



One Identity Manager 9.2

Administration Guide for Connecting to Microsoft Exchange

Copyright 2023 One Identity LLC.

ALL RIGHTS RESERVED.

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

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

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

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

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

Patents

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

Trademarks

One Identity and the One Identity logo are trademarks and registered trademarks of One Identity LLC. in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at www.OneIdentity.com/legal/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 Microsoft Exchange
Updated - 29 September 2023, 04:31

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

Contents

Managing Microsoft Exchange environments	8
Architecture overview	8
One Identity Manager users for managing Microsoft Exchange	9
Configuration parameters for managing Microsoft Exchange environments	10
Synchronizing a Microsoft Exchange environment	12
Setting up initial synchronization with Microsoft Exchange	13
Users and permissions for synchronizing with Microsoft Exchange	14
Setting up the Microsoft Exchange synchronization server	16
System requirements for the Microsoft Exchange synchronization server	16
Installing One Identity Manager Service with a Microsoft Exchange connector	17
Configuring participating servers for remote access through Windows PowerShell	20
Testing Active Directory domain trusts	21
Extensions for creating linked mailboxes in a Microsoft Exchange resource forest	22
Recommendations for synchronizing Microsoft Exchange environments	23
Creating a synchronization project for initial synchronization of a Microsoft Exchange environment	26
Information required to set up a synchronization project	27
Creating an initial synchronization project for Microsoft Exchange	28
Configuring the synchronization log	33
Customizing the synchronization configuration	34
Configuring Microsoft Exchange synchronization	35
Customizing synchronization projects for send permissions and full access permissions	36
Changing system connection settings of Microsoft Exchange	37
Editing connection parameters in the variable set	37
Editing target system connection properties	38
Updating schemas	39
Speeding up synchronization with revision filtering	40
Configuring the provisioning of memberships	42
Configuring single object synchronization	43
Accelerating provisioning and single object synchronization	44

Running synchronization	45
Starting synchronization	46
Deactivating synchronization	47
Displaying synchronization results	47
Synchronizing single objects	48
Tasks following synchronization	49
Post-processing outstanding objects	49
Adding custom tables to the target system synchronization	51
Managing Microsoft Exchange mailboxes, mail users, and mail contacts through account definitions	52
Troubleshooting	53
Ignoring data error in synchronization	53
Pausing handling of target system specific processes (Offline mode)	54
Basic data for managing a Microsoft Exchange environment	56
Account definitions for Microsoft Exchange mailboxes, mail users, and mail contacts ..	57
Creating account definitions	58
Editing account definitions	58
Main data for account definitions	59
Editing manage levels	61
Creating manage levels	62
Assigning manage levels to account definitions	62
Main data for manage levels	63
Creating mapping rules for IT operating data	64
Entering IT operating data	65
Modify IT operating data	66
Assigning account definitions to identities	67
Assigning account definitions to departments, cost centers, and locations	68
Assigning account definitions to business roles	69
Assigning account definitions to all identities	70
Assigning account definitions directly to identities	70
Assigning account definitions to system roles	71
Adding account definitions in the IT Shop	71
Assigning account definitions to Active Directory domains	74
Deleting account definitions	74
Target system managers for Microsoft Exchange	77

Job server for Microsoft Exchange-specific process handling	79
General main data for Job servers	80
Specifying server functions	82
Microsoft Exchange structure	85
Microsoft Exchange organizations	86
Displaying hierarchical address books	87
Microsoft Exchange mailbox databases	88
Microsoft Exchange address lists	90
Microsoft Exchange public folders	92
Microsoft Exchange mailbox server	93
Microsoft Exchange data availability groups	94
Share policies	95
Retention policies	96
Mobile device mailbox policy	97
Folder administration policies	98
Role assignment policies	99
Outlook Web App mailbox policy	100
Address book policies	101
Microsoft Exchange mailboxes	102
Creating Microsoft Exchange mailboxes	103
Editing main data of Microsoft Exchange mailboxes	105
General main data for Microsoft Exchange mailboxes	106
Calendar settings for Microsoft Exchange mailboxes	109
Limits for Microsoft Exchange mailboxes	110
Microsoft Exchange mailbox archives	112
Storage for Microsoft Exchange mailboxes	112
Features for Microsoft Exchange mailboxes	113
Booking resources for Microsoft Exchange equipment mailboxes and Microsoft Exchange room mailboxes	114
Adjusting receive restrictions for Microsoft Exchange mailboxes	116
Microsoft Exchange mailbox permission: Send on behalf	117
Microsoft Exchange mailbox permission: Send as	118
Microsoft Exchange mailbox permission: Full access	119
Assigning extended properties to Microsoft Exchange mailbox	119
Microsoft Exchange deactivating mailboxes	120

Deleting and restoring Microsoft Exchange mailboxes	121
Microsoft Exchange mail users and Microsoft Exchange mail contacts	123
Creating Microsoft Exchange mail users	123
Editing main data of Microsoft Exchange mail users	125
Main data for Microsoft Exchange mail users	125
Receive restrictions for Microsoft Exchange mail users	128
Assigning extended properties to Microsoft Exchange mail users	128
Deleting and restoring Microsoft Exchange mail users	129
Creating Microsoft Exchange mail contacts	130
Editing main data of Microsoft Exchange mail contacts	131
Main data for Microsoft Exchange mail contacts	131
Receive restrictions for Microsoft Exchange mail contacts	134
Assigning extended properties to Microsoft Exchange mail contacts	135
Deleting and restoring Microsoft Exchange mail contacts	135
Microsoft Exchange mail-enabled distribution groups	137
Creating Microsoft Exchange mail-enabled distribution groups	137
Editing main data of Microsoft Exchange mail-enabled distribution groups	138
Main data for Microsoft Exchange mail-enabled distribution groups	139
Receive restrictions for Microsoft Exchange mail-enabled distribution groups	141
Microsoft Exchange mail-enabled distribution list: Send on behalf	142
Microsoft Exchange mail-enabled distribution list: Send as	143
Specifying Microsoft Exchange mail-enabled distribution groups	144
Specifying Microsoft Exchange moderated distribution group extensions	144
Adding a Microsoft Exchange dynamic distribution group to Microsoft Exchange mail-enabled distribution groups	146
Assigning extended properties to Microsoft Exchange mail-enabled distribution groups	146
Deleting Microsoft Exchange mail-enabled distribution groups	147
Microsoft Exchange dynamic distribution groups	148
Main data for Microsoft Exchange dynamic distribution groups	148
Customizing receive restrictions for Microsoft Exchange dynamic distribution groups	150
Customizing send permissions for Microsoft Exchange dynamic distribution groups	151
Adding Microsoft Exchange mail-enabled distribution groups to Microsoft Exchange dynamic distribution groups	152
Microsoft Exchange mail-enabled public folders	153

Extensions for supporting Exchange Hybrid environments	155
Advice for synchronizing remote mailboxes	156
Advice for migrating mailboxes	157
Creating remote mailboxes	160
Editing remote mailboxes	161
General main data for remote mailboxes	162
Information about remote configuration	164
Information about cloud-based archive mailboxes	165
Customizing receive restrictions for remote mailboxes	165
Specifying extensions for moderated remote mailboxes	166
Assigning extended properties to remote mailboxes	167
Appendix: Error handling	169
Error running the Windows PowerShell command Set-Mailbox	169
Possible errors when synchronizing an Exchange Hybrid environment	170
Appendix: Configuration parameters for managing a Microsoft Exchange environment	172
Appendix: Default project template for Microsoft Exchange	173
Default project template for Microsoft Exchange 2013, Microsoft Exchange 2016, and Microsoft Exchange 2019	173
Appendix: Processing methods of Microsoft Exchange system objects	175
Appendix: Microsoft Exchange connector settings	177
About us	180
Contacting us	180
Technical support resources	180
Index	181

Managing Microsoft Exchange environments

The key aspects of managing a Microsoft Exchange environment with One Identity Manager include the mapping of mailboxes, mail users, mail contacts, and the mail-enabled distribution group.

The system information for the Microsoft Exchange structure is loaded into the One Identity Manager database during data synchronization. It is not possible to customize this system information in One Identity Manager due to the complex dependencies and far reaching effects of changes.

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

Architecture overview

In One Identity Manager, the following servers play a role in managing Microsoft Exchange:

- Microsoft Exchange server
The Microsoft Exchange server against which Microsoft Exchange objects are synchronized. The synchronization server connects to this server in order to access the Microsoft Exchange objects.
- Synchronization server
Synchronization server for synchronizing One Identity Manager data with Microsoft Exchange. The One Identity Manager Service with the Microsoft Exchange connector is installed on this server. The synchronization server connects to the Microsoft Exchange server.

The One Identity Manager Microsoft Exchange connector uses Windows PowerShell to communicate with the Microsoft Exchange server.

Figure 1: Architecture for synchronization



One Identity Manager users for managing Microsoft Exchange

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

Table 1: Users

Users	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 administrators.• Do not assume any administrative tasks within the target system.
Target system managers	<p>Target system managers must be assigned to the Target systems Exchange 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.

Users	Tasks
	<ul style="list-style-type: none"> Edit password policies for the target system. 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.
One Identity Manager administrators	<p>One Identity Manager administrator and administrative system users Administrative system users are not added to application roles.</p> <p>One Identity Manager administrators:</p> <ul style="list-style-type: none"> Create customized permissions groups for application roles for role-based login to administration tools in the Designer as required. Create system users and permissions groups for non role-based login to administration tools in the Designer as required. Enable or disable additional configuration parameters in the Designer as required. Create custom processes in the Designer as required. Create and configure schedules as required. Create and configure password policies as required.

Configuration parameters for managing Microsoft Exchange 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 a Microsoft Exchange environment](#) on page 172.

Synchronizing a Microsoft Exchange environment

One Identity Manager supports synchronization with:

- Microsoft Exchange 2013 with cumulative update 23
- Microsoft Exchange 2016
- Microsoft Exchange 2019 with cumulative Update 1

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

Synchronization prerequisites

- Synchronization of the Active Directory system is carried out regularly.
- The Active Directory forest is declared in One Identity Manager.
- Explicit Active Directory domain trusts are declared in One Identity Manager
- Implicit two-way trusts between domains in an Active Directory forest are declared in One Identity Manager
- User account with password and domain controller on the Microsoft Exchange client domain are entered to create linked mailboxes within an Active Directory resource forest topology

This sections explains how to:

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

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

Detailed information about this topic

- [Setting up initial synchronization with Microsoft Exchange](#) on page 13
- [Customizing the synchronization configuration](#) on page 34
- [Running synchronization](#) on page 45
- [Tasks following synchronization](#) on page 49
- [Troubleshooting](#) on page 53
- [Processing methods of Microsoft Exchange system objects](#) on page 175

Setting up initial synchronization with Microsoft Exchange

The Synchronization Editor provides project templates that can be used to set up synchronization of Microsoft Exchange objects. You use these project templates to create synchronization projects with which you import the data from Microsoft Exchange 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.

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

1. Prepare a user account with sufficient permissions for synchronization.
2. One Identity Manager parts for managing Microsoft Exchange systems are available if the **TargetSystem | ADS | Exchange2000** 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. Check whether the domain trusts are entered correctly.
5. Enter the data for creating linked mailboxes within a resource forest.
6. Create a synchronization project with the Synchronization Editor.

Detailed information about this topic

- [Users and permissions for synchronizing with Microsoft Exchange](#) on page 14
- [System requirements for the Microsoft Exchange synchronization server](#) on page 16
- [Configuring participating servers for remote access through Windows PowerShell](#) on page 20
- [Testing Active Directory domain trusts](#) on page 21
- [Extensions for creating linked mailboxes in a Microsoft Exchange resource forest](#) on page 22
- [Creating a synchronization project for initial synchronization of a Microsoft Exchange environment](#) on page 26
- [Deactivating synchronization](#) on page 47
- [Recommendations for synchronizing Microsoft Exchange environments](#) on page 23
- [Customizing the synchronization configuration](#) on page 34
- [Configuration parameters for managing a Microsoft Exchange environment](#) on page 172
- [Default project template for Microsoft Exchange 2013, Microsoft Exchange 2016, and Microsoft Exchange 2019](#) on page 173

Users and permissions for synchronizing with Microsoft Exchange

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

Table 2: Users for synchronization

User	Permissions
User for accessing Microsoft Exchange	<p>You must provide a user account with at least the following authorizations for full synchronization of Microsoft Exchange objects with the supplied One Identity Manager default configuration.</p> <ul style="list-style-type: none">• Member of the Organization management role group• Member of the Public folder management role group• Member of the Recipient management role group• Security Group Creation and Membership role

User	Permissions
	<p>Create a new role group in Microsoft Exchange and assign the role and user account to this role group.</p> <p>For more information about managing permissions in Microsoft Exchange, see the Microsoft documentation.</p>
User for creating linked mailboxes	The user account is required for adding linked mailboxes. The user account requires read access in Active Directory.
One Identity Manager Service user account	<p>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).</p> <p>The user account must belong to the Domain users group.</p> <p>The user account must have the Login as a service extended user permissions.</p> <p>The user account requires permissions for the internal web service.</p> <p>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:</p> <pre>netsh http add urlacl url=http://<IP address>:<port number>/ user="NT AUTHORITY\NETWORKSERVICE"</pre> <p>The user account needs full access to the One Identity Manager Service installation directory in order to automatically update One Identity Manager.</p> <p>In the default installation, One Identity Manager is installed under:</p> <ul style="list-style-type: none"> • %ProgramFiles(x86)%\One Identity (on 32-bit operating systems) • %ProgramFiles%\One Identity (on 64-bit operating systems)
User for accessing the One Identity Manager database	The Synchronization default system user is provided to run synchronization using an application server.

Setting up the Microsoft Exchange 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 Microsoft Exchange connector must be installed on the synchronization server.

IMPORTANT: The Microsoft Exchange One Identity Manager connector uses Windows PowerShell to communicate with the Microsoft Exchange server. For communication, extra configuration is required on the synchronization server and the Microsoft Exchange server.

Detailed information about this topic

- [System requirements for the Microsoft Exchange synchronization server](#) on page 16
- [Installing One Identity Manager Service with a Microsoft Exchange connector](#) on page 17
- [Configuring participating servers for remote access through Windows PowerShell](#) on page 20

System requirements for the Microsoft Exchange synchronization server

To set up synchronization with a Microsoft Exchange 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.

- Windows Management Framework 4.0

IMPORTANT: The Microsoft Exchange One Identity Manager connector uses Windows PowerShell to communicate with the Microsoft Exchange server. For

communication, extra configuration is required on the synchronization server and the Microsoft Exchange server.

Related topics

- [Configuring participating servers for remote access through Windows PowerShell](#) on page 20

Installing One Identity Manager Service with a Microsoft Exchange connector

The One Identity Manager Service must be installed on the synchronization server with the Microsoft Exchange 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	Microsoft Exchange connector
Machine role	Server Job Server Active Directory Microsoft Exchange

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 **Microsoft Exchange**.
5. On the **Server functions** page, select **Microsoft Exchange connector**.

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**.

Configuring participating servers for remote access through Windows PowerShell

IMPORTANT: Run the configuration steps on the Microsoft Exchange server and the synchronization server.

To configure a server for remote access using Windows PowerShell

1. Run Windows PowerShell with administrator credentials from the **Run as Administrator** context menu.
2. Enter this command at the prompt:
`winrm quickconfig`
This command prepares for remote access usage.
3. Enter this command at the prompt:
`Set-ExecutionPolicy RemoteSigned`
This command permits the Windows PowerShell commands (Cmdlets) to be carried out. The script must be signed by a trusted publishers.
4. Enter this command at the prompt:
`Set-Item wsman:\localhost\client\trustedhosts * -Force`
This command modifies the list of trusted hosts to enable authentication.
The value `*` allows all connections. One Identity Manager uses the server's fully qualified domain name for the connection. You can limit the value.

To test remote access through Windows PowerShell from the synchronization server to the Microsoft Exchange server (sync.)

1. Run Microsoft Exchange on the Windows PowerShell synchronization server.
2. Enter this command at the prompt:
`$creds = New-Object System.Management.Automation.PSCredential
("<domain>\<user>", (ConvertTo-SecureString "<password>" -AsPlainText -
Force))`

- OR -

```
$creds = Get-Credential
```

This command finds the access data required for establishing the connection.

