



One Identity Manager 9.2

Administration Guide for Connecting to Exchange Online

Copyright 2024 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 website (<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/trademark-information.aspx. 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 Exchange Online
Updated - 17 October 2024, 09:23

For the most recent documents and product information, see [Online product documentation](#).

Contents

| | |
|--|-----------|
| About this guide | 9 |
| Managing Exchange Online environments | 10 |
| Architecture overview | 10 |
| One Identity Manager users for managing Exchange Online | 11 |
| Configuration parameters for managing Exchange Online environments | 13 |
| Synchronizing an Exchange Online environment | 14 |
| Setting up Exchange Online synchronization | 15 |
| Users and permissions for synchronizing with Exchange Online | 16 |
| Installing the Exchange Online PowerShell V3 module | 18 |
| Setting up the Exchange Online synchronization server | 19 |
| System requirements for the Exchange Online synchronization server | 19 |
| Installing One Identity Manager Service with an Exchange Online connector | 20 |
| Preparing the administrative workstation for access to Exchange Online | 23 |
| Preparing a remote connection server for access to Exchange Online | 24 |
| Creating a synchronization project for initial synchronization of an Exchange Online environment | 25 |
| Information required for Exchange Online synchronization projects | 25 |
| Creating an initial synchronization project for Exchange Online | 27 |
| Exchange Online synchronization features | 31 |
| Configuring the synchronization log | 33 |
| Customizing the synchronization configuration | 34 |
| How to configure Exchange Online synchronization | 35 |
| Changing system connection settings of Exchange Online | 36 |
| Editing connection parameters in the variable set | 36 |
| Editing target system connection properties | 37 |
| Advanced settings for the Exchange Online connector | 38 |
| Updating schemas | 41 |
| Speeding up Exchange Online synchronization with revision filtering | 42 |
| Configuring the provisioning of memberships | 43 |
| Configuring single object synchronization | 45 |
| Accelerating provisioning and single object synchronization | 46 |

| | |
|--|-----------|
| Running synchronization | 47 |
| Starting synchronization | 47 |
| Deactivating synchronization | 48 |
| Displaying synchronization results | 49 |
| Synchronizing single objects | 50 |
| Tasks following synchronization | 51 |
| Post-processing outstanding objects | 51 |
| Adding custom tables to the target system synchronization | 53 |
| Managing Exchange Online mail users and Exchange Online mail contacts through account definitions | 53 |
| Troubleshooting | 54 |
| Ignoring data error in synchronization | 55 |
| Pausing handling of target system specific processes (Offline mode) | 56 |
| Basic data for managing an Exchange Online environment | 58 |
| Account definitions for Exchange Online mail users and Exchange Online mail contacts | 59 |
| Creating account definitions | 60 |
| Editing account definitions | 61 |
| Main data for account definitions | 61 |
| Editing manage levels | 63 |
| Creating manage levels | 64 |
| Assigning manage levels to account definitions | 65 |
| Main data for manage levels | 65 |
| Creating mapping rules for IT operating data | 66 |
| Entering IT operating data | 67 |
| Modify IT operating data | 69 |
| Assigning account definitions to identities | 69 |
| Assigning account definitions to departments, cost centers, and locations | 71 |
| Assigning account definitions to business roles | 71 |
| Assigning account definitions to all identities | 72 |
| Assigning account definitions directly to identities | 73 |
| Assigning account definitions to system roles | 73 |
| Adding account definitions in the IT Shop | 74 |
| Assigning account definitions to Azure Active Directory tenants | 76 |
| Deleting account definitions | 77 |
| Target system managers for Exchange Online | 79 |

| | |
|---|------------|
| Job server for Exchange Online-specific process handling | 81 |
| General main data for Job servers | 82 |
| Specifying server functions | 85 |
| Exchange Online organization configuration | 87 |
| Extensions for Azure Active Directory tenants | 87 |
| Displaying hierarchical address books | 88 |
| Exchange Online public folders | 89 |
| Exchange Online policies | 89 |
| Exchange Online mailboxes | 91 |
| Creating Exchange Online mailboxes | 92 |
| Editing main data of Exchange Online mailboxes | 93 |
| General main data for Exchange Online mailboxes | 94 |
| Limits and usage of Exchange Online mailboxes | 96 |
| Policies and features of Exchange Online mailboxes | 98 |
| Booking resources for Exchange Online equipment mailboxes and Exchange Online room mailboxes | 100 |
| Booking permissions for Exchange Online equipment mailbox and Exchange Online room mailbox | 103 |
| Adjusting receive restrictions for Exchange Online mailboxes | 103 |
| Exchange Online mailbox permission: Send on behalf | 104 |
| Exchange Online mailbox permission: Send as | 105 |
| Exchange Online mailbox permission: Full access | 106 |
| Specifying moderators for Exchange Online mailboxes | 107 |
| Assigning extended properties to Exchange Online mailbox | 107 |
| Deleting Exchange Online mailboxes | 108 |
| Exchange Online mail users | 109 |
| Creating Exchange Online mail users | 110 |
| Editing main data of Exchange Online mail users | 110 |
| Main data for Exchange Online mail users | 111 |
| Receive restrictions for Exchange Online mail users | 116 |
| Customizing send permissions for Exchange Online mail users | 117 |
| Specifying moderators for Exchange Online mail users | 118 |
| Assigning extended properties to Exchange Online mail users | 118 |
| Deleting Exchange Online mail users | 119 |

| | |
|--|------------|
| Exchange Online mail contacts | 120 |
| Creating Exchange Online mail contacts | 121 |
| Editing main data of Exchange Online mail contacts | 121 |
| Main data for Exchange Online mail contacts | 122 |
| Receive restrictions for Exchange Online mail contacts | 127 |
| Customizing send permissions for Exchange Online mail contacts | 128 |
| Specifying moderators for Exchange Online mail contacts | 128 |
| Assigning extended properties to Exchange Online mail contacts | 129 |
| Deleting Exchange Online mail contacts | 129 |
| | |
| Exchange Online mail-enabled distribution groups | 131 |
| Creating Exchange Online mail-enabled distribution groups | 132 |
| Editing main data for Exchange Online mail-enabled distribution groups | 132 |
| Main data for Exchange Online mail-enabled distribution groups | 133 |
| Receive restrictions for Exchange Online mail-enabled distribution groups | 136 |
| Customizing send permissions for Exchange Online mail-enabled distribution groups | 137 |
| Specifying moderators for Exchange Online mail-enabled distribution groups | 138 |
| Specifying Exchange Online mail-enabled distribution groups | 138 |
| Assigning Exchange Online mail-enabled distribution groups to Exchange Online recipients | 139 |
| Prerequisites for indirect assignment of Exchange Online mail-enabled distribution groups | 141 |
| Assigning Exchange Online mail-enabled distribution groups to departments, cost centers, and locations | 142 |
| Assigning Exchange Online mail-enabled distribution groups to business roles | 143 |
| Adding Exchange Online mail-enabled distribution groups to system roles | 144 |
| Assigning Exchange Online mail-enabled distribution groups to the IT Shop | 145 |
| Adding Exchange Online mail-enabled distribution groups automatically to the IT Shop | 147 |
| Assigning Exchange Online recipients to Exchange Online mail-enabled distribution groups | 149 |
| Assigning Exchange Online mail-enabled distribution groups directly to Exchange Online mailboxes | 150 |
| Assigning Exchange Online mail-enabled distribution groups directly to Exchange Online mail users | 151 |
| Assigning Exchange Online mail-enabled distribution groups directly to Exchange Online mail contacts | 151 |
| Exchange Online mail-enabled distribution group inheritance based on categories | 152 |

| | |
|--|------------|
| Adding Exchange Online dynamic distribution groups to Exchange Online mail-enabled distribution groups | 153 |
| Adding an Exchange Online dynamic distribution group to Exchange Online mail-enabled distribution groups | 153 |
| Adding Exchange Online mail-enabled public folder to Exchange Online mail-enabled distribution groups | 154 |
| Assigning extended properties to Exchange Online mail-enabled distribution groups | 154 |
| Deleting Exchange Online mail-enabled distribution groups | 155 |
| Exchange Online Office 365 groups | 156 |
| Creating Exchange Online Office 365 groups | 156 |
| Editing main data of Exchange Online Office 365 groups | 157 |
| Exchange Online Office 365 group main data | 157 |
| Customizing receive restrictions for Exchange Online Office 365 groups | 161 |
| Assigning owners to Exchange Online Office 365 groups | 161 |
| Assigning subscribers to Exchange Online Office 365 groups | 162 |
| Assigning Exchange Online Office 365 groups to Azure Active Directory user accounts | 163 |
| Prerequisites for indirect assignment of Office 365 groups to Azure Active Directory user accounts | 164 |
| Assigning Exchange Online Office 365 groups to departments, cost centers, and locations | 166 |
| Assigning Exchange Online Office 365 groups to business roles | 167 |
| Adding Exchange Online Office 365 groups to system roles | 168 |
| Adding Exchange Online Office 365 groups to the IT Shop | 169 |
| Adding Exchange Online Office 365 groups automatically to the IT Shop | 171 |
| Assigning Exchange Online Office 365 groups directly to Azure Active Directory user accounts | 172 |
| Assigning Azure Active Directory user accounts directly to Exchange Online Office 365 groups | 173 |
| Exchange Online Office 365 group inheritance based on categories | 174 |
| Assigning extended properties to Exchange Online Office 365 groups | 175 |
| Deleting Exchange Online Office 365 groups | 175 |
| Exchange Online dynamic distribution groups | 176 |
| Editing main data of Exchange Online dynamic distribution groups | 176 |
| Main data for Exchange Online dynamic distribution groups | 177 |
| Customizing receive restrictions for Exchange Online dynamic distribution groups | 179 |
| Customizing send permissions for Exchange Online dynamic distribution groups | 180 |

| | |
|---|------------|
| Specifying moderators for Exchange Online dynamic distribution groups | 180 |
| Adding Exchange Online mail-enabled distribution groups to Exchange Online dynamic distribution groups | 181 |
| Deleting Exchange Online dynamic distribution groups | 182 |
| Exchange Online mail-enabled public folders | 183 |
| Displaying information about Exchange Online mail-enabled public folders | 183 |
| Assigning Exchange Online mail-enabled distribution groups to Exchange Online mail-enabled public folders | 184 |
| Reports about Exchange Online objects | 186 |
| Appendix: Configuration parameters for managing an Exchange Online environment | 188 |
| Appendix: Default project template for Exchange Online | 191 |
| Appendix: Editing Exchange Online system objects | 192 |
| Appendix: Exchange Online connector settings | 194 |
| About us | 196 |
| Contacting us | 196 |
| Technical support resources | 196 |
| Index | 197 |

About this guide

The *One Identity Manager Administration Guide for Connecting to Exchange Online* describes how you set up synchronization of Exchange Online with One Identity Manager. The guide explains how to use One Identity Manager to manage the mailboxes, email users, mail contacts, mail-enabled distribution groups, and Office 365 groups of your Exchange Online environment.

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

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

Available documentation

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

Managing Exchange Online environments

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

The system information for the Exchange Online structure is loaded into the One Identity Manager database during data synchronization. It is only possible to customize certain system information in One Identity Manager due to the complex dependencies and far reaching effects of changes.

For more information about the Exchange Online structure, see the *Exchange Online documentation* from Microsoft.

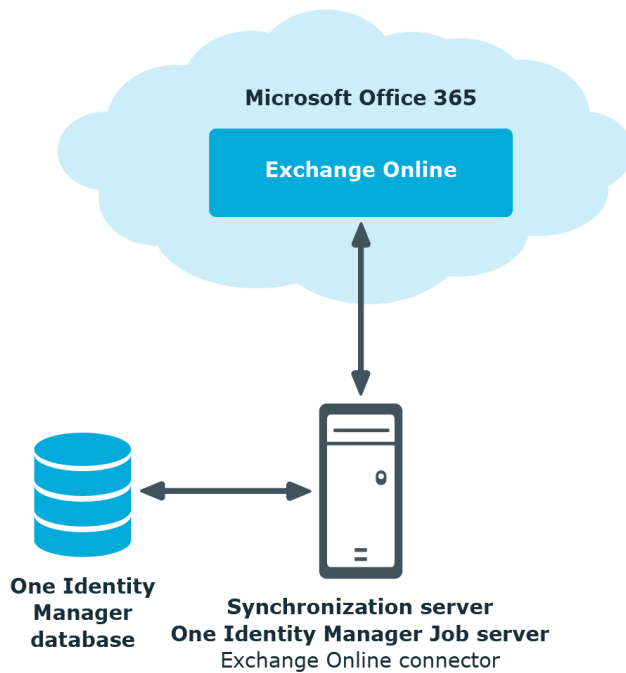
NOTE: The Exchange Online module must be installed as a prerequisite for managing One Identity Manager in Exchange Online Module For more information about installing, see the *One Identity Manager Installation Guide*.

Architecture overview

To access Exchange Online organizational data, the Exchange Online connector is installed on a synchronization server. The synchronization server ensures data is compared between the One Identity Manager database and Exchange Online. The Exchange Online connector is part of the Exchange Online Module and responsible for communicating with the Microsoft Office 365 subscriptions of Exchange Online in the cloud. The Exchange Online PowerShell V3 module is used to access Exchange Online data.

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

Figure 1: The synchronization architecture



One Identity Manager users for managing Exchange Online

The following users are used for setting up and administration of Exchange Online.

Table 1: Users

| User | Tasks |
|------------------------------|--|
| Target system administrators | <p>Target system administrators must be assigned to the Target systems Administrators application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none"> • Administer application roles for individual target system types. • Specify the target system manager. • Set up other application roles for target system managers if required. • Specify which application roles for target system managers are mutually exclusive. • Authorize other identities to be target system |

| User | Tasks |
|-------------------------------------|---|
| Target system managers | <p data-bbox="619 264 823 293">administrators.</p> <ul data-bbox="588 315 1385 376" style="list-style-type: none"> <li data-bbox="588 315 1385 376">• Do not assume any administrative tasks within the target system. <p data-bbox="539 400 1305 499">Target system managers must be assigned to the Target systems Exchange Online application role or a child application role.</p> <p data-bbox="539 517 956 546">Users with this application role:</p> <ul data-bbox="588 568 1394 1137" style="list-style-type: none"> <li data-bbox="588 568 1299 598">• Assume administrative tasks for the target system. <li data-bbox="588 620 1262 649">• Create, change, or delete target system objects. <li data-bbox="588 672 1209 701">• Edit password policies for the target system. <li data-bbox="588 723 1118 752">• Prepare groups to add to the IT Shop. <li data-bbox="588 775 1390 835">• Can add identities that do not have the Primary identity identity type. <li data-bbox="588 857 1394 956">• Configure synchronization in the Synchronization Editor and define the mapping for comparing target systems and One Identity Manager. <li data-bbox="588 978 1294 1039">• Edit the synchronization's target system types and outstanding objects. <li data-bbox="588 1061 1390 1137">• Authorize other identities within their area of responsibility as target system managers and create child application roles if required. |
| One Identity Manager administrators | <p data-bbox="539 1167 1385 1265">One Identity Manager administrator and administrative system users Administrative system users are not added to application roles.</p> <p data-bbox="539 1283 1043 1312">One Identity Manager administrators:</p> <ul data-bbox="588 1335 1390 1769" style="list-style-type: none"> <li data-bbox="588 1335 1342 1433">• Create customized permissions groups for application roles for role-based login to administration tools in the Designer as required. <li data-bbox="588 1456 1390 1554">• Create system users and permissions groups for non role-based login to administration tools in the Designer as required. <li data-bbox="588 1576 1366 1637">• Enable or disable additional configuration parameters in the Designer as required. <li data-bbox="588 1659 1329 1688">• Create custom processes in the Designer as required. <li data-bbox="588 1711 1203 1740">• Create and configure schedules as required. <li data-bbox="588 1762 1305 1792">• Create and configure password policies as required. |

Configuration parameters for managing Exchange Online environments

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

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

For more information, see [Configuration parameters for managing an Exchange Online environment](#) on page 188.

Synchronizing an Exchange Online environment

NOTE: Synchronization of the following cloud deployments with the Exchange Online connector is supported.

- Microsoft 365 Global Service
- Microsoft 365 GCC High

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

This sections explains how to:

- Set up synchronization to import initial data from Exchange Online Organization to the One Identity Manager database.
- Adjust a synchronization configuration
- Start and deactivate the synchronization.
- Analyze synchronization results.

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

Detailed information about this topic

- [Setting up Exchange Online synchronization](#) on page 15
- [Customizing the synchronization configuration](#) on page 34
- [Running synchronization](#) on page 47
- [Tasks following synchronization](#) on page 51
- [Troubleshooting](#) on page 54
- [Ignoring data error in synchronization](#) on page 55
- [Editing Exchange Online system objects](#) on page 192

Setting up Exchange Online synchronization

The Synchronization Editor provides a project template that can be used to set up Exchange Online synchronization. You use these project templates to create synchronization projects with which you import the data from an Exchange Online organization into your One Identity Manager database. In addition, processes are created that are required to provision changes to target system objects from the One Identity Manager database into the target system.

Prerequisites for synchronizing Exchange Online are:

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

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

To load Exchange Online objects into the One Identity Manager database for the first time

1. Prepare a user account in the Azure Active Directory tenant with sufficient permissions for synchronization.
2. One Identity Manager parts for managing Exchange Online systems are available if the **TargetSystem | AzureAD | ExchangeOnline** configuration parameter is set.
 - In the Designer, check if the configuration parameter is set. Otherwise, set the configuration parameter and compile the database.
NOTE: If you disable the configuration parameter at a later date, model components and scripts that are no longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*.
 - Other configuration parameters are installed when the module is installed. Check the configuration parameters and modify them as necessary to suit your requirements.
3. Install and configure a synchronization server and declare the server as a Job server in One Identity Manager.
4. Create a synchronization project with the Synchronization Editor.

Detailed information about this topic

- [Users and permissions for synchronizing with Exchange Online](#) on page 16
- [Setting up the Exchange Online synchronization server](#) on page 19
- [Preparing the administrative workstation for access to Exchange Online](#) on page 23
- [Preparing a remote connection server for access to Exchange Online](#) on page 24

- [Creating a synchronization project for initial synchronization of an Exchange Online environment](#) on page 25
- [Exchange Online synchronization features](#) on page 31
- [Customizing the synchronization configuration](#) on page 34
- [Configuration parameters for managing an Exchange Online environment](#) on page 188
- [Default project template for Exchange Online](#) on page 191

Users and permissions for synchronizing with Exchange Online

The following users play a role in synchronizing One Identity Manager with Exchange Online.

Table 2: Users for synchronization

| User | Permissions |
|---|--|
| Exchange Online access with user account or App-only authentication | <p>Synchronization with Exchange Online supports authentication through a user account with sufficient permissions or app-only authentication using a self-signed certificate.</p> <ul style="list-style-type: none"> • To authenticate with a specific user account, provision a user account with at least the following permissions. <ul style="list-style-type: none"> • Member of the Recipient Management Exchange Online role group • Member of the Records Management Exchange Online role group • Member of the View-Only Organization Management Exchange Online role group • Member of the Security Group Creation and Membership Exchange Online role group <p>NOTE: Create a new role group in Exchange Online. Assign the role and the user account to this role group.</p> • Member of the Group administrator Azure Active Directory administrator role <p>NOTE: The user account used to access Exchange Online must not use multifactor</p> |

User

Permissions

authentication to allow automated logins in a user context.

Use the Exchange Admin Center to assign Exchange Online role groups to user accounts. Use the Azure Active Directory Admin Center to assign the Azure Active Directory administrator role to the user account. For example, you can reach the Admin Center over <https://admin.microsoft.com/>. For more information on managing permissions in Exchange Online and in Azure Active Directory, see the *Microsoft documentation*.

- To use app-only authentication with a self-signed certificate, register and configure an application for Exchange Online PowerShell in the Azure Active Directory tenant.

NOTE: Adding and editing **O3EUnifiedGroups** is not possible by app-only authentication. To use these permissions, authentication with a user account is required.

For more information on how to set up app-only authentication, see [Set up app-only authentication](#).

- For the Exchange Online connector, assign at least the **Global administrator** and the **Exchange administrator** Azure Active Directory administrator roles.

One Identity Manager Service user account

The user account for the One Identity Manager Service requires user permissions to carry out operations at file level (adding and editing directories and files).

The user account must belong to the **Domain users** group.

The user account must have the **Login as a service** extended user permissions.

The user account requires permissions for the internal web service.

NOTE: If the One Identity Manager Service runs under the network service (**NT Authority\NetworkService**), you can grant permissions for the internal web service with the following command line call:

| User | Permissions |
|--|---|
| User for accessing the One Identity Manager database | <pre data-bbox="654 257 1197 358">netsh http add urlacl url=http://<IP address>:<port number>/ user="NT AUTHORITY\NETWORKSERVICE"</pre> <p data-bbox="646 369 1356 481">The user account needs full access to the One Identity Manager Service installation directory in order to automatically update One Identity Manager.</p> <p data-bbox="646 492 1324 560">In the default installation, One Identity Manager is installed under:</p> <ul data-bbox="694 571 1348 728" style="list-style-type: none"> • %ProgramFiles(x86)%\One Identity (on 32-bit operating systems) • %ProgramFiles%\One Identity (on 64-bit operating systems) |

Installing the Exchange Online PowerShell V3 module

The Exchange Online connector uses Exchange Online PowerShell V3 module to access data in Exchange Online.

- The Exchange Online PowerShell V3 module must be installed on the synchronization server.
- If Exchange Online is accessed directly from the workstation on which Synchronization Editor is installed, the Exchange Online PowerShell V3 module must also be installed on this workstation.
- If direct access from the workstation to Exchange Online is not possible, you can set up a remote connection. The Exchange Online PowerShell V3 module must be installed on the remote connection server.

For more information about prerequisites and installing the Exchange Online PowerShell V3 module, see the [Exchange Online PowerShell documentation from Microsoft](#).

Related topics

- [Setting up the Exchange Online synchronization server on page 19](#)
- [Preparing the administrative workstation for access to Exchange Online on page 23](#)
- [Preparing a remote connection server for access to Exchange Online on page 24](#)

Setting up the Exchange Online synchronization server

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

The One Identity Manager Service with the Exchange Online connector must be installed on the synchronization server.

IMPORTANT:

- The Exchange Online connector uses Exchange Online PowerShell V3 module to access data in Exchange Online. The Exchange Online PowerShell V3 module must be installed on the synchronization server.
- If you want to use app-only authentication through a self-signed certificate to authenticate the Exchange Online connector against Exchange Online, the certificate must be installed on the synchronization server in the certificate store of the user under which the One Identity Manager Service is running.

Detailed information about this topic

- [System requirements for the Exchange Online synchronization server](#) on page 19
- [Installing the Exchange Online PowerShell V3 module](#) on page 18
- [Installing One Identity Manager Service with an Exchange Online connector](#) on page 20
- [Users and permissions for synchronizing with Exchange Online](#) on page 16

System requirements for the Exchange Online synchronization server

To set up synchronization with an Exchange Online environment, a server has to be available that has the following software installed on it:

- Windows operating system
The following versions are supported:
 - Windows Server 2022
 - Windows Server 2019
 - Windows Server 2016
 - Windows Server 2012 R2
 - Windows Server 2012
- Microsoft .NET Framework version 4.8 or later

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

- PowerShell 5.1 or later
- Exchange Online PowerShell module version 3.2.0 or later

Related topics

- [Installing the Exchange Online PowerShell V3 module](#) on page 18
- [Installing One Identity Manager Service with an Exchange Online connector](#) on page 20

Installing One Identity Manager Service with an Exchange Online connector

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

Table 3: Properties of the Job server

| Property | Value |
|-----------------|---------------------------------------|
| Server function | Exchange Online connector |
| Machine role | Server Job Server Exchange Online |

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).

To set up a Job server, perform the following steps.

1. Create a Job server and install and configure the One Identity Manager Service.

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

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

Use the Server Installer to install the One Identity Manager Service locally or remotely.

To remotely install the One Identity Manager Service, provide an administrative workstation on which the One Identity Manager components are installed. Ensure that the One Identity Manager components are installed on the server before installing locally. For more information about installing One Identity Manager components, see the *One Identity Manager Installation Guide*.

2. If you are working with an encrypted One Identity Manager database, declare the database key in the One Identity Manager Service. For more information about working with an encrypted One Identity Manager database, see the *One Identity Manager Installation Guide*.
3. 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 more information about connection data, see the *One Identity Manager Configuration Guide*.

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

1. Start the Server Installer program.

NOTE: To install remotely, start the Server Installer program on your administrative workstation. To install locally, start the program on the server.

2. On the **Database connection** page, enter the valid connection credentials for the One Identity Manager database.

You can connect via the application server or directly to connect to the database.

3. On the **Server properties** page, specify the server on which you want to install the One Identity Manager Service.

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

- OR -

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

- b. Enter the following data for the Job server.

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

Syntax:

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

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

4. On the **Machine roles** page, select **Exchange Online**.
5. On the **Server functions** page, select **Exchange Online connector (via PowerShell)**.
6. On the **Service Settings** page, enter the connection data and check the One Identity Manager Service configuration.

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

For a direct connection to the database:

- a. In the module list, 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.
- d. Click **OK**.

For a connection to the application server:

- a. In the module list, select the **Process collection** entry and click the **Insert** button.
 - b. Select **AppServerJobProvider** and click **OK**.
 - c. In the module list, select **Process collection > AppServerJobProvider**.
 - d. Click the **Connection parameter** entry, then click the **Edit** button.
 - e. Enter the address (URL) for the application server and click **OK**.
 - f. Click the **Authentication data** entry and click the **Edit** button.
 - g. In the **Authentication method** dialog, select the authentication module for logging in. Depending on the authentication module, other data may be required, such as user and password. For more information about One Identity Manager authentication modules, see the *One Identity Manager Authorization and Authentication Guide*.
 - h. Click **OK**.
7. To configure the installation, click **Next**.
 8. Confirm the security prompt with **Yes**.
 9. On the **Select installation source** page, select the directory with the install files. Change the directory if necessary.
 10. On the **Service access** page, enter the service's installation data.
 - **Computer:** Select the server, on which you want to install and start the service, from the menu or enter the server's name or IP address.

To run the installation locally, select **Local installation** from the menu.

- **Service account:** Enter the details of the user account that the One Identity Manager Service is running under. Enter the user account, the user account's password and password confirmation.

The service is installed using the user account with which you are logged in to the administrative workstation. If you want to use another user account for installing the service, you can enter it in the advanced options.

You can also change the One Identity Manager Service details, such as the installation directory, name, display name, and the One Identity Manager Service description, using the advanced options.

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

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

12. 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**.

