You must declare each group to be excluded from a group separately. Exclusion definitions cannot be inherited.
- One Identity Manager does not check if membership of an excluded group is permitted in another group (table).

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

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

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

By using suitable controls, you want to prevent an employee from being able to trigger a request and to pay invoices. That means, groups A, B, and C are mutually

exclusive. An employee that checks invoices may not be able to make invoice payments as well. That means, groups B and C are mutually exclusive.

Table 33: Specifying excluded groups (`AADGroupExclusion` table)

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

Table 34: Effective assignments

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

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

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

Table 35: Excluded groups and effective assignments

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

Prerequisites

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

To exclude a group

1. In the Manager, select the **Azure Active Directory | Groups** category.
2. Select a group in the result list.
3. Select the **Exclude groups** task.
4. In the **Add assignments** pane, assign the groups that are mutually exclusive to the selected group.

   - OR -

   In the **Remove assignments** pane, remove the groups that are not longer mutually exclusive.
5. Save the changes.

Azure Active Directory group inheritance based on categories

In One Identity Manager, groups, administrator roles, subscriptions, and disabled services plans can be selectively inherited by user accounts. For this purpose, the groups (administrator roles, subscriptions, disabled service plans) and the user accounts are divided into categories. The categories can be freely selected and are specified using a mapping rule. Each category is given a specific position within the template. The mapping rule contains different tables. Use the user account table to specify categories for target system dependent user accounts. In the other tables enter your categories for the target system-dependent groups, administrator roles, subscriptions, and disabled service plans. Each table contains the **Position 1** to **Position 31** category positions.

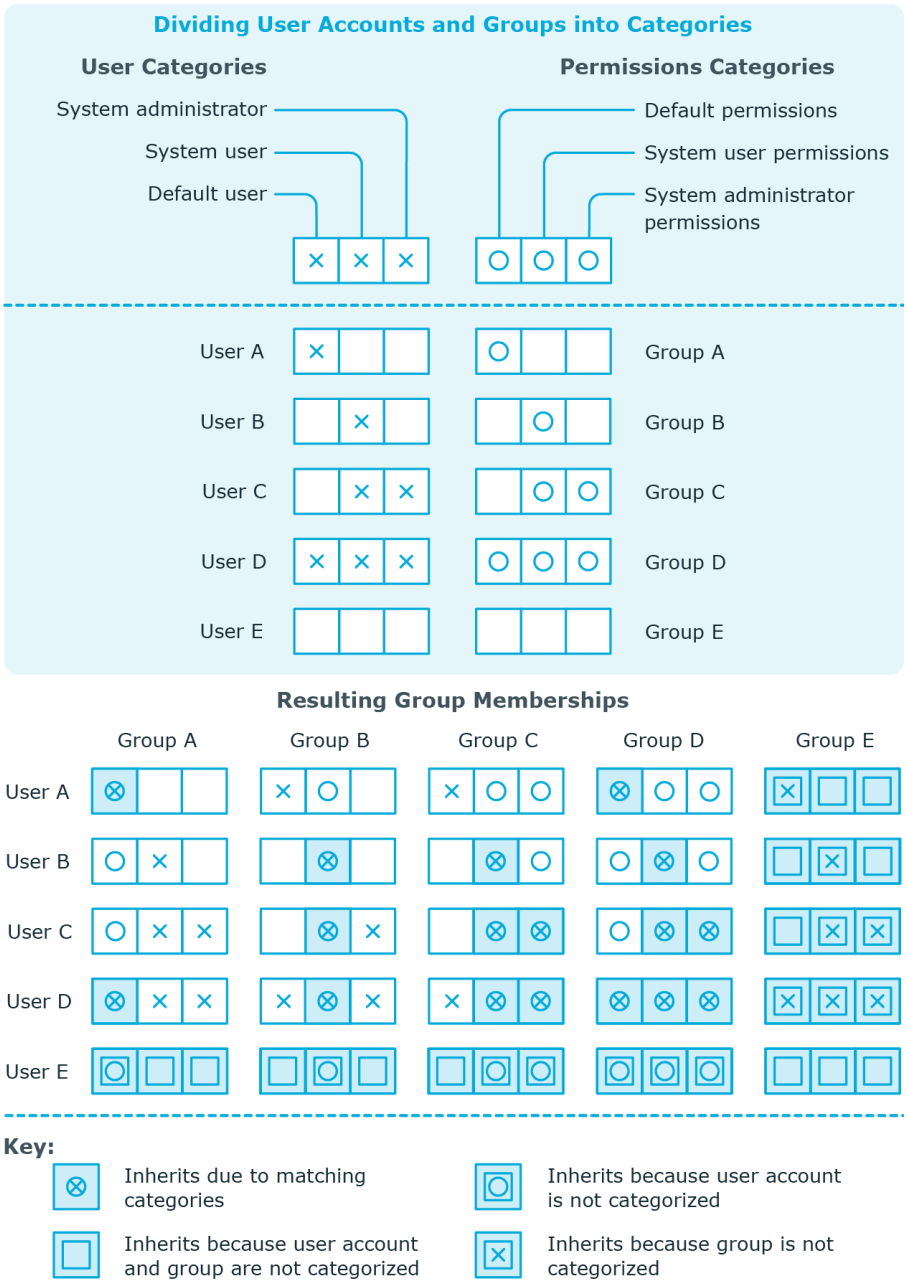
Every user account can be assigned to one or more categories. Each group can also be assigned to one or more categories. The group is inherited by the user account when at least one user account category items matches an assigned group. The group is also inherited by the user account if the group or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