3. Enter this command at the prompt:

```
$session = New-PSSession -Configurationname Microsoft.Exchange -  
ConnectionUri http://<ServerName as FQDN>/powershell -Credential $creds -  
Authentication Kerberos
```

This command creates a remote session.

NOTE: One Identity Manager establishes a connection using the fully qualified domain name of the Microsoft Exchange server. The server name must therefore be in the list configured with trusted hosts.

4. Enter this command at the prompt:

```
Import-PsSession $session
```

This command imports the remote session so that the connection can be accessed.

5. Test the functionality with any Microsoft Exchange command. For example, enter the following command at the prompt:

```
Get-Mailbox
```

Testing Active Directory domain trusts

For synchronization with a Microsoft Exchange environment, Active Directory domain trusts must be declared in One Identity Manager. Users can access resources in other domains depending on the domain trusts.

- Explicit trusts are loaded into Active Directory by synchronizing with One Identity Manager. Domains which are trusted by the currently synchronized domains are found.
- To declare implicit two-way trusts between domains within an Active Directory forest in One Identity Manager, ensure that the parent domain is entered in all child domains.

To enter the parent domain

1. In the Manager, select the **Active Directory > Domains** category.
2. Select the domain in the result list.
3. Select the **Change main data** task.
4. Enter the parent domain.
5. Save the changes.

Implicit trusts are created automatically.

To test trusted domains

1. In the Manager, select the **Active Directory > Domains** category.
2. Select the domain in the result list.
3. Select **Specify trust relationships**.

This shows domains that trust the selected domain.

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

Extensions for creating linked mailboxes in a Microsoft Exchange resource forest

To create linked mailboxes in a Microsoft Exchange resource forest, you must declare the user account with which the linked mailboxes are going to be created as well as the Active Directory domain controller for each Active Directory Client domain.

To edit main data of a domain

1. In the Manager, select the **Active Directory > Domains** category.
2. Select the domain in the result list and run the **Change main data** task.
3. On the **Exchange** tab, enter the following information.

Table 4: Domain main data for creating linked mailboxes

Property	Description
User (linked mailboxes)	User account used to create linked mailboxes.
Password	The user account's password.
Confirmation	Repeat the password of the user account.
DC (linked mailboxes)	Active Directory domain controller for creating linked mailboxes.

4. Save the changes.

Related topics

- [Users and permissions for synchronizing with Microsoft Exchange](#) on page 14

Recommendations for synchronizing Microsoft Exchange environments

The following scenarios for synchronizing Microsoft Exchange are supported.

Scenario: synchronizing Microsoft Exchange infrastructure including all Microsoft Exchange organization recipients

It is recommended on principal that you synchronize the Microsoft Exchange infrastructure including all Microsoft Exchange organization recipients.

The Microsoft Exchange infrastructure elements (server, address lists, policies, for example) and recipients (mailboxes, mail-enabled distribution groups, mail users, mail contacts) of the entire Microsoft Exchange organization are synchronized.

- Set up a synchronization project and use the **Complete organization** recipient scope.

For more information, see [Creating a synchronization project for initial synchronization of a Microsoft Exchange environment](#) on page 26.

Scenario: synchronizing Microsoft Exchange infrastructure and recipients of a select Active Directory domain in the Microsoft Exchange organization.

It is possible to synchronize Microsoft Exchange infrastructure and recipients separately if synchronization of the entire Microsoft Exchange organization is not possible due to the large number of recipients.

First the Microsoft Exchange infrastructure elements (server, address lists, policies, for example) are loaded. Then recipients (mailboxes, mail-enabled distribution groups, mail users, mail contacts) are synchronized from the given Active Directory domain in the Microsoft Exchange organization.

The following synchronization project configuration is recommended in this case:

NOTE: Use the Synchronization Editor expert mode for the following configurations.

1. Set up the synchronization project for synchronizing the entire Microsoft Exchange infrastructure.
 - Select the recipient **Complete organization**.
 - Customize the synchronization workflow.
 - Disable synchronization steps of all schema types representing recipients. These are:
 - Mailbox
 - MailContact

- MailUser
 - DistributionList
 - DynamicDistributionList
 - MailPublicFolder
 - Check that all schema types, not representing recipients, are synchronized. These are:
 - AddressBookPolicy
 - ActiveSyncMailboxPolicy
 - DatabaseAvailabilityGroup
 - MailboxDatabase
 - OfflineAddressBook
 - Organization
 - PublicFolder
 - RetentionPolicy
 - RoleAssingmentPolicy
 - Server
 - SharingPolicy
 - AddressList
 - GlobalAddressList
2. Set up the synchronization project for synchronizing recipient of an Active Directory domain.
- Select the recipient scope **Only recipients of the following domain** and select a Microsoft Exchange organization domain.
 - Customize the synchronization workflow.
 - Disable synchronization steps of all schema types that do not represent recipients. These are:
 - AddressBookPolicy
 - ActiveSyncMailboxPolicy
 - DatabaseAvailabilityGroup
 - MailboxDatabase
 - OfflineAddressBook
 - Organization
 - PublicFolder
 - RetentionPolicy
 - RoleAssingmentPolicy

- Server
 - SharingPolicy
 - AddressList
 - GlobalAddressList
 - Check that all schema types not representing recipients are synchronized. These are:
 - Mailbox
 - MailContact
 - MailUser
 - DistributionList
 - DynamicDistributionList
 - MailPublicFolder
3. Specify more base objects for the remaining Active Directory domains.
- In the Synchronization Editor, open the first synchronization project for the synchronization of recipients.
 - Create a new base object for every other domain. Use the wizards to attach a base object.
 - In the wizard, select the Microsoft Exchange connector and enter the connection parameters. The connection parameters are saved in a special variable set.

NOTE: When setting up the connection, note the following:

 - If possible, select a Microsoft Exchange server that is in the domain.
 - Select the **Only recipients of the following domain** recipient scope.
 - Create a new start up configuration for each domain. In the start configuration, use the newly created variable sets.
 - Run a consistency check.
 - Activate the synchronization project.
4. Customize the synchronization schedule.
- IMPORTANT:** Set up the synchronization schedules such that the Microsoft Exchange infrastructure is synchronized before Microsoft Exchange recipients.

Several synchronization runs maybe necessary before all the data is synchronized depending on references between the Microsoft Exchange organization domains.

Creating a synchronization project for initial synchronization of a Microsoft Exchange environment

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

IMPORTANT: It must be possible to reach the Microsoft Exchange server 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 [Recommendations for synchronizing Microsoft Exchange environments](#) on page 23.

Use the Synchronization Editor to configure synchronization between the One Identity Manager database and Microsoft Exchange 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.

Synchronization prerequisites

- Synchronization of the Active Directory system is carried out regularly.
- The Active Directory forest is declared in One Identity Manager.
- Explicit Active Directory domain trusts are declared in One Identity Manager
- Implicit two-way trusts between domains in an Active Directory forest are declared in One Identity Manager
- User account with password and domain controller on the Microsoft Exchange client domain are entered to create linked mailboxes within an Active Directory resource forest topology

Related topics

- [Recommendations for synchronizing Microsoft Exchange environments](#) on page 23
- [Information required to set up a synchronization project](#) on page 27
- [Creating an initial synchronization project for Microsoft Exchange](#) on page 28
- [Testing Active Directory domain trusts](#) on page 21
- [Extensions for creating linked mailboxes in a Microsoft Exchange resource forest](#) on page 22

- [Customizing synchronization projects for send permissions and full access permissions](#) on page 36

Information required to set up a synchronization project

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

Table 5: Information required for setting up a synchronization project

Data	Explanation
Microsoft Exchange version	One Identity Manager supports synchronization with Microsoft Exchange 2013 with Cumulative Update 23, Microsoft Exchange 2016, and Microsoft Exchange 2019 with Cumulative Update 1.
Server (fully qualified)	<p>Fully qualified name (FQDN) of the Microsoft Exchange server to which the synchronization server connects to access Microsoft Exchange objects.</p> <p>Syntax:</p> <p><Name of servers>.<Fully qualified domain name></p> <p>IMPORTANT: It must be possible to reach the Microsoft Exchange server by DNS query for successful authentication. If the DNS cannot be resolved, the target system connection is refused.</p>
User account and password for logging in	<p>Fully qualified name (FQDN) of the user account and password for logging in on the Microsoft Exchange.</p> <p>Example:</p> <p>user@domain.com</p> <p>domain.com\user</p> <p>Make a user account available with sufficient permissions. For more information, see Users and permissions for synchronizing with Microsoft Exchange on page 14.</p>
Synchronization server for Microsoft Exchange	<p>The One Identity Manager Service with the Microsoft Exchange connector must be installed on the synchronization server.</p> <ul style="list-style-type: none"> • Server function: Microsoft Exchange connector • Machine role: Server Job Server Active Directory Microsoft Exchange <p>For more information, see Setting up the Microsoft Exchange synchronization server on page 16.</p>

Data	Explanation
One Identity Manager database connection data	<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	<p>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.</p> <p>The remote connection server and the workstation must be in the same Active Directory domain.</p> <p>Remote connection server configuration:</p> <ul style="list-style-type: none"> • One Identity Manager Service is started • RemoteConnectPlugin is installed • Microsoft Exchange connector is installed <p>The remote connection server must be declared as a Job server in One Identity Manager. The Job server name is required.</p> <p>TIP: The remote connection server requires the same configuration as the synchronization server (with regard to the installed software and entitlements). Use the synchronization as remote connection server at the same time by installing the RemoteConnectPlugin as well.</p> <p>For more detailed information about setting up a remote connection, see the <i>One Identity Manager Target System Synchronization Reference Guide</i>.</p>

Creating an initial synchronization project for Microsoft Exchange

IMPORTANT: Each Microsoft Exchange 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 Microsoft Exchange

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 Microsoft Exchange** entry and click **Start**.

This starts the Synchronization Editor's project wizard.

3. Select the connector on the **Select target system** page.

- To synchronize a Microsoft Exchange 2013 environment, select the **Microsoft Exchange 2013 connector**.
- To synchronize a Microsoft Exchange 2016 environment, select the **Microsoft Exchange 2016 connector**.
- To synchronize a Microsoft Exchange 2019 environment, select the **Microsoft Exchange 2019 connector**.

4. On the wizard's start page, click **Next**.

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

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

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

6. Enter the information about the Microsoft Exchange server on the **Select Microsoft Exchange server** page to which the synchronization server connects to access Microsoft Exchange objects.

- a. Under **Server**, enter the fully qualified name (FQDN) of the Microsoft Exchange server. To check the data, click **DNS query**.

NOTE: If you only know the IP address of the server, enter the IP address in the **Server** field and click **DNS query**. The server's fully qualified name is found and entered.

- b. Under **Max. concurrent connections**, enter the number of connections that can be used at the same time.

A maximum 4 simultaneous connection are recommended. Synchronization tries to use this many connections. The number may not always be reached depending on the load. Warnings are given respectively.

A default timeout is defined for connecting. The timeout is 5 minutes long for the first connection and 30 seconds for all following connections. The connections are closed if the connection is idle for the duration.

- c. To use the **Basic** authentication method, enable **Basic authentication (requires SSL)**.

NOTE: Microsoft Exchange does not support this authentication type by default. You must configure support for this method in Microsoft Exchange. In addition, an SSL connection is used to authenticate using the **Basic** method. By default, authentication uses Kerberos.

7. Enter login data on the **Enter connection credentials** page to connect to Microsoft Exchange.

- To use a defined user account, select the **Use following account** option and enter the following data:

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

Example:

user@domain.com

domain.com\user

- **Password:** Password for the user account.

- Select the **Use account of One Identity Manager Service service** option if the user account to use is that of the current user. The user account running under the One Identity Manager Service requires the permissions described in [Users and permissions for synchronizing with Microsoft Exchange](#) on page 14.

NOTE: If this setting is used, the current user account is also used in the Synchronization Editor during configuration. This user account may be different to the One Identity Manager Service's user account

In this case, it is recommended you use the **RemoteConnectPlugin**. This ensures that the same user account is used during configuration with the Synchronization Editor as is used in the service context.

8. On the **Recipient scope** page, specify whether the recipient of any domain or complete Microsoft Exchange organization should be taken into account.

- To synchronize the recipients of the Microsoft Exchange organization, select the **Entire organization** option (recommended). As a prerequisite, the trusted domains of the Active Directory domains must be declared in One Identity Manager.

- Select the **Only recipients of the following domain** option to synchronize recipients with specific domains and select a domain. The target system domain is listed as a minimum.
9. On the last page of the system connection wizard, you can save the connection data.
 - Set the **Save connection data on local computer** option to save the connection data. This can be reused when you set up other synchronization projects.
 - Click **Finish**, to end the system connection wizard and return to the project wizard.
 10. 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.
11. 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.
 12. On the **Restrict target system access** page, specify how system access should work. You have the following options:


Table 6: Specify target system access

Option	Meaning
	<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


Option	Meaning
	<p>system.</p> <ul style="list-style-type: none"> 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.

13. 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.

- Click  to add a new Job server.
- 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.

- Click **OK**.

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

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

14. 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

- [Recommendations for synchronizing Microsoft Exchange environments](#) on page 23
- [Information required to set up a synchronization project](#) on page 27
- [Users and permissions for synchronizing with Microsoft Exchange](#) on page 14
- [Setting up the Microsoft Exchange synchronization server](#) on page 16
- [Testing Active Directory domain trusts](#) on page 21
- [Configuring the synchronization log](#) on page 33
- [Customizing the synchronization configuration](#) on page 34
- [Tasks following synchronization](#) on page 49
- [Default project template for Microsoft Exchange 2013, Microsoft Exchange 2016, and Microsoft Exchange 2019](#) on page 173
- [Microsoft Exchange connector settings](#) on page 177

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 47

Customizing the synchronization configuration

Having used the Synchronization Editor to set up a synchronization project for initial synchronization of Microsoft Exchange, you can use the synchronization project to load Microsoft Exchange objects into the One Identity Manager database. When you manage mailboxes, mail users, mail contacts, and mail-enabled distribution groups with One Identity Manager, modifications are provisioned in the Microsoft Exchange system.

You must customize the synchronization configuration in order to compare the One Identity Manager database with the Microsoft Exchange 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 Microsoft Exchange objects and database objects are included in synchronization, edit the scope of the target system connection and the One Identity Manager database connection. To prevent data inconsistencies, define the same scope in both systems. If no scope is defined, all objects will be synchronized.
- Update the schema in the synchronization project if the One Identity Manager schema or target system schema has changed. Then you can add the changes to the mapping.
- To synchronize additional schema properties, update the schema in the synchronization project. Include the schema extensions in the mapping.

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

Detailed information about this topic

- [Configuring Microsoft Exchange synchronization](#) on page 35
- [Updating schemas](#) on page 39
- [Changing system connection settings of Microsoft Exchange](#) on page 37
- [Updating schemas](#) on page 39
- [Speeding up synchronization with revision filtering](#) on page 40
- [Configuring the provisioning of memberships](#) on page 42
- [Configuring single object synchronization](#) on page 43
- [Accelerating provisioning and single object synchronization](#) on page 44

Configuring Microsoft Exchange synchronization

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

To create a synchronization configuration for synchronizing Microsoft Exchange

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.

Customizing synchronization projects for send permissions and full access permissions

Synchronizing the **Send as** and **Full access** permissions is very time-consuming. Synchronization is disabled by default. In order to synchronize these permissions, the synchronization project must be customized.

- In the **Initial Synchronization** workflow, enable the **Mailbox Permissions** synchronization step.
- In the **Provisioning** workflow, enable the **Mailbox Permissions** synchronization step.
- In the **Initial Synchronization** workflow, enable the **DistributionGroup Permissions** synchronization step.
- In the **Provisioning** workflow, enable the **DistributionGroup Permissions** synchronization step.

To enable synchronization steps

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Workflows** category.
3. Select a workflow in the navigation view.
4. Click  in the workflow view's toolbar.
5. Deselect the **Disable** check boxes on all synchronization steps that you want to enable.
6. Click **OK**.

Permissions for synchronizing the permissions

The user for accessing the Microsoft Exchange requires, in addition to the permissions mentioned in [Users and permissions for synchronizing with Microsoft Exchange](#) on page 14 above, the following:

- **Active Directory Permissions** role (Active Directory Permissions)

Create a new role group in Microsoft Exchange and assign the role and user account to this role group. For more information about managing permissions in Microsoft Exchange, see the Microsoft documentation.