Preparing the administrative workstation for access to Exchange Online

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

- PowerShell Version 5.1 or later
- Exchange Online PowerShell module version 3.2.0 or later

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

Related topics

- [Installing the Exchange Online PowerShell V3 module on page 18](#)
- [Users and permissions for synchronizing with Exchange Online on page 16](#)
- [Preparing a remote connection server for access to Exchange Online on page 24](#)

Preparing a remote connection server for access to Exchange Online

To configure synchronization with a target system, One Identity Manager must load the data from the target system. One Identity Manager communicates directly with the target system to do this. Sometimes direct access from the workstation, on which the Synchronization Editor is installed, is not possible. For example, because of the firewall configuration or the workstation does not fulfill the necessary hardware and software requirements. If direct access is not possible from the workstation, you can set up a remote connection.

Remote connection server configuration:

- One Identity Manager Service is started
- **RemoteConnectPlugin** is installed and an authentication method is set up
- PowerShell version 5.1 or above is installed
- Exchange Online PowerShell V2 module is installed.
- Exchange Online connector is installed

The remote connection server must be declared as a Job server in One Identity Manager. The Job server name is required.

TIP: The remote connection server requires the same configuration as the synchronization server (with regard to the installed software and entitlements). Use the synchronization server as remote connection server as well by installing the RemoteConnectPlugin.

For more detailed information about setting up a remote connection, see the *One Identity Manager Target System Synchronization Reference Guide*.

Related topics

- [Setting up the Exchange Online synchronization server](#) on page 19
- [Installing the Exchange Online PowerShell V3 module](#) on page 18
- [Installing One Identity Manager Service with an Exchange Online connector](#) on page 20
- [Users and permissions for synchronizing with Exchange Online](#) on page 16
- [Preparing the administrative workstation for access to Exchange Online](#) on page 23

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

Use the Synchronization Editor to configure synchronization between the One Identity Manager database and Exchange Online environment. The following describes the steps for initial configuration of a synchronization project. For more information about setting up synchronization, see the *One Identity Manager Target System Synchronization Reference Guide*.

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

IMPORTANT: Each Exchange Online environment should have its own synchronization project.

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

NOTE: When setting up the synchronization, note the recommendations described under [Exchange Online synchronization features](#) on page 31.

Prerequisites for setting up a synchronization project

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

Related topics

- [Information required for Exchange Online synchronization projects](#) on page 25
- [Creating an initial synchronization project for Exchange Online](#) on page 27
- [Exchange Online synchronization features](#) on page 31
- [Customizing the synchronization configuration](#) on page 34
- [Default project template for Exchange Online](#) on page 191
- [Exchange Online connector settings](#) on page 194

Information required for Exchange Online synchronization projects

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

Table 4: Information required to set up a synchronization project

| Data | Explanation |
|--|--|
| Authentication information | <p>Synchronization with Exchange Online supports authentication through a user account with sufficient permissions or through app-only authentication using a self-signed certificate.</p> <p>For more information, see Users and permissions for synchronizing with Exchange Online on page 16.</p> <p>Information required to authenticate through a user account:</p> <ul style="list-style-type: none">• User account and password for logging in to Exchange Online. <p>Example:</p> <pre><user>@<domain.com> sync.user@<yourorganization>.onmicrosoft.com</pre> <p>Information required to authenticate using a self-signed certificate (app-only authentication):</p> <ul style="list-style-type: none">• Application ID created when the application is registered for Exchange Online PowerShell in the Azure Active Directory tenant.• Self-signed certificate thumbprint <p>For more information on how to set up app-only authentication, see Set up app-only authentication.</p> |
| Organization domains | <p>Azure Active Directory name of the domain for logging in to Azure Active Directory.</p> <p>Example:</p> <pre><yourorganization>.onmicrosoft.com</pre> |
| Synchronization server for Exchange Online | <p>All One Identity Manager Service actions are run against the target system environment on the synchronization server. Data entries required for synchronization and administration with the One Identity Manager database are processed by the synchronization server.</p> <p>The One Identity Manager Service with the Exchange Online connector must be installed on the synchronization server.</p> <p>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.</p> <ul style="list-style-type: none">• Server function: Exchange Online connector• Machine role: Server Job Server Exchange Online |

| Data | Explanation |
|---|---|
| One Identity Manager database connection data | <p>For more information, see Setting up the Exchange Online synchronization server on page 19.</p> <ul style="list-style-type: none"> • Database server • Database name • SQL Server login and password • Specifies whether integrated Windows authentication is used <p>Use of the integrated Windows authentication is not recommended. If you decide to use it anyway, ensure that your environment supports Windows authentication.</p> |
| Remote connection server | For more information, see Preparing a remote connection server for access to Exchange Online on page 24. |

Creating an initial synchronization project for Exchange Online

IMPORTANT: Each Exchange Online environment should have its own synchronization project.

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

- Run in default mode
- Started from the Launchpad

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

To set up initial synchronization project for Exchange Online

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

NOTE: If synchronization is run by an application server, connect the database through the application server.
2. Select the **Target system type Exchange Online** entry and click **Start**.
This starts the Synchronization Editor's project wizard.
3. On the wizard's start page, click **Next**.
4. 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.

Select the **Connect using remote connection server** and enter the remote connection properties.

Remote connection properties

- **Access parameters**

- **Server:** Full server name or IP address of the server.

To select an existing Job server as the remote connection server, click  and select the server from the menu. This displays all the Job servers that have the **One Identity Manager Service installed** server function selected.

- **Port:** Port that is configured for the RemoteConnectPlugin.

- **Authentication**

If **SecretAuthentication** is configured for the RemoteConnectPlugin:

- **Secret:** Secret used by the Synchronization Editor to authenticate on the RemoteConnectPlugin.

If **ADGroupAuthentication** is configured for the RemoteConnectPlugin, no data is required.

- **Options**

- **Request timeout:** Maximum time allowed for a server query in seconds. If the time is exceeded, the request is canceled.
- **Accept self-signed certificates:** Specifies whether self-signed certificates can be accepted.

5. On the **Deployment/organization domain** page, you record the following information.

- **Deployment:** Select the cloud deployment where your Exchange Online environment will run. Your options include **Microsoft 365 global service** and **Microsoft 365 GCC High**.

- **Organization domain:** Enter the Azure Active Directory name of the domain.

Example:

<yourorganization>.onmicrosoft.com

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

- If you want to authenticate with a specific user account, enter the following information.

- **User name:** Enter the fully qualified name (FQDN) of the user account for logging in.

Example:


<user>@<domain.com>

sync.user@<yourorganization>.onmicrosoft.com

- **Password:** Enter the pass word of the user account.
- If you want to authenticate with a self-signed certificate (the app-only authentication), enter the following information.
 - **Application ID:** Application ID created when the application is registered for Exchange Online PowerShell in the Azure Active Directory tenant.
 - **Certificate thumbprint:** Self-signed certificate thumbprint.

Click to test the connection parameters.

NOTE:

- Use the  **Add set** button to enter more connection parameters. These connection parameters are queried cyclically by the Exchange Online connector when queries are sent to Exchange Online. By using multiple connection sets, it takes longer to reach the throttling limit.

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

- If you authenticate with a self-signed certificate, you must ensure that each connection set has its own application registration. The same certificate cannot be used more than once for different application registrations.
- Click **Check all sets** to perform a one-off test of all the connection parameter sets.

7. On the last page of the system connection wizard, click **Finish** to return to the project wizard.

8. 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.

9. 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.


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

Table 5: Specify target system access

| Option | Meaning |
|--|--|
| Read-only access to target system. | <p>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.</p> <p>The synchronization workflow has the following characteristics:</p> <ul style="list-style-type: none">• 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. | <p>Specifies whether a provisioning workflow is set up in addition to the synchronization workflow for the initial loading of the target system.</p> <p>The provisioning workflow displays the following characteristics:</p> <ul style="list-style-type: none">• 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. |

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

If the synchronization server is not declared as a Job server for this target system 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.

TIP: You can also implement an existing Job server as the synchronization server for this target system.

- To select a Job server, click .

This automatically assigns the server function matching this Job server.

- c. Click **OK**.

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

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

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

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

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

NOTE:

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

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

Related topics

- [Users and permissions for synchronizing with Exchange Online](#) on page 16
- [Information required for Exchange Online synchronization projects](#) on page 25
- [Setting up the Exchange Online synchronization server](#) on page 19
- [Configuring the synchronization log](#) on page 33
- [Customizing the synchronization configuration](#) on page 34
- [Running synchronization](#) on page 47
- [Tasks following synchronization](#) on page 51
- [Default project template for Exchange Online](#) on page 191
- [Exchange Online connector settings](#) on page 194

Exchange Online synchronization features

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

Dependency resolution

By default, automatic dependency resolution for synchronization steps is not set in the synchronization workflow. This reduces the number of calls required to Exchange Online. This can lead to unresolved references during synchronization that are handled in the maintenance phase at the end of synchronization.

Multiple organizations are not supported

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

Changing mailbox types in the Exchange Online portal

The default project template for Exchange Online support the conversion of mailbox types as follows:

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

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

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

Synchronization of mailbox statistic data

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

The following usage information is synchronized:

| Schema property in the Target System | Description |
|--|--|
| AssociatedItemCount | Number of elements associated with this mailbox. |
| DeletedItemCount | Number of deleted elements. |
| DumpsterMessagesPerFolderCountReceiveQuota | Maximum number of messages allowed in a folder in the Recoverable items folder. |

| Schema property in the Target System | Description |
|--|---|
| DumpsterMessagesPerFolderCountWarningQuota | Number of items a folder in the Recoverable items folder can contain before a warning is sent to the user. |
| ItemCount | Number of messages in a mailbox (for example, email, calendar, or contacts) that are visible to the user. |
| LastLoggedOnUserAccount | Name of the last logged on user. |
| LastLogOffTime | Last log off time |
| LastLogonTime | Last log on time |
| StorageLimitStatus | Information about the current storage state with respect to the specified limits. |
| TotalDeletedItemSize | Size of items in the Recoverable Items mailbox. |
| TotalItemSize | Size of items in mailbox in KB. |

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

Number of external slots for the Job server configuration

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

You can set the number of connections for each connection parameter set and customize the connector definition. For more information, see [Advanced settings for the Exchange Online connector](#) on page 38.

Configuring the synchronization log

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

To configure the content of the synchronization log for a system connection

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

To configure the synchronization log for the database connection, in the Synchronization Editor, select the **Configuration > One Identity Manager connection** category.

2. In the **General** section, click **Setup**.
3. In the **Synchronization log** section, set **Create synchronization log**.
4. Enable the data to be logged.

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

5. Click **OK**.

To configure the content of the synchronization log for a synchronization workflow

1. In the Synchronization Editor, select the **Workflows** category.
2. Select a workflow in the navigation view.
3. In the **General** section, click **Edit**.
4. Select the **Synchronization log** tab.
5. Enable the data to be logged.

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

6. Click **OK**.

Synchronization logs are stored for a fixed length of time.

To modify the retention period for synchronization logs

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

Related topics

- [Displaying synchronization results](#) on page 49

Customizing the synchronization configuration

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

groups with One Identity Manager, modifications are provisioned in the Exchange Online system.

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

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

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

Detailed information about this topic

- [Exchange Online synchronization features](#) on page 31
- [How to configure Exchange Online synchronization](#) on page 35
- [Changing system connection settings of Exchange Online](#) on page 36
- [Updating schemas](#) on page 41
- [Speeding up Exchange Online synchronization with revision filtering](#) on page 42
- [Configuring the provisioning of memberships](#) on page 43
- [Configuring single object synchronization](#) on page 45
- [Accelerating provisioning and single object synchronization](#) on page 46

How to configure Exchange Online synchronization

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

To create a synchronization configuration for synchronizing Exchange Online

1. In the Synchronization Editor, open the synchronization project.
2. Check whether the existing mappings can be used to synchronize into the target system. Create new maps if required.
3. Create a new workflow with the workflow wizard.
This creates a workflow with **Target system** as its direction of synchronization.
4. Create a new start up configuration. Use the new workflow to do this.
5. Save the changes.
6. Run a consistency check.

Changing system connection settings of Exchange Online

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

- a. Specify a specialized variable set and change the values of the affected variables.
The default values remain untouched in the default variable set. The variables can be reset to the default values at any time. (Recommended action).
- b. Edit the target system connection with the system connection wizard and change the effected values.
The system connection wizard supplies additional explanations of the settings. The default values can only be restored under particular conditions.

Detailed information about this topic





- [Editing connection parameters in the variable set](#) on page 36
- [Editing target system connection properties](#) on page 37
- [Advanced settings for the Exchange Online connector](#) on page 38
- [Exchange Online connector settings](#) on page 194

Editing connection parameters in the variable set

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

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

To customize connection parameters in a specialized variable set

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Configuration > Target system** category.
3. Open the **Connection parameters** view.
Some connection parameters can be converted to variables here. For other parameters, variables are already created.
4. Select a parameter and click **Convert**.
5. Select the **Configuration > Variables** category.
All specialized variable sets are shown in the lower part of the document view.
6. Select a specialized variable set or click on  in the variable set view's toolbar.
 - To rename the variable set, select the variable set and click the variable set view in the toolbar . Enter a name for the variable set.
7. Select the previously added variable and enter a new value.
8. Select the **Configuration > Start up configurations** category.
9. Select a start up configuration and click **Edit**.
10. Select the **General** tab.
11. Select the specialized variable set in the **Variable set** menu.
12. Select the **Configuration > Base objects** category.
13. Select the base object and click .
- OR -
To add a new base object, click .
14. Select the specialized variable set in the **Variable set** menu.
15. Save the changes.

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

Related topics

- [Editing target system connection properties](#) on page 37

Editing target system connection properties

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

set.

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

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

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

To edit connection parameters using the system connection wizard

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

NOTE: If the default variable set is selected, the default values are overwritten and cannot be restored at a later time.

3. Select the **Configuration > Target system** category.
4. Click **Edit connection**.
This starts the system connection wizard.
5. Follow the system connection wizard instructions and change the relevant properties.
6. Save the changes.

Related topics

- [Editing connection parameters in the variable set](#) on page 36

Advanced settings for the Exchange Online connector

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

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

Number of concurrent connections per connection parameter set

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

Use this option to set the number of concurrent connections for each connection parameter set or for each user account for synchronization. The setting specifies how many concurrent

connections will be created for each user account. The default value is 2. Exchange Online currently allows 3 connections per user account on the server side.

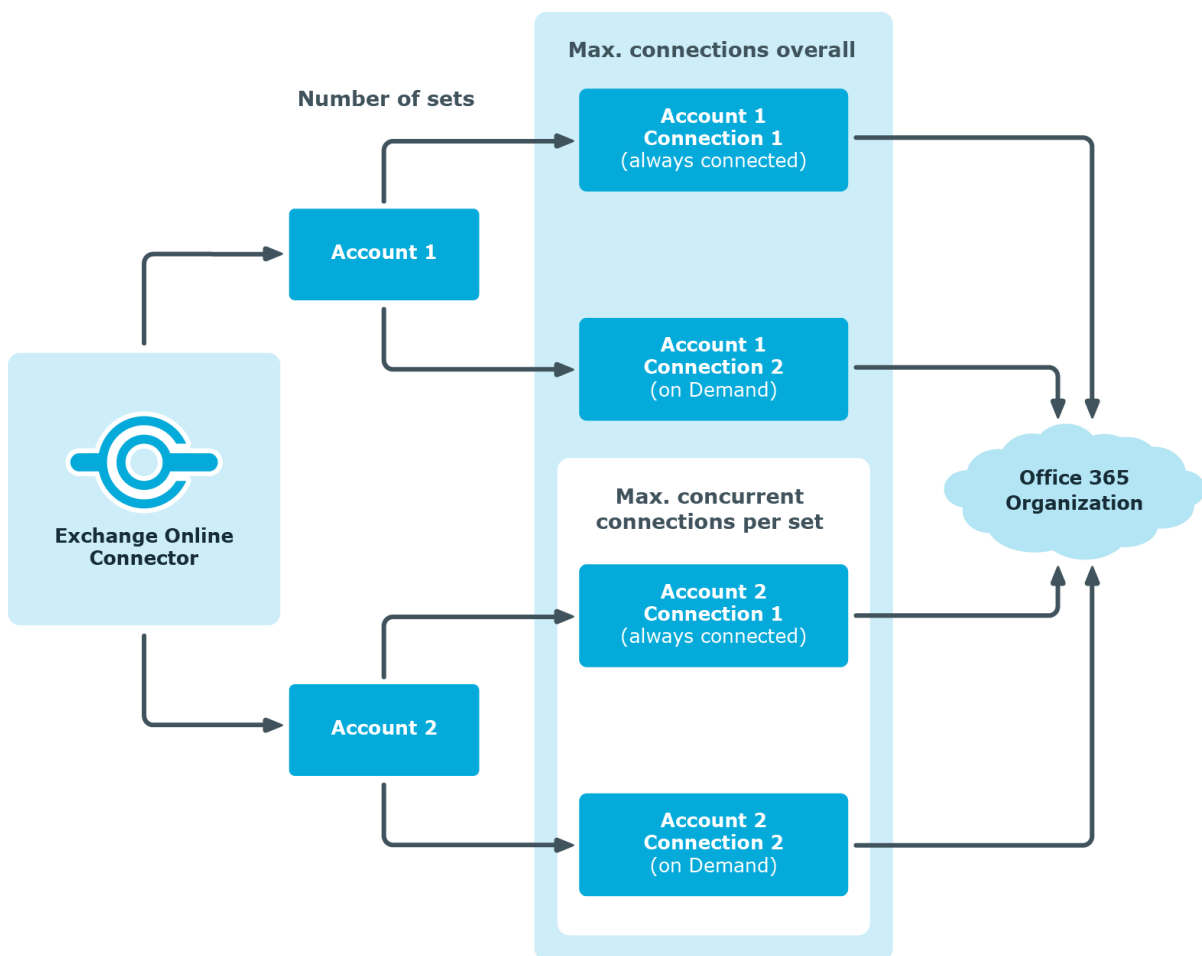
When the Exchange Online connector creates the connection, it creates one PowerShell session per connection parameter set regardless of the number of queries that follow. Further connections are created on demand, for example, when loading multiple objects during the synchronization.

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

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

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

Figure 2: Determining sessions



To change the number of concurrent connections

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Configuration > Target system** category.
1. Click **Edit connection**.
This starts the system connection wizard.
3. On the system connection wizard's start page, enable **Show advanced options**.
4. On the Advanced settings page, in the **concurrent connections per connection parameter set** input field, enter a value between **1** and **3**.
5. Follow the system connection wizard further instructions.
6. Save the changes.

Customizing the connection definition

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

IMPORTANT: The connector definition should only be customized to temporarily work around problems if needed.




IMPORTANT: A customized connection definition is not overwritten when a new version of the connector or an update to the connector definition is released. No patches are applied.

If you customize the connector definition, you must manually apply your changes to any new versions of the connector or updated connector definitions, as required.

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

To customize the connector definition

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Configuration > Target system** category.
3. Click **Edit connection**.
This starts the system connection wizard.
4. Enable **Show advanced options** on the system connection wizard's start page.
5. Customize the connector definition as required on the **Advanced options** page.
 - a. Select **Customize connector definition**.
 - b. Edit the definition according to the instructions given by the support desk staff. You take the following action:

- Choose  to load the definition from a file.
 - Use  to test the definition for errors.
 - Choose  to display the differences to the standard version.
6. Follow the system connection wizard further instructions.
 7. Save the changes.

Updating schemas

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

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

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

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

To update a system connection schema

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Configuration > Target system** category.
- OR -
Select the **Configuration > One Identity Manager connection** category.
3. Select the **General** view and click **Update schema**.
4. Confirm the security prompt with **Yes**.
This reloads the schema data.

To edit a mapping

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

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

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

Speeding up Exchange Online synchronization with revision filtering

When you start synchronization, all synchronization objects are loaded. Some of these objects have not be modified since the last synchronization and, therefore, must not be processed. Synchronization is accelerated by only loading those object pairs that have changed since the last synchronization. One Identity Manager uses revision filtering to accelerate synchronization.

Exchange Online supports revision filtering for the schema types Mailbox, MailUser, MailContact, MailPublicFolder, DistributionGroup, DynamicDistributionGroup, and UnifiedGroup.

You can configure the change time stamp for revision filtering using the following connection parameters in the synchronization project.

- **Use local server time for the revision:** If the value is **true**, the local server time of the server is used for revision filtering. (default) This makes it unnecessary to load target system object for determining the revision. If the value is **false**, the change time stamp of the underlying Azure Active Directory objects are used for revision filtering.

Variable: CP_UseLocalServerTimeAsRevision

- **Max. time difference (local/remote) in minutes:** Defines the maximum time difference in minutes between the synchronization server and the Exchange Online server. The default value is 60 minutes. If the time difference is more than 60 minutes, alter the value.

Variable: CP_LocalServerRevisionMaxDifferenceInMinutes

The time resulting from the local server time and the maximum time difference is saved as the revision number in the One Identity Manager database (DPRRevisionStore table, Value column). If the local server time is used, the revision number is calculated from the time at which the object was changed.

This value is used as a comparison for revision filtering when the same workflow is synchronized the next time. The next time synchronization is run, only those objects that have been changed since this date are loaded. This avoids unnecessary updating of objects that have not changed since the last synchronization.

The revision is found at start of synchronization. Objects modified by synchronization are loaded and checked by the next synchronization. This means that the second synchronization after initial synchronization is not significantly faster.

Revision filtering can be applied to workflows and start up configuration.

To permit revision filtering on a workflow

- In the Synchronization Editor, open the synchronization project.
- Edit the workflow properties. Select the **Use revision filter** item from **Revision filtering** menu.

To permit revision filtering for a start up configuration

- In the Synchronization Editor, open the synchronization project.
- Edit the start up configuration properties. Select the **Use revision filter** item from the **Revision filtering** menu.

For more information about revision filtering, adjusting connections parameters and editing variables, see the *One Identity Manager Target System Synchronization Reference Guide*.

Related topics

- [Changing system connection settings of Exchange Online](#) on page 36

Configuring the provisioning of memberships

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

- Memberships are saved as an object property in list form in the target system.
Example: List of mailboxes in the `AcceptMessagesOnlyFrom` property of an Exchange Online mailbox (`Mailbox`)
- Memberships can be modified in either of the connected systems.
- A provisioning workflow and provisioning processes are set up.

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

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

To allow separate provisioning of memberships

1. In the Manager, select the **Azure Active Directory > Basic configuration data > Target system types** category.
2. In the result list, select the **Exchange Online** target system type.
3. Select the **Configure tables for publishing** task.
4. Select the assignment tables that you want to set up for single provisioning. Multi-select is possible.
5. Click **Merge mode**.


NOTE:

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

6. Save the changes.

For each assignment table labeled like this, the changes made in One Identity Manager are saved in a separate table. Therefore, only newly added and deleted assignments are processed. During modification provisioning, the members list in the target system is compared to the entries in this table. This means that only modified memberships are provisioned and not the entire members list.

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

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

To restore the original condition

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

NOTE: To create the reference to the added or deleted assignments in the condition, use the *i* table alias.

Example of a condition on the O3EUnifiedGroupAcceptRcpt assignment table:

```
exists (select top 1 1 from O3EUnifiedGroup g
        where g.UID_O3EUnifiedGroup = i.UID_O3EUnifiedGroup
        and <limiting condition>)
```

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

Configuring single object synchronization

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

Prerequisites

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

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

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

1. In the Manager, select the **Azure Active Directory > Basic configuration data > Target system types** category.
2. In the result list, select the **Exchange Online** target system type.
3. Select the **Assign synchronization tables** task.
4. In the **Add assignments** pane, assign the custom table for which you want to use single object synchronization.
5. Save the changes.
6. Select the **Configure tables for publishing** task.
7. Select the custom table and enter the **Root object path**.
Enter the path to the base object in the ObjectWalker notation of the VI.DB.
Example: `FK(UID_AADOrganization).XObjectKey`
8. Save the changes.

Related topics

- [Synchronizing single objects](#) on page 50
- [Post-processing outstanding objects](#) on page 51

Accelerating provisioning and single object synchronization

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

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

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

To configure load balancing

1. Configure the server and declare it as a Job server in One Identity Manager.
 - Job servers that share processing must have the **No process assignment** option enabled.
 - Assign the **Exchange Online connector** server function to the Job server.

All Job servers must access the same Azure Active Directory tenant as the synchronization server for the respective base object.

2. In the Synchronization Editor, assign a custom server function to the base object.

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

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

For more information about editing base objects, see the *One Identity Manager Target System Synchronization Reference Guide*.

3. In the Manager, assign this server function to all the Job servers that will be processing provisioning and single object synchronization for the base object.

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

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

Detailed information about this topic

- [Job server for Exchange Online-specific process handling](#) on page 81

Running synchronization

Synchronization is started using scheduled process plans. It is possible to start synchronization manually in the Synchronization Editor. You can simulate synchronization beforehand to estimate synchronization results and discover errors in the synchronization configuration. If synchronization stopped unexpectedly, you must reset the start information to be able to restart synchronization.

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

Detailed information about this topic

- [Starting synchronization](#) on page 47
- [Deactivating synchronization](#) on page 48
- [Displaying synchronization results](#) on page 49
- [Synchronizing single objects](#) on page 50
- [Pausing handling of target system specific processes \(Offline mode\)](#) on page 56

Starting synchronization

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

To synchronize on a regular basis

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

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

To start initial synchronization manually

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

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

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

Deactivating synchronization

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

To prevent regular synchronization

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

Now you can only start synchronization manually.

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

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

To deactivate the synchronization project

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

3. Click **Deactivate project**.


Related topics

- [Creating a synchronization project for initial synchronization of an Exchange Online environment](#) on page 25
- [Pausing handling of target system specific processes \(Offline mode\)](#) on page 56


Displaying synchronization results

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

To display a synchronization log

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Logs** category.
3. Click  in the navigation view toolbar.
Logs for all completed synchronization runs are displayed in the navigation view.
4. Select a log by double-clicking it.
An analysis of the synchronization is shown as a report. You can save the report.

To display a provisioning log

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Logs** category.
3. Click  in the navigation view toolbar.
Logs for all completed provisioning processes are displayed in the navigation view.
4. Select a log by double-clicking it.
An analysis of the provisioning is shown as a report. You can save the report.

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

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

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.

Synchronizing single objects

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

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

To synchronize a single object

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

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

Features of synchronizing memberships

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

Example:

Base object for assigning receive restrictions for Exchange Online email users and mail-enabled distribution groups is the distribution group.

In the target system, mail acceptance for a mail-enabled distribution group was allowed for an email user. To synchronize this assignment, in the Manager, select this distribution group and run single object synchronization. In the process, all of the distribution group's assignments are synchronized.

The email user must already exist as an object in the One Identity Manager database for the assignment to be made.