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

Table 36: Category examples

Category item	Categories for user accounts	Categories for groups
1	Default user	Default permissions
2	System users	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

- Defining categories for the inheritance of entitlements on page 78
- General master data of Azure Active Directory user accounts on page 90
- General master data for an Azure Active Directory group on page 107
- Editing Azure Active Directory subscription master data on page 134

Assigning owners to Azure Active Directory groups

A group owner can edit group properties.

To assign owners to a group

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

    - OR -

    In the **Remove assignments** pane, remove owners.
6. Save the changes.

Assigning extended properties to Azure Active Directory groups

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

To specify extended properties for a group

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

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

properties.

To remove an assignment

- Select the extended property and double-click .

5. Save the changes.

For more detailed information about setting up 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 **Azure Active Directory | Groups** category.
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, locations, business roles, or the IT Shop.

Editing master data of Azure Active Directory administrator roles

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

Table 37: Administrator role master data

Property	Description
Display name	The display name is used to display the administrator role in the One Identity Manager tools' user interface.
Tenant	The administrator role's tenant.
Template ID.	ID of the administrator role template on which this administrator role was based.
IT Shop	Specifies whether the administrator role can be requested through the IT Shop. The administrator role can be ordered by its employees over the Web Portal and distributed using a defined approval process. The administrator role can still be assigned directly to user accounts and hierarchical roles.
Only for use in IT Shop	Specifies whether the administrator role can only be requested through the IT Shop. The administrator role can be ordered by its employees over the Web Portal and distributed using a defined approval process. You cannot assign an administrator role directly to a hierarchical role.
Service item	Specifies a service item for requesting the administrator role through the IT Shop.
Risk index	Value for assessing the risk of assigning administrator roles to user accounts. Enter a value between 0 and 1. This input field is only visible if the **QER | CalculateRiskIndex** configuration parameter is set. For more detailed information about risk assessment, see the *One Identity Manager Risk Assessment Administration Guide*.
Category	Categories for inheriting administrator roles. Administrator roles can be selectively inherited by user accounts. To do this, administrator roles and user accounts are divided into categories. Use the menu to allocate one or more categories to the administrator role.
Description	Text field for additional explanation.

Related topics

- Azure Active Directory administrator role inheritance based on categories on page 131
- 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 the indirect assignment of employees to user accounts:

- Assignment of employees and administrator roles is permitted for role classes (departments, cost centers, locations, or business roles).
- User accounts are marked with the **Groups can be inherited** option.

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 administrator roles to departments, cost centers, and locations on page 125
- Assigning Azure Active Directory administrator roles to business roles on page 127
- Assigning Azure Active Directory user accounts directly to Azure Active Directory administrator roles on page 128
- Adding Azure Active Directory administrator roles to system roles on page 128
- Adding Azure Active Directory administrator roles in the IT Shop on page 129

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

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

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

1. Select the **Azure Active Directory | Administrator roles** category.
2. Select the administrator role in the result list.
3. Select the **Assign organizations** task.
4. In the **Add assignments** pane, assign the organizations:
   - On the **Departments** tab, assign departments.
   - On the **Locations** tab, assign locations.
   - On the **Cost centers** tab, assign cost centers.