Related topics

- [Microsoft Exchange mailbox permission: Send as on page 118](#)
- [Microsoft Exchange mailbox permission: Full access on page 119](#)
- [Microsoft Exchange mail-enabled distribution list: Send as on page 143](#)

Changing system connection settings of Microsoft Exchange

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 37](#)
- [Editing target system connection properties on page 38](#)
- [Microsoft Exchange connector settings on page 177](#)

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 38

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 37

Updating schemas

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

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

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

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

To update a system connection schema

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

To edit a mapping

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Mappings** category.
3. Select a mapping in the navigation view.
Opens the Mapping Editor. For more information about mappings, see the *One Identity Manager Target System Synchronization Reference Guide*.

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

Speeding up synchronization with revision filtering

IMPORTANT: The revision algorithm can only be enabled in synchronization projects created with One Identity Manager version 8.0 or higher.

If revisioning was enabled in old 7.x synchronization projects, modifications made directly in Microsoft Exchange are also not identified. We recommend that you set up the synchronization project again using the synchronization project template implemented from version 8.0 onwards.

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.

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

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 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 Microsoft Exchange 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 Microsoft Exchange](#) on page 37

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 a Microsoft Exchange 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 **Active Directory > Basic configuration data > Target system types** category.
2. In the result list, select the **Microsoft Exchange** 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 EX0MailUserAcceptRcpt assignment table:

```
exists (select top 1 1 from EX0MailUser u
        where u.UID_EX0MailUser = i.UID_EX0MailUser
        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 **Active Directory > Basic configuration data > Target system types** category.
2. In the result list, select the **Microsoft Exchange** 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_EX0Organization).XObjectKey`
8. Save the changes.

Related topics

- [Synchronizing single objects](#) on page 48
- [Post-processing outstanding objects](#) on page 49

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 **Microsoft Exchange connector** server function to the Job server.

All Job servers must access the same Microsoft Exchange organization 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 Microsoft Exchange-specific process handling](#) on page 79

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 46
- [Deactivating synchronization](#) on page 47

- [Displaying synchronization results](#) on page 47
- [Synchronizing single objects](#) on page 48
- [Pausing handling of target system specific processes \(Offline mode\)](#) on page 54

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 a Microsoft Exchange environment](#) on page 26
- [Pausing handling of target system specific processes \(Offline mode\)](#) on page 54

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.

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 **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 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 43

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 49
- [Adding custom tables to the target system synchronization](#) on page 51
- [Managing Microsoft Exchange mailboxes, mail users, and mail contacts through account definitions](#) on page 52

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 **Active Directory > Target system synchronization: Exchange** category.

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

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

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



- The synchronization log has already been deleted.
- OR -
- An assignment from a member list has been deleted from the target system.
The base object of the assignment was updated during the synchronization. A corresponding entry appears in the synchronization log. The entry in the assignment table is marked as outstanding, but there is no entry in the synchronization log.
- An object that contains a member list has been deleted from the target system.
During synchronization, the object and all corresponding entries in the assignment tables are marked as outstanding. However, an entry in the synchronization log appears only for the deleted object.


TIP:

To display object properties of an outstanding object

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

Table 7: 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.

Icon	Method	Description
		<p>This runs a target system specific process that triggers the provisioning process for the object.</p> <p>Prerequisites:</p> <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 **Active Directory > Basic configuration data > Target system types** category.
2. In the result list, select the **Microsoft Exchange** 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 49

Managing Microsoft Exchange mailboxes, mail users, and mail contacts through account definitions

In the default installation, after synchronizing, identities are automatically created for Microsoft Exchange mailboxes, mail users, and mail contacts. If an account definition for the Microsoft Exchange organization is not known at the time of synchronization, Microsoft Exchange mailboxes, mail users, and mail contacts are linked to the identities. However, account definitions are not assigned. The Microsoft Exchange mailboxes, mail users, and mail contacts are therefore in a **Linked** state.

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

To manage Microsoft Exchange mailboxes, mail users, and mail contacts through account definitions

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

Related topics

- [Account definitions for Microsoft Exchange mailboxes, mail users, and mail contacts](#) on page 57
- [Assigning account definitions to Active Directory domains](#) on page 74

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 47

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 47

Basic data for managing a Microsoft Exchange environment

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

- Account definitions

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

For more information, see [Account definitions for Microsoft Exchange mailboxes, mail users, and mail contacts](#) on page 57.

- 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 49.

- 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 Microsoft Exchange organizations in One Identity Manager.

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

For more information, see [Target system managers for Microsoft Exchange](#) on page 77.

- Servers

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

For more information, see [Job server for Microsoft Exchange-specific process handling](#) on page 79.

Account definitions for Microsoft Exchange mailboxes, mail users, and mail contacts

One Identity Manager has account definitions for automatically allocating mailboxes, mail users, and mail contacts to identities. You can create account definitions for every target system. If an identity does not yet have a mailbox (mail user, mail contact) in a target system, a new mailbox (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 58
- [Editing manage levels](#) on page 61
- [Creating mapping rules for IT operating data](#) on page 64
- [Entering IT operating data](#) on page 65
- [Assigning account definitions to identities](#) on page 67
- [Assigning account definitions to Active Directory domains](#) on page 74

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

Related topics

- [Main data for account definitions](#) on page 59
- [Editing account definitions](#) on page 58
- [Assigning manage levels to account definitions](#) on page 62

Editing account definitions

You can edit the main data of account definitions.

To edit an account definition

1. In the Manager, select the **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 59
- [Creating account definitions](#) on page 58
- [Assigning manage levels to account definitions](#) on page 62

Main data for account definitions

Enter the following data for an account definition:

Table 8: Main data for an account definition

Property	Description
Account definition	Account definition name.
User account table	<p>Table in the One Identity Manager schema that maps mailboxes, mail users or mail contacts.</p> <p>For Microsoft Exchange mailboxes, select EX0Mailbox. For Microsoft Exchange mail users, select EX0MailUser. For Microsoft Exchange mail contacts, select EX0MailContact.</p>
Target system	Target system to which the account definition applies.
Required account definition	<p>Specifies the required account definition. Define the dependencies between account definitions. When this account definition is requested or assigned, the required account definition is assigned automatically.</p> <p>Enter the account definition of the associated Active Directory domain.</p>
Description	Text field for additional explanation.
Manage level (initial)	Manage level to use by default when you add new mailboxes, 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

Property	Description
	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	<p>Specifies the account definition assignment to permanently deactivated identities.</p> <p>Option set: The account definition assignment remains in effect. The mail user or mail contact or the mailbox 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 or the associated mailbox 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 or the mailbox 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 or the associated mailbox 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 or the mailbox 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 or the associated mailbox is disabled.</p>
Retain account definition on security risk	Specifies the account definition assignment to identities posing a security risk.

Property	Description
	Option set: The account definition assignment remains in effect. The email user or mail contact or the mailbox remains intact. Option not set (default): The account definition assignment is not in effect. The associated mail user or the associated mail contact or the associated mailbox is disabled.
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 **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 63
- [Creating manage levels](#) on page 62
- [Assigning manage levels to account definitions](#) on page 62


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 **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 63
- [Editing manage levels](#) on page 61
- [Assigning manage levels to account definitions](#) on page 62

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 **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 9: 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 permanently disabled	Specifies whether user accounts of permanently deactivated 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.

- Microsoft Exchange mailbox database

To create a mapping rule for IT operating data

1. In the Manager, select the **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.

To change the mail template, in the Designer, adjust the **TargetSystem | ADS | Exchange2000 | Accounts | MailTemplateDefaultValues** configuration parameter.

5. Save the changes.

Related topics

- [Entering IT operating data](#) on page 65

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 domain A. In addition, certain identities in department A obtain administrative user accounts in the domain A.

Create an account definition A for the default user account of the domain A and an account definition B for the administrative user account of domain 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 domain 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

- Click → next to the field.
 - Under **Table**, select the table that maps the target system for select the TSBAccountDef table or an account definition.
 - Select the specific target system or account definition under **Effects on**.
 - 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 64

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 **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 68
- [Assigning account definitions to business roles](#) on page 69
- [Assigning account definitions to all identities](#) on page 70
- [Assigning account definitions directly to identities](#) on page 70
- [Assigning account definitions to Active Directory domains](#) on page 74

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 **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 69
- [Assigning account definitions to all identities](#) on page 70
- [Assigning account definitions directly to identities](#) on page 70

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 **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 68
- [Assigning account definitions to all identities](#) on page 70
- [Assigning account definitions directly to identities](#) on page 70

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 **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 68
- [Assigning account definitions to business roles](#) on page 69
- [Assigning account definitions directly to identities](#) on page 70

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 **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 68
- [Assigning account definitions to business roles](#) on page 69
- [Assigning account definitions to all identities](#) on page 70

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 **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 **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 **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 **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 59
- [Assigning account definitions to departments, cost centers, and locations](#) on page 68
- [Assigning account definitions to business roles](#) on page 69
- [Assigning account definitions directly to identities](#) on page 70
- [Assigning account definitions to system roles](#) on page 71

Assigning account definitions to Active Directory domains

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 domain in the **Active Directory > Domains** category.
2. Select the **Change main data** task.
3. On the **Exchange** tab, enter the account definition.
 - a. From the **Mailbox definition (initial)** menu, select the account definitions for user mailboxes.
 - b. From the **Mail contact definition (initial)** menu, select the account definition for mail contacts.
 - c. From the **Mail user definition (initial)** menu, select the account definition for mail users.
4. Save the changes.

Related topics

- [Assigning account definitions to identities](#) on page 67

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 **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 **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 **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 **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 **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 **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 domain in the **Active Directory > Domains** 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 **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 Microsoft Exchange

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 Microsoft Exchange organizations in One Identity Manager.

Define additional application roles if you want to limit the permissions for target system managers to individual Microsoft Exchange organizations. 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 Microsoft Exchange organizations 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 Microsoft Exchange organizations.

Table 10: Default application roles for target system managers

User	Tasks
Target system managers	<p>Target system managers must be assigned to the Target systems Exchange 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.• 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.

User	Tasks
	<ul style="list-style-type: none"> • 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** 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 **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 Microsoft Exchange organizations

1. Log in to the Manager as a target system manager.
2. Select the **Active Directory > Exchange system administration** category.
3. Select the **Change main data** task.
4. On the **General** tab, select the application role in the **Target system manager** menu.

- OR -

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

- a. Enter the application role name and assign the **Target systems | Exchange** parent application role.

- b. Click **OK** to add the new application role.
5. Save the changes.

Related topics

- [One Identity Manager users for managing Microsoft Exchange](#) on page 9
- [Microsoft Exchange organizations](#) on page 86

Job server for Microsoft Exchange-specific process handling

Servers must be informed of your server functionality in order to handle Microsoft Exchange-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 **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 **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 80
- [Specifying server functions](#) on page 82

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 11: Job server properties

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

Property	Meaning
	<p>that exists physically and where the processes are handled.</p> <p>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.</p>
Queue	Name of the queue to handle the process steps. The process steps are requested by the Job queue using this queue identifier. The queue identifier is entered in the One Identity Manager Service configuration file.
Server operating system	Operating system of the server. This input is required to resolve the path name for replicating software profiles. The values Win32 , Windows , Linux , and Unix are permitted. If no value is specified, Win32 is used.
Service account data	One Identity Manager Service user account information. In order to replicate between non-trusted systems (non-trusted domains, Linux server), the One Identity Manager Service user information has to be declared for the servers in the database. This means that the service account, the service account domain, and the service account password have to be entered for the server.
One Identity Manager Service installed	<p>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.</p> <p>The option is not automatically removed. If necessary, you can reset this option manually for servers whose queue is no longer enabled.</p>
Stop One Identity Manager Service	<p>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.</p> <p>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>.</p>
Paused due to unavailability of	Specifies whether task processing for this queue has

Property	Meaning
a target system	<p>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.</p> <p>For more information about offline mode, see the <i>One Identity Manager Target System Synchronization Reference Guide</i>.</p>
No automatic software update	<p>Specifies whether to exclude the server from automatic software updating.</p> <p>NOTE: Servers must be manually updated if this option is set.</p>
Software update running	Specifies whether a software update is currently running.
Server function	Server functionality in One Identity Manager. One Identity Manager processes are handled with respect to the server function.

Related topics

- [Specifying server functions](#) on page 82

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 12: Permitted server functions

Server function	Remark
Active Directory connector	Server on which the Active Directory connector is installed. This server synchronizes the Active Directory target system.
CSV connector	Server on which the CSV connector for synchronization is installed.
Domain controller	The Active Directory domain controller. Servers that are

Server function	Remark
	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.
Microsoft Exchange connector	Server on which the Microsoft Exchange connector is installed. This server synchronizes the Microsoft Exchange target system.
Microsoft Exchange server	This is a Microsoft Exchange Server.
Update server	<p>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.</p> <p>The server with the One Identity Manager database installed on it is labeled with this functionality during initial installation of the schema.</p>