Detailed information about this topic

- [Configuring single object synchronization](#) on page 45

Tasks following synchronization

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

- [Post-processing outstanding objects](#) on page 51
- [Adding custom tables to the target system synchronization](#) on page 53
- [Managing Exchange Online mail users and Exchange Online mail contacts through account definitions](#) on page 53

Post-processing outstanding objects

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

Outstanding objects:

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

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

Start target system synchronization to do this.

To post-process outstanding objects

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

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

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

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

- The synchronization log has already been deleted.
- OR -
- An assignment from a member list has been deleted from the target system.

The base object of the assignment was updated during the synchronization. A corresponding entry appears in the synchronization log. The entry in the

assignment table is marked as outstanding, but there is no entry in the synchronization log.




- An object that contains a member list has been deleted from the target system. During synchronization, the object and all corresponding entries in the assignment tables are marked as outstanding. However, an entry in the synchronization log appears only for the deleted object.

TIP:

To display the properties of an outstanding object

1. Select the object on the target system synchronization form.
 2. Open the context menu and click **Show object**.
 3. For memberships, select the object whose properties you want to display.
3. Select the objects you want to rework. Multi-select is possible.
 4. Click on one of the following icons in the form toolbar to run the respective method.

Table 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. Indirect memberships cannot be deleted. |
|  | Publish | The object is added to the target system. The Outstanding label is removed from the object. This runs a target system specific process that triggers the provisioning process for the object. Prerequisites: <ul style="list-style-type: none">• 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. |

TIP: If a method cannot be run due to certain restrictions, the respective icon is disabled.


- To display the constraint's details, click the **Show** button in the **Constraints** column.

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

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

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

To disable bulk processing

- Disable the  icon in the form's toolbar.

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

Adding custom tables to the target system synchronization

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

To add custom tables to target system synchronization

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

Related topics

- [Post-processing outstanding objects](#) on page 51

Managing Exchange Online mail users and Exchange Online mail contacts through account definitions

In the default installation, after synchronizing, identities are automatically created for Exchange Online mail users and Exchange Online mail contacts. If an account definition for

the Exchange Online organization is not known at the time of synchronization, mail users and mail contacts are linked to the identities. However, account definitions are not assigned. The mail users and mail contacts are therefore in a **Linked** state.

To manage mail users and mail contacts through account definitions, assign an account definition and a manage level.

To manage Exchange Online mail users and mail contacts through account definitions

1. Create an account definition.
2. Assign an account definition to the Azure Active Directory tenant.
3. Assign the account definition and manage level to user accounts in **linked** status.
 - a. In the Manager, select the **Azure Active Directory > Mail users > Linked but not configured > <Azure Active Directory tenant>** category.
- OR -
In the Manager, select the **Azure Active Directory > Mail contacts > Linked but not configured > <Azure Active Directory tenant>** category.
 - b. Select the **Assign account definition to linked accounts** task.

Related topics

- [Account definitions for Exchange Online mail users and Exchange Online mail contacts](#) on page 59
- [Assigning account definitions to Azure Active Directory tenants](#) on page 76

Troubleshooting

Synchronization Editor helps you to analyze and eliminate synchronization errors.

- **Simulating synchronization**
The simulation allows you to estimate the result of synchronization. This means you can, for example, recognize potential errors in the synchronization configuration.
- **Analyzing synchronization**
You can generate the synchronization analysis report for analyzing problems which occur during synchronization, for example, insufficient performance.
- **Logging messages**
One Identity Manager offers different options for logging errors. These include the synchronization log, the log file for One Identity Manager Service, the logging of messages with NLOG, and similar.
- **Reset start information**

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

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

Related topics

- [Displaying synchronization results](#) on page 49

Ignoring data error in synchronization

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

To ignoring data errors during synchronization in One Identity Manager

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

This starts the system connection wizard.

4. On the **Additional options** page, enable **Try to ignore data errors**.

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

Default columns, such as primary keys, UID columns, or mandatory input columns cannot be ignored.

5. Save the changes.

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

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

Pausing handling of target system specific processes (Offline mode)

If a target system connector is not able to reach the target system temporarily, you can enable offline mode for the target system. This stops target system specific processes from being frozen and having to be manually re-enabled later.

Whether offline mode is generally available for a target system connection is set in the base object of the respective synchronization project. Once a target system is truly unavailable, the target system connection can be switched offline and online again with the Launchpad.


In offline mode, all Job servers assigned to the base object are stopped. This includes the synchronization server and all Job servers involved in load balancing. If one of the Job servers also handles other tasks, these are not processed either.

Prerequisites

Offline mode can only be specified for a base object if certain prerequisites are fulfilled.

- The synchronization server is not used for any other base object as a synchronization server.
- If a server function is assigned to the base object, none of the Job servers with this server function may have any other server function (for example, update server).
- A dedicated synchronization server must be set up to exclusively process the Job queue for this base object. The same applies to all Job servers that are determined by the server function.

To allow offline mode for a base object

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Base objects** category.
3. Select a base object in the document view and click .
4. Enable **Offline mode available**.
5. Click **OK**.
6. Save the changes.

IMPORTANT: To prevent data inconsistencies, the offline phase should be kept as short as possible.

The number of processes to handle depends on the extent of the changes in the One Identity Manager database and their effect on the target system during the offline phase. To establish data consistency between the One Identity Manager database and the target system, all pending processes must be handled before synchronization can start.

Only use offline mode, if possible, for short system downtimes such as maintenance windows.

To flag a target system as offline

1. Start the Launchpad and log in on the One Identity Manager database.
2. Select **Manage > System monitoring > Flag target systems as offline**.
3. Click **Run**.

This opens the **Manage offline systems** dialog. The **Base objects** section displays the base objects of target system connections that can be switched to offline.

4. Select the base object whose target system connection is not available.
5. Click **Switch offline**.
6. Confirm the security prompt with **OK**.

This stops all the Job servers assigned to the base object. No more synchronization or provisioning Jobs are performed. The Job Queue Info program shows when a Job server has been switched offline and the corresponding tasks are not being processed.

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

Related topics

- [Deactivating synchronization](#) on page 48

Basic data for managing an Exchange Online environment

To manage an Exchange Online environment in One Identity Manager, the following basic data is relevant.

- Account definitions

One Identity Manager has account definitions for automatically allocating user accounts to identities. You can create account definitions for every target system. If an identity 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 identity.

For more information, see [Account definitions for Exchange Online mail users and Exchange Online mail contacts](#) on page 59.

- Password policies

One Identity Manager provides you with support for creating complex password policies, for example, for system user passwords, the identities' central password as well as passwords for individual target systems. Password policies 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.

Azure Active Directory configuration settings are used for implementing password policies. For more information, see the *One Identity Manager Administration Guide for Connecting to Azure Active Directory*.

- Initial password for new mail users.

You can issue an initial password for mail users in the following ways: Enter a password or use a random generated initial password when you create a mail user.

Azure Active Directory configuration settings are used for generating random passwords for new mail users. For more information, see the *One Identity Manager Administration Guide for Connecting to Azure Active Directory*.

- Email notifications about credentials

When a new mail user 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.

Azure Active Directory configuration settings are used for sending login credentials. For more information, see the *One Identity Manager Administration Guide for Connecting to Azure Active Directory*.

- Target system types

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

For more information, see [Post-processing outstanding objects](#) on page 51.

- Target system managers

A default application role exists for the target system manager in One Identity Manager. Assign identities to this application role who have permission to edit all Exchange Online objects in One Identity Manager.

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

For more information, see [Target system managers for Exchange Online](#) on page 79.

- Servers

Servers must be informed of your server functionality in order to handle Exchange Online-specific processes in One Identity Manager. For example, the synchronization server.

For more information, see [Job server for Exchange Online-specific process handling](#) on page 81.

Account definitions for Exchange Online mail users and Exchange Online mail contacts

NOTE: Exchange Online user mailboxes are create or deleted respectively by assigning and removing licenses through Azure Active Directory subscriptions. For more information, see the *One Identity Manager Administration Guide for Connecting to Azure Active Directory*.

One Identity Manager has account definitions for automatically allocating mail users and mail contacts to identities. You can create account definitions for every target system. If an identity does not yet have a mail user or mail contact in a target system, a new mail user or mail contact is created by assigning the account definition to an identity.

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


Detailed information about this topic

- [Creating account definitions](#) on page 60
- [Editing account definitions](#) on page 61
- [Main data for account definitions](#) on page 61
- [Editing manage levels](#) on page 63
- [Creating manage levels](#) on page 64
- [Assigning manage levels to account definitions](#) on page 65
- [Main data for manage levels](#) on page 65
- [Creating mapping rules for IT operating data](#) on page 66
- [Entering IT operating data](#) on page 67
- [Modify IT operating data](#) on page 69
- [Assigning account definitions to identities](#) on page 69
- [Assigning account definitions to Azure Active Directory tenants](#) on page 76
- [Deleting account definitions](#) on page 77

Creating account definitions

Create one or more account definitions for the target system.

To create a new account definition

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

Detailed information about this topic

- [Main data for account definitions](#) on page 61
- [Editing account definitions](#) on page 61
- [Assigning manage levels to account definitions](#) on page 65

Editing account definitions

You can edit the main data of account definitions.

To edit an account definition

1. In the Manager, select the **Azure Active Directory > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Change main data** task.
4. Enter the account definition's main data.
5. Save the changes.

Related topics

- [Main data for account definitions](#) on page 61
- [Creating account definitions](#) on page 60
- [Assigning manage levels to account definitions](#) on page 65

Main data for account definitions

Enter the following data for an account definition:

Table 7: Main data for an account definition

| Property | Description |
|--------------------|--|
| Account definition | Account definition name. |
| User account table | Table in the One Identity Manager schema that maps mail users or mail contacts. For Exchange Online mail users, select 03EMailUser . For Exchange Online mail contacts, select 03EMailContact . |
| Target system | Target system to which the account definition applies. |
| Required account | Specifies the required account definition. Define the depend- |

| Property | Description |
|---|---|
| definition | <p>encies between account definitions. When this account definition is requested or assigned, the required account definition is assigned automatically.</p> <p>Leave empty for Exchange Online.</p> |
| Description | Text field for additional explanation. |
| Manage level (initial) | Manage level to use by default when you add new mail users or mail contacts. |
| Risk index | <p>Value for evaluating the risk of assigning the account definition to identities. Set a value in the range 0 to 1. This input field is only visible if the QER CalculateRiskIndex configuration parameter is set.</p> <p>For more information, see the <i>One Identity Manager Risk Assessment Administration Guide</i>.</p> |
| Service item | Service item through which you can request the account definition resource in the IT Shop. Assign an existing service item or add a new one. |
| IT Shop | Specifies whether the account definition can be requested through the IT Shop. This account definition can be requested through the Web Portal and allocated by defined approval processes. The resource can also be assigned directly to identities 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. This account definition can be requested through the Web Portal and allocated by defined approval processes. The account definition cannot be directly assigned to roles outside the IT Shop. |
| Automatic assignment to identities | <p>Specifies whether the account definition is automatically assigned to all internal identities. To automatically assign the account definition to all internal identity, use the Enable automatic assignment to identities. The account definition is assigned to every identity that is not marked as external. Once a new internal identity is created, they automatically obtain this account definition.</p> <p>To automatically remove the account definition assignment from all identities, use the Disable automatic assignment to identities. The account definition cannot be reassigned to identities from this point on. Existing account definition assignments remain intact.</p> |
| Retain account definition if permanently disabled | Specifies the account definition assignment to permanently deactivated identities. |

| Property | Description |
|---|---|
| | <p>Option set: The account definition assignment remains in effect. The mail user or mail contact remains intact.</p> <p>Option not set (default): The account definition assignment is not in effect. The associated mail user or the associated mail contact is disabled.</p> |
| Retain account definition if temporarily disabled | <p>Specifies the account definition assignment to temporarily deactivated identities.</p> <p>Option set: The account definition assignment remains in effect. The mail user or mail contact remains intact.</p> <p>Option not set (default): The account definition assignment is not in effect. The associated mail user or the associated mail contact is disabled.</p> |
| Retain account definition on deferred deletion | <p>Specifies the account definition assignment on deferred deletion of identities.</p> <p>Option set: The account definition assignment remains in effect. The mail user or mail contact remains intact.</p> <p>Option not set (default): The account definition assignment is not in effect. The associated mail user or the associated mail contact is disabled.</p> |
| Retain account definition on security risk | <p>Specifies the account definition assignment to identities posing a security risk.</p> <p>Option set: The account definition assignment remains in effect. The email user or mail contact remains intact.</p> <p>Option not set (default): The account definition assignment is not in effect. The associated mail user or the associated mail contact is disabled.</p> |
| 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. |

Editing manage levels

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

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

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

To edit a manage level

1. In the Manager, select the **Azure Active Directory > Basic configuration data > Account definitions > Manage levels** category.
2. Select the manage level in the result list.
3. Select the **Change main data** task.
4. Edit the manage level's main data.
5. Save the changes.

Related topics

- [Main data for manage levels](#) on page 65
- [Creating manage levels](#) on page 64
- [Assigning manage levels to account definitions](#) on page 65


Creating manage levels

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

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

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

To create a manage level

1. In the Manager, select the **Azure Active Directory > Basic configuration data > Account definitions > Manage levels** category.
2. Click  in the result list.
3. On the main data form, edit the main data of the manage level.
4. Save the changes.

Related topics

- [Main data for manage levels](#) on page 65
- [Editing manage levels](#) on page 63
- [Assigning manage levels to account definitions](#) on page 65

Assigning manage levels to account definitions


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

To assign manage levels to an account definition

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

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

To remove an assignment

- Select the manage level and double-click .
5. Save the changes.

Main data for manage levels

Enter the following data for a manage level.

Table 8: Main data for manage levels

| Property | Description |
|--|---|
| Manage level | Name of the manage level. |
| Description | Text field for additional explanation. |
| IT operating data overwrites | Specifies whether user account data formatted from IT operating data is automatically updated. Permitted values are: <ul style="list-style-type: none">• Never: Data is not updated. (Default)• Always: Data is always updated.• Only initially: Data is only determined at the start. |
| Retain groups if temporarily disabled | Specifies whether user accounts of temporarily deactivated retain their group memberships. |
| Lock user accounts if temporarily disabled | Specifies whether user accounts of temporarily deactivated identities are locked. |
| Retain groups if | Specifies whether user accounts of permanently deactivated |

| Property | Description |
|--|--|
| permanently disabled | identities retain group memberships. |
| Lock user accounts if permanently disabled | Specifies whether user accounts of permanently deactivated identities are locked. |
| Retain groups on deferred deletion | Specifies whether user accounts of identities marked for deletion retain their group memberships. |
| Lock user accounts if deletion is deferred | Specifies whether user accounts of identities marked for deletion are locked. |
| Retain groups on security risk | Specifies whether user accounts of identities posing a security risk retain their group memberships. |
| Lock user accounts if security is at risk | Specifies whether user accounts of identities 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 identity's primary roles.

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

- Groups can be inherited

To create a mapping rule for IT operating data

1. In the Manager, select the **Azure Active Directory > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Edit IT operating data mapping** task.
4. Click **Add** and enter the following information:
 - **Column:** User account property for which the value is set. In the menu, you can select the columns that use the TSB_ITDataFromOrg script in their template. For more information about this, see the *One Identity Manager Target System Base Module Administration Guide*.

- **Source:** Specifies which roles to use in order to find the user account properties. You have the following options:
 - Primary department
 - Primary location
 - Primary cost center
 - Primary business roles

NOTE: The business role can only be used if the Business Roles Module is available.

 - Empty

If you select a role, you must specify a default value and set the **Always use default value** option.
- **Default value:** Default value of the property for an identity's user account if the value is not determined dynamically from the IT operating data.
- **Always use default value:** Specifies whether the user account property is always set with the default value. IT operating data is not determined dynamically from a role.
- **Notify when applying the default:** Specifies whether an email is sent to a specific mailbox when the default value is used. The **Identity - new user account with default properties created** mail template is used.

5. Save the changes.

Related topics

- [Entering IT operating data](#) on page 67

Entering IT operating data

To create user accounts for an identity with the **Full managed** manage level, you need to know which IT operating data is required. The operating data required for each specific target system is defined with its business roles, departments, locations, or cost centers. An identity 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 identity in department A obtains a default user account in the tenant A. In addition, certain identities 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. In the IT operating data mapping rule for the account definitions A and B, specify the **Department** property in order to determine the valid IT operating data.

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

To define IT operating data

1. In the Manager, select the role in the **Organizations** or **Business roles** category.
2. Select the **Edit IT operating data** task.
3. Click **Add** and enter the following data.

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

To specify an application scope

- a. Click **→** next to the field.
 - b. Under **Table**, select the table that maps the target system for select the **TSBAccountDef** table or an account definition.
 - c. Select the specific target system or account definition under **Effects on**.
 - d. Click **OK**.
- **Column:** Select the user account property for which the value is set.
In the menu, you can select the columns that use the `TSB_ITDataFromOrg` script in their template. For more information about this, see the *One Identity Manager Target System Base Module Administration Guide*.
 - **Value:** Enter a fixed value to assign to the user account's property.
4. Save the changes.

Related topics

- [Creating mapping rules for IT operating data](#) on page 66

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 identity to a primary department, cost center, to a primary business role or to a primary location changes, the templates are automatically run.

To run the template

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

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

- **Old value:** Value of the object property before changing the IT operating data.
 - **New value:** Value of the object property after changing the IT operating data.
 - **Selection:** Specifies whether the new value is copied to the user account.
4. Mark all the object properties in the **selection** column that will be given the new value.
 5. Click **Apply**.

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

Assigning account definitions to identities

Account definitions are assigned to company identities.

Indirect assignment is the default method for assigning account definitions to identities. Account definitions are assigned to departments, cost centers, locations, or roles. The

identities 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 identities.

You can automatically assign special account definitions to all company identities. 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 identities 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 identity already has a user account in the target system that has an account definition. If no user account exists, a new user account is created with the account definition's default manage level.

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

NOTE: As long as an account definition for an identity is valid, the identity retains the user account that was created by it. If the account definition assignment is removed, the user account that was created from this account definition, is deleted. User accounts marked as **Outstanding** are only deleted if the **QER | Person | User | DeleteOptions | DeleteOutstanding** configuration parameter is set.

Prerequisites for indirect assignment of account definitions to identities

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

To configure assignments to roles of a role class

1. In the Manager, select role classes in the **Organizations > Basic configuration data > Role classes** category.
- OR -
In the Manager, select role classes in the **Business roles > Basic configuration data > Role classes** category.
2. Select the **Configure role assignments** task and configure the permitted assignments.
 - To generally allow an assignment, enable the **Assignments allowed** column.
 - To allow direct assignment, enable the **Direct assignments permitted** column.
3. Save the changes.

For more 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 71
- [Assigning account definitions to business roles](#) on page 71
- [Assigning account definitions to all identities](#) on page 72
- [Assigning account definitions directly to identities](#) on page 73
- [Assigning account definitions to Azure Active Directory tenants](#) on page 76

Assigning account definitions to departments, cost centers, and locations


Assign account definitions to departments, cost centers, and locations in order to assign identities to them through these organizations.

To add account definitions to hierarchical roles

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

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

To remove an assignment

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

Related topics

- [Assigning account definitions to business roles](#) on page 71
- [Assigning account definitions to business roles](#) on page 71
- [Assigning account definitions directly to identities](#) on page 73

Assigning account definitions to business roles

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


You can assign account definitions to business roles in order to assign them to identities through business roles.

To add account definitions to hierarchical roles

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

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

To remove an assignment

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

Related topics

- [Assigning account definitions to departments, cost centers, and locations](#) on page 71
- [Assigning account definitions to all identities](#) on page 72
- [Assigning account definitions directly to identities](#) on page 73

Assigning account definitions to all identities

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

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

To assign an account definition to all identities

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

NOTE: To automatically remove the account definition assignment from all identities, run the [DISABLE AUTOMATIC ASSIGNMENT TO IDENTITIES](#) task. The account definition cannot be reassigned to identities from this point on. Existing assignments remain intact.

Related topics

- [Assigning account definitions to departments, cost centers, and locations](#) on page 71
- [Assigning account definitions to business roles](#) on page 71
- [Assigning account definitions directly to identities](#) on page 73

Assigning account definitions directly to identities

Account definitions can be assigned directly or indirectly to identities. Indirect assignment is carried out by allocating identities and account definitions in company structures, like departments, cost centers, locations, or business roles.


To react quickly to special requests, you can assign account definitions directly to identities.

To assign an account definition directly to identities

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 identities** task.
4. In the **Add assignments** pane, add identities.

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

To remove an assignment

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

Related topics

- [Assigning account definitions to departments, cost centers, and locations](#) on page 71
- [Assigning account definitions to business roles](#) on page 71
- [Assigning account definitions to all identities](#) on page 72

Assigning account definitions to system roles

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

Use this task to add an account definition to system roles.


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

To add account definitions to a system role

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

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

To remove an assignment

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

Adding account definitions in the IT Shop

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

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

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

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

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

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

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

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

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

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

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

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

1. In the Manager, select the **Azure Active Directory > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Add to IT Shop** task.
4. In the **Remove assignments** pane, remove the account definitions from the IT Shop shelves.
5. Save the changes.

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

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

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

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

1. In the Manager, select the **Azure Active Directory > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Remove from all shelves (IT Shop)** task.
4. Confirm the security prompt with **Yes**.
5. Click **OK**.

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

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

Related topics

- [Main data for account definitions](#) on page 61
- [Assigning account definitions to departments, cost centers, and locations](#) on page 71
- [Assigning account definitions to business roles](#) on page 71
- [Assigning account definitions directly to identities](#) on page 73
- [Assigning account definitions to system roles](#) on page 73

Assigning account definitions to Azure Active Directory tenants

The following prerequisites must be fulfilled if you implement automatic assignment of user accounts and identities 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 identity (**Linked** state) if no account definition is given. This is the case on initial synchronization, for example.

To assign the account definition to a target system

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

4. From the **Mail contact definition (initial)** menu, select the account definition for mail contacts.
5. From the **Mail user definition (initial)** menu, select the account definition for mail users.
6. Save the changes.

Related topics

- [Assigning account definitions to identities](#) on page 69

Deleting account definitions

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

To delete an account definition

1. Remove automatic assignments of the account definition from all identities.
 - a. In the Manager, select the **Azure Active Directory > Basic configuration data > Account definitions > Account definitions** category.
 - b. Select an account definition in the result list.
 - c. Select the **Change main data** task.
 - d. Select the **Disable automatic assignment to identities** task.
 - e. Confirm the security prompt with **Yes**.
 - f. Save the changes.
2. Remove direct assignments of the account definition to identities.
 - 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 identities** task.
 - d. In the **Remove assignments** pane, remove identities.
 - e. Save the changes.
3. Remove the account definition's assignments to departments, cost centers, and locations.
 - a. In the Manager, select the **Azure Active Directory > Basic configuration data > Account definitions > Account definitions** category.
 - b. Select an account definition in the result list.
 - c. Select the **Assign organizations** task.

- d. In the **Remove assignments** pane, remove the relevant departments, cost centers, and locations.
 - e. Save the changes.
 4. Remove the account definition's assignments to business roles.
 - a. In the Manager, select the **Azure Active Directory > Basic configuration data > Account definitions > Account definitions** category.
 - b. Select an account definition in the result list.
 - c. Select the **Assign business roles** task.
 - d. In the **Remove assignments** pane, remove the business roles.
 - e. Save the changes.
 5. If the account definition was requested through the IT Shop, it must be canceled and removed from all IT Shop shelves.

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

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

- a. In the Manager, select the **Entitlements > Account definitions** category.
- b. Select an account definition in the result list.
- c. Select the **Remove from all shelves (IT Shop)** task.
- d. Confirm the security prompt with **Yes**.
- e. Click **OK**.

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


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

- a. In the Manager, select the **Azure Active Directory > Basic configuration data > Account definitions > Account definitions** category.
- b. Select an account definition in the result list.
- c. Select the **Remove from all shelves (IT Shop)** task.
- d. Confirm the security prompt with **Yes**.
- e. Click **OK**.

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

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

definitions.

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

Target system managers for Exchange Online

A default application role exists for the target system manager in One Identity Manager. Assign identities to this application role who have permission to edit all Exchange Online objects in One Identity Manager.

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

For more 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 identities to be target system administrators.
2. These target system administrators add identities to the default application role for target system managers.

Target system managers with the default application role are authorized to edit all the Exchange Online objects in One Identity Manager.

3. Target system managers can authorize other identities within their area of responsibility as target system managers and if necessary, create additional child application roles and assign these to individual tenants.

Table 9: Default application roles for target system managers

| User | Tasks |
|------------------------|---|
| Target system managers | <p>Target system managers must be assigned to the Target systems Exchange Online application role or a child application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none"> • Assume administrative tasks for the target system. • Create, change, or delete target system objects. • Edit password policies for the target system. • Prepare groups to add to the IT Shop. • Can add identities that do not have the Primary identity identity type. • 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 identities within their area of responsibility as target system managers and create child application roles if required. |

To initially specify identities 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 identities** task.
4. Assign the identity and save the changes.

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

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

To authorize other identities 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 identities** task.
4. Assign the identities 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 main data** task.
5. On the **General** tab, select the application role in the **Target system manager (Exchange Online)** menu.

- OR -

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

- a. Enter the application role name and assign the **Target systems | Exchange Online** parent application role.
 - b. Click **OK** to add the new application role.
6. Save the changes.
 7. Assign identities to this application role who are permitted to edit the tenant in One Identity Manager.

Related topics

- [One Identity Manager users for managing Exchange Online](#) on page 11

Job server for Exchange Online-specific process handling

Servers must be informed of your server functionality in order to handle Exchange Online-specific processes in One Identity Manager. For example, the synchronization server.

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

- In the Designer, create an entry for the Job server in the **Base Data > Installation > Job server** category. For more information about this, see the

One Identity Manager Configuration Guide.

- In the Manager, select an entry for the Job server in the **Azure Active Directory > Basic configuration data > Server** category and edit the Job server main data.