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

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

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

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

   - OR -

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

   - OR -

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

   - OR -

   In the **Remove assignments** pane, remove administrator roles.
5. Save the changes.

Related topics

- Assigning Azure Active Directory administrator roles to business roles on page 127
- Assigning Azure Active Directory user accounts directly to Azure Active Directory administrator roles on page 128
- Adding Azure Active Directory administrator roles to system roles on page 128
- Adding Azure Active Directory administrator roles in the IT Shop on page 129
- One Identity Manager users for managing an Azure Active Directory environment 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 **Azure Active Directory | Administrator roles** category.
2. Select the administrator role in the result list.
3. Select the **Assign business roles** task.
4. In the **Add assignments** pane, assign business roles.

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

   To remove an assignment

   - Select the business role and double-click ✓.
5. Save the changes.

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

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

   - OR -

   In the **Remove assignments** pane, remove administrator roles.
5. Save the changes.

Related topics

- Assigning Azure Active Directory administrator roles to departments, cost centers, and locations on page 125
- Assigning Azure Active Directory user accounts directly to Azure Active Directory administrator roles on page 128
- Adding Azure Active Directory administrator roles to system roles on page 128
- Adding Azure Active Directory administrator roles in the IT Shop on page 129
- One Identity Manager users for managing an Azure Active Directory environment 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 **Azure Active Directory | Administrator roles** category.
2. Select the administrator role in the result list.
3. Select the **Assign user accounts** task.
4. In **Add assignments** pane, assign user accounts.

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

   To remove an assignment

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

Related topics

- Assigning Azure Active Directory administrator roles directly to Azure Active Directory user accounts on page 96
- Assigning Azure Active Directory administrator roles to departments, cost centers, and locations on page 125
- Assigning Azure Active Directory administrator roles to business roles on page 127
- Adding Azure Active Directory administrator roles to system roles on page 128
- Adding Azure Active Directory administrator roles in the IT Shop on page 129

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

To assign an administrator role to system roles

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

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

   To remove an assignment

   - Select the system role and double-click ✓.
5. Save the changes.

Related topics

- Assigning Azure Active Directory administrator roles to departments, cost centers, and locations on page 125
- Assigning Azure Active Directory administrator roles to business roles on page 127
- Assigning Azure Active Directory user accounts directly to Azure Active Directory administrator roles on page 128
- Adding Azure Active Directory administrator roles in the IT Shop on page 129

Adding Azure Active Directory administrator roles in the IT Shop

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

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

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

To add an administrator role in the IT Shop

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

   - OR -

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

To remove an administrator role from individual IT Shop shelves

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

   - OR -

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

To remove an administrator role from all IT Shop shelves

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

   - OR -

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

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

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

Related topics

- Editing master data of Azure Active Directory administrator roles on page 123
- Assigning Azure Active Directory administrator roles to departments, cost centers, and locations on page 125
- Assigning Azure Active Directory administrator roles to business roles on page 127
- Assigning Azure Active Directory user accounts directly to Azure Active Directory administrator roles on page 128
- Adding Azure Active Directory administrator roles to system roles on page 128

Additional tasks for managing Azure Active Directory administrator roles

After you have entered the master data, you can run the following tasks.

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

Azure Active Directory administrator role inheritance based on categories

The procedure described under Azure Active Directory group inheritance based on categories on page 119 can also be applied for administrator 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

- Defining categories for the inheritance of entitlements on page 78
- General master data of Azure Active Directory user accounts on page 90
- Editing master data of Azure Active Directory administrator roles on page 123

Assigning extended properties to an Azure Active Directory administrator role

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

To specify extended properties for an administrator role

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

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

   To remove an assignment

   - Select the extended property and double-click .
5. Save the changes.

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

8

Azure Active Directory subscriptions and service plans

The user requires a subscription to access the service plans 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.

To prevent users from using individual service plans, so-called "disabled service plans" are mapped in One Identity Manager. Disabled service plans are created automatically in One Identity Manager after synchronization of the subscription. 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. In One Identity Manager, you cannot create new subscriptions or service plans. However, in One Identity Manager, you can edit certain master data for requesting the subscription in the IT Shop and for user account assignments.