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.

Server function	Remark
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.
Windows PowerShell connector	The server can run Windows PowerShell version 3.0 or later.

Related topics

- [General main data for Job servers](#) on page 80

Microsoft Exchange structure

Structure elements in Microsoft Exchange that are not server dependent are matched by each Microsoft Exchange Server. This affects the organization, global address lists, offline address lists, and folders. Double entries are avoided by running a check routine immediately before entry in the One Identity Manager database. Microsoft Exchange structure objects below server level are only matched by the respective server itself. This affects mailbox databases and public folder databases.

The names and frequency of the structure objects listed below can vary depending on the version of the Microsoft Exchange server in use.

NOTE: The system information for the Microsoft Exchange structure is loaded into the One Identity Manager database during data synchronization. It is not possible to customize this system information in One Identity Manager due to the complex dependencies and far reaching effects of changes.

Detailed information about this topic

- [Microsoft Exchange organizations](#) on page 86
- [Microsoft Exchange mailbox databases](#) on page 88
- [Microsoft Exchange address lists](#) on page 90
- [Microsoft Exchange public folders](#) on page 92
- [Microsoft Exchange mailbox server](#) on page 93
- [Microsoft Exchange data availability groups](#) on page 94
- [Share policies](#) on page 95
- [Retention policies](#) on page 96
- [Mobile device mailbox policy](#) on page 97
- [Folder administration policies](#) on page 98
- [Role assignment policies](#) on page 99
- [Outlook Web App mailbox policy](#) on page 100
- [Address book policies](#) on page 101
- [Synchronizing single objects](#) on page 48

Microsoft Exchange organizations


A Microsoft Exchange organization is specified during installation of the Microsoft Exchange server. The global settings for message delivery are not made in One Identity Manager.

To edit organization main data

1. In the Manager, select the **Active Directory > Exchange system administration** category.
2. Select the organization from the result list.
3. Select the **Change main data** task.
4. Save the changes.

The following main data is displayed:

Table 13: Organization main data

Property	Description
Name	Name of the organization.
Distinguished name	Distinguished name of the organization.
Canonical name	Canonical of the organization.
Administrative description	An administrative description about the organization.
LDAP Path	Path to the organization in LDAP notation.
Exchange version	Version of Microsoft Exchange implemented.
Forest	The name of the forest to which the domain belongs.
Organization in mixed mode	Specifies whether the organization operates in mixed or unified mode.
Target system manager	<p>Application role in which target system managers are specified for the organization. Target system managers only edit the organization objects assigned to them. Therefore, each organization can have a different target system manager assigned to it.</p> <p>Select the One Identity Manager application role whose members are responsible for administration of this organization. Use the  button to add a new application role.</p>
Synchronized by	Type of synchronization through which the data is synchronized between the organization and One Identity Manager. You can no longer change the synchronization type once objects for this organization are present in One Identity Manager.

Property	Description
	When you create a organization with the Synchronization Editor, One Identity Manager is used.

Table 14: Permitted values

Value	Synchronization by	Provisioned by
One Identity Manager	Microsoft Exchange connector	Microsoft Exchange connector
No synchronization	None	none

NOTE: If you select **No synchronization**, you can define custom processes to exchange data between One Identity Manager and the organization.

Related topics

- [Target system managers for Microsoft Exchange](#) on page 77
- [Displaying hierarchical address books](#) on page 87
- [Synchronizing single objects](#) on page 48

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?view=exchserver-2019>.

The hierarchy structure is based on the Active Directory group hierarchy. The Active Directory group that represents the root of the hierarchical address book is linked to the Microsoft Exchange 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.
- **Simple display:** If no phonetic display name is entered, sorting is done according to the display name.
- **Alias:** If no simple display name is entered, the alias is used for sorting.

To display the hierarchical address book

1. In the Manager, select the **Active Directory > Exchange system administration** category.
2. Select the organization from the result list.
3. Select the **Show hierarchical address book** report.

Related topics

- [Main data for Microsoft Exchange mail-enabled distribution groups](#) on page 139
- [General main data for Microsoft Exchange mailboxes](#) on page 106
- [Main data for Microsoft Exchange mail users](#) on page 125
- [Main data for Microsoft Exchange mail contacts](#) on page 131

Microsoft Exchange mailbox databases

Mailbox data such as messages received, attachments, folders, documents is stored in the mailbox database.

To display mailbox database main data

1. In the Manager, select the **Active Directory > Exchange system administration > <organization> > Organization configuration > Mailbox databases** category.
2. Select a mailbox database in the result list.
3. Select the **Change main data** task.

To display the mailbox server of a mailbox database main data

1. In the Manager, select the **Active Directory > Exchange system administration > <organization> > Organization configuration > Mailbox databases** category.
2. Select a mailbox database in the result list.
3. Select the **Change main data** task.

The following main data is displayed:

Table 15: Mailbox database main data

Property	Description
Exchange organization	Name of the organization.

Property	Description
Name	Name of the mailbox database.
Administrative description	Administrative description of the mailbox database.
Master	Specifies where to find the mailbox database master. A server or a database availability group can be entered.
Master type	Type of mailbox database master.
Exchange database	Storage location of the server.
Store	Name of the storage group.
Public folder database	Name of the public folder database.
Offline address list	Name of the default offline address list.
Store deleted mailboxes [days]	Number of days the deleted mailboxes stay on the server before they are finally removed.
Store deleted objects [days]	Number of days the deleted objects (email message for example) remain on the server before being removed.
Warn at [KB]	Global setting for the maximum size of mailboxes in KB. If this size is exceeded the user is sent a warning that messages must be deleted in the archive mailbox.
Prohibit send at [KB]	Global setting for the 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.
Prohibit transfer at [KB]	Global setting for the size of mailboxes in KB above which, sending, and receiving messages is prohibited.
Warning interval	Interval for warnings for mailbox databases.
Do not delete permanently before a backup is made	Specifies whether objects are allowed to be deleted after a final backup is run.
Journal recipient	All messages sent using the mailbox database are logged in this mailbox or distribution group.

Property	Description
Maintenance schedule	Maintenance schedule for the database.
Mounted	Status of the database. Specifies whether the database is linked in or not.
Circular logging	Specifies whether the log data are reused or new.
Recovery	Specifies whether the database is a recovery database.
Exclude from mailbox provisioning load balancing	Specifies whether to permanently exclude the database from the mailbox provisioning load balancing that randomly and evenly distributes new mailboxes among available databases.
Temporarily exclude from mailbox provisioning load balancing	Specifies whether to temporarily exclude the database from the mailbox provisioning load balancing that randomly and evenly distributes new mailboxes among available databases.

Microsoft Exchange address lists

Microsoft Exchange offers you the possibility to manage address lists for your Microsoft Exchange organization. Members in address lists can be mailboxes, mail users, mail contacts or email enabled distribution groups and email enabled public folders. Offline address lists allow a mailbox user to get the address list data and work with it offline.

To display address list main data

1. In the Manager, select the **Active Directory > Exchange system administration > <organization> > Organization configuration > Address lists** category.
2. Select the address list in the result list.
3. Select the **Change main data** task.

The following main data is displayed:

Table 16: Address list main data

Property	Description
Exchange organization	Name of the organization.
Name	Address list name.
Parent address list	Name of the parent address list.

Property	Description
Display name	Display name of the address list. This name is used to display the address lists in clients, for example, Outlook.
Administrative description	Administrative description of the mailbox database.
Container	Container for the address list.
Condition	Additional condition for the filter rule.
Filter rules	Filter rules for finding members in the address list.
Global address list	Specifies whether the list is global.
All recipient types	Specifies whether all recipient types are permitted in the address list.
User mailboxes	Specifies whether user mailboxes are permitted in the address list.
Mail users	Specifies whether mail users are permitted in the address list.
Mail contacts	Specifies whether mail contacts are permitted in the address list.
Mail-enabled distribution groups	Specifies whether mail-enabled distribution groups are permitted in the address list.
Resource mailboxes	Specifies whether resource mailboxes are permitted in the address list.
None	Specifies whether any recipients are permitted in the address list.

To display main data of an offline address list

1. In the Manager, select the **Active Directory > Exchange system administration > <organization> > Organization configuration > Offline address lists** category.
2. Select the offline address list in the result list.
3. Select the **Change main data** task.

Table 17: Offline address list main data

Property	Description
Exchange organization	Name of the organization.
Name	Name of the offline address list.
Administrative description	Administrative description of the offline address list.
Default offline address list	Labels this as a default offline address list.

Property	Description
Server	Microsoft Exchange server where the offline address list is stored.
Supports Outlook	Information about which Outlook versions are supported.
Schedule	Update interval for the offline address list.

Microsoft Exchange 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.

To display public folder main data

1. In the Manager, select the **Active Directory > Exchange system administration > <organization> > Organization configuration > Public folders** category.
2. Select the public folder in the result list.
3. Select the **Change main data** task.

The following main data is displayed:

Table 18: Public folder main data

Property	Description
Exchange organization	Name of the organization.
Name	Name of the public folder.
Parent public folder	Name of the parent public folder.
Path	Name of the public folder including path.
Read state per user	Specifies whether information about read and unread messages is tracked per user.

To display main data of a public folder

1. In the Manager, select the **Active Directory > Exchange system administration > <organization> > Organization configuration > Public folder database** category.
2. Select the public folder database in the result list.
3. Select the **Change main data** task.

The following main data is displayed:

Table 19: Main data for a public folder database

Property	Description
Exchange organization	Name of the organization.
Name	Name of the database.
Administrative description	Administrative description of the database.
Store	Name of the storage group.
Servers	If this is a copy of the database, the server on which the original copy is to be found is entered here.
Mounted	Status of the database. Specifies whether the database is linked in or not.
Replication interval [min]	Interval for replication the database in minutes.
Max. send size [KB]	Maximum size for replicated messages in KB.
Max. element size [KB]	Maximum size of elements in KB.
Warn at [KB]	Setting for the maximum size of the database in KB. A warning is sent if this size is exceeded.
Provisioning prohibited at [KB]	Setting for the size of messages in KB. Messages that exceed this size cannot be published.
Database path	Storage location of the server.
Folders expire after [days]	Expiry data for folders in this public folder store in days.
Store deleted objects [days]	Number of days the deleted objects (messages, for example) remain on the server before being removed.
Do not delete permanently before a backup is made	Specifies whether objects are allowed to be deleted after a final backup is run.
Distinguished name	Old style distinguished name of the database.
Circular logging	Specifies whether the log data are reused or new.

Microsoft Exchange mailbox server

The mailbox server is responsible for client processing. There is a copy of the mailbox database on the mailbox server.

To display server main data

1. In Manager, select the category **Active Directory > Exchange system administration > <organization> > Server configuration**.
2. Select the server in the result list.
3. Select the **Change main data** task.

To display a mailbox server's mailbox database.

1. In Manager, select the category **Active Directory > Exchange system administration > <organization> > Server configuration**.
2. Select the server in the result list.
3. Select the **Display mailbox database** task.

The following main data is displayed:

Table 20: Server main data

Property	Description
Exchange organization	Name of the organization.
Active Directory computers	Computer on which the Microsoft Exchange server is installed.
Server	Name of the server.
Distinguished name	Distinguished name of the server.
Function	Microsoft Exchange server roles of the server.
Exchange version	Installed version of the Microsoft Exchange server.

Microsoft Exchange data availability groups

Database availability groups (DAG) were implemented for increased availability and site resilience.

To display a database availability group

1. In the Manager, select the **Active Directory > Exchange system administration > <organization> > Organization configuration > Database availability groups** category.
2. Select the database availability group in the result list.
3. Select the **Change main data** task.

The following main data is displayed:

Table 21: Database availability group main data

Property	Description
Exchange organization	Name of the organization.
Database availability group	Name of the database availability group.
Administrative description	Administrative description of the mailbox database.

Share policies


Sharing policies are implement 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 Microsoft Exchange organization.

To assign policies to mailboxes

1. In the Manager, select the **Active Directory > Exchange system administration > <organization> > Policies > Share policies** category.
2. Select the policy in the result list.
3. Select the **Assign mailboxes** task.
4. In the **Add assignments** pane, assign mailboxes.

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

To remove an assignment

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

To display main data of a sharing policy

1. In the Manager, select the **Active Directory > Exchange system administration > <organization> > Policies > Share policies** category.
2. Select the policy in the result list.
3. Select the **Change main data** task.

The following main data is displayed:

Table 22: Sharing policy main data

Property	Description
Exchange organization	Name of the organization.

Property	Description
Name	Name of the policy.
Domain share	Domain and action which apply for this sharing policy.
Enabled	Specifies whether the policy is enabled. The calendar and contact data is shared for user accounts in the given domains.
Default	Specifies whether this is a default policy.

Retention policies


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

To assign policies to mailboxes

1. In Manager, select the **Active Directory > Exchange system administration > <organization> > Policies > Retention policies** category.
2. Select the policy in the result list.
3. Select the **Assign mailboxes** task.
4. In the **Add assignments** pane, assign mailboxes.

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

To remove an assignment

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

To display main data of a retention policy

1. In Manager, select the **Active Directory > Exchange system administration > <organization> > Policies > Retention policies** category.
2. Select the policy in the result list.
3. Select the **Change main data** task.

The following main data is displayed:

Table 23: Retention policy main data

Property	Description
Exchange organization	Name of the organization.
Name	Name of the policy.
Administrative description	Administrative description of the policy.

Mobile device mailbox policy


Mailbox policies for mobile devices contain settings that take effect when accessing the Microsoft Exchange organization's data with mobile devices using the Exchange ActiveSync synchronization protocol. The settings include, for example, password requirements, specifications for email attachments, device encryption data and access rules for shares.

To assign policies to mailboxes

1. In Manager, select the **Active Directory > Exchange system administration > <organization> > Policies > Mobile device mailbox policies** category.
2. Select the policy in the result list.
3. Select the **Assign mailboxes** task.
4. In the **Add assignments** pane, assign mailboxes.

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

To remove an assignment

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

To display the main data of a mobile device

1. In Manager, select the **Active Directory > Exchange system administration > <organization> > Policies > Mobile device mailbox policies** category.
2. Select the policy in the result list.
3. Select the **Change main data** task.

The following main data is displayed:

Table 24: Main data of a mailbox policy for mobile devices

Property	Description
Exchange organization	Name of the organization.
Name	Name of the policy.
Default	Specifies whether this is a default policy.
Devices permitted without a full policy	Specifies whether older devices can connect to the Microsoft Exchange server using Exchange ActiveSync.
File sharing	Specifies whether file sharing is permitted.
SharePoint services	Specifies whether access to SharePoint service files is permitted.
Password required	Specifies whether a device password is required.

Property	Description
Encrypt password	Specifies whether device encryption is required.
Simple passwords allowed	Specifies whether a simple password is allowed.
Minimum password length	Minimum length of the password. Minimum number of characters the password must have.
Password cycle	Number of new passwords that a user has to use before an 'old' one can be reused.
Password expiry period	Length of time a password can be used before it expires.
Password restorable	Specifies whether a recovery password is generated that can be used to unlock the device.
Requires alphanumeric characters	Specifies whether alphanumeric characters are expected in the password.
Failed logins	Number of incorrect password attempts. If the user has reached this number the user account is locked.
Lock if inactive for [min]	Number of minutes without activity before the device is locked.
Attachments download permitted	Specifies whether attachments can be automatically downloaded.
Max. mail attachment size	Maximum size of mail attachment that can be automatically downloaded.

Folder administration policies

Mailbox policies for folder management are used to group managed folders together. Managed folders are available in mailboxes when a policy is assigned to a Microsoft Exchange Organization mailbox.

To assign policies to mailboxes

1. In Manager, select the **Active Directory > Exchange system administration > <organization> > Policies > File management policies** category.
2. Select the policy in the result list.
3. Select the **Assign mailboxes** task.
4. In the **Add assignments** pane, assign mailboxes.

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

To remove an assignment