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

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

To edit a Job server and its functions

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

Detailed information about this topic

- [General main data for Job servers](#) on page 82
- [Specifying server functions](#) on page 85

General main data for Job servers

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

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

Table 10: Job server properties

| Property | Meaning |
|------------------|---|
| Server | Job server name. |
| Full server name | Full server name in accordance with DNS syntax. Syntax: <Name of servers>.<Fully qualified domain name> |
| Target system | Computer account target system. |
| Language | Language of the server. |

| Property | Meaning |
|------------------------------|--|
| 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. |
| Coding | Character set coding that is used to write files to the server. |
| Parent Job server | Name of the parent Job server. |
| Executing server | Name of the executing server. The name of the server that exists physically and where the processes are handled. This input is evaluated when the One Identity Manager Service is automatically updated. If the server is handling several queues, the process steps are not supplied until all the queues that are being processed on the same server have completed their automatic update. |
| Queue | Name of the queue to handle the process steps. The process steps are requested by the Job queue using this queue identifier. The queue identifier is entered in the One Identity Manager Service configuration file. |
| Server operating system | Operating system of the server. This input is required to resolve the path name for replicating software profiles. The values Win32 , Windows , Linux , and Unix are |

| Property | Meaning |
|---|---|
| | permitted. If no value is specified, win32 is used. |
| Service account data | One Identity Manager Service user account information. In order to replicate between non-trusted systems (non-trusted domains, Linux server), the One Identity Manager Service user information has to be declared for the servers in the database. This means that the service account, the service account domain, and the service account password have to be entered for the server. |
| One Identity Manager Service installed | Specifies whether a One Identity Manager Service is installed on this server. This option is enabled by the QBM_PJobQueueLoad procedure the moment the queue is called for the first time. The option is not automatically removed. If necessary, you can reset this option manually for servers whose queue is no longer enabled. |
| Stop One Identity Manager Service | Specifies whether the One Identity Manager Service has stopped. If this option is set for the Job server, the One Identity Manager Service does not process any more tasks. You can make the service start and stop with the appropriate administrative permissions in the Job Queue Info program. For more information, see the <i>One Identity Manager Process Monitoring and Troubleshooting Guide</i> . |
| Paused due to unavailability of a target system | Specifies whether task processing for this queue has been stopped because the target system that uses this Job server as a synchronization server is temporarily unavailable. As soon as the target system is available again, processing starts and all outstanding tasks are performed. For more information about offline mode, see the <i>One Identity Manager Target System Synchronization Reference Guide</i> . |
| No automatic software update | Specifies whether to exclude the server from automatic software updating. NOTE: Servers must be manually updated if this option is set. |
| Software update running | Specifies whether a software update is currently running. |

| Property | Meaning |
|-----------------|---|
| 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 85

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 11: 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. |
| Exchange Online connector (via PowerShell) | This server can connect to the Exchange Online endpoint. |
| CSV connector | Server on which the CSV connector for synchronization is installed. |
| Domain controller | The Active Directory domain controller. Servers that are not labeled as domain controllers are considered to be member servers. |
| Printer server | Server that acts as a print server. |
| Generic server | Server for generic synchronization with a custom target system. |
| Home server | Server for adding home directories for user accounts. |
| Update server | This server automatically updates the software on all the other servers. The server requires a direct connection to the database server that One Identity Manager database is installed on. It can run SQL tasks. |

| Server function | Remark |
|---|---|
| | The server with the One Identity Manager database installed on it is labeled with this functionality during initial installation of the schema. |
| SQL processing server | <p>It can run SQL tasks. The server requires a direct connection to the database server that One Identity Manager database is installed on.</p> <p>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.</p> |
| CSV script server | This server can process CSV files using the ScriptComponent process component. |
| Generic database connector | This server can connect to an ADO.Net database. |
| One Identity Manager database connector | Server on which the One Identity Manager connector is installed. This server synchronizes the One Identity Manager target system. |
| One Identity Manager Service installed | Server on which a One Identity Manager Service is installed. |
| Primary domain controller | Primary domain controller. |
| Profile server | Server for setting up profile directories for user accounts. |
| SAM synchronization Server | Server for synchronizing 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. |
| PowerShell connector | The server can run PowerShell version 3.0 or later. |

Related topics

- [General main data for Job servers](#) on page 82

Exchange Online organization configuration

The Exchange Online organization configurations of Azure Active Directory tenants are loaded into the One Identity Manager database. It is not possible to customize this information in One Identity Manager due to the complex dependencies and far reaching effects of changes.

Detailed information about this topic

- [Extensions for Azure Active Directory tenants](#) on page 87
- [Displaying hierarchical address books](#) on page 88
- [Exchange Online public folders](#) on page 89
- [Exchange Online policies](#) on page 89

Extensions for Azure Active Directory tenants

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

The following additional information is mapped to Azure Active Directory tenants for Exchange Online.

- Initial account definition for creating mail contacts (**Mail account definition (initial)**) or mail users (**Mail user definition (initial)**)

This account definition is used if automatic assignment of identities to user accounts is used for this Azure Active Directory tenant and mail contacts or mail users should be created that are already managed (**Linked configured** state). The account definition's default manage level is applied.

- **Target system managers (Exchange Online)**: Application role, in which Exchange Online target system managers are specified for those of the

Azure Active Directory tenant. Target system managers must be assigned to the **Target systems | Exchange Online** application role or a child application role.

- Defining categories for the inheritance of entitlements through categories
You can use Office 365 group and mail-enabled distribution group inheritance through categories for Exchange Online.

To edit Azure Active Directory tenant main data

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

Related topics

- [Assigning account definitions to Azure Active Directory tenants](#) on page 76
- [Target system managers for Exchange Online](#) on page 79
- [Exchange Online mail-enabled distribution group inheritance based on categories](#) on page 152
- [Exchange Online Office 365 group inheritance based on categories](#) on page 174

Displaying hierarchical address books

In a hierarchical address book (HAB), the recipients (mailboxes, mail users, mail contacts, mail-enabled distribution groups) are represented in a hierarchically organized structure.

For more information, see <https://learn.microsoft.com/en-us/exchange/address-books/hierarchical-address-books/hierarchical-address-books>.

The hierarchy structure is based on the Azure Active Directory group hierarchy. The Azure Active Directory group that represents the root of the hierarchical address book is linked to the Exchange Online organization. The mail-enabled distribution groups that map a hierarchical address book are labeled with the **Hierarchical group** option.

The following properties are used to define the order in which the recipients are displayed.

- **Sort order:** Specifies the order in which to display recipients in the hierarchical address book. The larger the value, the higher the ranking in the sort order.
- **Phonetic display name:** If no sort order is given or several entries have the same sort order, sorting is done by phonetic name.
- **Display name:** If no phonetic display name is entered, sorting is done according to the display name.

To display the hierarchical address book

1. In the Manager, select the **Azure Active Directory > Tenants** category.
2. In the result list, select the Azure Active Directory tenant.
3. Select the **Show hierarchical address book** report.

Related topics

- [Main data for Exchange Online mail-enabled distribution groups](#) on page 133
- [General main data for Exchange Online mailboxes](#) on page 94
- [Main data for Exchange Online mail users](#) on page 111
- [Main data for Exchange Online mail contacts](#) on page 122

Exchange Online public folders

Public folders are used to allow identities shared access to information. Public folders can be structured hierarchically and are connection with a public folder database.

Exchange Online public folders are loaded into One Identity Manager by synchronization and cannot be edited in One Identity Manager.

To display information about a public folder

1. In the Manager, select the **Azure Active Directory > Tenants > <Azure Active Directory tenant> > Exchange Online administration > Organization configuration > Public folders** category.
2. Select the public folder in the result list.
3. Select one of the following tasks:
 - **Exchange Online public folder overview:** This shows you an overview of the public folder and its dependencies.
 - **Change main data:** This shows the public folder's main data.

Related topics

- [Exchange Online mail-enabled public folders](#) on page 183
- [Synchronizing single objects](#) on page 50

Exchange Online policies

Exchange Online policies are loaded into One Identity Manager by synchronization and cannot be edited in One Identity Manager. You can assign policies to Exchange Online

mailboxes.

Sharing administration policies

Sharing policies are implemented to make calendar and contact data available to external users. Assigning a sharing policy to a mailbox regulates how calendar and contact data can be shared with user accounts outside the Exchange Online organization.

Retention policies

Retention policies have been implemented to group settings for retaining folders and email messages and to apply these to mailboxes.

Outlook Web App mailbox policy

Outlook Web App mailbox policies are implemented for managing access to functions in Outlook Web App.

Mobile device mailbox policy

Mailbox policies for mobile email queries contain settings that come into effect when data is accessed with mobile devices through the synchronization protocol Exchange ActiveSync. The settings include, for example, password requirements, specifications for email attachments, device encryption data and access rules for shares.

Role assignment policy

Policies for role assignments have been implemented to provide users with functions and tasks for managing their mailboxes.

To display information about a policy

1. In the Manager, select the **Azure Active Directory > tenants > <Azure Active Directory tenant> > Exchange Online administration > policies > <policy type>**.
2. Select the policy in the result list.
3. Select one of the following tasks:
 - **Exchange Online policy overview:** This shows you an overview of the policies and their dependencies.
 - **Change main data:** Shows the policy's main data.

Related topics

- [Synchronizing single objects](#) on page 50
- [Policies and features of Exchange Online mailboxes](#) on page 98

Exchange Online mailboxes

Exchange Online mailboxes can send, receive, and save messages. Exchange Online recognizes several mailbox types. The mailbox types listed below are supported in One Identity Manager. Exchange Online mailboxes are loaded into One Identity Manager by synchronization.

Table 12: Supported mailbox types

| Mailbox type | Description |
|-------------------|---|
| User mailbox | <p>User mailboxes are assigned to Azure Active Directory user accounts in an Exchange Online organization.</p> <p>You cannot create user mailboxes in One Identity Manager. User mailboxes are created by assigning the respective subscriptions to Azure Active Directory user accounts. By these means, user mailboxes are created that do not appear in One Identity Manager until after synchronization. The user mailboxes can be subsequently provisioned automatically in Exchange Online.</p> |
| Equipment mailbox | <p>Equipment mailboxes are resource mailboxes used for planning resources, such as computers or laptops.</p> <p>You can create equipment mailboxes in One Identity Manager. When you create an equipment mailbox, an Azure Active Directory user account is also created and linked to the mailbox.</p> |
| Room mailbox | <p>Room mailboxes are resource mailboxes used for planning meeting locations.</p> <p>You can room equipment mailboxes in One Identity Manager. When you create a room mailbox, an Azure Active Directory user account is also created and linked to the mailbox.</p> |
| Shared mailbox | <p>Shared mailboxes are mailboxes that are used by several users.</p> <p>You can create shared mailboxes in One Identity Manager. When you create a shared mailbox, an Azure Active Directory user account is also created and linked to the mailbox.</p> |

| Mailbox type | Description |
|-------------------|---|
| Discovery mailbox | In Exchange Online, a discovery mailbox that is used as target mailbox for searches using eDiscovery, is created by default. You cannot edit discovery mailboxes in One Identity Manager. |

Detailed information about this topic

- [Creating Exchange Online mailboxes](#) on page 92
- [Editing main data of Exchange Online mailboxes](#) on page 93
- [General main data for Exchange Online mailboxes](#) on page 94
- [Limits and usage of Exchange Online mailboxes](#) on page 96
- [Policies and features of Exchange Online mailboxes](#) on page 98
- [Booking resources for Exchange Online equipment mailboxes and Exchange Online room mailboxes](#) on page 100
- [Adjusting receive restrictions for Exchange Online mailboxes](#) on page 103
- [Exchange Online mailbox permission: Send on behalf](#) on page 104
- [Exchange Online mailbox permission: Send as](#) on page 105
- [Exchange Online mailbox permission: Full access](#) on page 106
- [Specifying moderators for Exchange Online mailboxes](#) on page 107
- [Assigning extended properties to Exchange Online mailbox](#) on page 107
- [Deleting Exchange Online mailboxes](#) on page 108
- [Synchronizing single objects](#) on page 50


Creating Exchange Online mailboxes

Exchange Online mailboxes are loaded into One Identity Manager by synchronization.

You cannot create user mailboxes in One Identity Manager. User mailboxes are created by assigning the respective subscriptions to Azure Active Directory user accounts. By these means, user mailboxes are created that do not appear in One Identity Manager until after synchronization. The user mailboxes can be subsequently provisioned automatically in Exchange Online.

You can create equipment mailboxes, room mailboxes, and shared mailboxes in One Identity Manager. When you create an equipment mailbox, a room mailbox, or a shared mailbox an Azure Active Directory user account is also created and linked to the mailbox.

To create a mailbox

1. In the Manager, select the **Azure Active Directory > Mailboxes** category.
2. Click  in the result list.
3. On the main data form, enter the main data of the mailbox.
4. Save the changes.

Related topics

- [General main data for Exchange Online mailboxes](#) on page 94
- [Limits and usage of Exchange Online mailboxes](#) on page 96
- [Policies and features of Exchange Online mailboxes](#) on page 98
- [Booking resources for Exchange Online equipment mailboxes and Exchange Online room mailboxes](#) on page 100
- [Editing main data of Exchange Online mailboxes](#) on page 93

Editing main data of Exchange Online mailboxes

To edit a mailbox

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

Related topics

- [General main data for Exchange Online mailboxes](#) on page 94
- [Limits and usage of Exchange Online mailboxes](#) on page 96
- [Policies and features of Exchange Online mailboxes](#) on page 98
- [Booking resources for Exchange Online equipment mailboxes and Exchange Online room mailboxes](#) on page 100
- [Creating Exchange Online mailboxes](#) on page 92


General main data for Exchange Online mailboxes

Enter the following general main data.

Table 13: Mailbox general main data

| Property | Description |
|-------------------------------------|--|
| Identity | Identity using the mailbox. |
| No link to an identity required | Specifies whether the mailbox is intentionally not assigned an identity. The value is determined from the linked user account. |
| Not linked to an identity | Indicates why the No link to an identity required option is enabled for this mailbox. The value is determined from the linked user account. Possible values: <ul style="list-style-type: none">• By administrator: The option was set manually by the administrator.• By attestation: The user account was attested.• By exclusion criterion: The user account is not associated with an identity due to an exclusion criterion. For example, the user account is included in the exclude list for automatic identity assignment (configuration parameter PersonExcludeList). |
| Azure Active Directory tenant | The Azure Active Directory tenant's name. |
| Azure Active Directory user account | Azure Active Directory user account that uses this mailbox. |
| Name | Name of the mailbox. |
| Display name | Name as used in the address book. |
| Simple display | Simple display name for systems that cannot interpret all the characters of normal display names. |
| Phonetic display name | Display name in phonetic letters. It is used if the pronunciation and spelling of the name do not match. For example, the display name is used to sort recipients in the hierarchical address book if no sort order is given. They are sorted in ascending order from A to Z. If no phonetic name is given, they are sorted by the display name. |
| Sort order | Specifies the order in which to display recipients in the hierarchical address book. The larger the value, the higher the |

| Property | Description |
|--------------------------------|---|
| | <p>ranking in the sort order.</p> <p>If no order is given or more than one entries have the same sort order, recipients are sorted by their phonetic display name.</p> |
| User ID | <p>User ID for the user to log in to the mailbox.</p> <p>Example:</p> <pre><alias>@<domain.com> <user>@yourorganization.onmicrosoft.com</pre> |
| Alias | <p>Unique email alias for identifying the mailbox.</p> |
| Proxy addresses | <p>Email addresses for the mailbox. You can also add other mail connectors (for example, CCMail, MS) in addition to the standard address type (SMTP, X400).</p> <p>Use the following syntax to set up other proxy addresses:</p> <p>Address type: new email address</p> |
| Recipient type (detail) | <p>Type of mailbox. Available mailboxes are: User, Room, Equipment, Shared, and Discovery.</p> |
| Do not display in address list | <p>Specifies whether the mailbox is visible in address books. Set this option if you want to prevent the mailbox from being displayed in address books. This option applies to all address books.</p> |
| Risk index (calculated) | <p>Maximum risk index value of all assigned groups. The property is only visible if the QER CalculateRiskIndex configuration parameter is set. For more information, see the <i>One Identity Manager Risk Assessment Administration Guide</i>.</p> |
| Category | <p>Categories the mailbox uses to inherit groups. Groups can be selectively inherited by mailboxes. To do this, the groups and mailboxes are divided into categories. Select one or more categories from the menu.</p> |
| Groups can be inherited | <p>Specifies whether the mailbox can inherit groups through the identity. If the option is set, the mailbox inherits groups through hierarchical roles, in which the identity is a member, or through IT Shop requests.</p> <ul style="list-style-type: none"> • If you add an identity with a mailbox to a department, for example, and you have assigned groups to this department, the mailbox inherits these groups. • If an identity has requested group membership in the IT Shop and the request is granted approval, the identity's mailbox only inherits the group if the option is set. |

| Property | Description |
|--------------------------------------|---|
| Send and forward | Specifies whether to send and forward messages. Set this option to send messages to alternative recipients and mailbox owners. |
| Alternative recipient | <p>Alternative recipient to which messages from this mailbox are forwarded. You can either enter an alternative recipient, a recipient group or a receive folder.</p> <p>To specify an alternative recipient</p> <ol style="list-style-type: none"> 1. Click  next to the field. 2. Select the table under Table which maps the recipient. 3. Select the recipient under Alternative recipient. 4. Click OK. |
| Sender authentication required | Specifies whether authentication data is requested from senders. Set this option to prevent anonymous senders mailing to the mailbox. |
| Moderation enabled | Specifies whether the mailbox is moderated. Use the Assign moderators task to specify the moderators. Then enable the option. |
| Sending message | <p>Specifies how senders are notified when they send messages to moderated mailbox. Permitted values are:</p> <ul style="list-style-type: none"> • Do not notify: The sender is not notified. • Only notify senders in your exchange organization: Only internal senders receive a notification. • Notify all senders: Internal and external senders receive notification. |
| Message read status tracking enabled | Specifies whether this mailbox can show the read status of sent messages. |

Related topics

- [Specifying moderators for Exchange Online mailboxes](#) on page 107
- [Assigning Exchange Online mail-enabled distribution groups to Exchange Online recipients](#) on page 139

Limits and usage of Exchange Online mailboxes

The following information is displayed on the **Usage** tab.

Table 14: Limits for a mailbox

| Property | Description |
|-----------------------------|--|
| Last login | Last time this mailbox was logged in to. This is determined during synchronization and cannot be edited. |
| Last logout | Last time this mailbox was logged out of. This is determined during synchronization and cannot be edited. |
| Last logged in user account | Name of the user account that was used for the last login. This data is determined through synchronization and cannot be edited manually. |
| Storage limit status | Information about the current storage state with respect to the specified limits. This data is determined through synchronization and cannot be edited manually. |
| Number of saved messages | Stored message count This data is determined through synchronization and cannot be edited manually. |
| Associated items count | Number of associated elements in this mailbox. This is determined during synchronization and cannot be edited. |
| Used disk space [byte] | Used disk space in bytes. This data is determined through synchronization and cannot be edited manually. |
| Recoverable items count | Number of items in the Recoverable items folder. This data is determined through synchronization and cannot be edited manually. |
| Size of recoverable items | Size of messages in the Recoverable items folder. This data is determined through synchronization and cannot be edited manually. |
| Use default database values | Specifies whether the mailbox database limits are used. This data is determined through synchronization and cannot be edited manually. Option set: Mailbox database limits are in use. Option not set: Mailbox database limits are not in use. |
| Max. recoverable items | Maximum number of messages allowed in a folder in the Recoverable items folder. This data is determined through synchronization and cannot be edited manually. |
| Warn at [recoverable items] | Number of items a folder in the Recoverable items folder can contain before a warning is sent to the user. This data is determined through synchronization and cannot be edited manually. |
| Keep deleted items [days] | Number of days the deleted objects (email message for example) remain on the server before being removed. |
| Rules quota [KB] | Limit on the number of rules. |
| Prohibit | Size of mailboxes in KB above which, sending, and receiving messages is |

| Property | Description |
|-----------------------|---|
| transfer at [KB] | prohibited. |
| Prohibit send at [KB] | Size of mailboxes in KB above which, sending messages is prohibited. If this size is exceeded the user is sent a message that messages must be deleted in the archive mailbox. The user is not able to send more messages until the size of the mailbox has been reduced. |
| Warn at [KB] | Maximum size in MB of the mailbox. If this size is exceeded the user is sent a warning that messages must be deleted in the archive mailbox. |

Policies and features of Exchange Online mailboxes

Enter the following main data on the **Features** tab.

Table 15: Mailbox features

| Property | Description |
|--------------------------------|--|
| Sharing policy | Sharing policy which applies for this mailbox. |
| Role assignment policy | Role assignment policy that applies to this mailbox. |
| Mobile device mailbox policy | Mobile device mailbox policy that applies to this mailbox. |
| Outlook Web App mailbox policy | Outlook Web App mailbox policy that applies to this mailbox. |
| Retention policy | Retention policy applying to this mailbox. |
| Outlook Web App enabled | Specifies whether the Microsoft Outlook Web App feature is enabled. Office Outlook Web App allows mailbox access over the web browser. |
| Mobile access | Specifies whether mobile devices can access the mailbox. |
| Exchange Web Services enabled | Specifies whether the mailbox can be accessed through Exchange Web Services. |
| IMAP4 enabled | Specifies whether IMAP4 access is enabled. |
| POP3 enabled | Specifies whether POP3 access is enabled. |

| Property | Description |
|--|---|
| MAPI enabled | Specifies whether MAPI access is enabled. MAPI allows mailbox access through a MAPI client, like Outlook. |
| Calendar repair disabled | Specifies whether it is possible to prevent calendar elements in the mailbox from being repaired by the Calendar Repair Assistant. |
| Calendar version disabled | Specifies whether it is possible to prevent changes to the calendar being entered in the mailbox. |
| Archiving enabled | Specifies whether a personal archive is created for this mailbox. Set this option if you want to set up a personal archive for this mailbox. |
| Archive name | Name of the archive. |
| Litigation hold | Specifies whether mailbox retention is mandatory. |
| Put on hold by | The user that enabled litigation hold. |
| Hold date | Date that litigation hold starts for this mailbox. |
| Comment for litigation hold | Additional comment with more information to keep the user informed, when the Litigation hold option is set. This data is displayed to the user in Outlook. |
| Website for litigation hold | Website or document with more information to keep the user informed, when the Litigation hold option is set. This data is displayed to the user in Outlook. |
| Retention policy hold during this period | Specifies whether retention policy is temporary halted during this period. Set this option if the policy for retention hold needs to be temporarily deferred, for example, during vacation. Specify the time period using the Start date and End date fields. |
| Start date | Start date on which to hold the retention policy. |
| End date | Date on which to end the retention policy hold. |
| Audit logging enabled | Specifies whether mailbox audit logging is enabled for this mailbox. |
| Log administrator actions | Specifies the mailbox operations that are logged for administrators as part of audit logging. For more information about mailbox audit logging and the mailbox actions that are logged, see the Microsoft documentation. |
| Log deputy actions | Specifies the mailbox operations that are logged for deputies as part of audit logging. For more information about mailbox audit logging and the mailbox actions that are logged, see the Microsoft documentation. |

| Property | Description |
|-------------------------------|---|
| Log owner actions | Specifies the mailbox operations that are logged for owners as part of audit logging. For more information about mailbox audit logging and the mailbox actions that are logged, see the Microsoft documentation. |
| Keep audit log entries [days] | Maximum age for audit log entries in a mailbox. Log entries that are older than the limit are deleted. |

Related topics

- [Exchange Online policies](#) on page 89

Booking resources for Exchange Online equipment mailboxes and Exchange Online room mailboxes

You can configure booking and planning of resources for equipment and room mailboxes. On the **Booking options** tab, enter the following main data.

Table 16: Main data for booking resources

| Property | Description |
|----------------------------|---|
| Resource capacity | Resource capacity, for example, the number of seats in a meeting room. |
| Enable Calendar Attendant | Specifies whether the Resource Booking Attendant is enabled for device mailboxes and room mailboxes so that booking requests can be processed automatically. Permitted values are: <ul style="list-style-type: none"> • Calendar Attendant not enabled: The calendar attendant is not activated. • Calendar Attendant enabled: The calendar attendant is activated. • Resource booking attendant enabled: The resource booking attendant is automatically enabled for mailboxes of type Room. |
| Allow reoccurring requests | Specifies whether a series of meetings is allowed. |

| Property | Description |
|--|--|
| Request only possible during working hours | Specifies whether the resource can be booked during working hours or outside them, as well. |
| Reject repeated meeting after max. planning period | Specifies whether booking series can be set up beyond the planning period. |
| Max. booking window [days] | Maximum planning period for meeting request in days. |
| Max. duration [min] | Maximum time allowed booking the resource. |
| Booking permissions for everyone | <p>Specifies whether meeting requests conforming to policy are automatically approved for all users.</p> <p>If this option is not set, use Assign booking permissions to specify individual users who can send requests conforming to policy, which are automatically approved.</p> |
| Booking permissions for everyone | <p>Specifies whether all users can send booking requests that conform to policy.</p> <p>If this option is not set, use Assign in-policy meeting request permissions to specify individual users who can send requests which are policy non-conform.</p> |
| Out-of-policy request permissions for everyone | <p>Specifies whether all user can send meeting requests that do not conform to policy.</p> <p>If this option is not set, use Assign out-of-policy meeting request permission to specify individual users who can send requests which are policy non-conform.</p> |
| Allow conflicts | Specifies whether conflicting meeting requests are allowed. |
| Max. series conflicts [%] | Threshold in percent for the permitted conflicts of meetings series that overlap with other meetings. If this value is exceeded, the series request is denied. |
| Max. conflicting instances | Maximum conflicts permitted for meeting series which overlap with other meetings. If the value is exceeded, the series request is denied. |
| Forward meeting requests | Specifies whether meeting requests are forwarded to the resource mailbox deputy managers. The deputy decides about the meeting request. |
| Permit meeting requests from external senders | Specifies whether meeting requests from external senders are entered in the calendar. |
| Add organizer's name | Specifies whether the organizer's name is given in the meeting |

| Property | Description |
|--|--|
| to subject | request's subject field. |
| Inform organizer about declined meeting request | Specifies whether the organizer is sent information when a meeting request is declined because of conflicts. |
| Send additional information about rejected request | Specifies whether additional information is sent in response to a meeting request. Enter the additional information in the Additional information input field. |
| Additional data | Additional information for responding to meeting requests. |
| Remove attachments from meeting requests | Specifies whether attachments are deleted from meeting requests. |
| Remove comments from meeting requests | Specifies whether message text is deleted from meeting requests. |
| Remove subject from meeting requests | Specifies whether the subject is deleted from meeting requests. |
| Only retain calendar meetings | Specifies whether elements that do not belong the calendar are deleted. |
| Response details enabled | Specifies whether the reasons for accepting or decline a meeting are added to the response email. |
| New meeting requests are marked with the status "tentative". | Specifies whether meeting requests are automatically entered in the calendar with the Tentative status. |
| Mark meeting requests as "Tentative" | Specifies whether meeting requests are marked with Tentative status in the calendar. If this option is disabled, meeting requests are marked with the Free status. |
| Remove "private" flag from accepted meeting | Specifies whether the Private status is deleted from meeting requests. |
| Delete expired meeting requests | Specifies whether to automatically delete messages to other attendees about forwarded meetings. These messages are moved to the Deleted items folder. |
| Delete expired meeting requests | Specifies whether to automatically delete old meeting requests from the calendar. |

Related topics

- [Booking permissions for Exchange Online equipment mailbox and Exchange Online room mailbox](#) on page 103

Booking permissions for Exchange Online equipment mailbox and Exchange Online room mailbox

You can configure booking permissions of resources for equipment and room mailboxes.