Editing Azure Active Directory subscription master data

To edit subscription master data

1. Select **Azure Active Directory | Subscriptions**.
2. Select a subscription in the result list.
3. Select the **Change master data** task.
4. Edit the subscription's master data.
5. Save the changes.

Table 38: 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** (active).
Purchased licenses	The number of licenses purchased.
Assigned licenses	Number of actively used licenses.
Suspended licenses	Number of suspended licenses.
Warning units	Number of licenses with a warn status.
IT Shop	Specifies whether the 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 input field is only visible if the **QER |**

Property	Description
	CalculateRiskIndex configuration parameter 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 119
- For 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 the indirect assignment of employees to user accounts:

- Assignment of employees and subscriptions is permitted for role classes (departments, cost centers, locations, or business roles).
- User accounts are marked with the **Groups can be inherited** option.

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, locations, or business roles, or an IT Shop request.

Detailed information about this topic

- Assigning Azure Active Directory subscriptions to departments, cost centers, and locations on page 136
- Assigning Azure Active Directory subscriptions to business roles on page 137
- Assigning Azure Active Directory user accounts directly to an Azure Active Directory subscription on page 138
- Adding Azure Active Directory subscriptions to system roles on page 139
- Adding Azure Active Directory subscriptions to the IT Shop on page 140

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 **Azure Active Directory | Subscriptions** category.
2. Select a subscription in the result list.
3. Select the **Assign organizations** task.
4. In the **Add assignments** pane, assign the organizations:
   - On the **Departments** tab, assign departments.
   - On the **Locations** tab, assign locations.
   - On the **Cost centers** tab, assign cost centers.

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

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

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

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

   - OR -

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

   - OR -

   Select the **Organizations | Locations** category.
2. Select the department, cost center, or location in the result list.

3. Select the **Assign Azure Active Directory subscriptions** task.
4. In the **Add assignments** pane, assign the subscriptions.

   - OR -

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

Related topics

- Assigning Azure Active Directory subscriptions to business roles on page 137
- Assigning Azure Active Directory user accounts directly to an Azure Active Directory subscription on page 138
- Adding Azure Active Directory subscriptions to system roles on page 139
- Adding Azure Active Directory subscriptions to the IT Shop on page 140
- One Identity Manager users for managing an Azure Active Directory environment 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 **Azure Active Directory | Subscriptions** category.
2. Select a subscription in the result list.
3. Select the **Assign business roles** task.
4. In the **Add assignments** pane, assign business roles.

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

   To remove an assignment

   - Select the business role and double-click ✓.
5. Save the changes.

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

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

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

   - OR -

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

Related topics

- Assigning Azure Active Directory subscriptions to departments, cost centers, and locations on page 136
- Assigning Azure Active Directory user accounts directly to an Azure Active Directory subscription on page 138
- Adding Azure Active Directory subscriptions to system roles on page 139
- Adding Azure Active Directory subscriptions to the IT Shop on page 140
- One Identity Manager users for managing an Azure Active Directory environment 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 **Azure Active Directory | Subscriptions** category.
2. Select a subscription in the result list.
3. Select the **Assign user accounts** task.
4. In **Add assignments** pane, assign user accounts.

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

   To remove an assignment

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

Related topics

- Assigning Azure Active Directory subscriptions directly to Azure Active Directory user accounts on page 97
- Assigning Azure Active Directory subscriptions to departments, cost centers, and locations on page 136
- Assigning Azure Active Directory subscriptions to business roles on page 137
- Adding Azure Active Directory subscriptions to system roles on page 139
- Adding Azure Active Directory subscriptions to the IT Shop on page 140

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

To assign a subscription to a system role

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

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

   To remove an assignment

   - Select the system role and double-click ✓.
5. Save the changes.

Related topics

- Assigning Azure Active Directory subscriptions to departments, cost centers, and locations on page 136
- Assigning Azure Active Directory subscriptions to business roles on page 137
- Assigning Azure Active Directory user accounts directly to an Azure Active Directory subscription on page 138
- Adding Azure Active Directory subscriptions to the IT Shop on page 140

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 **Only for use in IT Shop** option. 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 **Azure Active Directory | Subscriptions** (non role-based login) category.