- Select the mailbox and double-click .

5. Save the changes.

To display main data of a folder management policy

1. In the Manager, select the **Active Directory > Exchange system administration > <organization> > Policies > Folder management policies** category.
2. Select the policy in the result list.
3. Select the **Change main data** task.

The following main data is displayed:

Table 25: Main data for a folder management policy

Property	Description
Exchange organization	Name of the organization.
Name	Name of the policy.

Role assignment policies

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

To assign policies to mailboxes

1. In Manager, select the **Active Directory > Exchange system administration > <organization> > Policies > Role assignment policies** category.
2. Select the policy in the result list.
3. Select the **Assign mailboxes** task.
4. In the **Add assignments** pane, assign mailboxes.

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

To remove an assignment

- Select the mailbox and double-click .

5. Save the changes.

To display main data of a role assignment policy

1. In Manager, select the **Active Directory > Exchange system administration > <organization> > Policies > Role assignment policies** category.
2. Select the policy in the result list.
3. Select the **Change main data** task.

The following main data is displayed:

Table 26: Role assignment policy main data

Property	Description
Exchange organization	Name of the organization.
Name	Name of the policy.
Administrative description	Administrative description of the policy.
Description	Detail description of the policy.
Default policy	Specifies whether the policy is the default policy.

Outlook Web App mailbox policy


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

To assign policies to mailboxes

1. In Manager, select the **Active Directory > Exchange system administration > <organization> > Policies > Outlook Web App mailbox policies** category.
2. Select the policy in the result list.
3. Select the **Assign mailboxes** task.
4. In the **Add assignments** pane, assign mailboxes.

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

To remove an assignment

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

To display main data of a role assignment policy

1. In Manager, select the **Active Directory > Exchange system administration > <organization> > Policies > Outlook Web App mailbox policies** category.
2. Select the policy in the result list.
3. Select the **Change main data** task.

Address book policies


Address book policies define which mailboxes from the global address list are visible to users. Address book policies allow the provision of customized address books to users.

To assign policies to mailboxes

1. In Manager, select the **Active Directory > Exchange system administration > <organization> > Policies > Address book policies** category.
2. Select the policy in the result list.
3. Select the **Assign mailboxes** task.
4. In the **Add assignments** pane, assign mailboxes.

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

To remove an assignment

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

To display an address book policy's main data

1. In Manager, select the **Active Directory > Exchange system administration > <organization> > Policies > Address book policies** category.
2. Select the policy in the result list.
3. Select the **Change main data** task.

The following main data is displayed:

Table 27: Password policy main data

Property	Description
Exchange organization	Name of the organization.
Name	Name of the policy.
Administrative description	Administrative description of the policy.

Microsoft Exchange mailboxes

Mailbox-enabled recipients can send, receive, and save messages. Microsoft Exchange recognizes several mailbox types. The mailbox types listed below are supported in One Identity Manager.

Table 28: Supported mailbox types

Mailbox type	Description
User mailbox	User mailboxes are assigned to Active Directory user accounts in a Microsoft Exchange organization.
Equipment mailbox	Equipment mailboxes are resource mailboxes used for planning resources, such as computers or laptops. This mailbox type can only be created for disabled user accounts.
Room mailbox	Room mailboxes are resource mailboxes used for planning meeting locations.
Linked mailbox	Linked mailboxes are assigned to Active Directory user accounts in a trusted domain. This makes the Microsoft Exchange organization available within a domain. Active Directory user accounts in a trusted domain without an Exchange structure can obtain a linked mailbox in this Microsoft Exchange organization. This mailbox type can only be created for disabled user accounts.
Shared mailbox	Shared mailboxes are mailboxes that are used by several users. This mailbox type can only be created for disabled user accounts.
Legacy mailbox	Legacy mailboxes are mailboxes from earlier versions of Microsoft Exchange. These mailboxes are loaded into One Identity Manager by synchronization and cannot be edited.
Discovery mailbox	As from Microsoft Exchange Server 2013 onwards, a discovery mailbox, which is used as the target mailbox for eDiscovery searches in Microsoft Exchange, is created by default. These mailboxes are loaded into One Identity Manager by synchronization and cannot be edited.
Linked room	Linked room mailbox are used for planning meetings, for example, for

Mailbox type	Description
mailbox	conference rooms in Skype for Business. This mailbox type can only be created for disabled user accounts.

Detailed information about this topic

- [Creating Microsoft Exchange mailboxes](#) on page 103
- [Editing main data of Microsoft Exchange mailboxes](#) on page 105
- [General main data for Microsoft Exchange mailboxes](#) on page 106
- [Calendar settings for Microsoft Exchange mailboxes](#) on page 109
- [Limits for Microsoft Exchange mailboxes](#) on page 110
- [Microsoft Exchange mailbox archives](#) on page 112
- [Storage for Microsoft Exchange mailboxes](#) on page 112
- [Features for Microsoft Exchange mailboxes](#) on page 113
- [Booking resources for Microsoft Exchange equipment mailboxes and Microsoft Exchange room mailboxes](#) on page 114
- [Adjusting receive restrictions for Microsoft Exchange mailboxes](#) on page 116
- [Microsoft Exchange mailbox permission: Send on behalf](#) on page 117
- [Microsoft Exchange mailbox permission: Send as](#) on page 118
- [Microsoft Exchange mailbox permission: Full access](#) on page 119
- [Assigning extended properties to Microsoft Exchange mailbox](#) on page 119
- [Microsoft Exchange deactivating mailboxes](#) on page 120
- [Deleting and restoring Microsoft Exchange mailboxes](#) on page 121
- [Synchronizing single objects](#) on page 48

Creating Microsoft Exchange mailboxes


You always create mailboxes for Active Directory user accounts. An Active Directory user account can either have a mailbox or a mail user. If a user account already has a mail user, you must delete the mail user before a mailbox can be set up for the user account.

NOTE: Equipment mailboxes, shared mailboxes and linked mailboxes can only be created for disabled user accounts.

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

- In order to create mailboxes through account definitions, the identity 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 mailboxes is mapped from identity main data using templates.

To create a mailbox

1. In the Manager, select the **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.

To create a mailbox for an Active Directory user account, manually

1. In the Manager, select the **Active Directory > User accounts** category.
2. In the result list, select the user account then select the **Change main data** task.
3. Select the **Create mailbox** task.
4. Enter the following information:
 - **Active Directory user account:** The user account is already selected.
 - **Exchange organization:** The Microsoft Exchange organization is already selected. Check the setting.
 - (Optional) **Mailbox database:** Name of the mailbox database. If empty, Microsoft Exchange decides which mailbox database is used.
 - **Alias:** Unique alias for further identification of the mailbox.
5. Save the changes.

NOTE: Names and occurrences of the listed data and tasks can vary depending on which version of the Microsoft Exchange server is implemented and the type of Microsoft Exchange mailbox.

Detailed information about this topic

- [General main data for Microsoft Exchange mailboxes](#) on page 106
- [Calendar settings for Microsoft Exchange mailboxes](#) on page 109
- [Limits for Microsoft Exchange mailboxes](#) on page 110
- [Microsoft Exchange mailbox archives](#) on page 112
- [Storage for Microsoft Exchange mailboxes](#) on page 112
- [Features for Microsoft Exchange mailboxes](#) on page 113
- [Booking resources for Microsoft Exchange equipment mailboxes and Microsoft Exchange room mailboxes](#) on page 114

Related topics

- [Editing main data of Microsoft Exchange mailboxes](#) on page 105
- [Account definitions for Microsoft Exchange mailboxes, mail users, and mail contacts](#) on page 57
- [Microsoft Exchange deactivating mailboxes](#) on page 120
- [Deleting and restoring Microsoft Exchange mailboxes](#) on page 121
- [Deleting and restoring Microsoft Exchange mail users](#) on page 129

Editing main data of Microsoft Exchange mailboxes

NOTE: Names and occurrences of the listed data and tasks can vary depending on which version of the Microsoft Exchange server is implemented and the type of Microsoft Exchange mailbox.

To edit a mailbox

1. In the Manager, select the **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.

Detailed information about this topic

- [General main data for Microsoft Exchange mailboxes](#) on page 106
- [Calendar settings for Microsoft Exchange mailboxes](#) on page 109
- [Limits for Microsoft Exchange mailboxes](#) on page 110
- [Microsoft Exchange mailbox archives](#) on page 112
- [Storage for Microsoft Exchange mailboxes](#) on page 112
- [Features for Microsoft Exchange mailboxes](#) on page 113
- [Booking resources for Microsoft Exchange equipment mailboxes and Microsoft Exchange room mailboxes](#) on page 114

Related topics

- [Account definitions for Microsoft Exchange mailboxes, mail users, and mail contacts](#) on page 57
- [Microsoft Exchange deactivating mailboxes](#) on page 120
- [Deleting and restoring Microsoft Exchange mailboxes](#) on page 121

General main data for Microsoft Exchange mailboxes

Enter the following general main data.

Table 29: Mailbox general main data

Property	Description
Identity	<p>Identity using the mailbox.</p> <ul style="list-style-type: none">• An identity is already entered if the mailbox was generated by an account definition.• If you create the mailbox 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 mailbox, the mailbox might be locked or deleted depending on the configuration.</p>
No link to an identity required	<p>Specifies whether the mailbox 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 mailbox. 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 mailbox was created.</p> <p>Use the account definition to automatically populate mailbox main data and to specify a manage level for the mailbox.</p> <p>One Identity Manager finds the IT operating data of the assigned identity and uses it to populate the corresponding fields in the mailbox.</p> <p>NOTE: The account definition cannot be changed once the mailbox has been saved.</p>

Property	Description
Manage level	Manage level with which the mailbox 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.
Active Directory user account	Active Directory user account that uses this mailbox.
Linked mailbox	External Active Directory user account that has access to the Exchange organization through this mailbox. A linked mailbox is only permitted for mailboxes with the linked mailbox mailbox type. The linked mailbox itself is disabled. Disabling in Active Directory is done by the One Identity Manager Service. After the next synchronization, the linked mailbox is also disabled in the One Identity Manager database.
Exchange organization	Name of the Microsoft Exchange organization.
Canonical name	Mailbox's canonical name. The canonical name is generated automatically.
Mailbox type	Type of mailbox. Available mailbox types are: User, Room, Equipment, Linked, Legacy, Shared, Discovery, and Linked room.
Alias	Unique alias for further identification of the mailbox.
Mailbox database	<p>Name of the mailbox database. Mailbox data is stored in the mailbox database (messages received, attachments, folders, documents). The mailbox database for user mailboxes is determined from the current IT operating data for the assigned identity depending on the mailbox manage level.</p> <p>This data is optional. If empty, Microsoft Exchange automatically decides which mailbox database to use.</p>
Automatically update based on recipient policy	Specifies whether changes to recipient's email addresses are automatically updated based on recipient policies.
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>
Sender authentication required	Specifies whether authentication data is requested from senders. Set this option to prevent anonymous senders mailing to the mailbox.

Property	Description
Max. number of recipients	Maximum number of recipients to which the mailbox user can send messages. If there is no limit, the global setting for Microsoft Exchange organization message delivery in the Microsoft Exchange System Manager.
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.
Simple display name	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 simple 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>
Folder policy	Mailbox policy for folder administration.
Role assignment policy	Role assignment policy which applies for this mailbox.
Sharing policy	Sharing policy which applies for this mailbox.
Outlook Web App mailbox policy	Outlook Web App mailbox policy, which applies to this mailbox.
Address book policy	Address book policy to apply to this mailbox.
Mailbox is locked	Specifies whether the mail box is locked.

Property	Description
Do not display in address list	Specifies whether the mailbox is visible in address books. Enable this option if you want to prevent the mailbox from being displayed in address books. This option applies to all address books.
Distinguished name	Active Directory user account's distinguished name.
Distinguished Exchange name	Mailbox's distinguished name.

Related topics

- [Account definitions for Microsoft Exchange mailboxes, mail users, and mail contacts](#) on page 57
- [Share policies](#) on page 95
- [Folder administration policies](#) on page 98
- [Role assignment policies](#) on page 99
- [Address book policies](#) on page 101
- [Microsoft Exchange deactivating mailboxes](#) on page 120
- [Microsoft Exchange mailbox databases](#) on page 88

Calendar settings for Microsoft Exchange mailboxes

You can enable the Calendar Attendant to automatically update changes to meeting data, such as meeting times or responses from attendees in the calendar. Enter the following calendar settings.

Table 30: Mailbox calendar settings

Property	Description
Enable Calendar Attendant	<p>Specifies whether the Calendar Attendant is enabled for mailboxes. Other settings become available once the Calendar Attendant is enabled.</p> <p>Permitted values are:</p> <ul style="list-style-type: none"> • Calendar Attendant not enabled: The calendar attendant is not activated. • Calendar Attendant enabled: The calendar attendant is activated.

Property	Description
	<ul style="list-style-type: none"> • Resource booking attendant enabled: The resource booking attendant is automatically enabled for mailboxes of type Room.
New meeting requests are marked with the status "tentative".	Specifies whether meeting requests are automatically entered in the calendar with the Tentative status.
Permit meeting requests from external senders	Specifies whether meeting requests from external senders are entered in the calendar.
Delete expired meeting requests	Specifies whether to automatically delete old meeting requests from the calendar.
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.

Related topics

- [Booking resources for Microsoft Exchange equipment mailboxes and Microsoft Exchange room mailboxes](#) on page 114

Limits for Microsoft Exchange mailboxes

Enter the following mailbox limits.

Table 31: Limits for a mailbox

Property	Description
Number of saved messages	Number of saved messages. This data is determined through synchronization and cannot be edited manually.
Used disk space [byte]	Used disk space in bytes. This data is determined through synchronization and cannot be edited manually.
Max. send size [KB]	Maximum size for message in KB that a mailbox can send. The Microsoft Exchange organization global settings in the Microsoft Exchange System Manager come into effect for message delivery if there are no limitations.
Max. receiving	Maximum size for message in KB that a mailbox can receive. The

Property	Description
size [KB]	Microsoft Exchange organization global settings in the Microsoft Exchange System Manager come into effect for message delivery if there are no limitations.
Use default database values	Specifies whether the mailbox database limits are used. Option set: Mailbox database limits are in use. Option not set: Mailbox database limits are not in use.
Prohibit transfer at [KB]	Size of mailboxes in KB above which, sending, and receiving messages is 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.
Use default retention settings	Specifies whether to use the mailbox's default retention settings. Option set: Mailbox database default settings are in use. Option not set: Mailbox database default settings are not in use.
Store deleted objects [days]	Number of days the deleted objects (email message for example) remain on the server before being removed.
Do not delete permanently before a backup is made	Specifies whether objects are allowed to be deleted after a final backup is run.
Max. number subfolders	Maximum number of subfolders allowed in a mailbox.
Warn at [subfolder]	Number of subfolders which can be created in a mailbox before the user is sent a warning.
Max. folder levels	Maximum number of levels in the mailbox folder structure.
Warn at [folder levels]	Number of folder levels which can be created before the user is sent a warning.
Max. recoverable items	Maximum number of messages allowed in a folder in the Recoverable items folder.
Warn at [recoverable items]	Number of items a folder in the Recoverable items folder can contain before a warning is sent to the user.

Related topics

- [Microsoft Exchange mailbox databases](#) on page 88

Microsoft Exchange mailbox archives

You can configure personal archives with which users can save messages in an archive mailbox. Enter the following main data:

Table 32: Archiving a mailbox

Property	Description
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 mailbox database	Name of the archive mailbox database.
Archive name	Name of the archive.
Max. size of archive [MB]	Maximum size in MB that the personal archive of a mailbox may reach.
Archive warning from [MB]	Maximum size in MB of the archive mailbox. If this size is exceeded, the user is sent a warning that messages must be deleted in the archive mailbox.

Storage for Microsoft Exchange mailboxes

Enter the following main data of mailbox retention.

Table 33: Mailbox retention main data

Property	Description
Retention policy	Retention policy applying to this mailbox.
Retention 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

Property	Description
	Start date and End date fields.
Start date	Start date on which to stop retention actions.
End date	Date on which to end retention actions.
Litigation hold	Specifies whether mailbox retention is mandatory.
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.
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.
Single item recovery	Specifies whether single item recovery is enabled.

Related topics

- [Retention policies](#) on page 96

Features for Microsoft Exchange mailboxes

Set up the following features of the mailbox.

Table 34: Mailbox features

Property	Description
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.
Mobile device mailbox policy	Mailbox policy for mobile email queries. Mailbox policies for mobile devices contain settings that take effect when accessing the Microsoft Exchange organization's data with mobile devices using the Exchange ActiveSync synchronization protocol.
MAPI enabled	Specifies whether MAPI access is enabled. MAPI allows mailbox access through a MAPI client, like Outlook.

Property	Description
POP3 enabled	Specifies whether POP3 access is enabled.
IMAP4 enabled	Specifies whether IMAP4 access is enabled.

Related topics

- [Mobile device mailbox policy](#) on page 97

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

You can configure booking and planning of resources for equipment and room mailboxes. Enter the following main data:

Table 35: Main data for booking resources

Property	Description