Assuming that booking a resource is not going to result in a planning conflict or the resource's limits being exceeded, like the room capacity or the planned duration, you can allow meeting requests to be automatically approved.

Automatically approve meeting request if the resource is available

- If the **Booking permissions for everyone** option is set, every user can automatically reserve the resource with a meeting request that conform to the policy.
- Use the **Assign booking permissions** options to specify individual users whose meeting requests are automatically approved.

Allow meeting requests if the resource is available

- If the **Booking permissions for everyone** option is set, all users that adhere to the guidelines, are allowed to send meeting requests.
- Use the **Assign in-policy meeting request permissions** to specify individual users who can send requests which do not conform to the policies.

Automatically approve meeting requests if the resource is available and send meeting requests if the resource is not available.

- If the **Out-of-policy request permissions for everyone** is set, every user can automatically reserve the resource using a meeting request that conforms to the policy. Users can send meeting requests that do not conform to the policies. Meeting requests that do not fulfill the policies can be approved by the mailbox's delegate.
- Use the **Assign out-of-policy meeting request permissions** to specify individual users whose policy conform meeting requests are automatically approved and who can send meeting requests that do not conform to the policies. Meeting requests that do not fulfill the policies can be approved by the mailbox's delegate.

Adjusting receive restrictions for Exchange Online mailboxes

NOTE: The **Assign mail acceptance** and **Assign mail rejection** assignments are mutually exclusive. You can specify whether to accept or deny the recipient's message.

To adjust mail acceptance for mailboxes

1. In the Manager, select the **Azure Active Directory > Mailboxes** category.
2. Select a mailbox in the result list.
3. Select the **Assign mail acceptance** task to specify recipients whose messages are accepted.

- OR -

Select the **Assign mail rejection** task to specify recipients whose messages are rejected.

4. Select the table containing the recipient from the menu at the top of the form. You have the following options:
 - Mail-enabled distribution groups
 - Dynamic distribution groups
 - Mailboxes
 - Mail users
 - Mail contacts
 - Office 365 groups

5. In the **Add assignments** pane, assign recipients.

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

To remove an assignment

- Select the recipient and double-click .

6. Save the changes.

Exchange Online mailbox permission: Send on behalf

You use the **Send on behalf of** send permissions to specify which users can send messages on behalf of the mailbox owner.

To customize send permissions for mailboxes

1. In the Manager, select the **Azure Active Directory > Mailboxes** category.
2. Select a mailbox in the result list.
3. Select the **Assign send authorizations** task.
4. Select the table which contains the user from the menu at the top of the form. You have the following options:

- Mail-enabled distribution groups
 - Mailboxes
 - Mail users
5. In the **Add assignments** pane, assign users.

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

To remove an assignment

- Select the user and double-click ✓.
6. Save the changes.

NOTE: Mailbox permissions are disabled by default. For more information about mailbox permissions, see [Exchange Online Postfachberechtigungen](#).

Related topics

- [Exchange Online mailbox permission: Send as](#) on page 105
- [Exchange Online mailbox permission: Full access](#) on page 106

Exchange Online mailbox permission: Send as

You use the **Send as** mailbox permissions to specify which users can send notifications about a mailbox. The notification is displayed as if it came from the mailbox owner.

To customize send permissions for mailboxes

1. In the Manager, select the **Azure Active Directory > Mailboxes** category.
2. Select a mailbox in the result list.
3. Select the **Assign send as permissions** task.
4. Select the table which contains the user from the menu at the top of the form. You have the following options:
 - Azure Active Directory user accounts
 - Azure Active Directory groups
5. In the **Add assignments** pane, assign the user accounts.

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

To remove an assignment

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

NOTE: Mailbox permissions are disabled by default. For more information about mailbox permissions, see [Exchange Online Postfachberechtigungen](#).

Related topics

- [Exchange Online mailbox permission: Full access](#) on page 106
- [Exchange Online mailbox permission: Send on behalf](#) on page 104

Exchange Online mailbox permission: Full access


The **Full Access** mailbox permission allows a user to log in to a mailbox and view and edit the contents of the mailbox. Mailbox permissions for sending notifications from this mailbox must be granted separately.

To customize send permissions for mailboxes

1. In the Manager, select the **Azure Active Directory > Mailboxes** category.
2. Select a mailbox in the result list.
3. Select the **Assign full access permissions** task.
4. Select the table which contains the user from the menu at the top of the form. You have the following options:
 - Azure Active Directory user accounts
 - Azure Active Directory groups
5. In the **Add assignments** pane, assign users.

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

To remove an assignment

- Select the user and double-click .
6. Save the changes.

NOTE: Mailbox permissions are disabled by default. For more information about mailbox permissions, see [Exchange Online Postfachberechtigungen](#).

Related topics

- [Exchange Online mailbox permission: Send on behalf](#) on page 104
- [Exchange Online mailbox permission: Send as](#) on page 105

Specifying moderators for Exchange Online mailboxes


Moderated mailboxes are implemented to allow messages sent to a mailbox to be approved or denied by a moderator. The message is not sent on until it has been approved by the moderator.

To specify moderators for a mailbox

1. In the Manager, select the **Azure Active Directory > Mailboxes** category.
2. Select a mailbox in the result list.
3. Select the **Assign moderators** task.
4. Select the table which contains the user from the menu at the top of the form. You have the following options:
 - Mailboxes
 - Mail contacts
 - Mail users
5. In the **Add assignments** pane, add the moderators.

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

To remove an assignment

- Select the moderator and double-click .
6. Save the changes.

Assigning extended properties to Exchange Online mailbox

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


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

To specify extended properties for a mailbox

1. In the Manager, select the **Azure Active Directory > Mailboxes** category.
2. Select a mailbox 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.

Deleting Exchange Online mailboxes

User mailboxes are deleted by removing the subscriptions from their Azure Active Directory user accounts.

You can delete equipment mailboxes, room mailboxes, and shared mailboxes in One Identity Manager. When equipment mailboxes, room mailboxes, or shared mailboxes are deleted, the Azure Active Directory user account linked to the mailbox is deleted at the same time.

To delete a mailbox

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

Exchange Online mail users

Mail users obtain information about users from outside the Exchange Online organization. Mail users are assigned at least one email address. Notification is automatically forwarded to this email address. As opposed to mail contacts, mail contacts have login credentials and access to resources.

Mail users are loaded into One Identity Manager by synchronization. You can create and edit mail users in One Identity Manager. When you create a mail user, an Azure Active Directory user account is also created and linked to the mail user.

NOTE: It is recommended to use account definitions to set up mail users for company identities.

- In order to create mail users through account definitions, identities must have a central user account and obtain the IT operating data through assignment to a primary department, primary location, or a primary cost center.
- Some of the main data of the mail user is mapped from identity main data using templates.

Detailed information about this topic

- [Account definitions for Exchange Online mail users and Exchange Online mail contacts](#) on page 59
- [Creating Exchange Online mail users](#) on page 110
- [Editing main data of Exchange Online mail users](#) on page 110
- [Main data for Exchange Online mail users](#) on page 111
- [Receive restrictions for Exchange Online mail users](#) on page 116
- [Customizing send permissions for Exchange Online mail users](#) on page 117
- [Specifying moderators for Exchange Online mail users](#) on page 118
- [Assigning extended properties to Exchange Online mail users](#) on page 118
- [Deleting Exchange Online mail users](#) on page 119
- [Synchronizing single objects](#) on page 50

Creating Exchange Online mail users


When you create a mail user, an Azure Active Directory user account is also created and linked to the mail user.

Azure Active Directory configuration settings are used for generating random passwords for new mail users, for sending login credentials, and for applying password policies. For more information, see the *One Identity Manager Administration Guide for Connecting to Azure Active Directory*.

NOTE: It is recommended to use account definitions to set up mail users for company identities.

- In order to create mail users through account definitions, identities must have a central user account and obtain the IT operating data through assignment to a primary department, primary location, or a primary cost center.
- Some of the main data of the mail users is mapped from identity main data using templates.

To create a mail user

1. In the Manager, select the **Azure Active Directory > Mail user** category.
2. Click  in the result list.
3. On the main data form, enter the main data for the mail user.
4. Save the changes.

Related topics

- [Account definitions for Exchange Online mail users and Exchange Online mail contacts](#) on page 59
- [Editing main data of Exchange Online mail users](#) on page 110
- [Main data for Exchange Online mail users](#) on page 111

Editing main data of Exchange Online mail users

To edit a mail user.

1. In the Manager, select the **Azure Active Directory > Mail users** category.
2. Select the mail user in the result list and run the **Change main data** task.
3. Edit the mail user's main data.
4. Save the changes.

Related topics

- [Creating Exchange Online mail users](#) on page 110
- [Main data for Exchange Online mail users](#) on page 111

Main data for Exchange Online mail users

Table 17: Mail user main data


| Property | Description |
|---------------------------------|---|
| Identity | <p>Identity to use the mail user.</p> <ul style="list-style-type: none">• An identity is already entered if the mail user was generated by an account definition.• If you create the mail user manually, you can select an identity from the menu. <p>The menu displays activated and deactivated identities by default. If you do not want to see any deactivated identities, set the QER Person HideDeactivatedIdentities configuration parameter.</p> <p>NOTE: If you assign a deactivated identity to a mail user, the mail user might be locked or deleted depending on the configuration.</p> |
| No link to an identity required | <p>Specifies whether the mail user is intentionally not assigned an identity. The value is determined from the linked user account.</p> |
| Not linked to an identity | <p>Indicates why the No link to an identity required option is enabled for this mail user. The value is determined from the linked user account. Possible values:</p> <ul style="list-style-type: none">• By administrator: The option was set manually by the administrator.• By attestation: The user account was attested.• By exclusion criterion: The user account is not associated with an identity due to an exclusion criterion. For example, the user account is included in the exclude list for automatic identity assignment (configuration parameter PersonExcludeList). |
| Account definition | <p>Account definition through which the mail user was created.</p> <p>Use the account definition to automatically populate mail user main data and to specify a manage level for the mail user.</p> |

| Property | Description |
|-------------------------------------|---|
| | <p>One Identity Manager finds the IT operating data of the assigned identity and uses it to populate the corresponding fields in the mail user.</p> <p>NOTE: The account definition cannot be changed once the mail user has been saved.</p> |
| Manage level | Manage level with which the mail user is created. 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. |
| Azure Active Directory tenant | The Azure Active Directory tenant's name. |
| Azure Active Directory user account | Azure Active Directory user account that uses this mail user. |
| 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. |
| Initials | The user's initials. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level. |
| Name | The mail user's identifier. |
| Display name | Name as used in the address book. |
| Alias | Unique alias for further identification of the mail user. |
| User ID | <p>User ID that user uses to log in.</p> <p>Example:</p> <p><alias>@<domain.com> <user>@yourorganization.onmicrosoft.com</p> |
| Password | <p>Login password. The identity's central password can be mapped to the mail user's password. For more information about an identity's central password, see <i>One Identity Manager Identity Management Base Module Administration Guide</i>.</p> <p>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.</p> |

| Property | Description |
|--------------------------------|--|
| | Azure Active Directory configuration settings are used for generating random passwords for new mail users, for sending login credentials, and for applying password policies. For more information, see the <i>One Identity Manager Administration Guide for Connecting to Azure Active Directory</i> . |
| Confirmation | Reconfirm password. |
| Proxy addresses | Other email addresses for the mail user. Use the following syntax to set up other proxy addresses: Address type: new email address |
| Recipient type (detail) | Type of mail user. You can select either Mail users or Guest mail users . |
| External email address | Email address for forwarding messages. |
| Destination address type | Address type of the email address. Permitted value is SMTP . |
| Do not display in address list | Specifies whether the mail user is visible in address books. Set this option if you want to prevent the mail user from being displayed in address books. This option applies to all address books. |
| Risk index (calculated) | Maximum risk index value of all assigned groups. The property is only visible if the QER CalculateRiskIndex configuration parameter is set. For more information, see the <i>One Identity Manager Risk Assessment Administration Guide</i> . |
| Category | Categories the mail user uses to inherit groups. Groups can be selectively inherited by mail users. To do this, the groups and mail users are divided into categories. Select one or more categories from the menu. |
| Groups can be inherited | Specifies whether the mail user can inherit groups through the identity. If the option is set, the mail user inherits groups through hierarchical roles, in which the identity is a member, or through IT Shop requests. <ul style="list-style-type: none"> • If you add an identity with a user accounts to, for example, a department and you have assigned groups to this department, the mail user inherits these groups. • If an identity has requested group membership in the IT Shop and the request is granted approval, the identity's mail user only inherits the group if the option is set. |
| Simple display | Simple display name for systems that cannot interpret all the |

| Property | Description |
|--------------------------------|---|
| | characters of normal display names. |
| Phonetic display name | <p>Display name in phonetic letters. It is used if the pronunciation and spelling of the name do not match. For example, the display name is used to sort recipients in the hierarchical address book if no sort order is given. They are sorted in ascending order from A to Z.</p> <p>If no phonetic name is given, they are sorted by the display name.</p> |
| Sort order | <p>Specifies the order in which to display recipients in the hierarchical address book. The larger the value, the higher the ranking in the sort order.</p> <p>If no order is given or more than one entries have the same sort order, recipients are sorted by their phonetic display name.</p> |
| Message format | Format for messages that are sent to mail u. Permitted values are MIME (default) and Text . |
| Message body format | <p>Format for body text of messages that are sent to mail users. Options are Text, HTML and TextAndHtml. The permitted values depend on the selected message format.</p> <ul style="list-style-type: none"> • If the MIME message formation is fixed, the format of the body text can be Text, HTML and TextAndHtml (default). • If the message format is Text, the format of the body text can be Text. |
| Attachment format | The Apple Macintosh operating system's attachment format for messages that are sent to mail users. Options are BinHex (default), UuEncode , AppleSingle , and AppleDouble . |
| Use preferred message format | Specifies whether message format settings configured for the recipient are overwritten by the global settings. |
| Use MAPI-RTF | Specifies whether the mail user can receive messages in MAPI format. Available options are Never , Always , and Use default settings . |
| Sender authentication required | Specifies whether authentication data is requested from senders. Set this option to prevent anonymous senders mailing the mail user. |
| Moderation enabled | Specifies whether the mail user is moderated. Use the Assign moderators task to specify the moderators. Then enable the option. |
| Sending message | Specifies how senders are notified when they send messages to moderated mail users. Permitted values are: |

| Property | Description |
|----------------------------|--|
| | <ul style="list-style-type: none"> • Do not notify: The sender is not notified. • Only notify senders in your exchange organization: Only internal senders receive a notification. • Notify all senders: Internal and external senders receive notification. |
| Street | Street or road. 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 identities assigned based on the town. |
| Mailbox | Mailbox. 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. |
| 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 or region | The country ID. |
| Office | Office address. |
| Business phone | Business telephone numbers. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level. |
| Additional phone numbers | Other business telephone numbers. |
| Fax | Fax number. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level. |
| Additional fax numbers | Additional fax numbers. |
| Home phone | Private telephone number. |
| Additional private numbers | Additional 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. |

| Property | Description |
|--------------|---|
| Mobile phone | Mobile phone number. |
| Website. | The user's website. |
| Notes | More information about the user. |
| Item | The user's job title. |
| Department | Department. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level. |
| Company | Company. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level. |
| Manager | <p>Manager responsible for the mail user.</p> <p>To specify a manager</p> <ol style="list-style-type: none"> 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. |
| Assistant | Name of the mail contact's assistant. |

Related topics

- [Account definitions for Exchange Online mail users and Exchange Online mail contacts on page 59](#)
- [Specifying moderators for Exchange Online mailboxes on page 107](#)
- [Assigning Exchange Online mail-enabled distribution groups to Exchange Online recipients on page 139](#)

Receive restrictions for Exchange Online mail users

NOTE: The **Assign mail acceptance** and **Assign mail rejection** assignments are mutually exclusive. You can specify whether to accept or deny the recipient's message.

To customize mail acceptance for a mail user

1. In the Manager, select the **Azure Active Directory > Mail user** category.
2. Select the mail user in the result list.

3. Select the **Assign mail acceptance** task to specify recipients whose messages are accepted.

- OR -

Select the **Assign mail rejection** task to specify recipients whose messages are rejected.

4. Select the table containing the recipient from the menu at the top of the form. You have the following options:
 - Mail-enabled distribution groups
 - Dynamic distribution groups
 - Mailboxes
 - Mail users
 - Mail contacts
 - Office 365 groups
5. In the **Add assignments** pane, assign recipients.

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

To remove an assignment

- Select the recipient and double-click .

6. Save the changes.

Customizing send permissions for Exchange Online mail users

You use the **Send on behalf of** send permissions to specify which users can send messages on behalf of the mail users.

To customize send permissions for a mail user

1. In the Manager, select the **Azure Active Directory > Mail user** category.
2. Select the mail user in the result list.
3. Select the **Assign send authorizations** task.
4. Select the table which contains the user from the menu at the top of the form. You have the following options:
 - Mail-enabled distribution groups
 - Mailboxes
 - Mail users
5. In the **Add assignments** pane, assign users.

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

To remove an assignment

- Select the user and double-click .

6. Save the changes.

Specifying moderators for Exchange Online mail users

Moderated mail users are implemented to accept or reject messages sent to a mail user by a moderator. The message is not sent on until it has been approved by the moderator.

To specify moderators for a mail user

1. In the Manager, select the **Azure Active Directory > Mail users** category.
2. Select the mail user in the result list.
3. Select the **Assign moderators** task.
4. Select the table which contains the user from the menu at the top of the form. You have the following options:
 - Mailboxes
 - Mail contacts
 - Mail users
5. In the **Add assignments** pane, add the moderators.

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

To remove an assignment

- Select the moderator and double-click .

6. Save the changes.

Assigning extended properties to Exchange Online mail users

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


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

To specify extended properties for a mail user

1. In the Manager, select the **Azure Active Directory > Mail users** category.
2. Select the mail user in the result list.
3. Select **Assign extended properties**.
4. In the **Add assignments** pane, assign extended properties.

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

To remove an assignment


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

Deleting Exchange Online mail users

When you delete a mail user, the **Do not display in address lists** option is enabled and the mail user is no longer shown in address books. In addition, the Azure Active Directory user account that is linked to the mail user is deleted.

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

To delete a mail user

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

Exchange Online mail contacts

Mail contacts obtain information about users from outside the Exchange Online organization. Mail contacts are assigned at least one email address. Notification is automatically forwarded to this email address. As opposed to mail users, mail contacts do not have login credentials or access to resources.

Mail contacts are loaded into One Identity Manager by synchronization. You can create and edit mail contacts in One Identity Manager.

NOTE: It is recommended to use account definitions to set up mail contacts for company identities.

- In order to create mail contacts through account definitions, identities must have a central user account and a default email address and obtain their IT operating data through assignment to a primary department, primary location, or a primary cost center.
- Some of the main data of the mail contact is mapped from identity main data using templates.

Detailed information about this topic


- [Account definitions for Exchange Online mail users and Exchange Online mail contacts](#) on page 59
- [Creating Exchange Online mail contacts](#) on page 121
- [Editing main data of Exchange Online mail contacts](#) on page 121
- [Main data for Exchange Online mail contacts](#) on page 122
- [Receive restrictions for Exchange Online mail contacts](#) on page 127
- [Customizing send permissions for Exchange Online mail contacts](#) on page 128
- [Specifying moderators for Exchange Online mail contacts](#) on page 128
- [Assigning extended properties to Exchange Online mail contacts](#) on page 129
- [Deleting Exchange Online mail contacts](#) on page 129
- [Synchronizing single objects](#) on page 50

Creating Exchange Online mail contacts

NOTE: It is recommended to use account definitions to set up mail contacts for company identities.

- In order to create mail contacts through account definitions, identities must have a central user account and a default email address and obtain their IT operating data through assignment to a primary department, primary location, or a primary cost center.
- Some of the main data of the mail contacts is mapped from identity main data using templates.

To create a mail contact

1. In the Manager, select the **Azure Active Directory > Mail contacts** category.
2. Click  in the result list.
3. On the main data form, enter the main data for the mail contact.
4. Save the changes.

Related topics

- [Account definitions for Exchange Online mail users and Exchange Online mail contacts](#) on page 59
- [Editing main data of Exchange Online mail contacts](#) on page 121
- [Main data for Exchange Online mail contacts](#) on page 122

Editing main data of Exchange Online mail contacts

To edit a mail contact

1. In the Manager, select the **Azure Active Directory > Mail contacts** category.
2. Select the mail contact in the result list and run the **Change main data** task.
3. Edit the mail contact's main data.
4. Save the changes.

Related topics

- [Creating Exchange Online mail contacts](#) on page 121
- [Main data for Exchange Online mail contacts](#) on page 122

Main data for Exchange Online mail contacts


Table 18: Mail contacts main data

| Property | Description |
|---------------------------------|--|
| Identity | <p>Identity to use the mail contact.</p> <ul style="list-style-type: none"> An identity is already entered if the mail contact was generated by an account definition. If you create the mail contact manually, you can select an identity from the menu. <p>The menu displays activated and deactivated identities by default. If you do not want to see any deactivated identities, set the QER Person HideDeactivatedIdentities configuration parameter.</p> <p>NOTE: If you assign a deactivated identity to a mail contact, the mail contact might be locked or deleted depending on the configuration.</p> |
| No link to an identity required | <p>Specifies whether the contact is intentionally not assigned an identity. The option is automatically set if a contact is included in the exclusion list for automatic identity assignment or a corresponding attestation is carried out. You can set the option manually. Enable the option if the contact does not need to be linked with an identity (for example, if several identities use the contact).</p> <p>If attestation approves these contacts, these contacts will not be submitted for attestation in the future. In the Web Portal, contact that are not linked to an identity can be filtered according to various criteria.</p> |
| Not linked to an identity | <p>Indicates why the No link to an identity required option is enabled for this contact. Possible values:</p> <ul style="list-style-type: none"> By administrator: The option was set manually by the administrator. By attestation: The contact was attested. By exclusion criterion: The contact is not associated with an identity due to an exclusion criterion. For example, the contact is included in the exclude list for automatic identity assignment (configuration parameter PersonExcludeList). |
| Account definition | Account definition through which the mail contact was created. |

| Property | Description |
|--------------------------------|---|
| | <p>Use the account definition to automatically populate mail contact main data and to specify a manage level for the mail contact. One Identity Manager finds the IT operating data of the assigned identity and uses it to populate the corresponding fields in the mail contact.</p> <p>NOTE: The account definition cannot be changed once the mail contact has been saved.</p> |
| Manage level | Manage level with which the mail contact is created. 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. |
| Azure Active Directory tenant | The Azure Active Directory tenant's name. |
| First name | The contact'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 contact's last name. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level. |
| Initials | The contact's initials. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level. |
| Name | The mail contact's identifier. |
| Display name | Name as used in the address book. |
| Alias | Unique alias for further identification of the mail contact. |
| Proxy addresses | Other email addresses for the mail contact. Use the following syntax to set up other proxy addresses: Address type: new email address |
| External email address | Email address for forwarding messages. |
| Destination address type | Address type of the email address. Permitted value is SMTP . |
| Do not display in address list | Specifies whether the mail contact is visible in address books. Set this option if you want to prevent the mail contact from being displayed in address books. This option applies to all address books. |
| Risk index (calculated) | Maximum risk index value of all assigned groups. The property |

| Property | Description |
|-------------------------|---|
| | is only visible if the QER CalculateRiskIndex configuration parameter is set. For more information, see the <i>One Identity Manager Risk Assessment Administration Guide</i> . |
| Category | Categories the mail contact uses to inherit groups. Groups can be selectively inherited by mail contacts. To do this, the groups and mail contacts are divided into categories. Select one or more categories from the menu. |
| Groups can be inherited | <p>Specifies whether the mail contact can inherit groups through the identity. If the option is set, the mail contact inherits groups through hierarchical roles, in which the identity is a member, or through IT Shop requests.</p> <ul style="list-style-type: none"> • If you add an identity with a user accounts to, for example, a department and you have assigned groups to this department, the mail contact inherits these groups. • If an identity has requested group membership in the IT Shop and the request is granted approval, the identity's mail contact only inherits the group if the option is set. |
| Simple display | Simple display name for systems that cannot interpret all the characters of normal display names. |
| Phonetic display name | <p>Display name in phonetic letters. It is used if the pronunciation and spelling of the name do not match. For example, the display name is used to sort recipients in the hierarchical address book if no sort order is given. They are sorted in ascending order from A to Z.</p> <p>If no phonetic name is given, they are sorted by the display name.</p> |
| Sort order | <p>Specifies the order in which to display recipients in the hierarchical address book. The larger the value, the higher the ranking in the sort order.</p> <p>If no order is given or more than one entries have the same sort order, recipients are sorted by their phonetic display name.</p> |
| Message format | Format for messages that are sent to mail contacts. Permitted values are MIME (default) and Text . |
| Message body format | <p>Format for body text of messages that are sent to mail contacts. Options are Text, HTML and TextAndHtml. The permitted values depend on the selected message format.</p> <ul style="list-style-type: none"> • If the MIME message formation is fixed, the format of the body text can be Text, HTML and TextAndHtml (default). |

| Property | Description |
|--------------------------------|---|
| | <ul style="list-style-type: none"> If the message format is Text, the format of the body text can be Text. |
| Attachment format | The Apple Macintosh operating system's attachment format for messages that are sent to mail contacts. Options are BinHex (default), UuEncode , AppleSingle , and AppleDouble . |
| Use preferred message format | Specifies whether message format settings configured for the recipient are overwritten by the global settings. |
| Use MAPI-RTF | Specifies whether the mail contact can receive messages in MAPI format. Available options are Never , Always , and Use default settings . |
| Sender authentication required | Specifies whether authentication data is requested from senders. Set this option to prevent anonymous senders mailing the mail contact. |
| Moderation enabled | Specifies whether the mail contact is moderated. Use the Assign moderators task to specify the moderators. Then enable the option. |
| Sending message | Specifies how senders are notified when they send messages to moderated mail contacts. Permitted values are: <ul style="list-style-type: none"> Do not notify: The sender is not notified. Only notify senders in your exchange organization: Only internal senders receive a notification. Notify all senders: Internal and external senders receive notification. |
| Street | Street or road. 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 identities assigned based on the town. |
| Mailbox | Mailbox. 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. |
| 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 or region | The country ID. |

| Property | Description |
|----------------------------|--|
| Office | Office address. |
| Business phone | Business telephone numbers. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level. |
| Additional phone numbers | Other business telephone numbers. |
| Fax | Fax number. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level. |
| Additional fax numbers | Additional fax numbers. |
| Home phone | Private telephone number. |
| Additional private numbers | Additional 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. |
| Mobile phone | Mobile phone number. |
| Web page | Contact's web page. |
| Notes | More information about the contact. |
| Title | The contact's job title. |
| Department | Department. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level. |
| Company | Company. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level. |
| Manager | <p>Manager responsible for the mail contact.</p> <p>To specify a manager</p> <ol style="list-style-type: none"> 1. Click  next to the field. 2. In the Table menu, select the table that maps the account manager. 3. In the Manager menu, select the manager. 4. Click OK. |
| Assistant | Name of the mail contact's assistant. |
| Assistant phone | Telephone number of the assistant. |

Related topics

- [Account definitions for Exchange Online mail users and Exchange Online mail contacts](#) on page 59
- [Specifying moderators for Exchange Online mail contacts](#) on page 128
- [Assigning Exchange Online mail-enabled distribution groups to Exchange Online recipients](#) on page 139

Receive restrictions for Exchange Online mail contacts

NOTE: The **Assign mail acceptance** and **Assign mail rejection** assignments are mutually exclusive. You can specify whether to accept or deny the recipient's message.