   - OR -

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

To remove a subscription from individual IT Shop shelves

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

   - OR -

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

To remove a subscription from all IT Shop shelves

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

   - OR -

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

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

For more detailed information about requesting 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 134
- Assigning Azure Active Directory subscriptions to departments, cost centers, and locations on page 136
- Assigning Azure Active Directory subscriptions to business roles on page 137
- Assigning Azure Active Directory user accounts directly to an Azure Active Directory subscription on page 138
- Adding Azure Active Directory subscriptions to system roles on page 139

Additional tasks for managing Azure Active Directory subscriptions

After you have entered the master data, you can run the following tasks.

The Azure Active Directory subscriptions overview

To obtain an overview of a subscription

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

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

To obtain an overview of a service plan

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

To obtain an overview of a disabled service plan

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

Effectiveness of subscription assignments

The procedure described under Effectiveness of group memberships on page 117 can also be used for subscriptions. The effect of the assignments is mapped in the `AADUserHasSubSku` and `AADBaseTreeHasSubSku` tables through the `XIsInEffect` column.

Prerequisites

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

To exclude subscriptions

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

   - OR -

   In the **Remove assignments** pane, delete the subscriptions that no longer exclude each other.
5. Save the changes.

Inheriting Azure Active Directory subscriptions based on categories

The procedure described under Azure Active Directory group inheritance based on categories on page 119 can also be used for 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

- Defining categories for the inheritance of entitlements on page 78
- General master data of Azure Active Directory user accounts on page 90
- Editing Azure Active Directory subscription master data on page 134

Assigning additional properties to an Azure Active Directory subscription

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

To specify extended properties for a subscription

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

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

   To remove an assignment

   - Select the extended property and double-click ✓.
5. Save the changes.

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

Disabled Azure Active Directory service plans

To prevent users from using individual service plans, so-called "disabled service plans" are mapped in One Identity Manager. Disabled service plans are created automatically in One Identity Manager after synchronization of the subscription. 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 **Azure Active Directory | Disabled service plans** category.
2. Select the service plan in the result list.
3. Select the **Change master data** task.
4. Edit the service plan's master data.
5. Save the changes.

Table 39: 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 119
- For detailed information about preparing 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 the indirect assignment of employees to user accounts:

- Assignment of employees and disabled service plans is permitted for role classes (departments, cost centers, locations, or business roles).
- User accounts are marked with the **Groups can be inherited** option.

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 directly to departments, cost centers, and locations on page 145
- Assigning disabled Azure Active Directory service plans to business roles on page 147
- Assigning Azure Active Directory user accounts directly to Azure Active Directory service plans on page 148
- Adding disabled Azure Active Directory service plans to system roles on page 149
- Adding disabled Azure Active Directory service plans to the IT Shop on page 149

Assigning disabled Azure Active Directory service plans directly 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 **Azure Active Directory | Disabled service plans** category.
2. Select the service plan in the result list.
3. Select the **Assign organizations** task.
4. In the **Add assignments** pane, assign the organizations:
   - On the **Departments** tab, assign departments.
   - On the **Locations** tab, assign locations.
   - On the **Cost centers** tab, assign cost centers.

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

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

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

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

   - OR -

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

   - OR -

   Select the **Organizations | Locations** category.
2. Select the department, cost center or location in the result list.
3. Select **Assigning disabled Azure Active Directory service plans**.
4. In the **Add assignments** pane, select the Azure Active Directory subscription and assign the disabled service plans.

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

   To remove an assignment
   - Select the service plan and double-click ✓.
5. Save the changes.

Related topics

- Assigning disabled Azure Active Directory service plans to business roles on page 147
- Assigning Azure Active Directory user accounts directly to Azure Active Directory service plans on page 148
- Adding disabled Azure Active Directory service plans to system roles on page 149
- Adding disabled Azure Active Directory service plans to the IT Shop on page 149

- One Identity Manager users for managing an Azure Active Directory environment 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 so that they can be assigned to user accounts through these business roles.

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

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

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

   To remove an assignment

   - Select the business role and double-click ✓.
5. Save the changes.

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

1. Select the **Business roles | <Role class>** category.
2. Select the business role in the result list.
3. Select the **Assigning disabled Azure Active Directory service plans** task.
4. In the **Add assignments** pane, select the Azure Active Directory subscription and assign the disabled service plans.