Enable Calendar Attendant	<p>Specifies whether the Resource Booking Attendant is enabled for device mailboxes and room mailboxes so that booking requests can be processed automatically.</p> <p>Permitted values are:</p> <ul style="list-style-type: none"> • Calender Attendant not enabled: The calendar attendant is not activated. • Calender Attendant enabled: The calendar attendant is activated. • Resource booking attendant enabled: The resource booking attendant is automatically enabled for mailboxes of type Room.
Reject repeated meeting after max. planning period	Specifies whether booking series can be set up beyond the planning period.
Forward meeting requests	Specifies whether meeting requests are forwarded to the resource mailbox deputy managers. The deputy decides about the meeting request.

Property	Description
Max. booking window [days]	Maximum planning period for meeting request in days.
Max. duration [min]	Maximum time allowed booking the resource.
Max. conflicting instances	Maximum conflicts permitted for meeting series which overlap with other meetings. If the value is exceeded, the series request is denied.
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.
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.
Add organizer's name to subject	Specifies whether the organizer's name is given in the meeting request's subject field.
Remove "private" flag from accepted meeting	Specifies whether the Private status is deleted from meeting requests.
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.
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.
Booking permissions for everyone	Specifies whether meeting requests conforming to policy are automatically approved for all users.

Property	Description
	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.
Booking permissions for everyone	Specifies whether all users can send booking requests that conform to policy. 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.
Out-of-policy request permissions for everyone	Specifies whether all user can send meeting requests that do not conform to policy. These requests are decided by the mailbox deputy. 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.
Allow conflicts	Specifies whether conflicting meeting requests are allowed.
Allow reoccurring requests	Specifies whether a series of meetings is allowed.
Request only possible during working hours	Specifies whether the resource can be booked during working hours or outside them, as well.
Resource capacity	Resource capacity, for example, the number of seats in a meeting room.

Related topics

- [Microsoft Exchange mailbox permission: Send on behalf](#) on page 117

Adjusting receive restrictions for Microsoft Exchange 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 customize mail acceptance for mailboxes

1. In the Manager, select the **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

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.

Microsoft Exchange mailbox permission: Send on behalf

You use the **Send on behalf** mailbox 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 **Active Directory > Mailboxes** category.
2. Select a mailbox in the result list.
3. Select the task **Assign sending on behalf permissions**.
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.

Related topics

[Microsoft Exchange mailbox permission: Send as](#) on page 118

[Microsoft Exchange mailbox permission: Full access](#) on page 119

Microsoft Exchange mailbox permission: Send as

Further configuration of mailbox permissions is required in the synchronization project. For more information, see [Customizing synchronization projects for send permissions and full access permissions](#) on page 36.

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 **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:
 - Active Directory user accounts
 - 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.

Related topics

- [Microsoft Exchange mailbox permission: Send on behalf](#) on page 117
- [Microsoft Exchange mailbox permission: Full access](#) on page 119

Microsoft Exchange mailbox permission: Full access

Further configuration of mailbox permissions is required in the synchronization project. For more information, see [Customizing synchronization projects for send permissions and full access permissions](#) on page 36.


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 **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:
 - Active Directory user accounts
 - 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.

Related topics

- [Microsoft Exchange mailbox permission: Send on behalf](#) on page 117
- [Microsoft Exchange mailbox permission: Send as](#) on page 118

Assigning extended properties to Microsoft Exchange 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.

To specify extended properties for a mailbox

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

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

Microsoft Exchange deactivating mailboxes

How you deactivate mailboxes depends on the type of mailbox administration. When you deactivate a mailbox, the **Do not display in address list** option is enabled and the mailbox is no longer shown in address books.

Scenario:

Mailboxes are managed through account definitions.

Mailboxes managed through account definitions are disabled when the identity is temporarily or permanently disabled. The behavior depends on the mailbox's manage level. Mailboxes with the **Full managed** manage level are deactivated depending on the account definition settings. Use the EXOMailbox.IsLocked column to configure the behavior for mailboxes with another manage level.

Scenario:

Mailboxes are not managed through account definitions.

The behavior depends on the **QER | Person | TemporaryDeactivation** configuration parameter

- If the configuration parameter is set, mailboxes for an identity are disabled if the identity is temporarily or permanently disabled.
- If the configuration parameter is not set, the identity data does not have any effect on the linked mailboxes.

To lock a mailbox when the configuration parameter is not set

1. In the Manager, select the **Active Directory > Mailboxes** category.
2. Select a mailbox in the result list.
3. Select the **Change main data** task.
4. Set the **Mailbox is disabled** option on the **General** tab.
5. Save the changes.

Scenario:

Mailboxes not linked to identities.

To lock a mailbox, which is not linked to an identity

1. In the Manager, select the **Active Directory > Mailboxes** category.
2. Select a mailbox in the result list.
3. Select the **Change main data** task.
4. Set **Mailbox is disabled** on the **General** tab.
5. Save the changes.

Related topics

- [Creating account definitions](#) on page 58
- [Creating manage levels](#) on page 62
- [Deleting and restoring Microsoft Exchange mailboxes](#) on page 121


Deleting and restoring Microsoft Exchange mailboxes

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


When you delete a mailbox, the **Do not display in address lists** option is enabled and the mailbox is no longer shown in address books. The settings **Use default database values**, **Max. send size [KB]**, **Max. receiving size [KB]**, **Prohibit transfer above [KB]**, and **Prohibit send at [KB]** are reset, so that no email messages can be sent or received with this mailbox.

To delete a mailbox

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

To restore a mailbox

1. In the Manager, select the **Active Directory > Mailboxes** category.
2. Select a mailbox in the result list.
3. Click  in the result list.

Configuring deferred deletion

By default, mailboxes are finally deleted from the database after 30 days. During this period you have the option to reactivate the mailboxes. A restore is not possible once deferred deletion has expired.

In the Designer, you can set an alternative delay on the EX0MailContact table. For more information about configuring deferred deletion, see the *One Identity Manager Configuration Guide*.

Related topics

- [Microsoft Exchange deactivating mailboxes](#) on page 120

Microsoft Exchange mail users and Microsoft Exchange mail contacts

Mail-enabled recipients obtain data about users from outside the Microsoft Exchange organization. There is at least one email address defined for a mail recipient. Notification is automatically forwarded to this email address. You can manage mail-enabled One Identity Manager user accounts (mail users) and mail-enabled Active Directory contacts (mail contacts) in Active Directory.

Detailed information about this topic

- [Creating Microsoft Exchange mail users](#) on page 123
- [Editing main data of Microsoft Exchange mail users](#) on page 125
- [Receive restrictions for Microsoft Exchange mail users](#) on page 128
- [Assigning extended properties to Microsoft Exchange mail users](#) on page 128
- [Deleting and restoring Microsoft Exchange mail users](#) on page 129
- [Creating Microsoft Exchange mail contacts](#) on page 130
- [Editing main data of Microsoft Exchange mail contacts](#) on page 131
- [Main data for Microsoft Exchange mail contacts](#) on page 131
- [Receive restrictions for Microsoft Exchange mail contacts](#) on page 134
- [Assigning extended properties to Microsoft Exchange mail contacts](#) on page 135
- [Deleting and restoring Microsoft Exchange mail contacts](#) on page 135
- [Synchronizing single objects](#) on page 48


Creating Microsoft Exchange mail users

Enter mail users for Active Directory user accounts. Active Directory user accounts can either have a mailbox or be mail-enabled. If a user account already has a mailbox, you must delete the mailbox before you set up a mail user for this user account.

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 **Active Directory > Mail users** category.
2. Click  in the result list.
3. On the main data form, enter the main data of the user.
4. Save the changes.

To create a mail user for an Active Directory user account manually

1. In the Manager, select the **Active Directory > User accounts** category.
2. In the result list, select the user account then select the **Change main data** task.
3. Select **Create mail user**.
4. Enter the following information:
 - **Active Directory user account:** The user account is already selected.
 - **Exchange organization:** The Microsoft Exchange organization is already selected. Check the setting.
 - **Destination address type:** Target address type of the email address.
 - **Destination address:** Email address to which the messages should be forwarded.
 - **Alias:** Unique alias for further identification of the mail user.
5. Save the changes.

Related topics

- [Main data for Microsoft Exchange mail users on page 125](#)
- [Editing main data of Microsoft Exchange mail users on page 125](#)
- [Account definitions for Microsoft Exchange mailboxes, mail users, and mail contacts on page 57](#)
- [Deleting and restoring Microsoft Exchange mail users on page 129](#)
- [Deleting and restoring Microsoft Exchange mailboxes on page 121](#)

Editing main data of Microsoft Exchange mail users

To edit a mail user.

1. In the Manager, select the **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

- [Main data for Microsoft Exchange mail users on page 125](#)
- [Account definitions for Microsoft Exchange mailboxes, mail users, and mail contacts on page 57](#)
- [Deleting and restoring Microsoft Exchange mail users on page 129](#)

Main data for Microsoft Exchange mail users

Enter the following general main data.

Table 36: General data of a mail user

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>

Property	Description
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. 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	<p>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.</p>
Active Directory account	<p>Active Directory user account for which the mail user is created.</p>
Exchange organization	<p>Name of the organization.</p>
Canonical name	<p>Canonical name of the mail user. The canonical name is generated automatically.</p>
Destination address	<p>Email address for forwarding messages.</p>
Destination address type	<p>Target address type of the email address. You can also add other mail connectors (e.g. CCMail, MS) apart from the standard destination address type (SMTP, X400).</p>
Alias	<p>Unique alias for further identification of the mail user.</p>
Automatically update based on recipient policy	<p>Specifies whether changes to recipient's email addresses are automatically updated based on recipient policies.</p>

Property	Description
Proxy addresses	<p>Other email addresses for the mail user. 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>
Max. send size [KB]	Maximum size for message in KB that a mail user can send. The Microsoft Exchange organization global settings in the Microsoft Exchange System Manager come into effect for message delivery if there are no limitations.
Max. receiving size [KB]	Maximum size for message in KB that a mail user can receive. The Microsoft Exchange organization global settings in the Microsoft Exchange System Manager come into effect for message delivery if there are no limitations.
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.
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.
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 simple 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>
Distinguished name	Mail user's distinguished name.

Related topics

- [Account definitions for Microsoft Exchange mailboxes, mail users, and mail contacts](#) on page 57

Receive restrictions for Microsoft Exchange mail users


NOTE: The **Assign mail acceptance** and **Assign mail rejection** assignments are mutually exclusive. You can either specify from whom messages are accepted or you can specify from whom they are rejected.

To customize mail acceptance for mail users

1. In the Manager, select the **Active Directory > Mail users** 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
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 extended properties to Microsoft Exchange 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.

To specify extended properties for a mail user

1. In the Manager, select the **Active Directory > Mail users** category.
2. Select the email 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.


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

Deleting and restoring Microsoft Exchange mail users


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.

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.

To delete a mail user

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

To restore a mail user

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

Configuring deferred deletion

By default, mail users are finally deleted from the database after 30 days. During this period you have the option to reactivate the mail users. A restore is not possible once deferred deletion has expired.

In the Designer, you can set an alternative delay on the EX0MailUser table. For more information about configuring deferred deletion, see the *One Identity Manager Configuration Guide*.


Creating Microsoft Exchange mail contacts

Enter mail contacts for Active Directory 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 default email address and obtain their company IT 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 **Active Directory > Mail contacts** category.
2. Click  in the result list.
3. On the main data form, enter the main data of the contact.
4. Save the changes.

To create a mail contact for an Active Directory contact manually

1. In the Manager, select the **Active Directory > Contacts** category.
2. In the result list, select the contact then select the **Change main data** task.
3. Select the **Create mail contact** task.
4. Enter the following information:
 - **Active Directory contact:** the contact is already selected.
 - **Exchange organization:** The Microsoft Exchange organization is already selected. Check the setting.
 - **Destination address type:** Target address type of the email address.
 - **Destination address:** Email address to which the messages should be forwarded.
 - **Alias:** Unique alias for further identification of the mail contact.
5. Save the changes.

Related topics

- [Editing main data of Microsoft Exchange mail contacts](#) on page 131
- [Main data for Microsoft Exchange mail contacts](#) on page 131
- [Deleting and restoring Microsoft Exchange mail contacts](#) on page 135

Editing main data of Microsoft Exchange mail contacts

To edit a mail contact

1. In the Manager, select the **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 Microsoft Exchange mail contacts](#) on page 130
- [Main data for Microsoft Exchange mail contacts](#) on page 131
- [Deleting and restoring Microsoft Exchange mail contacts](#) on page 135

Main data for Microsoft Exchange mail contacts

Enter the following general main data.

Table 37: General data of a mail contact

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</p>

Property	Description
	<p>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	<p>Account definition through which the mail contact was created.</p> <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	<p>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.</p>
Active Directory contact	<p>Active Directory contact for whom the email is created.</p>
Exchange organ-	<p>Name of the organization.</p>

Property	Description
ization	
Canonical name	Canonical name of the mail contact. The canonical name is generated automatically.
Destination address	Email address for forwarding messages.
Destination address type	Target address type of the email address. You can also add other mail connectors (e.g. CCMail, MS) apart from the standard destination address type (SMTP, X400).
Alias	Unique alias for further identification of the mail contact.
Automatically update based on recipient policy	Specifies whether changes to recipient's email addresses are automatically updated based on recipient policies.
Proxy addresses	Other email addresses for the mail contact. 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
Max. send size [KB]	Maximum size for message in KB that a mail contact can send. The Microsoft Exchange organization global settings in the Microsoft Exchange System Manager come into effect for message delivery if there are no limitations.
Max. receiving size [KB]	Maximum size for message in KB that a mail contact can receive. The Microsoft Exchange organization global settings in the Microsoft Exchange System Manager come into effect for message delivery if there are no limitations.
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.
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.
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

Property	Description
	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 simple 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.
Distinguished name	Mail contact's distinguished name.

Related topics

- [Account definitions for Microsoft Exchange mailboxes, mail users, and mail contacts](#) on page 57

Receive restrictions for Microsoft Exchange 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 mail contacts

1. In the Manager, select the **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
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 extended properties to Microsoft Exchange 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.

To specify extended properties for a mail contact

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


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

Deleting and restoring Microsoft Exchange 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 **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**.

To restore a mail contact

1. In the Manager, select the **Active Directory > Mail contacts** category.
2. Select the mail contact in the result list.
3. Click  in the result list.

Configuring deferred deletion

By default, mail contacts are finally deleted from the database after 30 days. During this period you have the option to reactivate the mail contacts. A restore is not possible once deferred deletion has expired.

In the Designer, you can set an alternative delay on the EX0MailContact table. For more information about configuring deferred deletion, see the *One Identity Manager Configuration Guide*.

Microsoft Exchange mail-enabled distribution groups

You can email-enable universal security groups and universal distribution groups to distribute messages to a group of recipients.


Detailed information about this topic

- [Creating Microsoft Exchange mail-enabled distribution groups](#) on page 137
- [Editing main data of Microsoft Exchange mail-enabled distribution groups](#) on page 138
- [Receive restrictions for Microsoft Exchange mail-enabled distribution groups](#) on page 141
- [Microsoft Exchange mail-enabled distribution list: Send on behalf](#) on page 142
- [Microsoft Exchange mail-enabled distribution list: Send as](#) on page 143
- [Specifying Microsoft Exchange mail-enabled distribution groups](#) on page 144
- [Specifying Microsoft Exchange moderated distribution group extensions](#) on page 144
- [Adding a Microsoft Exchange dynamic distribution group to Microsoft Exchange mail-enabled distribution groups](#) on page 146
- [Assigning extended properties to Microsoft Exchange mail-enabled distribution groups](#) on page 146