To customize mail acceptance for a mail contact

1. In the Manager, select the **Azure Active Directory > Mail contacts** category.
2. Select the mail contact in the result list.
3. Select the **Assign mail acceptance** task to specify recipients whose messages are accepted.

- OR -


Select the **Assign mail rejection** task to specify recipients whose messages are rejected.

4. Select the table containing the recipient from the menu at the top of the form. You have the following options:
 - Mail-enabled distribution groups
 - Dynamic distribution groups
 - Mailboxes
 - Mail users
 - Mail contacts
 - Office 365 groups

5. In the **Add assignments** pane, assign recipients.

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

To remove an assignment

- Select the recipient and double-click .
6. Save the changes.

Customizing send permissions for Exchange Online mail contacts


You use the **Send on behalf of** send permissions to specify which users can send messages on behalf of the mail contacts.

To customize send permissions for a mail contact

1. In the Manager, select the **Azure Active Directory > Mail contacts** category.
2. Select the mail contact in the result list.
3. Select the **Assign send authorizations** task.
4. Select the table which contains the user from the menu at the top of the form. You have the following options:
 - Mail-enabled distribution groups
 - Mailboxes
 - Mail users
5. In the **Add assignments** pane, assign users.

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

To remove an assignment

- Select the user and double-click .
6. Save the changes.

Specifying moderators for Exchange Online mail contacts

Moderated mail contacts are implemented to accept or reject messages sent to a mail contacts by a moderator. The message is not sent on until it has been approved by the moderator.


To specify moderators for a mail contact

1. In the Manager, select the **Azure Active Directory > Mail contacts** category.
2. Select the mail contact in the result list.
3. Select the **Assign moderators** task.
4. Select the table which contains the user from the menu at the top of the form. You have the following options:

- Mailboxes
 - Mail contacts
 - Mail users
5. In the **Add assignments** pane, add the moderators.

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

To remove an assignment

 - Select the moderator and double-click .
 6. Save the changes.

Assigning extended properties to Exchange Online mail contacts

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


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

To specify extended properties for a mail contact

1. In the Manager, select the **Azure Active Directory > Mail contacts** category.
2. Select the mail contact 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.

Deleting Exchange Online mail contacts

NOTE: As long as an account definition for an identity is valid, the identity retains the mail contact that was created by it. If the account definition assignment is removed, the mail contact created through this account definition, is deleted.

When you delete a mail contact, the **Do not display in address lists** option is enabled and the mail contact is no longer shown in address books.

To delete a mail contact

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

Exchange Online mail-enabled distribution groups

You can use mail-enabled universal security groups and mail-enabled universal distribution groups to distribute messages to a group of recipients.

Mail-enabled distribution groups are loaded into One Identity Manager by synchronization. You can create and edit mail-enabled distribution groups in One Identity Manager. When you create a mail-enabled distribution group, an Azure Active Directory group is also created and linked to the mail-enabled distribution group.

In One Identity Manager, you can assign mail-enabled distribution groups directly to mailboxes, mail users, and mail contacts or they can be inherited through departments, cost centers, locations, or business roles. Users can also request mail-enabled distribution groups through the Web Portal. To do this, the mail-enabled distribution groups are supplied by the IT Shop.

Detailed information about this topic


- [Creating Exchange Online mail-enabled distribution groups on page 132](#)
- [Editing main data for Exchange Online mail-enabled distribution groups on page 132](#)
- [Main data for Exchange Online mail-enabled distribution groups on page 133](#)
- [Receive restrictions for Exchange Online mail-enabled distribution groups on page 136](#)
- [Customizing send permissions for Exchange Online mail-enabled distribution groups on page 137](#)
- [Specifying moderators for Exchange Online mail-enabled distribution groups on page 138](#)
- [Specifying Exchange Online mail-enabled distribution groups on page 138](#)
- [Assigning Exchange Online mail-enabled distribution groups to Exchange Online recipients on page 139](#)
- [Exchange Online mail-enabled distribution group inheritance based on categories on page 152](#)

- [Adding Exchange Online dynamic distribution groups to Exchange Online mail-enabled distribution groups](#) on page 153
- [Adding an Exchange Online dynamic distribution group to Exchange Online mail-enabled distribution groups](#) on page 153
- [Adding Exchange Online mail-enabled public folder to Exchange Online mail-enabled distribution groups](#) on page 154
- [Assigning extended properties to Exchange Online mail-enabled distribution groups](#) on page 154
- [Deleting Exchange Online mail-enabled distribution groups](#) on page 155
- [Synchronizing single objects](#) on page 50

Creating Exchange Online mail-enabled distribution groups

When you create a mail-enabled distribution group, an Azure Active Directory group is also created and linked to the mail-enabled distribution group.

To create a mail-enabled distribution group

1. In the Manager, select the **Azure Active Directory > Mail-enabled distribution groups** category.
2. Click  in the result list.
3. On the main data form, enter the main data for the mail-enabled distribution group.
4. Save the changes.

Related topics

- [Editing main data for Exchange Online mail-enabled distribution groups](#) on page 132
- [Main data for Exchange Online mail-enabled distribution groups](#) on page 133

Editing main data for Exchange Online mail-enabled distribution groups

To edit a mail-enabled distribution group

1. In the Manager, select the **Azure Active Directory > Mail-enabled distribution groups** category.

2. Select the mail-enabled distribution group in the result list and run the **Change main data** task.
3. Edit the mail-enabled distribution group's main data.
4. Save the changes.

Related topics

- [Creating Exchange Online mail-enabled distribution groups](#) on page 132
- [Main data for Exchange Online mail-enabled distribution groups](#) on page 133

Main data for Exchange Online mail-enabled distribution groups

Table 19: Mail-enabled distribution group main data

| Property | Description |
|-------------------------------|---|
| Azure Active Directory group | Azure Active Directory group for which the mail-enabled distribution group is created. |
| Azure Active Directory tenant | The Azure Active Directory tenant's name. |
| Name | Name of the mail-enabled distribution group. |
| Simple display | Simple display name for systems that cannot interpret all the characters of normal display names. |
| Phonetic display name | Display name in phonetic letters. It is used if the pronunciation and spelling of the name do not match. For example, the display name is used to sort recipients in the hierarchical address book if no sort order is given. They are sorted in ascending order from A to Z. If no phonetic name is given, they are sorted by the display name. |
| Sort order | Specifies the order in which to display recipients in the hierarchical address book. The larger the value, the higher the ranking in the sort order. If no order is given or more than one entries have the same sort order, recipients are sorted by their phonetic display name. |
| Display name | Name as used in the address book. |
| Alias | Unique alias for further identification of the mail-enabled distribution group. |

| Property | Description |
|--|--|
| Group type | The type of group. Permitted values are Universal (default) and Universal, security-enabled . |
| Proxy addresses | Email addresses for the mail-enabled distribution 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 |
| Do not display in address list | Specifies whether the mail-enabled distribution group is visible in address books. Set this option if you want to prevent the mail-enabled distribution group from being displayed in address books. This option applies to all address books. |
| Email address | Email addresses for the mail-enabled distribution group. |
| Report to sender | Specifies whether the delivery reports are sent to the message sender. |
| Report to owner | Specifies whether the delivery reports are sent to the message owner. |
| Only limit messages from authenticated users | Specifies whether authentication data is requested from senders. Set this option if only messages from authenticated users are permitted. |
| Out-of-office message to sender | Set this option if the message sender should receive out-of-office messages. |
| Add to group | Specifies how members can join the mail-enabled distribution group. Permitted values are: <ul style="list-style-type: none"> • Open: Members can be added to the group without approval. • Closed: Only mail-enabled distribution group administrators can add members to the group. Requests to be added to the group are automatically denied. • Owner approval: Requests to be added to the group can be made and are approved by the mail-enabled distribution group administrators. <p>Use the Assign administrators task to specify administrators.</p> |
| Leave group | Use this option to specify how members can leave the distribution group. Permitted values are: <ul style="list-style-type: none"> • Open: Members can leave the group without approval. |

| Property | Description |
|----------------------------------|---|
| | <ul style="list-style-type: none"> • Closed: Members can only leave the group with administrator approval. Requests to leave the group are automatically denied. <p>Use the Assign administrators task to specify administrators.</p> |
| Moderation enabled | Specifies whether the mail-enabled distribution group is moderated. Set this option if the distribution group should be moderated. Use the task Assign moderators to specify moderators. |
| Allow moderation of child groups | Specifies how to approve messages if a moderate group appears in other moderated groups as a member. |
| Sending message | Specifies how senders are notified when they send messages to moderated distribution groups. Permitted values are: <ul style="list-style-type: none"> • Do not notify: The sender is not notified. • Only notify senders in your exchange organization: Only internal senders receive a notification. • Notify all senders: Internal and external senders receive notification. |
| 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 mailboxes, mail users and mail contacts, and 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 mailboxes, mail users and mail contacts is not permitted. |
| Service item | Service item data for requesting the group through the IT Shop. |
| Risk index | Value for assessing the risk of assigning the group to mailboxes, mail users, and mail contacts. Set a value in the range 0 to 1 . This field is only visible if the QER CalculateRiskIndex configuration parameter is set. For more information about risk assessment, see the <i>One Identity Manager Risk Assessment Administration Guide</i> . |

| Property | Description |
|----------|--|
| Category | Categories used by mailboxes, mail users, and mail contacts to inherit groups. Groups can be selectively inherited by mailboxes, mail users, and mail contacts. To do this, the group and mailboxes, mail users, and mail contacts are divided into categories. Select one or more categories from the menu. |

Related topics

- [Specifying moderators for Exchange Online mail-enabled distribution groups](#) on page 138
- [Specifying Exchange Online mail-enabled distribution groups](#) on page 138

Receive restrictions for Exchange Online mail-enabled distribution groups

NOTE: The **Assign mail acceptance** and **Assign mail rejection** assignments are mutually exclusive. You can specify whether to accept or deny the recipient's message.


To modify mail acceptance for mail-enabled distribution groups

1. In the Manager, select the **Azure Active Directory > Mail-enabled distribution groups** category.
2. Select the mail-enabled distribution group in the result list.
3. Select the **Assign mail acceptance** task to specify recipients whose messages are accepted.
- OR -
Select the **Assign mail rejection** task to specify recipients whose messages are rejected.
4. Select the table containing the recipient from the menu at the top of the form. You have the following options:
 - Mail-enabled distribution groups
 - Dynamic distribution groups
 - Mailboxes
 - Mail users
 - Mail contacts
 - Office 365 groups

5. In the **Add assignments** pane, assign recipients.

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

To remove an assignment

- Select the recipient and double-click .

6. Save the changes.

Customizing send permissions for Exchange Online mail-enabled distribution groups


Use the **Send on behalf of** send permission to specify which users can send messages on behalf of the distribution group.

To customize send permissions for mail-enabled distribution groups

1. In the Manager, select the **Azure Active Directory > Mail-enabled distribution groups** category.
2. Select the mail-enabled distribution group in the result list.
3. Select the **Assign send authorizations** task.
4. Select the table which contains the user from the menu at the top of the form. You have the following options:
 - Mail-enabled distribution groups
 - Mailboxes
 - Mail users
5. In the **Add assignments** pane, assign users.

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

To remove an assignment

- Select the user and double-click .

6. Save the changes.

Specifying moderators for Exchange Online mail-enabled distribution groups


Moderated distribution groups let a moderator approve or deny messages sent to a mail-enabled distribution group. Only after a message has been approved by a moderator can it be forwarded to members of the mail-enabled distribution group.

To specify moderators for a mail-enabled distribution group

1. In the Manager, select the **Azure Active Directory > Mail-enabled distribution groups** category.
2. Select the mail-enabled distribution group in the result list.
3. Select the **Assign moderators** task.
4. Select the table which contains the user from the menu at the top of the form. You have the following options:
 - Mailboxes
 - Mail contacts
 - Mail users
5. In the **Add assignments** pane, add the moderators.

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

To remove an assignment

- Select the moderator and double-click .
6. Save the changes.

Specifying Exchange Online mail-enabled distribution groups

Membership in mail-enabled distribution groups can be applied for and approved. Specify which users manage the mail-enabled distribution group and therefore can grant approval for membership in the group.


To specify a mail-enabled distribution group

1. In the Manager, select the **Azure Active Directory > Mail-enabled distribution groups** category.
2. Select the mail-enabled distribution group in the result list.

3. Select the **Assign administrators** task.
4. Select the table which contains the administrators from the menu at the top of the form. You have the following options:
 - Azure Active Directory user accounts
 - Mail-enabled distribution groups
5. In the **Add assignments** pane, assign the administrators.

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

To remove an assignment

- Select the administrator and double-click .
6. Save the changes.

Delete this text and replace it with your own.

Assigning Exchange Online mail-enabled distribution groups to Exchange Online recipients

Exchange Online mail-enabled distribution groups can be assigned directly or indirectly to mailboxes, mail users, and mail contacts.

In the case of indirect assignment, identities and mail-enabled distribution groups are assigned to hierarchical roles, such as departments, cost centers, locations, or business roles. The mail-enabled distribution groups assigned to an identity are calculated from the position in the hierarchy and the direction of inheritance.

- If you add an identity in roles and the identity has a mailbox, the mailbox is added to the mail-enabled distribution groups.
- If you add an identity to roles and that identity has a mail user, the mail user is added to the mail-enabled distribution groups.
- If you add an identity to roles and that identity has a mail contact, the mail contact is added to the mail-enabled distribution groups.

Furthermore, Exchange Online mail-enabled distribution groups can be requested in the Web Portal. To do this, add identities to a shop as customers. All Exchange Online mail-enabled distribution groups that are assigned to this shop as products can be requested by the customers. Requested Exchange Online mail-enabled distribution groups are assigned to the identities after approval is granted.

Through system roles, Exchange Online mail-enabled distribution groups can be grouped together and assigned to identities and workdesks as a package. You can create system roles that contain only Exchange Online mail-enabled distribution groups. You can also group any number of company resources into a system role.

To react quickly to special requests, you can assign Exchange Online mail-enabled distribution groups directly to mailboxes, mail users, and mail contacts.

For more information see the following guides:

| Topic | Guide |
|---|---|
| Basic principles for assigning and inheriting company resources | <i>One Identity Manager Identity Management Base Module Administration Guide</i> <i>One Identity Manager Business Roles Administration Guide</i> |
| Assigning company resources through IT Shop requests | <i>One Identity Manager IT Shop Administration Guide</i> |
| System roles | <i>One Identity Manager System Roles Administration Guide</i> |

Detailed information about this topic

- [Prerequisites for indirect assignment of Exchange Online mail-enabled distribution groups](#) on page 141
- [Assigning Exchange Online mail-enabled distribution groups to departments, cost centers, and locations](#) on page 142
- [Assigning Exchange Online mail-enabled distribution groups to business roles](#) on page 143
- [Adding Exchange Online mail-enabled distribution groups to system roles](#) on page 144
- [Assigning Exchange Online mail-enabled distribution groups to the IT Shop](#) on page 145
- [Assigning Exchange Online recipients to Exchange Online mail-enabled distribution groups](#) on page 149
- [Assigning Exchange Online mail-enabled distribution groups directly to Exchange Online mailboxes](#) on page 150
- [Assigning Exchange Online mail-enabled distribution groups directly to Exchange Online mail users](#) on page 151
- [Assigning Exchange Online mail-enabled distribution groups directly to Exchange Online mail contacts](#) on page 151

Prerequisites for indirect assignment of Exchange Online mail-enabled distribution groups

In the case of indirect assignment, identities and Exchange Online mail-enabled distribution groups are assigned to hierarchical roles, such as departments, cost centers, locations, or business roles. When assigning Exchange Online mail-enabled distribution groups indirectly, check the following settings and modify them if necessary.

1. Assignment of identities and Exchange Online mail-enabled distribution groups is permitted for role classes (departments, cost centers, locations, or business roles).

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

To configure assignments to roles of a role class

1. In the Manager, select role classes in the **Organizations > Basic configuration data > Role classes** category.
- OR -
In the Manager, select role classes in the **Business roles > Basic configuration data > Role classes** category.
2. Select the **Configure role assignments** task and configure the permitted assignments.
 - To generally allow an assignment, enable the **Assignments allowed** column.
 - To allow direct assignment, enable the **Direct assignments permitted** column.
3. Save the changes.
2. Setting for assigning mail-enabled distribution groups to mailboxes.
 - The mailbox is labeled with the **Groups can be inherited** option.
 - The mailbox's Azure Active Directory user account is linked to an identity.
3. Settings for assigning mail-enabled distribution groups to mail users.
 - The mail user is labeled with the **Groups can be inherited** option.
 - The mail user is linked to an identity.
4. Settings for assigning mail-enabled distribution groups to mail contacts.
 - The mail contact is labeled with the **Groups can be inherited** option.
 - The mail contact is linked to an identity.

NOTE: There are other configuration settings that play a role when company resources are inherited through departments, cost centers, locations, and business roles. For example, role inheritance might be blocked or inheritance of identities not allowed. For

more detailed information about the basic principles for assigning company resources, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Related topics

- [General main data for Exchange Online mailboxes](#) on page 94
- [Main data for Exchange Online mail users](#) on page 111
- [Main data for Exchange Online mail contacts](#) on page 122

Assigning Exchange Online mail-enabled distribution groups to departments, cost centers, and locations


Assign mail-enabled distribution groups to departments, cost centers, or locations so that the mail-enabled distribution groups can be assigned to mailboxes, mail users, and mail contacts through these organizations.

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

1. In the Manager, select the **Azure Active Directory > Mail-enabled distribution groups** category.
2. Select the mail-enabled distribution 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 mail-enabled distribution groups to a department, a cost center, or a location (non role-based login or role-based login)

1. In the Manager, select the **Organizations > Departments** category.
- OR -
In the Manager, select the **Organizations > Cost centers** category.


- OR -

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

2. Select the department, cost center or location in the result list.
3. Select the **Assign Exchange Online mail-enabled distribution list** task.
4. In the **Add assignments** pane, assign mail-enabled distribution groups.

TIP: In the **Remove assignments** pane, you can remove assigned mail-enabled distribution groups.

To remove an assignment

- Select the mail-enabled distribution group and double-click .
5. Save the changes.

Related topics

- [Prerequisites for indirect assignment of Exchange Online mail-enabled distribution groups](#) on page 141
- [Assigning Exchange Online mail-enabled distribution groups to business roles](#) on page 143
- [Adding Exchange Online mail-enabled distribution groups to system roles](#) on page 144
- [Assigning Exchange Online mail-enabled distribution groups to the IT Shop](#) on page 145
- [One Identity Manager users for managing Exchange Online](#) on page 11

Assigning Exchange Online mail-enabled distribution groups to business roles

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


Assign the mail-enabled distribution group to business roles so that the mail-enabled distribution group is assigned to user accounts through these business roles.

To assign a mail-enabled distribution group to business roles (non role-based login)

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

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

To remove an assignment

- Select the business role and double-click .


5. Save the changes.

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

1. In the Manager, select the **Business roles > <role class>** category.
2. Select the business role in the result list.
3. Select the **Assign Exchange Online mail-enabled distribution list** task.
4. In the **Add assignments** pane, assign mail-enabled distribution groups.

TIP: In the **Remove assignments** pane, you can remove assigned mail-enabled distribution groups.

To remove an assignment

- Select the mail-enabled distribution group and double-click .

5. Save the changes.

Related topics

- [Prerequisites for indirect assignment of Exchange Online mail-enabled distribution groups on page 141](#)
- [Assigning Exchange Online mail-enabled distribution groups to departments, cost centers, and locations on page 142](#)
- [Adding Exchange Online mail-enabled distribution groups to system roles on page 144](#)
- [Assigning Exchange Online mail-enabled distribution groups to the IT Shop on page 145](#)
- [One Identity Manager users for managing Exchange Online on page 11](#)

Adding Exchange Online mail-enabled distribution groups to system roles

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

Use this task to add a group to system roles. When you assign a system role to an identity, the mail-enabled distribution group are inherited by all mailboxes, mail users, and mail contacts that these identities have.


NOTE: Mail-enabled distribution groups with the **Only use in IT Shop** option 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 mail-enabled distribution group to system roles

1. In the Manager, select the **Azure Active Directory > Mail-enabled distribution groups** category.
2. Select the mail-enabled distribution 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 Exchange Online mail-enabled distribution groups to departments, cost centers, and locations](#) on page 142
- [Assigning Exchange Online mail-enabled distribution groups to business roles](#) on page 143
- [Assigning Exchange Online mail-enabled distribution groups to the IT Shop](#) on page 145

Assigning Exchange Online mail-enabled distribution groups to the IT Shop

Once a mail-enabled distribution group 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 mail-enabled distribution group must be labeled with the **IT Shop** option.
- The mail-enabled distribution group 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 mail-enabled distribution group easier to find in the Web Portal, assign a service category to the service item.

- If you want the mail-enabled distribution group to be assigned to identities only through the IT Shop, the mail-enabled distribution group must also be marked with the **Only use in IT Shop** option. Direct assignment to hierarchical roles or mailboxes, mail users and mail contacts is then no longer permitted.

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

To add a mail-enabled distribution group in the IT Shop

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

- OR -

In the Manager, select the **Entitlements > Exchange Online mail-enabled distribution groups** (role-based login) category.

2. Select the mail-enabled distribution group in the result list.
3. Select **Add to IT Shop**.
4. In the **Add assignments** pane, assign mail-enabled distribution groups to IT Shop shelves.
5. Save the changes.

To add a mail-enabled distribution group to individual IT Shop shelves

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

- OR -

In the Manager, select the **Entitlements > Exchange Online mail-enabled distribution groups** category (role-based login).

2. Select the mail-enabled distribution group in the result list.
3. Select the **Add to IT Shop** task.
4. In the **Remove assignments** pane, removed assigned mail-enabled distribution groups from IT Shop shelves.
5. Save the changes.

To add a mail-enabled distribution group to all the IT Shop shelves

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

- OR -

In the Manager, select the **Entitlements > Exchange Online mail-enabled distribution groups** category (role-based login).

2. Select the mail-enabled distribution group 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 One Identity Manager Service removes the mail-enabled distribution group from all the shelves. All requests and assignment requests with this mail-enabled distribution group are canceled at the same time.

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

Related topics

- [Main data for Exchange Online mail-enabled distribution groups on page 133](#)
- [Adding Exchange Online mail-enabled distribution groups automatically to the IT Shop on page 147](#)
- [Assigning Exchange Online mail-enabled distribution groups to departments, cost centers, and locations on page 142](#)
- [Assigning Exchange Online mail-enabled distribution groups to business roles on page 143](#)
- [Adding Exchange Online mail-enabled distribution groups to system roles on page 144](#)

Adding Exchange Online mail-enabled distribution groups automatically to the IT Shop

The following steps can be used to automatically add mail-enabled distribution groups to the IT Shop. Synchronization ensures that the mail-enabled distribution groups are added to the IT Shop. If necessary, you can manually start synchronization with the Synchronization Editor. Mail-enabled distribution groups created in One Identity Manager also are added automatically to the IT Shop.

To add mail-enabled distribution groups automatically to the IT Shop

1. In the Designer, set the **QER | ITShop | AutoPublish | O3EDL** configuration parameter.
2. In order not to add mail-enabled distribution groups to the IT Shop automatically, in the Designer, set the **QER | ITShop | AutoPublish | O3EDL | ExcludeList** configuration parameter.

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

3. Compile the database.

From this time on, local mail-enabled distribution groups are added to the IT Shop automatically.

The following steps are run to add a local mail-enabled distribution group to the IT Shop automatically.

1. A service item is determined for the mail-enabled distribution group.

The service item is tested for each mail-enabled distribution group and modified if necessary. The name of the service item corresponds to the name of the mail-enabled distribution group.

- The service item is modified if the mail-enabled distribution group has a service item.
- Mail-enabled distribution groups without a service item are allocated a new service item.

2. The service item is assigned to the **Azure Active Directory groups | Exchange Online distribution groups** default service category.

3. An application role for product owners is determined and assigned to the service item.

Product owners can approve requests for membership in these mail-enabled distribution groups. By default, the administrator of a mail-enabled distribution group is determined to be the product owner.

NOTE: The application role for the product owner must be added under the **Request & Fulfillment | IT Shop | Product owner** application role.

- If the administrator of the mail-enabled distribution group is already a member of a product owner application role, then this application role is assigned to the service item. Therefore, all members of this application role become product owners of the mail-enabled distribution group.
- If the account manager of the mail-enabled distribution group is not yet a member of an application role for product owners, a new application role is created. The name of the application corresponds to the name of the owner.
 - If the administrator is a user account, the user account's identity is added to the application role.
 - If it is a group of administrators, the identities of all this group's user accounts are added to the application role.

4. The mail-enabled distribution group is labeled with the **IT Shop** option and assigned to the **IT Shop distribution groups** Exchange Online shelf in the **Identity & Access Lifecycle** shop.

Then the shop customers can use the Web Portal to request memberships in the mail-enabled distribution groups.

NOTE: When a mail-enabled distribution group is irrevocably deleted from the One Identity Manager database, the associated service item is also deleted.

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

Related topics

- [Assigning Exchange Online mail-enabled distribution groups to the IT Shop](#) on page 145
- [Assigning Exchange Online mail-enabled distribution groups to departments, cost centers, and locations](#) on page 142
- [Assigning Exchange Online mail-enabled distribution groups to business roles](#) on page 143
- [Adding Exchange Online mail-enabled distribution groups to system roles](#) on page 144
- [Assigning Exchange Online recipients to Exchange Online mail-enabled distribution groups](#) on page 149
- [Adding Exchange Online dynamic distribution groups to Exchange Online mail-enabled distribution groups](#) on page 153
- [Specifying Exchange Online mail-enabled distribution groups](#) on page 138


Assigning Exchange Online recipients to Exchange Online mail-enabled distribution groups

To react quickly to special requests, you can assign mail-enabled distribution groups directly to mailboxes, mail users, and mail contacts. You cannot directly assign mail-enabled distribution groups that have the **Only use in IT Shop** option set.