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

   To remove an assignment

   - Select the service plan and double-click ✓.
5. Save the changes.

Related topics

- Assigning disabled Azure Active Directory service plans directly to departments, cost centers, and locations on page 145
- Assigning Azure Active Directory user accounts directly to Azure Active Directory service plans on page 148

- Adding disabled Azure Active Directory service plans to system roles on page 149
- Adding disabled Azure Active Directory service plans to the IT Shop on page 149
- One Identity Manager users for managing an Azure Active Directory environment 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 **Azure Active Directory | Disabled service plans** category.
2. Select the service plan in the result list.
3. Select the **Assign user accounts** task.
4. In **Add assignments** pane, assign user accounts.

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

   To remove an assignment

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

Related topics

- Assigning disabled Azure Active Directory service plans directly to Azure Active Directory user accounts on page 98
- Assigning disabled Azure Active Directory service plans directly to departments, cost centers, and locations on page 145
- Assigning disabled Azure Active Directory service plans to business roles on page 147
- Adding disabled Azure Active Directory service plans to system roles on page 149
- Adding disabled Azure Active Directory service plans to the IT Shop on page 149

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

To assign a disabled service plan to system roles

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

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

   To remove an assignment

   - Select the system role and double-click ✓.
5. Save the changes.

Related topics

- Assigning disabled Azure Active Directory service plans directly to departments, cost centers, and locations on page 145
- Assigning disabled Azure Active Directory service plans to business roles on page 147
- Assigning Azure Active Directory user accounts directly to Azure Active Directory service plans on page 148
- Adding disabled Azure Active Directory service plans to the IT Shop on page 149

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 **IT Shop** option.
- The disabled service plan must be assigned to a service item.

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

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

To add a disabled service plan in the IT Shop

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

   - OR -

   Select the **Entitlements | Disabled Azure Active Directory service plans** (role-based login) category.
2. Select the service plan in the result list.
3. Select the **Add to IT Shop** task.
4. In the **Add assignments** pane, assign the disabled service plan to the IT Shop shelves.
5. Save the changes.

To remove a disabled service plan from individual IT Shop shelves

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

   - OR -

   Select the **Entitlements | Disabled Azure Active Directory service plans** (role-based login) category.
2. Select the service plan in the result list.
3. Select the **Add to IT Shop** task.
4. In the **Remove assignments** pane, remove the disabled service plan from the IT Shop shelves.
5. Save the changes.

To remove a disabled service plan from all IT Shop shelves

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

   - OR -

   Select the **Entitlements | Disabled Azure Active Directory service plans** (role-based login) category.
2. Select the service plan in the result list.
3. Select the **Remove from all shelves (IT Shop)** task.
4. Confirm the security prompt with **Yes**.

5. Click **OK**.

   The disabled service plan is removed from all shelves by One Identity Manager Service. All requests and assignment requests with this disabled service plan are canceled at the same time.

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

Related topics

- Assigning disabled Azure Active Directory service plans directly to departments, cost centers, and locations on page 145
- Assigning disabled Azure Active Directory service plans to business roles on page 147
- Assigning Azure Active Directory user accounts directly to Azure Active Directory service plans on page 148
- Adding disabled Azure Active Directory service plans to system roles on page 149

Additional tasks for managing disabled Azure Active Directory service plans

After you have entered the master data, you can run the following tasks.

The disabled Azure Active Directory service plans overview

To obtain an overview of a disabled service plan

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

Effectiveness of assignments of disabled service plans

The procedure described under Effectiveness of group memberships on page 117 can also be used for disabled service plans. The effect of the assignments is mapped in the `AADUserHasDeneiedService` and `AADBaseTreeHasDeniedService` tables through the `XIsInEffect` column.

Prerequisites

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

To exclude subscriptions

1. Select the **Azure Active Directory | Disabled service plans** category.
2. Select the disabled service plan from the result list.
3. Select the **Exclude disabled service plans** task.
4. In the **Add assignments** pane, assign the disabled service plans that are excluded with the selected service plan.

   - OR -

   In the **Remove assignments** pane, delete the disabled service plans that no longer exclude each other.
5. Save the changes.