- [Deleting Microsoft Exchange mail-enabled distribution groups](#) on page 147
- [Synchronizing single objects](#) on page 48

Creating Microsoft Exchange mail-enabled distribution groups

Set up mail-enabled distribution groups for universal security groups and universal distribution groups.

To create a mail-enabled distribution group

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

To create a mail-enabled distribution list for an Active Directory group

1. In the Manager, select the **Active Directory > Groups > Universal groups** category.
2. In the result list, select the group then select the **Change main data** task.
3. Select the **Create mail-enabled distribution list** task.
4. Enter the following information:
 - **Active Directory group:** The group is already selected.
 - **Exchange organization:** The Microsoft Exchange organization is already selected. Check the setting.
 - **Alias:** Unique alias for further identification of the mail-enabled distribution group.
5. Save the changes.

Related topics

- [Editing main data of Microsoft Exchange mail-enabled distribution groups](#) on page 138
- [Main data for Microsoft Exchange mail-enabled distribution groups](#) on page 139

Editing main data of Microsoft Exchange mail-enabled distribution groups

To edit a mail-enabled distribution group

1. In the Manager, select the **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

- [Main data for Microsoft Exchange mail-enabled distribution groups](#) on page 139

Main data for Microsoft Exchange mail-enabled distribution groups

Enter the following general main data.

Table 38: Mail-enabled distribution group main data

Property	Description
Active Directory group	Active Directory group for which the mail-enabled distribution group is created.
Exchange organization	Name of the organization.
Alias	Unique alias for further identification 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	<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 simple 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>
Recipient type (detail)	<p>Name of the recipient type. Permitted values are Mail-enabled non-universal groups, Mail-enabled universal distribution groups, Mail-enabled universal security groups, and Room list.</p> <p>NOTE: When you create a mail-enabled distribution group for room lists, select the Room list value. For all other distribution group types, leave this empty. It is determined and entered by synchronization.</p>

Property	Description
Expansion server	Server on to which to expand the mail-enabled distribution group.
Proxy addresses	<p>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).</p> <p>Use the following syntax to set up other proxy addresses:</p> <p>Address type: new email address</p>
Hierarchical group	Specifies whether the mail-enabled distribution group in the hierarchical address book are used.
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.
Max. send size [KB]	Maximum size of message in KB that a mail-enabled distribution group can send. The Microsoft Exchange organization global settings in the Microsoft Exchange System Manager come into effect for message delivery if there are no limitations.
Max. receiving size [KB]	Maximum size of message in KB that a mail-enabled distribution group can receive. The Microsoft Exchange organization global settings in the Microsoft Exchange System Manager come into effect for message delivery if there are no limitations.
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.
Automatically update based on recipient policy	Specifies whether changes to recipient's email addresses are automatically updated based on recipient policies.
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 sender should receive out-of-office messages.
Add to group	<p>Specifies how users can join the mail-enabled distribution group. Permitted values are:</p> <ul style="list-style-type: none"> • Open: Members can be added to the group without approval.

Property	Description
	<ul style="list-style-type: none"> • 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.
Leave group	<p>Specifies how users can leave the mail-enabled distribution group. Permitted values are:</p> <ul style="list-style-type: none"> • Open: Members can leave the group without approval. • Closed: Members can only leave the group with administrator approval. Requests to leave the group are automatically denied.
Distribution group moderation	<p>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.</p>
Sending message to	<p>Specifies how senders are notified when they send messages to moderated distribution groups. 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.

Receive restrictions for Microsoft Exchange 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 **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
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.

Microsoft Exchange mail-enabled distribution list: Send on behalf

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

To customize permissions for mail-enabled distribution groups

1. In the Manager, select the **Active Directory > Mail-enabled distribution groups** category.
2. Select the mail-enabled distribution group in the result list.
3. Select the **Assign sending on behalf permissions** 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.

Related topics

- [Microsoft Exchange mail-enabled distribution list: Send as](#) on page 143

Microsoft Exchange mail-enabled distribution list: Send as

The synchronization project must be additionally configured for permissions. For more information, see [Customizing synchronization projects for send permissions and full access permissions](#) on page 36.

You use the **Send as** permissions to specify which users can send notifications through a distribution list.

To customize permissions for mail-enabled distribution groups

1. In the Manager, select the **Active Directory > Mail-enabled distribution groups** category.
2. Select the mail-enabled distribution group 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:
 - Active Directory user accounts
 - 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.

Related topics

- [Microsoft Exchange mail-enabled distribution list: Send on behalf](#) on page 142

Specifying Microsoft Exchange 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 **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:
 - Active Directory user accounts
 - Active Directory 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.

Specifying Microsoft Exchange moderated distribution group extensions

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.

Define the moderators of a mail-enabled distribution group. Furthermore, you can specify users whose messages to the moderated distribution group are excluded from moderation.

Read the documentation from your Microsoft Exchange server on the concept of moderated distribution groups.


To specify moderators for mail-enabled distribution groups

1. In the Manager, select the **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.


To exclude users from moderation

1. In the Manager, select the **Active Directory > Mail-enabled distribution groups** category.
2. Select the mail-enabled distribution group in the result list.
3. Select the **Exclude from moderation** 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
 - Dynamic distribution groups
 - Mailboxes
 - Mail users
 - Mail contacts

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.

Adding a Microsoft Exchange dynamic distribution group to Microsoft Exchange mail-enabled distribution groups


Use this task to add dynamic distribution groups to mail-enabled distribution groups.

To add dynamic distribution groups to a mail-enabled distribution group

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

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

To remove an assignment

- Select the distribution group and double-click .
4. Save the changes.

Related topics

- [Adding Microsoft Exchange mail-enabled distribution groups to Microsoft Exchange dynamic distribution groups](#) on page 152

Assigning extended properties to Microsoft Exchange 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.

To specify extended properties for mail-enabled distribution groups

1. In the Manager, select the **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.

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

Deleting Microsoft Exchange mail-enabled distribution groups

The mail-enabled distribution group is permanently from the One Identity Manager database and Microsoft Exchange system.

To delete a mail-enabled distribution group

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

Microsoft Exchange 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.

Detailed information about this topic

- [Main data for Microsoft Exchange dynamic distribution groups](#) on page 148
- [Customizing receive restrictions for Microsoft Exchange dynamic distribution groups](#) on page 150
- [Customizing send permissions for Microsoft Exchange dynamic distribution groups](#) on page 151
- [Adding Microsoft Exchange mail-enabled distribution groups to Microsoft Exchange dynamic distribution groups](#) on page 152

Main data for Microsoft Exchange dynamic distribution groups

Dynamic distribution groups are loaded into the One Identity Manager by synchronization.

To display a dynamic distribution group

1. In the Manager, select the **Active Directory > Exchange system administration > <Organization> > Recipient configuration > Dynamic distribution groups** category.
2. Select the dynamic distribution list in the result list.
3. Select the **Change main data** task.

The following main data is displayed:

Table 39: Dynamic distribution list main data

Property	Description
Exchange organization	Name of the organization.
Expansion server	Server on to which to expand the dynamic distribution group.
Name	Name of the dynamic distribution group.
Alias	Unique alias for further identification of the dynamic distribution group.
Display name	Display name of the dynamic distribution group.
Proxy addresses	Other email addresses for the dynamic distribution group.
Email address	Email addresses of the dynamic distribution group.
Simple display	Simple display name for systems that cannot interpret all the characters of normal display names.
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.
Max. receiving size [KB]	Maximum size of message in KB that a dynamic distribution group can receive. The Microsoft Exchange organization global settings in the Exchange System Manager come into effect for message delivery if there are no limitations.
Container	Active Directory container of the dynamic distribution group.
Domain	Active Directory domain of the dynamic distribution group.
Recipient container	Recipient's root container. The condition for finding distribution group members is applied to the selected recipient container and its sub containers.
All recipient types	Specifies whether all recipient types are permitted in the dynamic distribution group.
User mailboxes	Specifies whether user mailboxes are permitted in the dynamic distribution group.
Mail users	Specifies whether mail users are permitted in the dynamic distribution group.
Mail contacts	Specifies whether mail contacts are permitted in the dynamic distribution group.

Property	Description
Mail-enabled distribution groups	Specifies whether mail-enabled distribution groups are permitted in the dynamic distribution group.
Resource mailboxes	Specifies whether resource mailboxes are permitted in the dynamic distribution group.
None	Specifies whether any recipients are permitted in the dynamic distribution group.
Condition	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.
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.
Automatically update based on recipient policy	Specifies whether changes to recipient's email addresses are automatically updated based on recipient policies.
Only limit messages from authenticated users	Specifies whether authentication data is requested from senders.
Out-of-office message to sender	Specifies whether the message sender should receive out-of-office messages.

Customizing receive restrictions for Microsoft Exchange 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 **Active Directory > Exchange system administration > <Organization> > 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

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 Microsoft Exchange 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 customize send permissions for dynamic distribution groups

1. In the Manager, select the **Active Directory > Exchange system administration > <Organization> > 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.

Adding Microsoft Exchange mail-enabled distribution groups to Microsoft Exchange dynamic distribution groups

You can add dynamic distribution groups to mail-enabled distribution groups.

To add a dynamic distribution group to mail-enabled distribution groups

1. In the Manager, select the **Active Directory > Exchange system administration > <Organization> > Recipient configuration > Dynamic distribution groups** category.
2. Select the dynamic distribution group in the result list and run the **Assign distribution groups** task.
3. In the **Add assignments** pane, assign the distribution groups.

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

To remove an assignment

- Select the distribution group and double-click ✓.
4. Save the changes.

Related topics

- [Adding a Microsoft Exchange dynamic distribution group to Microsoft Exchange mail-enabled distribution groups](#) on page 146

Microsoft Exchange mail-enabled public folders

Mail-enabled public folders are loaded into the One Identity Manager database by synchronization and cannot be edited in One Identity Manager.

To display mail-enabled public folders

1. In the Manager, select the **Active Directory > Exchange system administration > <Organization> > Recipient configuration > Mail-enabled public folders** category.
2. Select the mail-enabled distribution group in the result list.
3. Select the **Change main data** task.

To display mail acceptance for mail-enabled public folders

1. In the Manager, select the **Active Directory > Exchange system administration > <Organization> > Recipient configuration > Mail-enabled public folders** category.
2. Select the mail-enabled distribution group in the result list.
3. Select the **Assign mail acceptance** task to display recipients whose messages are accepted.
- OR -
Select the **Assign mail rejection** task to display recipients whose messages are rejected.

To display the sent permission for a mail-enabled public folder

1. In the Manager, select the **Active Directory > Exchange system administration > <Organization> > Recipient configuration > Mail-enabled public folders** category.
2. Select the mail-enabled distribution group in the result list.
3. Select the **Assign send permissions** task.

The following main data is displayed:

Table 40: Mail-enabled public folder main data

Property	Description
Exchange organization	Name of the organization.
Public Folder	Connected public folder.
Name	Name of the mail-enabled public folder.
Alias	Unique alias for further identification of the mail-enabled public folder.
Display name	Display name of the mail-enabled public folder.
Simple display	Simple display name for systems that cannot interpret all the characters of normal display names.
Domain	Active Directory domain of the mail-enabled public folder.
Container	Active Directory container of the mail-enabled public folder.
Proxy addresses	Other email addresses for the mail-enabled public folder.
Email address	Email address of the mail-enabled public folder.
Alternative recipient	Alternative recipient to which messages from this mail-enabled public folder are forwarded.
Do not display in address list	Specifies whether the mail-enabled public folder is visible in address books. Set this option if you want to prevent the mail-enabled public folder from being displayed in address books. This option applies to all address books.
Max. send size [KB]	Maximum size of message in KB that a mail-enabled public folder can send. The Microsoft Exchange organization global settings in the Exchange System Manager come into effect for message delivery if there are no limitations.
Max. send size [KB]	Maximum size of message in KB that a mail-enabled public folder can receive. The Microsoft Exchange organization global settings in the Exchange System Manager come into effect for message delivery if there are no limitations.
Send and forward	Specifies whether to send and forward messages. If this option is set, messages are sent to alternative recipients and mailbox owners.

Extensions for supporting Exchange Hybrid environments

NOTE: The following modules must be installed to support Exchange Hybrid:

- Active Directory Module
- Microsoft Exchange Module
- Azure Active Directory Module
- Exchange Online Module
- Exchange Hybrid Module

NOTE: You cannot move mailboxes between local Microsoft Exchange and Exchange Online with One Identity Manager. Microsoft offers migration scenarios for moving mailboxes. For more information, see your Microsoft documentation.

One Identity Manager support creating, editing, and deleting of remote mailboxes in Exchange Hybrid. Remote mailboxes are mailboxes that are declared in the local Microsoft Exchange environment but were added in an Exchange Online environment.

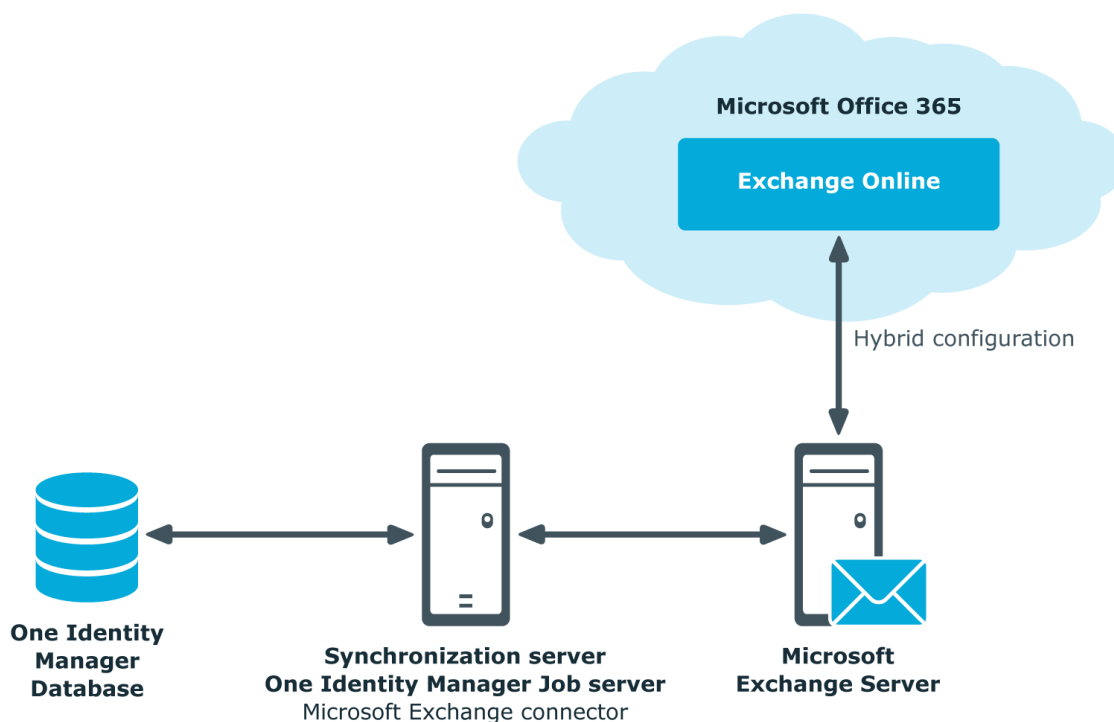
There are the following different types of remote mailboxes:

- Remote mailbox
- Remote room mailbox
- Remote equipment mailbox
- Remote shared mailbox

These mailboxes can be added to distribution lists or be given sending limits in the local Microsoft Exchange environment, for example.

The synchronization server running the Microsoft Exchange connector is responsible for synchronizing remote mailboxes. The other target system involved (Active Directory, Microsoft Exchange, Azure Active Directory, and Exchange Online) must be synchronized in order to access remote mailboxes.

Figure 2: Architecture for synchronization



Detailed information about this topic

- [Advice for synchronizing remote mailboxes](#) on page 156
- [Advice for migrating mailboxes](#) on page 157
- [Editing remote mailboxes](#) on page 161

Advice for synchronizing remote mailboxes

Take the following into account when synchronizing Exchange Hybrid remote mailboxes:

- The mapping for remote mailboxes is part of the Microsoft Exchange project template. Remote mailboxes are synchronized using the Microsoft Exchange connector.
- If an Exchange Hybrid environment already exists but there is no Exchange Hybrid module installed, a warning appears when you synchronize. Install the Exchange Hybrid module and create a new synchronization project.

- The following order is recommended for synchronizing the target systems.

1. Azure Active Directory

2. Local Active Directory

Synchronization can be simultaneous with Azure Active Directory synchronization.

3. Exchange Online

4. Local Microsoft Exchange

It is better to synchronize after synchronizing Exchange Online.

- In One Identity Manager, the connection must be defined between the local Microsoft Exchange organization (EX00organization) and the corresponding Azure Active Directory tenant (AAD0organization).

This connection is normally created automatically when the synchronization project is created for local Microsoft Exchange. This assumes that Azure Active Directory was already loaded in to the One Identity Manager at the time. You can establish this link manually at any time.

To declare the Azure Active Directory tenant in a Microsoft Exchange organization

1. In the Manager, select the **Active Directory > Exchange system administration** category.
2. Select the organization from the result list.
3. Select the **Change main data** task.
4. On the **Hybrid configuration** tab, under **Azure Active Directory tenant**, select the Azure Active Directory tenant to which your local Microsoft Exchange is connected.
5. Save the changes.

Related topics

- [Creating a synchronization project for initial synchronization of a Microsoft Exchange environment](#) on page 26
- [Default project template for Microsoft Exchange](#) on page 173

Advice for migrating mailboxes

You cannot move mailboxes between local One Identity Manager and Microsoft Exchange with Exchange Online. Microsoft offers migration scenarios for moving mailboxes. For more information, see your Microsoft documentation.

Synchronizing Microsoft Exchange after moving a mailbox from local Exchange Online to Microsoft Exchange in One Identity Manager results in:

- A remote mailbox being created
- The local mailbox being marked as **outstanding**.

After successful migration, delete outstanding mailboxes in One Identity Manager.

1. Check whether the mailbox was migrated and whether the Active Directory user account is connected with the local mailbox and a remote mailbox.

Migrated mailboxes are displayed in the Manager in the **Active Directory > Troubleshooting > Mailboxes migrated to Exchange Online** category.

- Select the mailbox and switch to the Active Directory user account overview. Here you can see whether the user account is connected with a local mailbox and a remote mailbox.