To assign mailboxes, mail users, and mail contacts directly to a mail-enabled distribution group

1. In the Manager, select the **Azure Active Directory > Mail-enabled distribution groups** category.
2. Select the mail-enabled distribution group in the result list.
3. Select the **Assign members** task.
4. To assign mailboxes, select the **Mailboxes** tab.
- OR -
To assign mail users, select the **Mail users** tab.
- OR -
To assign mail contacts, select the **Mail contacts** tab.
5. In the **Add assignments** pane, add the mailboxes, mail users, or mail contacts.
TIP: In the **Remove assignments** pane, you can remove mailboxes, mail users, and mail contacts.

To remove an assignment

- Select the mailbox, mail user, or mail contact and double-click .
6. Save the changes.

Related topics

- [Assigning Exchange Online mail-enabled distribution groups directly to Exchange Online mailboxes](#) on page 150
- [Assigning Exchange Online mail-enabled distribution groups directly to Exchange Online mail users](#) on page 151
- [Assigning Exchange Online mail-enabled distribution groups directly to Exchange Online mail contacts](#) on page 151

Assigning Exchange Online mail-enabled distribution groups directly to Exchange Online mailboxes


To react quickly to special requests, you can assign mail-enabled distribution groups directly to mailboxes.

To assign mail-enabled distribution groups to a mailbox

1. In the Manager, select the **Azure Active Directory > Mailboxes** category.
2. Select a mailbox in the result list.
3. Select the **Assign mail-enabled distribution list** task.
4. In the **Add assignments** pane, assign mail-enabled distribution groups.

TIP: In the **Remove assignments** pane, you can remove assigned mail-enabled distribution groups.

To remove an assignment

- Select the mail-enabled distribution group and double-click .
5. Save the changes.

Related topics

- [Assigning Exchange Online recipients to Exchange Online mail-enabled distribution groups](#) on page 149

Assigning Exchange Online mail-enabled distribution groups directly to Exchange Online mail users


To react quickly to special requests, you can assign mail-enabled distribution groups directly to mail users.

To assign mail-enabled distribution groups directly to a mail user

1. In the Manager, select the **Azure Active Directory > Mail user** category.
2. Select the mail user in the result list.
3. Select the **Assign mail-enabled distribution list** task.
4. In the **Add assignments** pane, assign mail-enabled distribution groups.

TIP: In the **Remove assignments** pane, you can remove assigned mail-enabled distribution groups.

To remove an assignment

- Select the mail-enabled distribution group and double-click .
5. Save the changes.

Related topics

- [Assigning Exchange Online recipients to Exchange Online mail-enabled distribution groups](#) on page 149

Assigning Exchange Online mail-enabled distribution groups directly to Exchange Online mail contacts


To react quickly to special requests, you can assign mail-enabled distribution groups directly to mail contacts.

To assign mail-enabled distribution groups directly to a mail contact

1. In the Manager, select the **Azure Active Directory > Mail contacts** category.
2. Select the mail contact in the result list.
3. Select the **Assign mail-enabled distribution list** task.
4. In the **Add assignments** pane, assign mail-enabled distribution groups.

TIP: In the **Remove assignments** pane, you can remove assigned mail-enabled distribution groups.

To remove an assignment

- Select the mail-enabled distribution group and double-click .

5. Save the changes.

Related topics

- [Assigning Exchange Online recipients to Exchange Online mail-enabled distribution groups](#) on page 149

Exchange Online mail-enabled distribution group inheritance based on categories

In Exchange Online, mail-enabled distribution groups can be inherited by mailboxes, mail users, and mail contacts through categories.

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

To use inheritance through categories

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

To edit Azure Active Directory tenant main data

1. In the Manager, select the **Azure Active Directory > Tenants** category.
 2. In the result list, select the Azure Active Directory tenant.
 3. Select the **Change main data** task.
 4. Edit the Azure Active Directory tenant's main data.
 5. Save the changes.
2. In the Manager, assign categories to mailboxes, mail users, and mail contacts through their main data.
 3. In the Manager, assign categories to mail-enabled distribution groups through their main data.

Related topics

- [General main data for Exchange Online mailboxes](#) on page 94
- [Main data for Exchange Online mail users](#) on page 111

- [Main data for Exchange Online mail contacts](#) on page 122
- [Main data for Exchange Online mail-enabled distribution groups](#) on page 133


Adding Exchange Online dynamic distribution groups to Exchange Online mail-enabled distribution groups

To add dynamic distribution groups to a mail-enabled distribution group

1. In the Manager, select the **Azure Active Directory > Mail-enabled distribution groups** category.
2. Select the mail-enabled distribution group in the result list.
3. Select the **Assign mail-enabled distribution list** task.
4. In the **Add assignments** pane, assign mail-enabled distribution groups.

TIP: In the **Remove assignments** pane, you can remove assigned mail-enabled distribution groups.

To remove an assignment

- Select the mail-enabled distribution group and double-click .
5. Save the changes.


Adding an Exchange Online dynamic distribution group to Exchange Online mail-enabled distribution groups

To add dynamic distribution groups to a mail-enabled distribution group

1. In the Manager, select the **Azure Active Directory > Mail-enabled distribution groups** category.
2. Select the mail-enabled distribution group in the result list.
3. Select the **Assign members** task.
4. Select the **Dynamic distribution groups** tab.
5. In the **Add assignments** pane, assign dynamic distribution groups.

TIP: In the **Remove assignments** pane, you can remove assigned dynamic mail-enabled distribution groups.

To remove an assignment

- Select the dynamic mail-enabled distribution group and double-click .
6. Save the changes.

Related topics

- [Adding Exchange Online mail-enabled distribution groups to Exchange Online dynamic distribution groups](#) on page 181


Adding Exchange Online mail-enabled public folder to Exchange Online mail-enabled distribution groups

To add mail-enabled public folders to a mail-enabled distribution group

1. In the Manager, select the **Azure Active Directory > Mail-enabled distribution groups** category.
2. Select the mail-enabled distribution group in the result list.
3. Select the **Assign mail-enabled public folder** task.
4. In the **Add assignments** pane, assign mail-enabled public folders.

TIP: In the **Remove assignments** pane, you can remove assigned mail-enabled public folders.

To remove an assignment

- Select the mail-enabled public folder and click .
5. Save the changes.

Assigning extended properties to Exchange Online mail-enabled distribution groups

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


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

To specify extended properties for mail-enabled distribution groups

1. In the Manager, select the **Azure Active Directory > Mail-enabled distribution groups** category.
2. Select the mail-enabled distribution group in the result list.
3. Select **Assign extended properties**.
4. In the **Add assignments** pane, assign extended properties.

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


To remove an assignment

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

Deleting Exchange Online mail-enabled distribution groups

When you delete a mail-enabled distribution group, the Azure Active Directory group associated with the mail-enabled distribution group is also deleted.

To delete a mail-enabled distribution group

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

Exchange Online Office 365 groups

Office 365 groups are loaded into One Identity Manager by synchronization. You can create and edit Office 365 groups in One Identity Manager. When you create an Office 365 group, an Azure Active Directory group is also created and linked to the Office 365 group.

In One Identity Manager, you can assign Office 365 groups directly to mailboxes, mail users, and mail contacts or they can be inherited through departments, cost centers, locations, or business roles. Users can also request Office 365 groups through the Web Portal. To do this, Office 365 groups are supplied by the IT Shop.


Detailed information about this topic

- [Creating Exchange Online Office 365 groups](#) on page 156
- [Editing main data of Exchange Online Office 365 groups](#) on page 157
- [Exchange Online Office 365 group main data](#) on page 157
- [Customizing receive restrictions for Exchange Online Office 365 groups](#) on page 161
- [Assigning owners to Exchange Online Office 365 groups](#) on page 161
- [Assigning subscribers to Exchange Online Office 365 groups](#) on page 162
- [Assigning Exchange Online Office 365 groups to Azure Active Directory user accounts](#) on page 163
- [Exchange Online Office 365 group inheritance based on categories](#) on page 174
- [Assigning extended properties to Exchange Online Office 365 groups](#) on page 175
- [Deleting Exchange Online Office 365 groups](#) on page 175
- [Synchronizing single objects](#) on page 50

Creating Exchange Online Office 365 groups

When you create an Office 365 group, an Azure Active Directory group is also created and linked to the Office 365 group.

To create a Office 365 group

1. In the Manager, select the **Azure Active Directory > Office 365 groups** category.
2. Click  in the result list.
3. On the main data form, enter the main data for the Office 365 group.
4. Save the changes.

Related topics

- [Editing main data of Exchange Online Office 365 groups](#) on page 157
- [Exchange Online Office 365 group main data](#) on page 157

Editing main data of Exchange Online Office 365 groups

To edit an Office 365 group

1. In the Manager, select the **Azure Active Directory > Office 365 groups** category.
2. Select the Office 365 group in the result list and run the **Change main data** task.
3. Edit the Office 365 group's main data.
4. Save the changes.

Related topics

- [Creating Exchange Online Office 365 groups](#) on page 156
- [Exchange Online Office 365 group main data](#) on page 157

Exchange Online Office 365 group main data

Table 20: Exchange Online group main data

| Property | Description |
|-------------------------------|---|
| Azure Active Directory tenant | The Azure Active Directory tenant's name. |
| Name | Name of the Office 365 group. |

| Property | Description |
|------------------------------|--|
| Display name | Name as used in the address book. |
| Simple display | Simple display name for systems that cannot interpret all the characters of normal display names. |
| Alias | Unique alias for further identification of the Office 365 group. |
| Group type | The type of group. |
| Proxy addresses | Office 365 group's email addresses 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 |
| Yammer email address | Yammer email address. |
| Notes | More information about the Office 365 group. |
| Azure Active Directory group | Azure Active Directory group for which an Office 365 group is created. |
| 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 mailboxes, mail users and mail contacts, and 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 mailboxes, mail users and mail contacts is not permitted. |
| Service item | Service item data for requesting the group through the IT Shop. |
| Risk index | Value for assessing the risk of assigning the group to mailboxes, mail users and mail contacts. Set a value in the range 0 to 1. This field is only visible if the QER CalculateRiskIndex configuration parameter is set. For more information about risk assessment, see the <i>One Identity Manager Risk Assessment Administration Guide</i> . |
| Category | Categories used by mailboxes, mail users and mail contacts to inherit groups. Groups can be selectively inherited by mailboxes, mail users and mail contacts. To do this, the group |

| Property | Description |
|---|--|
| | and mailboxes, mail users and mail contacts are divided into categories. Select one or more categories from the menu. |
| Privacy | Privacy type for Office 365 groups. Options are Private (default) or Public . |
| Language | Language of the Office 365 group. |
| Classification | Office 365 group classification. |
| Do not display in address list | Specifies whether the Office 365 group is visible in address books. Set this option if you want to prevent the Office 365 group from being displayed in address books. This option applies to all address books. |
| Hide group memberships | Specifies whether to hide the members of the Office 365 group from users who are not members of the group. This option can only be enabled for private groups. |
| Hide group in Outlook | Specifies whether the Office 365 group is shown in Outlook. Set this option if you want to prevent the Office 365 group from being displayed in Outlook. The Office 365 groups is also hidden in address books. |
| Exchange version | Specifies the version of Exchange. |
| Mailbox configured | Specifies whether a mailbox is configured for the Office 365 group. |
| Inbox URL | URL of the inbox. |
| Max. send size [KB] | Maximum size of outgoing messages in KB. |
| Sender authentication required | Specifies whether authentication data is requested from senders. Set this option to prevent anonymous senders mailing the Office 365 group. |
| Mailbox provisioning constraint | Additional options for mailbox provisioning. |
| MailTip | Specifies the custom MailTip text for this recipient. |
| MailTip translations | Languages for the custom MailTip text. |
| Welcome message enabled | Specifies whether the welcome message is sent. |
| Migration to Office 365 group in progress | Specifies the migration status. |
| Valid | Specifies whether this Office 365 group is valid. |

| Property | Description |
|---|--|
| Dynamic membership | Specifies whether memberships are dynamic memberships. |
| Allow adding of new guests | Specifies whether new guests can be added to the Office 365 group. |
| External members count | Number of external group members. |
| Allow subscriptions | Specifies whether subscriptions to conversations and calendar events are enabled for the Office 365 group. Use the Assign subscriptions task to assign subscribers. |
| Automatically subscribe new members | Specifies whether to automatically subscribe new members of the Office 365 group to conversations and calendar events. |
| Always subscribe members to calendar events | Specifies whether to subscribe members of the Office 365 group only to group calendar events, and not conversations. |
| External resources published | Specifies whether external resources are published. |
| Connectors enabled | Specifies whether to enable the use of connectors for apps, tools, or services for the Office 365 group. |
| Synchronized with local Active Directory | Specifies whether the group has been synchronized with the local Active Directory and with Exchange Online. |
| File notification settings | Settings for file notification. |
| Identity URL | URL of the identity. |
| Photo URL | Photo URL. |
| SharePoint documents URL | URL of the SharePoint documents. |
| SharePoint notebook URL | URL of the SharePoint notebook. |
| SharePoint site URL | URL of the SharePoint site. |
| Custom attribute 01 - Custom attribute 15 | Additional company-specific information. Use the Designer to customize display names, formats, and templates for the input fields. |
| Attribute extension 01 - attribute extension 15 | Additional company-specific information. Use the Designer to customize display names, formats, and templates for the input fields. |

Related topics

- [Assigning subscribers to Exchange Online Office 365 groups](#) on page 162

Customizing receive restrictions for Exchange Online Office 365 groups


NOTE: The **Assign mail acceptance** and **Assign mail rejection** assignments are mutually exclusive. You can specify whether to accept or deny the recipient's message.

To customize mail acceptance for Office 365 mailboxes groups

1. In the Manager, select the **Azure Active Directory > Office 365 groups** category.
2. Select the Office 365 group in the result list.
3. Select the **Assign mail acceptance** task to specify recipients whose messages are accepted.
- OR -
Select the **Assign mail rejection** task to specify recipients whose messages are rejected.
4. Select the table containing the recipient from the menu at the top of the form. You have the following options:
 - Mail-enabled distribution groups
 - Dynamic distribution groups
 - Mailboxes
 - Mail users
 - Mail contacts
 - Office 365 groups
5. In the **Add assignments** pane, assign recipients.

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

To remove an assignment

- Select the recipient and double-click .
6. Save the changes.

Assigning owners to Exchange Online Office 365 groups

When you assign owners to an Office 365 group, the owners are also added as members to the Office 365 group.


NOTE: Owners cannot be manually assigned to Office 365 groups.

To assign owners to an Office 365 group

1. In the Manager, select the **Azure Active Directory > Office 365 groups** category.
2. Select the Office 365 group in the result list.
3. Select the **Assign owners** task.
4. In the **Add assignments** pane, assign owners.

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

To remove an assignment

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

Related topics

- [Assigning Azure Active Directory user accounts directly to Exchange Online Office 365 groups](#) on page 173

Assigning subscribers to Exchange Online Office 365 groups

You can assign subscribers to Office 365 groups if the **Allow subscriptions** option is set. If you assign subscribers to an Office 365 group, the subscribers are also added as members to the Office 365 group.


NOTE: Subscribers cannot be manually assigned to dynamic Office 365 groups.

To assign subscribers to an Office 365 group

1. In the Manager, select the **Azure Active Directory > Office 365 groups** category.
2. Select the Office 365 group in the result list.
3. Select the **Assign subscribers** task.
4. In the **Add assignments** pane, add subscribers.

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

To remove an assignment

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

Related topics

- [Exchange Online Office 365 group main data on page 157](#)
- [Editing main data of Exchange Online Office 365 groups on page 157](#)
- [Assigning Azure Active Directory user accounts directly to Exchange Online Office 365 groups on page 173](#)

Assigning Exchange Online Office 365 groups to Azure Active Directory user accounts

Office 365 groups can be assigned directly or indirectly to Azure Active Directory user accounts.

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

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

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

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

For more information see the following guides:

| Topic | Guide |
|---|---|
| Basic principles for assigning and inheriting company resources | <i>One Identity Manager Identity Management Base Module Administration Guide</i> <i>One Identity Manager Business Roles Administration Guide</i> |
| Assigning company resources through IT Shop requests | <i>One Identity Manager IT Shop Administration Guide</i> |
| System roles | <i>One Identity Manager System Roles Administration Guide</i> |

Detailed information about this topic

- [Prerequisites for indirect assignment of Office 365 groups to Azure Active Directory user accounts on page 164](#)
- [Assigning Exchange Online Office 365 groups to departments, cost centers, and locations on page 166](#)
- [Assigning Exchange Online Office 365 groups to business roles on page 167](#)
- [Adding Exchange Online Office 365 groups to system roles on page 168](#)
- [Adding Exchange Online Office 365 groups to the IT Shop on page 169](#)
- [Adding Exchange Online Office 365 groups automatically to the IT Shop on page 171](#)
- [Assigning Azure Active Directory user accounts directly to Exchange Online Office 365 groups on page 173](#)
- [Assigning Exchange Online Office 365 groups directly to Azure Active Directory user accounts on page 172](#)

Prerequisites for indirect assignment of Office 365 groups to Azure Active Directory user accounts

In the case of indirect assignment, identities and Office 365 groups are assigned to hierarchical roles, such as departments, cost centers, locations, or business roles. When assigning Office 365 groups indirectly, check the following settings and modify them if necessary.

1. Assignment of identities and Exchange Online Office 365 groups is permitted for role classes (departments, cost centers, locations, or business roles).

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

To configure assignments to roles of a role class

1. In the Manager, select role classes in the **Organizations > Basic configuration data > Role classes** category.
- OR -
In the Manager, select role classes in the **Business roles > Basic configuration data > Role classes** category.
2. Select the **Configure role assignments** task and configure the permitted assignments.

- To generally allow an assignment, enable the **Assignments allowed** column.
 - To allow direct assignment, enable the **Direct assignments permitted** column.
3. Save the changes.
 2. Settings for assigning Office 365 groups to Azure Active Directory user accounts.
 - The Azure Active Directory user account is linked to an identity.
 - The Azure Active Directory user account has the **Office 365 groups can be inherited** option set.

The option specifies whether the Azure Active Directory user account can inherit Office 365 groups through the linked identity. If the option is set, the user account inherits Office 365 groups through hierarchical roles, in which the identity is a member, or through IT Shop requests.

- If you add an identity with a user account to a department, for example, and you have assigned Office 365 groups to this department, the Azure Active Directory user account inherits these Office 365 groups.
- If an identity has requested group membership in the IT Shop and the request is granted approval, the identity's Azure Active Directory user account only inherits the Office 365 group if the option is set.

To edit main data of a user account

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

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

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

Assigning Exchange Online Office 365 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 > Office 365 groups** category.
2. Select the group in the result list.
3. Select the **Assign organizations** task.
4. In the **Add assignments** pane, assign the organizations:
 - On the **Departments** tab, assign departments.
 - On the **Locations** tab, assign locations.
 - On the **Cost centers** tab, assign cost centers.

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

To remove an assignment


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

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

1. In the Manager, select the **Organizations > Departments** category.
- OR -
In the Manager, select the **Organizations > Cost centers** category.
- OR -
In the Manager, select the **Organizations > Locations** category.
2. Select the department, cost center, or location in the result list.
3. Select the **Assign Office 365 groups** task.
4. In the **Add assignments** pane, assign groups.

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

To remove an assignment

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

Related topics

- [Prerequisites for indirect assignment of Office 365 groups to Azure Active Directory user accounts](#) on page 164
- [Assigning Exchange Online Office 365 groups to business roles](#) on page 167
- [Adding Exchange Online Office 365 groups to system roles](#) on page 168
- [Adding Exchange Online Office 365 groups to the IT Shop](#) on page 169
- [One Identity Manager users for managing Exchange Online](#) on page 11

Assigning Exchange Online Office 365 groups to business roles

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


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

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

1. In the Manager, select the **Azure Active Directory > Office 365 groups** category.
2. Select the group in the result list.
3. Select the **Assign business roles** task.
4. In the **Add assignments** pane, select the role class and assign business roles.

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

To remove an assignment


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

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

1. In the Manager, select the **Business roles > <role class>** category.
2. Select the business role in the result list.
3. Select the **Assign Office 365 groups** task.
4. In the **Add assignments** pane, assign the groups.

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

To remove an assignment

- Select the group and double-click .

5. Save the changes.

Related topics

- [Prerequisites for indirect assignment of Office 365 groups to Azure Active Directory user accounts on page 164](#)
- [Assigning Exchange Online Office 365 groups to departments, cost centers, and locations on page 166](#)
- [Adding Exchange Online Office 365 groups to system roles on page 168](#)
- [Adding Exchange Online Office 365 groups to the IT Shop on page 169](#)
- [One Identity Manager users for managing Exchange Online on page 11](#)

Adding Exchange Online Office 365 groups to system roles

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

Use this task to add a group to system roles.

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

This task is not available for dynamic groups.

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

To assign a group to system roles

1. In the Manager, select the **Azure Active Directory > Office 365 groups** category.
2. Select the group in the result list.
3. Select the **Assign system roles** task.
4. In the **Add assignments** pane, assign system roles.

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

To remove an assignment

- Select the system role and double-click ✓.

5. Save the changes.

Related topics

- [Prerequisites for indirect assignment of Office 365 groups to Azure Active Directory user accounts](#) on page 164
- [Assigning Exchange Online Office 365 groups to departments, cost centers, and locations](#) on page 166
- [Assigning Exchange Online Office 365 groups to business roles](#) on page 167
- [Adding Exchange Online Office 365 groups to the IT Shop](#) on page 169

Adding Exchange Online Office 365 groups to the IT Shop

When an Office 365 group is assigned to an IT Shop shelf, the Office 365 group can be requested by the customers of the shop. To ensure it can be requested, further prerequisites need to be guaranteed.

- The group is not a dynamic group.
- The Office 365 group must be labeled with the **IT Shop** option.
- The Office 365 group 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 Web Portal group easier to find in the Office 365, assign a service category to the service item.

- If you want the Office 365 group to be assigned only to identities through the IT Shop, the Office 365 group must also be marked with the **Only use in IT Shop** option. Direct assignment to hierarchical roles or Active Directory user accounts is then no longer permitted.

NOTE: IT Shop administrators can assign Office 365 groups to the IT Shop shelves if login is role-based. Target system administrators are not authorized to add Office 365 groups in the IT Shop.

To add a Office 365 group to the IT Shop

1. In the Manager, select the **Azure Active Directory > Office 365 groups** (non role-based login) category.

- OR -

In the Manager, select the **Entitlements > Office 365 groups** (role-based login) category.

2. Select the Office 365 group in the result list.
3. Select **Add to IT Shop**.
4. In the **Add assignments** pane, assign the Office 365 group to the IT Shop shelves.
5. Save the changes.

To remove an Office 365 group from individual IT Shop shelves

1. In the Manager, select the **Azure Active Directory > Office 365 groups** (non role-based login) category.
- OR -
In the Manager, select the **Entitlements > Office 365 groups** (role-based login) category.
2. Select the Office 365 group in the result list.
3. Select **Add to IT Shop**.
4. In the **Remove assignments** pane, remove the Office 365 group from the IT Shop shelves.
5. Save the changes.

To remove an Office 365 group from all IT Shop shelves

1. In the Manager, select the **Azure Active Directory > Office 365 groups** (non role-based login) category.
- OR -
In the Manager, select the **Entitlements > Office 365 groups** (role-based login) category.
2. Select the Office 365 group 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 Office 365 group is removed from all shelves by the One Identity Manager Service. All requests and assignment requests with this Office 365 group are canceled in the process.

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

Related topics

- [Exchange Online Office 365 group main data](#) on page 157
- [Prerequisites for indirect assignment of Office 365 groups to Azure Active Directory user accounts](#) on page 164
- [Adding Exchange Online Office 365 groups automatically to the IT Shop](#) on page 171

- [Assigning Exchange Online Office 365 groups to departments, cost centers, and locations](#) on page 166
- [Assigning Exchange Online Office 365 groups to business roles](#) on page 167
- [Adding Exchange Online Office 365 groups to system roles](#) on page 168

Adding Exchange Online Office 365 groups automatically to the IT Shop

The following steps can be used to automatically add Exchange Online Office 365 teams to the IT Shop. Synchronization ensures that the Office 365 groups are added to the IT Shop. If necessary, you can manually start synchronization with the Synchronization Editor. New Office 365 groups created in One Identity Manager also are added automatically to the IT Shop.

To add Office 365 groups automatically to the IT Shop

1. In the Designer, set the **QER | ITShop | AutoPublish | O3EUnifiedGroup** configuration parameter.
2. In order not to add Office 365 groups to the IT Shop automatically, in the Designer, set the **QER | ITShop | AutoPublish | O3EUnifiedGroup | ExcludeList** configuration parameter.

This configuration parameter contains a listing of all Office 365 groups that should not be allocated to the IT Shop automatically. You can extend this list if required. To do this, enter the name of the groups in the configuration parameter. Names are listed in a pipe (|) delimited list. Regular expressions are supported.

3. Compile the database.

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

The following steps are run to add a Office 365 group to the IT Shop.

1. A service item is determined for the Office 365 group.
The service item is tested for each Office 365 group and modified if necessary. The name of the service item corresponds to the name of the Office 365 group.
 - The service item is modified for Office 365 groups with service items.
 - Office 365 groups without service items are allocated new service items.
2. The service item is assigned to the **Azure Active Directory groups | Office 365 groups** default service category.
3. An application role for product owners is determined and assigned to the service item.

Product owners can approve requests for membership in these Office 365 groups. The default product owner is the Office 365 group's owner.

NOTE: The application role for the product owner must be added under the **Request & Fulfillment | IT Shop | Product owner** application role.

- If the owner of the Office 365 group is already a member of an application role for product owners, this application role is assigned to the service item. Therefore, all members of this application role become product owners of the Azure Active Directory group.
 - If the owner of the Office 365 group is not yet a member of an application role for product owners, a new application role is created. The name of the application corresponds to the name of the owner.
 - If the owner is a user account, the user account's identity is added to the application role.
 - If it is a group of owners, the identities of all this group's user accounts are added to the application role.
4. The Office 365 group is labeled with the **IT Shop** option and assigned to the **Office 365 groups** IT Shop shelf in the **Identity & Access Lifecycle** shop.

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

NOTE: If an Office 365 group is irrevocably deleted from the One Identity Manager database, the associated service item is also deleted.

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

Related topics

- [Adding Exchange Online Office 365 groups to the IT Shop on page 169](#)
- [Assigning Exchange Online Office 365 groups to departments, cost centers, and locations on page 166](#)
- [Assigning Exchange Online Office 365 groups to business roles on page 167](#)
- [Adding Exchange Online Office 365 groups to system roles on page 168](#)
- [Assigning Azure Active Directory user accounts directly to Exchange Online Office 365 groups on page 173](#)

Assigning Exchange Online Office 365 groups directly to Azure Active Directory user accounts


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

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 Office 365 groups** task.
4. In the **Add assignments** pane, assign the groups.