Inheritance of disabled Azure Active Directory service plans based on categories

The procedure described under Azure Active Directory group inheritance based on categories on page 119 can also be used 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

- Defining categories for the inheritance of entitlements on page 78
- General master data of Azure Active Directory user accounts on page 90
- Editing master data of disabled Azure Active Directory service plans on page 144

Assigning extended properties to a disabled Azure Active Directory service plan

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

To specify extended properties for a disabled service plan

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

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

   To remove an assignment

   - Select the extended property and double-click .
5. Save the changes.

For 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 40: Reports for the target system

Report	Description
Overview of all assignments	This report identifies 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 that 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 contains 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 that are the result of manual operations in the target system rather than provisioned by 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 **My One Identity Manager** category.
Data quality summary for	This report contains different evaluations of user account

Report	Description
Azure Active Directory user accounts	data quality in all tenants. You can find this report in the **My One Identity Manager** category.

Overview of all assignments

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

Examples

- If the report is created for a resource, all roles are determined in which there are employees with this resource.
- If the report is created for a group or another system entitlement, all roles are determined in which there are employees with this group or system entitlement.
- If the report is created for a compliance rule, all roles are determined in which there are employees who violate this compliance rule.
- If the report is created for a department, all roles are determined in which employees of the selected department are also members.
- If the report is created for a business role, all roles are determined in which employees of the selected business role are also members.

To display detailed information about assignments

- To display the report, select the base object from the navigation or the result list and select the **Overview of all assignments** report.
- Click the **Used by** button in the report toolbar to select the role class for which you want to determine whether roles exist that contain employees with the selected base object.

  All the roles of the selected role class are shown. The color coding of elements identifies the role in which there are employees with the selected base object. The meaning of the report control elements is explained in a separate legend. To access the legend, click the icon in the report's toolbar.
- Double-click a control to show all child roles belonging to the selected role.
- By clicking the button in a role's control, you display all employees in the role with the base object.
- Use the small arrow next to to start a wizard that allows you to bookmark this list of employees for tracking. This creates a new business role to which the employees are assigned.

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

Table 41: 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 A

Configuration parameters for managing an Azure Active Directory environment

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

Table 42: Configuration parameters

Configuration parameter	Description
TargetSystem | AzureAD	Preprocessor relevant configuration parameter for controlling the database model components for the administration of the Azure Active Directory target system. If the parameter is set, the target system components are available. Changes to this parameter require the database to be recompiled.
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 **TargetSystem | AzureAD | DefaultAddress** configuration parameter.
TargetSystem | AzureAD | Accounts | InitialRandomPassword | SendTo |	This configuration parameter contains the name of the mail template sent to provide users with the login data for their user accounts. The **Employee - new user account created** mail template is used.

Configuration parameter	Description
MailTemplateAccountName	
TargetSystem | AzureAD | Accounts | InitialRandomPassword | SendTo | MailTemplatePassword	This configuration parameter contains the name of the mail template sent to provide users with information about their initial password. The **Employee - initial password for new user account** mail template is used.
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. The **Employee - new user account with default properties created** mail template is used.
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 parameter specifies whether employees are automatically assigned to disabled user accounts. User accounts do not obtain an account definition.
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.

Configuration parameter	Description
TargetSystem | AzureAD | PersonExcludeList	List of all user accounts for which automatic employee assignment should not take place. Names are listed in a pipe (|) delimited list that is handled as a regular search pattern. Example: `ADMINISTRATOR`

Appendix B

Default project template for Azure Active Directory

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

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

The template uses mappings for the following schema types.

Table 43: 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 and other inquiries, such as licensing, support, and renewals, visit https://www.oneidentity.com/company/contact-us.aspx.

Technical support resources

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

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

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

Index

A

account definition 36
- add to IT Shop 51
- assign automatically 49
- assign to all employees 49
- assign to Azure Active Directory tenant 52
- assign to business role 48
- assign to cost center 47
- assign to department 47
- assign to employee 46, 49
- assign to location 47
- assign to system roles 50
- create 37
- delete 53
- IT operating data 42, 44
- manage level 40

architecture overview 8

Azure Active Directory
- use case 14

Azure Active Directory administrator role 123
- add to IT Shop 129
- add to system role 128
- assign extended properties 132
- assign to business role 127
- assign to cost center 125
- assign to department 125
- assign to location 125
- assign user account 96, 125, 128
- Azure Active Directory tenant 123
- category 123, 131
- display name 123
- edit 123
- risk index 123
- service item 123
- template 123

Azure Active Directory domain 79

Azure Active Directory duty roster 133, 135
- disabled service plan
  - add to IT Shop 140, 149
  - add to system role 149
  - assign to business role 147
  - assign to cost center 145
  - assign to department 145
  - assign to location 145
  - assign user account 98, 145, 148
  - category 152
  - edit 144
  - effective 151
  - exclusion 151

Azure Active Directory group
- add to IT Shop 114
- add to system role 113
- alias 107
- assign extended properties 121
- assign group 116
- assign to business role 111
- assign to cost center 110
- assign to department 110
- assign to location 110
- assign user account 96, 109, 112

Azure Active Directory tenant 107
category 107, 119
delete 122
distribution group 106
edit 107
effective 117
email address 107
exclusion 117
group type 106-107
mail-enabled security policy 106
Office 365 group 106
owner 121
risk index 107
security group 106-107
service item 107
Azure Active Directory license 133
Azure Active Directory subscription 133
add to IT Shop 140
add to system role 139
assign extended properties 143, 152
assign to business role 137
assign to cost center 136
assign to department 136
assign to location 136
assign user account 97, 135, 138, 145
category 142
edit 134
effective 142
exclusion 142
Azure Active Directory tenant
account definition 76
account definition (initial) 52
application roles 9
category 78, 119, 131, 142, 152
edit 75
employee assignment 101
local Active Directory 78
overview of all assignments 155
report 154
synchronization 76
target system manager 9, 67, 76
Azure Active Directory user account
account definition 52, 90
account manager 93
alias 90
assign administrator role 96, 128
assign disabled service plan 98, 148
assign employee 81, 88, 90, 99
assign extended properties 98
assign group 96, 112
assign subscription 97, 138
Azure Active Directory tenant 90
category 90, 119, 131, 142, 152
company 93
delete 104
department 92-93
disable 90, 103
domain 90
email address 90, 92
employee 90
identity 90
Immutable identifier 94
inherit group 90
job description 93
local user account 94
location 90
lock 104
login name 90
manage 81

manage level 90, 95
password 90
initial 66
password policies 90
privileged user account 90
proxy address 92
restore 104
risk index 90
set up 88
SID 94
town 92

C

calculation schedule
disable 33
configuration parameter 157

D

default user accounts 84
direction of synchronization
direction target system 18, 26
in Manager 18

E

email notification 66
employee assignment
automatic 99
manual 102
remove 102
search criteria 101
table column 101
exclusion definition 117, 142, 151

I

identity 82
IT operating data
change 45
IT Shop shelf
assign account definition 51

J

Job server
edit 15
load balancing 32

L

load balancing 32
login data 66

M

membership
modify provisioning 31

N

notification 66

O

object
delete immediately 28
outstanding 28
publish 28
One Identity Manager
administrator 9
register as application 14

target system administrator 9
target system manager 9, 67
user 9
outstanding object 28

P

password
initial 66
password policy 55
assign 57
character sets 61
check password 65
conversion script 62-63
default policy 57, 59
display name 59
edit 59
error message 59
excluded list 65
failed logins 60
generate password 65
initial password 60
name components 60
password age 60
password cycle 60
password length 60
password strength 60
predefined 55
test script 62
project template 160
provisioning
accelerate 32
members list 31

S

schema
changes 27
shrink 27
update 27
single object synchronization
accelerate 32
synchronization
authorizations 13
base object
create 27
configure 18, 25
connection parameter 18, 25, 27
different domains 27
extended schema 27
prevent 33
scope 25
set up 12
start 18
synchronization project
create 18
target system schema 27
user 13
variable 25
variable set 27
workflow 18, 26
synchronization analysis report 33
synchronization configuration
customize 25-27
synchronization log 24
synchronization project
create 18
disable 33
edit 79

project template 160
synchronization server
configure 15
install 15
Job server 15
synchronization workflow
create 18, 26

T

target system synchronization 28
template
IT operating data, modify 45

U

user account
administrative user account 85-86
apply template 45
default user accounts 84
identity 82
password
notification 66
privileged user account 82, 87
type 82, 84, 87