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

To remove an assignment

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

Related topics

- [Assigning Azure Active Directory user accounts directly to Exchange Online Office 365 groups](#) on page 173

Assigning Azure Active Directory user accounts directly to Exchange Online Office 365 groups

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

If you assign owners and subscribers to an Office 365 group, the user accounts are also added as members to the Office 365 group.


NOTE: User accounts cannot be manually added to dynamic Office 365 groups.

To assign user accounts directly to a group

1. In the Manager, select the **Azure Active Directory > Office 365 groups** category.
2. Select the Office 365 group in the result list.
3. Select the **Assign members** task.
4. In the **Add assignments** pane, assign the user accounts.

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

To remove an assignment

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

Related topics

- [Assigning Exchange Online Office 365 groups directly to Azure Active Directory user accounts](#) on page 172
- [Assigning owners to Exchange Online Office 365 groups](#) on page 161
- [Assigning subscribers to Exchange Online Office 365 groups](#) on page 162

Exchange Online Office 365 group inheritance based on categories

In Exchange Online, Office 365 groups can be inherited by Azure Active Directory user accounts through categories.

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

To use inheritance through categories

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

To edit Azure Active Directory tenant main data

1. In the Manager, select the **Azure Active Directory > Tenants** category.
 2. In the result list, select the Azure Active Directory tenant.
 3. Select the **Change main data** task.
 4. Edit the Azure Active Directory tenant's main data.
 5. Save the changes.
2. In the Manager, assign categories to Azure Active Directory user accounts through their main data.

To edit main data of a user account

1. In the Manager, select the **Azure Active Directory > User accounts** category.
 2. Select the user account in the result list.
 3. Select the **Change main data** task.
 4. Edit the user account's resource data.
 5. Save the changes.
3. In the Manager, assign categories to Office 365 groups through their main data.

Related topics

- [Exchange Online Office 365 group main data](#) on page 157

Assigning extended properties to Exchange Online Office 365 groups

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


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

To specify extended properties for an Office 365 group

1. In the Manager, select the **Azure Active Directory > Office 365 groups** category.
2. Select the Office 365 group in the result list.
3. Select **Assign extended properties**.
4. In the **Add assignments** pane, assign extended properties.

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


To remove an assignment

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

Deleting Exchange Online Office 365 groups

When you delete an Office 365 group, the Azure Active Directory group associated with the Office 365 group is also deleted.

To delete an Office 365 group

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

Exchange Online dynamic distribution groups

The members of a dynamic distribution group are not fixed but are determined using a filter criteria. Dynamic distribution groups are loaded into One Identity Manager through synchronization and can only be edited to a limited extent in One Identity Manager. You cannot create new dynamic distribution groups in One Identity Manager.

Detailed information about this topic

- [Editing main data of Exchange Online dynamic distribution groups](#) on page 176
- [Main data for Exchange Online dynamic distribution groups](#) on page 177
- [Customizing receive restrictions for Exchange Online dynamic distribution groups](#) on page 179
- [Customizing send permissions for Exchange Online dynamic distribution groups](#) on page 180
- [Specifying moderators for Exchange Online dynamic distribution groups](#) on page 180
- [Adding Exchange Online mail-enabled distribution groups to Exchange Online dynamic distribution groups](#) on page 181
- [Deleting Exchange Online dynamic distribution groups](#) on page 182
- [Synchronizing single objects](#) on page 50

Editing main data of Exchange Online dynamic distribution groups

To edit the main data of a dynamic distribution group

1. In the Manager, select the **Azure Active Directory > Tenants > <Azure Active Directory tenant> > Exchange Online administration > Recipient configuration > Dynamic distribution groups** category.

2. Select the dynamic distribution group in the result list and run the **Change main data** task.
3. Edit the dynamic distribution group's main data.
4. Save the changes.


Related topics

- [Main data for Exchange Online dynamic distribution groups](#) on page 177

Main data for Exchange Online dynamic distribution groups

Table 21: Dynamic distribution list main data

| Property | Description |
|--------------------------------|--|
| Azure Active Directory tenant | The Azure Active Directory tenant's name. |
| Identifier | Unique name of the dynamic distribution group. |
| Name | Name of the dynamic distribution group. |
| Alias | Unique alias for further identification of the dynamic distribution group. |
| Display name | Name as used in the address book. |
| Simple display | Simple display name for systems that cannot interpret all the characters of normal display names. |
| Phonetic display name | Display name in phonetic letters. It is used if the pronunciation and spelling of the name do not match. |
| Proxy addresses | Other email addresses for the dynamic distribution group. |
| Email address | Email addresses of the dynamic distribution group. |
| Do not display in address list | Specifies whether the dynamic distribution group is visible in address books. Set this option if you want to prevent the dynamic distribution group from being displayed in address books. This option applies to all address books. |
| Recipient container | Recipient's root container. The condition for finding distribution group members is applied to the selected recipient container and its sub containers. |
| Recipient filter type | Type filter for the recipient. |
| Included recipients | Prescanned filter forms the basis of the recipient type. |

| Property | Description |
|--|--|
| | Permitted values are AllRecipient , Resources , MailUsers , MailboxUsers , MailContacts , and MailGroups . You can combine several recipient type in a comma delimited list. |
| Recipient filter | Condition with extra filter criteria, which is used to determine the members of the dynamic distribution group |
| Filter rules | Filter rules for finding members in the dynamic distribution group. |
| Administrator | Administrator for the dynamic distribution group. To specify an administrator <ol style="list-style-type: none"> 1. Click  next to the field. 2. In the Table menu, select the table that maps the account manager. 3. Under Administrators, select the administrators. 4. Click OK. |
| Notes | Additional information about the dynamic distribution group. |
| Report to sender | Specifies whether the delivery reports are sent to the message sender. |
| Report to owner | Specifies whether the delivery reports are sent to the message owner. |
| Moderation enabled | Specifies whether the mail user is moderated. Use the Assign moderators task to specify the moderators. Then enable the option. |
| Sending message | Specifies how senders are notified when they send messages to moderated dynamic distribution groups. Permitted values are: <ul style="list-style-type: none"> • Do not notify: The sender is not notified. • Only notify senders in your exchange organization: Only internal senders receive a notification. • Notify all senders: Internal and external senders receive notification. |
| Out-of-office message to sender | Specifies whether the message sender should receive out-of-office messages. |
| Only limit messages from authenticated users | Specifies whether authentication data is requested from senders. |

Related topics

- [Specifying moderators for Exchange Online dynamic distribution groups](#) on page 180

Customizing receive restrictions for Exchange Online dynamic distribution groups

NOTE: The **Assign mail acceptance** and **Assign mail rejection** assignments are mutually exclusive. You can specify whether to accept or deny the recipient's message.

To modify mail acceptance for dynamic distribution groups

1. In the Manager, select the **Azure Active Directory > Tenants > <Azure Active Directory tenant> > Exchange Online administration > Recipient configuration > Dynamic distribution groups** category.
2. Select the dynamic distribution list in the result list.
3. Select the **Assign mail acceptance** task to specify recipients whose messages are accepted.

- OR -


Select the **Assign mail rejection** task to specify recipients whose messages are rejected.

4. Select the table containing the recipient from the menu at the top of the form. You have the following options:
 - Mail-enabled distribution groups
 - Dynamic distribution groups
 - Mailboxes
 - Mail users
 - Mail contacts
 - Office 365 groups

5. In the **Add assignments** pane, assign recipients.

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

To remove an assignment

- Select the recipient and double-click .
6. Save the changes.

Customizing send permissions for Exchange Online dynamic distribution groups


Use the **Send on behalf of** send permission to specify which users can send messages on behalf of the distribution group.

To modify the send permission for dynamic distribution groups

1. In the Manager, select the **Azure Active Directory > Tenants > <Azure Active Directory tenant> > Exchange Online administration > Recipient configuration > Dynamic distribution groups** category.
2. Select the dynamic distribution list in the result list.
3. Select the **Assign send authorizations** task.
4. Select the table which contains the user from the menu at the top of the form. You have the following options:
 - Mail-enabled distribution groups
 - Mailboxes
 - Mail users
5. In the **Add assignments** pane, assign users.

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

To remove an assignment

- Select the user and double-click .
6. Save the changes.

Specifying moderators for Exchange Online dynamic distribution groups

Moderated distribution groups let a moderator approve or deny messages sent to a dynamic distribution group. Only after a message has been approved by a moderator can it be forwarded to members of the dynamic distribution group.


To specify moderators for a dynamic distribution group

1. In the Manager, select the **Azure Active Directory > Dynamic distribution groups** category.
2. Select the dynamic distribution list in the result list.
3. Select the **Assign moderators** task.
4. Select the table which contains the user from the menu at the top of the form. You have the following options:
 - Mailboxes
 - Mail contacts
 - Mail users

5. In the **Add assignments** pane, add the moderators.

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

To remove an assignment

- Select the moderator and double-click .
6. Save the changes.


Adding Exchange Online mail-enabled distribution groups to Exchange Online dynamic distribution groups

To add a dynamic distribution groups to mail-enabled distribution groups

1. In the Manager, select the **Azure Active Directory > Tenants > <Azure Active Directory tenant> > Exchange Online administration > Recipient configuration > Dynamic distribution groups** category.
2. Select the dynamic distribution list in the result list.
3. Select the **Assign mail-enabled distribution list** task.
4. In the **Add assignments** pane, assign mail-enabled distribution groups.

TIP: In the **Remove assignments** pane, you can remove assigned mail-enabled distribution groups.

To remove an assignment

- Select the mail-enabled distribution group and double-click .
5. Save the changes.


Related topics

- [Adding an Exchange Online dynamic distribution group to Exchange Online mail-enabled distribution groups](#) on page 153

Deleting Exchange Online dynamic distribution groups

The dynamic distribution group is permanently removed from the One Identity Manager database and Exchange Online system.

To delete a dynamic distribution group

1. In the Manager, select the **Azure Active Directory > Tenants > <Azure Active Directory tenant> > Exchange Online administration > Recipient configuration > Dynamic distribution groups** category.
2. Select the dynamic distribution list in the result list.
3. Click  in the result list.
4. Confirm the security prompt with **Yes**.

Exchange Online mail-enabled public folders

Public folders are used to allow identities shared access to information. Public folders can be structured hierarchically and are connected with a public folder database. Mail-enabling a public folder allows users to send emails to it.

Mail-enabled public folders are loaded into the One Identity Manager database by synchronization and cannot be edited in One Identity Manager.

Detailed information about this topic

- [Displaying information about Exchange Online mail-enabled public folders](#) on page 183
- [Assigning Exchange Online mail-enabled distribution groups to Exchange Online mail-enabled public folders](#) on page 184
- [Exchange Online public folders](#) on page 89
- [Synchronizing single objects](#) on page 50

Displaying information about Exchange Online mail-enabled public folders

To display information about mail-enabled public folders

1. In the Manager, select the **Azure Active Directory > Tenants > <Azure Active Directory tenant> > Exchange Online administration > Recipient configuration > Mail-enabled public folders** category.
2. Select the mail-enabled distribution group in the result list.
3. Select one of the following tasks:

- **Exchange Online public folder overview:** This shows you an overview of the mail-enabled public folder and its dependencies.
- **Change main data:** Shows the mail-enabled public folder's main data.
- **Assign mail acceptance:** Shows which recipients can accept messages.
- **Assign mail rejection:** Shows which recipients can reject messages.
- **Assign send permissions:** Shows who can send messages on behalf of the mail enabled public folder.
- **Assign moderators:** Shows who can accept or reject messages send to a moderated mail-enabled public folder.
- **Assign mail-enabled distribution groups:** Shows which mail-enabled distribution groups are assigned. You can assign more mail-enabled distribution group or remove them.

Related topics

- [Assigning Exchange Online mail-enabled distribution groups to Exchange Online mail-enabled public folders](#) on page 184
- [Exchange Online public folders](#) on page 89
- [Synchronizing single objects](#) on page 50


Assigning Exchange Online mail-enabled distribution groups to Exchange Online mail-enabled public folders

To assign mail-enabled distribution groups to a mail-enabled public folder

1. In the Manager, select the **Azure Active Directory > Tenants > <Azure Active Directory tenant> > Exchange Online administration > Recipient configuration > Mail-enabled public folders** category.
2. Select the mail-enabled distribution group in the result list.
3. Select the **Assign mail-enabled distribution list** task.
4. In the **Add assignments** pane, assign mail-enabled distribution groups.

TIP: In the **Remove assignments** pane, you can remove assigned mail-enabled distribution groups.

To remove an assignment

- Select the mail-enabled distribution group and double-click .
5. Save the changes.

Related topics

- [Adding Exchange Online mail-enabled public folder to Exchange Online mail-enabled distribution groups](#) on page 154

Reports about Exchange Online 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 Exchange Online.

NOTE: Other sections may be available depending on the which modules are installed.

Table 22: Data quality target system report

| Report | Published for | Description |
|---------------------------------|---|--|
| Show overview | Mailbox Mail users Mail contact | This report shows an overview of the user account and the assigned permissions. |
| Show overview including origin | Mailbox Mail users Mail contact | This report shows an overview of the user account and origin of the assigned permissions. |
| Show overview including history | Mailbox Mail user Mail contact | This report shows an overview of the user accounts including its history. Select the end date for displaying the history (Min. date). Older changes and assignments that were removed before this date, are not shown in the report. |
| Overview of all assignments | Mail-enabled distribution group Office 365 group | This report finds all roles containing identities who have the selected system entitlement. |
| Show overview | Mail-enabled distribution group | This report shows an overview of the system entitlement and its assignments. |

| Report | Published for | Description |
|---------------------------------|---|---|
| | Office 365 group | |
| Show overview including origin | Mail-enabled distribution group Office 365 group | This report shows an overview of the system entitlement and origin of the assigned user accounts. |
| Show overview including history | Mail-enabled distribution group Office 365 group | This report shows an overview of the system entitlement and including its history. Select the end date for displaying the history (Min. date). Older changes and assignments that were removed before this date, are not shown in the report. |

Configuration parameters for managing an Exchange Online environment

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

Table 23: Configuration parameters for managing an Exchange Online environment

| Configuration parameters | Meaning |
|--|--|
| TargetSystem AzureAD ExchangeOnline | <p>Preprocessor relevant configuration parameter for controlling database model components for Exchange Online target system administration. If the parameter is set, the target system components are available. Changes to this parameter require the database to be recompiled.</p> <p>If you disable the configuration parameter at a later date, model components and scripts that are no longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the <i>One Identity Manager Configuration Guide</i>.</p> |
| TargetSystem AzureAD ExchangeOnline Accounts | Allows configuration of recipient data. |
| TargetSystem AzureAD ExchangeOnline Accounts MailTemplateDefaultValues | Mail template used to send notifications about whether default IT operating data mapping values are used for automatically creating a user account. The Identity - new user account with default properties created mail template is used. |
| TargetSystem AzureAD | Default email address of the recipient for notifications |

| Configuration parameters | Meaning |
|---|---|
| ExchangeOnline DefaultAddress | about actions in the target system. |
| TargetSystem AzureAD ExchangeOnline MaxFullsyncDuration | Maximum runtime of a synchronization in minutes. No recalculation of group memberships by the DBQueue Processor can take place during this time. If the maximum runtime is exceeded, group membership are recalculated. |
| QER ITShop AutoPublish O3EDL | <p>Preprocessor relevant configuration parameter for automatically adding Exchange Online mail-enabled distribution groups to the IT Shop. If the parameter is set, all distribution groups are automatically assigned as products to the IT Shop. Changes to this parameter require the database to be recompiled.</p> <p>If you disable the configuration parameter at a later date, model components and scripts that are no longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the <i>One Identity Manager Configuration Guide</i>.</p> |
| QER ITShop AutoPublish O3EDL ExcludeList | <p>List of all Exchange Online mail-enabled distribution groups that must not to be automatically assigned to the IT Shop. Each entry is part of a regular search pattern and supports regular expression notation.</p> <p>Example:</p> <pre>.*Administrator.* Exchange.* .*Admins . *Operators II_S_IUSRS</pre> |
| QER ITShop AutoPublish O3EUnifiedGroup | <p>Preprocessor relevant configuration parameter for automatically adding Office 365 groups to the IT Shop. If the parameter is set, all groups are automatically assigned as products to the IT Shop. Changes to this parameter require the database to be recompiled.</p> <p>If you disable the configuration parameter at a later date, model components and scripts that are no longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the <i>One Identity Manager Configuration Guide</i>.</p> |
| QER ITShop AutoPublish | List of all Office 365 groups that must not be automatically |

Configuration parameters

Meaning

| O3EUnifiedGroup |
ExcludeList

assigned to the IT Shop. Each entry is part of a regular search pattern and supports regular expression notation.

Default project template for Exchange Online

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

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

The project template uses mappings for the following schema types.

Table 24: Exchange Online schema type mapping

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

Editing Exchange Online system objects

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

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

Table 25: Methods available for editing schema types

| Type | Read | Add | Delete | Refresh |
|---|------|-----|--------|---------|
| Public folder (PublicFolder) | Yes | No | No | No |
| Mail-enabled public folder (MailPublicFolder) | Yes | No | No | No |
| Policy for role assignment (RoleAssignmentPolicy) | Yes | No | No | No |
| Mailbox policy for mobile devices (MobileDeviceMailboxPolicy) | Yes | No | No | No |
| Sharing policy (SharingPolicy) | Yes | No | No | No |
| Retention policy (RetentionPolicy) | Yes | No | No | No |
| Outlook Web App mailbox policy (OWAMailboxPolicy) | Yes | No | No | No |
| Mail user (MailUser) | Yes | Yes | Yes | Yes |
| Mail contact (MailContact) | Yes | Yes | Yes | Yes |
| Mailbox: resource mailbox (Mailbox) | Yes | Yes | Yes | Yes |
| Mailbox: shared mailbox (Mailbox) | Yes | Yes | Yes | Yes |
| Mailbox: user mailbox (Mailbox) | Yes | No | No | Yes |
| Mailbox: calendar settings (Mailbox) | Yes | Yes | Yes | Yes |

| Type | Read | Add | Delete | Refresh |
|---|-------------|------------|---------------|----------------|
| Mailbox: statistics (Mailboxstatistics) | Yes | Yes | Yes | Yes |
| Mail-enabled distribution mailbox (DistributionGroup) | Yes | Yes | Yes | Yes |
| Dynamic distribution group (DynamicDistributionGroup) | Yes | No | Yes | Yes |
| Office 365 group (UnifiedGroup) | Yes | Yes | Yes | Yes |

Exchange Online connector settings

The following settings are configured for the system connection with the Exchange Online connector.

Table 26: Exchange Online connector settings

| Setting | Meaning |
|--|--|
| User name | Fully qualified name (FQDN) of the user account and password for logging in to Exchange Online. Example: <user>@<domain.com> sync.user@<yourorganization>.onmicrosoft.com Variable: CP_Username |
| Password | The user account's password. Variable: CP_Password |
| Environment | Internal name of the cloud deployment. Default value: 0365Default Variable: CP_ExchangeEnvironmentName |
| Organization name | Azure Active Directory name of the domain for logging in to Azure Active Directory. Example: <yourorganization>.onmicrosoft.com Variable: CP_Organization |
| Use local server time for the revision | Revision filtering data If the value is True , the local server time of the server is used for revision filtering. (default) This makes it unnecessary to load target system object for determining the revision. If the value is false , the change time stamp of the underlying Azure Active Directory objects are used for revision filtering. |

| Setting | Meaning |
|--|--|
| | Variable: CP_UseLocalServerTimeAsRevision |
| Max. time difference (local/remote) in minutes | <p>Revision filtering data</p> <p>Defines the maximum time difference in minutes between the synchronization server and the Exchange Online server. The default value is 60 minutes. If the time difference is more than 60 minutes, alter the value.</p> <p>Variable: CP_LocalServerRevisionMaxDifferenceInMinutes</p> |
| Max. concurrent connections | <p>Maximum number of connections that can be used concurrently. The value must be between 1 and 20.</p> <p>Default value: 2</p> <p>Variable: CP_ConnectionPoolSize</p> |
| Definition of PowerShell commands | <p>You can use this setting to adjust the definition used by the connector in order to convert inputs and outputs between the Exchange Online Cmdlets and the schema of the Synchronization Engine.</p> <p>IMPORTANT: You should only make changes to the connector definition with the help of support desk staff. Changes to this setting will have wide ranging effects on synchronization and must be made carefully.</p> |
| Application ID | Application ID created when the application is registered for Exchange Online PowerShell in the Azure Active Directory tenant. |
| Certificate thumbprint | Self-signed certificate thumbprint. |

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

A

- account definition 59
 - add to IT Shop 74
 - assign automatically 72
 - assign to all identities 72
 - assign to Azure Active Directory tenant 76
 - assign to business role 71
 - assign to cost center 71
 - assign to department 71
 - assign to identities 69, 73
 - assign to location 71
 - assign to system roles 73
 - create 60
 - delete 77
 - edit 61
 - IT operating data 66-67
 - manage level 63-64
- architecture overview 10
- Azure Active Directory tenant
 - account definition mail contact (initial) 76
 - account definition mail user (initial) 76
 - account definition mailbox (initial) 76
- Azure Active Directory user account
 - assign Office 365 group 172-173
 - can inherit Exchange Online group 164
 - category 174

B

- base object 36, 45

C

- calculation schedule 47
 - deactivate 48
- configuration parameter 188
- convert connection parameter 36

D

- direction of synchronization
 - direction target system 25, 35
 - in the Manager 25
- dynamic distribution group 176
 - add mail-enabled distribution groups 181
 - addressing 177
 - alias 177
 - assign mail-enabled distribution group 153
 - condition 177
 - display name 177
 - edit 176
 - expansion server 177
 - identifier 177
 - limit 177
 - mail acceptance 179
 - moderator 180
 - receive restriction 179

- recipient type 177
- send on behalf of 180

E

- Exchange Online
 - advanced settings 38
- Exchange Online connector 10
- Exchange Online mailbox 91, 93
- Exchange Online organization
 - application roles 11
 - target system manager 11, 79
- Exchange Online structure 87
 - hierarchical address book 88
 - public folder 89
 - sharing policy 89

I

- IT operating data
 - change 69
- IT Shop shelf
 - assign account definition 74

J

- Job server 81
 - edit 19
 - load balancing 46

L

- load balancing 46

M

- mail contact 120
 - account definition 76, 122

- addressing 122
- alias 122
- assign mail-enabled distribution group 149, 151
- category 152
- create 121
- delete 129
- destination address 122
- display name 122
- extended property 129
- identity 122
- mail acceptance 127
- manage level 122
- moderator 128
- receive restriction 127
- restore 129
- send on behalf of 128

- mail user 109
 - account definition 76, 111
 - Active Directory user account 111
 - addressing 111
 - alias 111
 - assign mail-enabled distribution group 149, 151
 - category 152
 - create 110
 - delete 119
 - destination address 111
 - display name 111
 - edit 110
 - extended property 118
 - identity 111
 - mail acceptance 116
 - manage level 111
 - moderator 118
 - receive restriction 116

- restore 119
- send on behalf of 117
- mailbox
 - addressing 94
 - alias 94
 - alternative recipient 94
 - archive size 98
 - assign mail-enabled distribution group 149-150
 - Azure Active Directory user account 94
 - book 100
 - Calendar Attendant 100
 - calendar setting 100
 - category 152
 - connected mailbox 94
 - create 92
 - deactivate 94
 - delete 108
 - discovery mailbox 91
 - display name 94
 - edit 93
 - equipment mailbox 91, 100
 - extended property 107
 - folder policy 94
 - functions 98
 - identity 94
 - limit 96
 - linked mailbox 91
 - mail acceptance 103
 - mailbox database 94
 - mailbox type 91, 94
 - mailbox usage 96
 - meeting request 103
 - moderator 107
 - Outlook Web App mailbox policy 94
 - personal archive 98
 - policies 98
 - receive restriction 103
 - Resource Attendant 100
 - resource mailbox 91, 100
 - restore 108
 - role assignment policy 94
 - room mailbox 91, 100
 - send on behalf of 104
 - shared mailbox 91
 - sharing policy 89, 94
 - size 96
 - user mailbox 91
- mailbox permissions
 - full access 106
 - send as 105
- mail-enabled distribution group 131
 - add to IT Shop 145, 147
 - add to system role 144
 - addressing 133
 - administrator 138
 - alias 133
 - assign dynamic distribution group 153
 - assign email user 149, 151
 - assign mail contact 149, 151
 - assign mailbox 149-150
 - assign mail-enabled distribution group 153
 - assign mail-enabled public folder 154, 184
 - assign to business role 143
 - assign to cost center 142
 - assign to department 142
 - assign to location 142
 - category 152

- create 132
- delete 155, 182
- display name 133
- edit 132
- extended property 154
- join 133
- leave 133
- mail acceptance 136
- moderate 133
- moderator 138
- receive restriction 136
- send on behalf of 137
- mail-enabled public folder 183
 - assign mail-enabled distribution group 154, 184
- membership
 - modify provisioning 43

O

- object
 - delete immediately 51
 - outstanding 51
 - publish 51
- Office 365 group 156
 - Active Directory group 133, 157
 - add to IT Shop 169, 171
 - add to system role 168
 - alias 157
 - allow subscription 157, 162
 - assign Azure Active Directory user account 163
 - assign owner 161
 - assign subscription 162
 - assign to business role 167
 - assign to cost center 166

- assign to department 166
- assign to location 166
- assign user account 172-173
- category 174
- create 156
- delete 175
- display name 157
- edit 157
- extended property 175
- mail acceptance 161
- receive restriction 161

- offline mode 56
- outstanding object 51

P

- project template 191
- provisioning
 - accelerate 46
 - members list 43
- public folder 89

R

- revision filter 42

S

- schema
 - changes 41
 - shrink 41
 - update 41
- server 81
- single object synchronization 45, 50
 - accelerate 46
- start up configuration 36

- synchronization
 - accelerate 42
 - calculation schedule 47
 - configure 25, 34
 - connection parameter 25, 34
 - Exchange Online 14-15
 - prevent 48
 - scope 34
 - set up 14-15
 - start 25, 47
 - synchronization project
 - create 25
 - variable 34
 - workflow 25, 35
- synchronization configuration
 - customize 34-35
- synchronization log 49
 - contents 33
 - create 33
- synchronization project
 - create 25
 - deactivate 48
 - project template 191
- synchronization server 10, 81
 - configure 19
 - install 19
 - Job server 19
- synchronization workflow
 - create 25, 35
- synchronize single object 50
- system connection
 - change 36
 - enabled variable set 37

T

- target system
 - not available 56
- target system manager 79
- target system synchronization 51
- template
 - IT operating data, modify 69

U

- user account
 - apply template 69

V

- variable set 36
 - active 37