2. Delete the outstanding mailbox.
 - In the Manager, in the **Active Directory > Target System Synchronization: Exchange** category, select the mailbox in the EX0Mailbox table and run the **Delete** method for the mailbox.

For more information, see [Post-processing outstanding objects](#) on page 49.

If you apply an account definition to local mailboxes, create a new account definition for remote mailboxes.

- If the mailbox account definition currently in use, expects an account definition for Active Directory user accounts, enter this account definition as prerequisite for the remote mailbox account definition.

IMPORTANT: The remote mailbox account definition may not be distributed automatically to everybody. Otherwise One Identity Manager creates new remote mailboxes.

Example of exchanging account definitions for migrated mailboxes

The following is an example explaining how you can replace account definitions with migrated mailboxes

NOTE: The workflows described here are only for orientation. Always take your customized workflows into account while replacing.

You always required a custom migration scenario if the account definitions are requested through the IT Shop.

Example:

Local mailboxes are managed through an account definition. This account definition requires an account definition for Active Directory user accounts.

The account definition is directly assigned to identities.

After migration, remote mailboxes are also managed through account definitions.

1. Create an account definition for remote mailboxes. Enter the Active Directory user account's account definition as prerequisite.
2. After migrating a local mailbox:
 - a. Make sure that the remote mailbox exists in One Identity Manager and is linked to the Active Directory user account.
 - b. In One Identity Manager, delete the outstanding local mailbox.
 - c. Assign the account definition for remote mailboxes to the identity.
 - d. Remove the account definition for local mailboxes from the identity.

Example:

Local mailboxes are managed through an account definition. This account definition requires an account definition for Active Directory user accounts.

The account definition is inherited by the identities through its department relation.

After migration, remote mailboxes are also managed through account definitions.

1. Create a parallel structure to the department and assign the account definition for local mailboxes to this parallel structure.

The purpose of this parallel structure is to retain the local mailboxes' account definition assignment to an identity until the mailbox has been successfully migrated.

- Configure a dynamic role for this parallel structure, to include all identities that:
 - Belong to the department and do not have a remote mailbox.
 - or
 - Belong to the department and own a remote mailbox and an outstanding local mailbox.
- 2. After completing DBQueue Processor processing, you can remove the account definition for local mailboxes from the department.
- 3. Create an account definition for remote mailboxes. Enter the Active Directory user account's account definition as prerequisite.
- 4. Create another parallel structure and assign the account definition for remote mailboxes to it..

The purpose of this parallel structure is to assign the remote mailboxes' account definition to identities after mailbox migration and to retain the assignment of the required account definition for Active Directory.

- Configure a dynamic role for this parallel structure, to include all identities that:
 - Belong to the department and own a remote mailbox.
- 5. Delete the outstanding mailbox after migrating the local mailbox successfully.
- 6. After migrating all the department's local mailboxes, you can:
 - a. Assign a department to the remote mailboxes' account definition.
 - b. Remove the parallel structure.

Creating remote mailboxes


NOTE: After creation of a new remote mailbox, it takes until the next synchronization of your Azure Active Directory tenant in Azure Active Directory Connect until a corresponding mailbox is created in the Exchange Online environment. Up to this point, the mailbox is acknowledged in the local Microsoft Exchange environment but is not yet available for use.

NOTE: After new remote mailboxes of **Remote user** type have been created by Azure Active Directory or Exchange Online internal processes, an appropriate Exchange license must be assigned for the resulting Azure Active Directory user account.

To display remote mailboxes without Exchange licenses

- In Manager, select the **Active Directory > Exchange system administration > <organization> > Recipient configuration > Remote mailboxes > Remote user mailbox > Without assigned licenses** category.

To create a remote mailbox

1. In the Manager, select the **Active Directory > Remote 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.

To create a mailbox for an Active Directory user account manually

1. In the Manager, select the **Active Directory > User accounts** category.
2. In the result list, select the user account then select the **Change main data** task.
3. Select the **Create remote mailbox** task.
4. Enter the following information:

- **Active Directory user account:** The user account is already selected.
- **Exchange organization:** The exchange organization is already selected. Check the setting.
- **Alias:** Unique alias for further identification of the mailbox.

5. Click **OK**.

Related topics

- [Editing remote mailboxes](#) on page 161
- [General main data for remote mailboxes](#) on page 162
- [Information about remote configuration](#) on page 164
- [Information about cloud-based archive mailboxes](#) on page 165
- [Customizing receive restrictions for remote mailboxes](#) on page 165
- [Specifying extensions for moderated remote mailboxes](#) on page 166

Editing remote mailboxes

To edit a mailbox

1. In the Manager, select the **Active Directory > Remote mailboxes** category.
2. In the result list, select the remote mailbox then select the **Change main data** task.
3. Edit the remote mailbox's main data.
4. Save the changes.

Related topics

- [General main data for remote mailboxes](#) on page 162
- [Information about remote configuration](#) on page 164
- [Information about cloud-based archive mailboxes](#) on page 165
- [Customizing receive restrictions for remote mailboxes](#) on page 165
- [Specifying extensions for moderated remote mailboxes](#) on page 166
- [Assigning extended properties to remote mailboxes](#) on page 167

General main data for remote mailboxes

Enter the following general main data.

Table 41: General main data of a remote mailbox

Property	Description
Identity	<p>Identity using the mailbox.</p> <ul style="list-style-type: none">• An identity is already entered if the mailbox was generated by an account definition.• If you create the mailbox 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 mailbox, the mailbox might be locked or deleted depending on the configuration.</p>
No link to an identity required	<p>Specifies whether the mailbox 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 mailbox. 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 mailbox was created.</p> <p>Use the account definition to automatically populate mailbox main data and to specify a manage level for the mailbox.</p> <p>One Identity Manager finds the IT operating data of the assigned identity and uses it to populate the corresponding fields in the mailbox.</p> <p>NOTE: The account definition cannot be changed once the mailbox has been saved.</p>
Manage level	<p>Manage level with which the mailbox is created. Select a manage level</p>

Property	Description
	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.
Active Directory user account	Active Directory user account for which this mailbox is created.
Exchange organization	Name of the Microsoft Exchange organization.
Canonical name	Mailbox's canonical name. The canonical name is generated automatically.
Recipient type (detail)	Type of recipient. The mailbox type is specified when a mailbox is added and cannot be changed afterward. You can choose from the following options: Remote user , Remote room , Remote equipment and Remote shared .
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 simple 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.
Alias	Unique alias for further identification of the mailbox.
User login name	User account login name. The user's login name is made up of the alias and the domain. User login names that are formatted like this correspond to the User Principal Name (UPN) in Active Directory.
Do not display in address list	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.
Moderation enabled	Specifies whether the mailbox is moderated. Enable this option if the mailbox is meant to be moderated. Use the task Assign moderators to specify moderators.
Sender authentication required	Specifies whether authentication data is requested from senders. Set this option to prevent anonymous senders mailing to the mailbox.
Automatically update based on	Specifies whether changes to recipient's email addresses are automatically updated based on recipient policies.

Property	Description
recipient policy	
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>
Sending message to	<p>Specifies how senders are notified when they send messages to a 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.
Distinguished name	Mailbox's distinguished name.

Information about remote configuration

The following information about remote configuration is mapped.

Property	Description
Azure Active Directory user account	Azure Active Directory user account identifier.
Exchange Online mailbox	Exchange Online mailbox identifier.
Recipient type	Type of recipient.
SMTP address	SMTP address of the mailbox assigned to this user.

Information about cloud-based archive mailboxes

The following main data for a cloud-based archive mailbox is mapped.

Table 42: Archiving a mailbox

Property	Description
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.
Archive state	Status of the archive mailbox.

Customizing receive restrictions for remote 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 customize mail acceptance for mailboxes

1. In the Manager, select the **Active Directory > Remote 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
 - Remote mailboxes
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.

Specifying extensions for moderated remote 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.

Define a mailbox's moderator. Furthermore, you can specify users whose messages to the moderated mailbox are excluded from moderation.

To specify moderators for a mailbox


1. In the Manager, select the **Active Directory > Remote 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
 - Remote 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.

To exclude users from moderation

1. In the Manager, select the **Active Directory > Remote mailboxes** category.
2. Select a mailbox in the result list.
3. Select the **Exclude from moderation** 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
 - Dynamic distribution groups
 - Mailboxes
 - Remote mailboxes
 - Mail users
 - Mail contacts
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.

Assigning extended properties to remote mailboxes


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

To specify extended properties for a remote mailbox

1. In the Manager, select the **Active Directory > Remote mailboxes** category.
2. Select a remote mailbox 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.

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

Error handling

Error running the Windows PowerShell command Set-Mailbox

Issue

In certain Active Directory/Microsoft Exchange topologies, the Set-Mailbox Cmdlet fails with the following error:

Error on proxy command 'Set-Mailbox...'

The operation couldn't be performed because object '...' couldn't be found on '...'.

For more information, see <https://support.microsoft.com/en-us/help/4295103>.

Possible workarounds

- Connect to the Microsoft Exchange server that the user mailbox is on. Use a custom process to do this. Use the `OverrideVariables` parameter (ProjectorComponent process component) to overwrite the server (CP_ExchangeServerFqdn variable).
- Because this problem only occurs with a few schema properties, you should consider protecting these schema properties in the synchronization project against write operations. You can set the schema properties in a custom process using the `PowershellComponentNet4` process component through a user-defined Windows PowerShell call.

Possible errors when synchronizing an Exchange Hybrid environment

Problem

A warning is displayed while setting up a new synchronization project for an Exchange Hybrid environment:

The given Exchange Organization has an Office 365 Hybrid Configuration. The Exchange Hybrid Module (EXH) It is recommended you install the Exchange Hybrid Module first.

Cause

The schema extensions for synchronizing Exchange Hybrid are not declare in the One Identity Manager database yet.

Solution

Update the One Identity Manager and select the Exchange Hybrid Module as an additional module. For more information about updating One Identity Manager, see the *One Identity Manager Installation Guide*.

Problem

The following error message appears when synchronizing Exchange Hybrid memberships with an existing synchronization project.

The schema type (RemoteMailbox) does not exist in schema (...).

Cause

The Microsoft Exchange Module has already been updated. Therefore, the Microsoft Exchange connector recognizes the extensions for synchronizing Exchange Hybrid. The Exchange Hybrid Module was not installed.

Solution

If you want to synchronize Exchange Hybrid

- Update the One Identity Manager and select the Exchange Hybrid Module as an additional module. For more information about updating One Identity Manager, see the *One Identity Manager Installation Guide*.
- Create a new synchronization project. For more information, see [Creating a synchronization project for initial synchronization of a Microsoft Exchange environment](#) on page 26.

If you do not want to synchronize Exchange Hybrid:

- Apply the patch with the patch ID VPR#28904 to the synchronization project. This patch modifies the member filter's excluded lists.

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

Configuration parameters for managing a Microsoft Exchange environment

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

Table 43: Configuration parameters for managing a Microsoft Exchange environment

Configuration parameters	Meaning
TargetSystem ADS Exchange2000	<p>Preprocessor relevant configuration parameter for controlling database model components for Microsoft Exchange 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 ADS Exchange2000 Accounts	Allows configuration of recipient data.
TargetSystem ADS Exchange2000 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 ADS Exchange2000 DefaultAddress	Default email address of the recipient for notifications about actions in the target system.

Default project template for Microsoft Exchange

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.

Detailed information about this topic

- [Default project template for Microsoft Exchange 2013, Microsoft Exchange 2016, and Microsoft Exchange 2019](#) on page 173

Default project template for Microsoft Exchange 2013, Microsoft Exchange 2016, and Microsoft Exchange 2019

The project template uses mappings for the following schema types.

Table 44: Mapping Microsoft Exchange 2013, Microsoft Exchange 2016, and Microsoft Exchange 2019 schema types to tables in the One Identity Manager schema.

Schema type in Microsoft Exchange	Table in the One Identity Manager schema
AddressbookPolicy	EX0AddrBookPolicy
CalendarProcessing	EX0Mailbox
DatabaseAvailabilityGroup	EX0DAG
DistributionGroup	EX0DL
DynamicDistributionGroup	EX0DynDL
ExchangeServer	EX0Server
GlobalAddressList	EX0AddrList
LocalAddressList	EX0AddrList
Mailbox	EX0Mailbox
MailboxDatabase	EX0MailboxDatabase
Mailboxstatistics	EX0Mailbox
MailContact	EX0MailContact
MailPublicFolder	EX0MailPublicFolder
MailUser	EX0MailUser
MobileDeviceMailboxPolicy	EX0ActiveSyncMBPolicy
OfflineAddressBook	EX0OfflAddrBook
Organization	EX0Organization
OwaMailboxPolicy	EX0OwaMailboxPolicy
PublicFolder	EX0PublicFolder
PublicFolderDatabase	EX0PublicFolderDatabase
RemoteMailbox	EXHRemoteMailbox
	NOTE: This table only exists if the Exchange Hybrid Module is installed.
RetentionPolicy	EX0RetentionPolicy
RoleAssignmentPolicy	EX0RoleAssignPolicy
SharingPolicy	EX0SharingPolicy
Mailbox Permissions	EX0Mailbox

Processing methods of Microsoft Exchange system objects

The following table describes permitted editing methods for Microsoft Exchange schema types and the necessary restrictions for processing the system objects.

Table 45: Methods available for processing Microsoft Exchange schema types

Type	Read	Add	Delete	Refresh
Organization (Organization)	Yes	No	No	No
Microsoft Exchange server (ExchangeServer)	Yes	No	No	No
Data availability group (DatabaseAvailabilityGroup)	Yes	No	No	No
Public folder (PublicFolder)	Yes	No	No	No
Mailbox database (MailboxDatabase)	Yes	No	No	No
Mail-enabled public folder (MailPublicFolder)	Yes	No	No	No
Global address list (EX0AddrList)	Yes	No	No	No
Local address list (EX0AddrList)	Yes	No	No	No
Offline address list (OfflineAddressBook)	Yes	No	No	No
Outlook Web App mailbox policy (OwaMailboxPolicy)	Yes	No	No	No
Address book policy (AddressBookPolicy)	Yes	No	No	No
Retention policy (RetentionPolicy)	Yes	No	No	No
Sharing policy (SharingPolicy)	Yes	No	No	No
Mailbox policy for mobile devices (MobileDeviceMailboxPolicy)	Yes	No	No	No
Policy for role assignment (RoleAssignmentPolicy)	Yes	No	No	No
Mail user (MailUser)	Yes	Yes	Yes	Yes
Mail contact (MailContact)	Yes	Yes	Yes	Yes
Mailbox: user mailbox (Mailbox)	Yes	Yes	Yes	Yes
Mailbox: resource mailbox (Mailbox)	Yes	Yes	Yes	Yes

Type	Read	Add	Delete	Refresh
Mailbox: shared mailbox (Mailbox)	Yes	Yes	Yes	Yes
Mailbox: linked mailbox (Mailbox)	Yes	Yes	Yes	Yes
Mailbox: legacy mailbox (Mailbox)	Yes	No	No	No
Mailbox: discovery mailbox (Mailbox)	Yes	No	No	No
Mailbox: calendar settings (Mailbox)	Yes	Yes	Yes	Yes
Mailbox: statistics (Mailboxstatistics)	Yes	Yes	Yes	Yes
Mailbox: remote mailbox (RemoteMailbox)	Yes	Yes	Yes	Yes
Mailbox: mailbox permissions (MailboxPermissions)	Yes	Yes	Yes	Yes
Dynamic distribution group (DynamicDistributionGroup)	Yes	No	Yes	Yes
Distribution group (DistributionGroup)	Yes	Yes	Yes	Yes

Microsoft Exchange connector settings

The following settings are configured for the system connection with the Microsoft Exchange connector.

Table 46: Microsoft Exchange connector settings

Setting	Meaning
Servers	Fully qualified name (FQDN) of the Microsoft Exchange server. Variable: CP_ExchangeServerFqdn
Basic authentication (requires SSL)	Specifies whether to use the Basic authentication method. Default: False Variable: CP_UseSSL NOTE: Microsoft Exchange does not support this authentication type by default. You must configure support for this method in Microsoft Exchange. In addition, an SSL connection is used to authenticate using the Basic method. By default, authentication uses Kerberos.
Max. concurrent connections	Maximum number of connections that can be used concurrently. The value must be between 1 and 20 . Variable: CP_ConnectionPoolSize
User name (user@domain)	Fully qualified name (FQDN) of the user account and password for logging in to Microsoft Exchange. Variable: CP_Username
Password	The user account's password. Variable: CP_Password

Setting	Meaning
Use the One Identity Manager Service account	<p>Specifies whether to use the credentials of the currently logged in user.</p> <p>Default: False</p> <p>Variable: CP_UseServiceCredential</p> <p>The user account running under the One Identity Manager Service requires the permissions described in Users and permissions for synchronizing with Microsoft Exchange on page 14.</p> <p>NOTE: If this setting is used, the current user account is also used in the Synchronization Editor during configuration. This user account may be different to the One Identity Manager Service's user account</p> <p>In this case, it is recommended you use the RemoteConnectPlugin. This ensures that the same user account is used during configuration with the Synchronization Editor as is used in the service context.</p>
Recipient: Complete organization	<p>If this setting is set to True, the recipients will be available to the entire organization for reading/writing. If the setting is set to False, only the recipients of the specified domain (CP_RecipientDomain) are available.</p> <p>Default: True</p> <p>Variable: CP_SynchronizeEntireOrganization</p>
Recipient: Only recipients of the following domain	<p>Domain whose recipients will be synchronized if the complete organization is not synchronized (CP_SynchronizeEntireOrganization = False).</p> <p>Variable: CP_RecipientDomain</p>
Use local server time for the revision	<p>Revision filtering data</p> <p>If the value is True, the local server time of the server is used for revision filtering. 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 Active Directory objects are used for revision filtering.</p> <p>Default: True</p> <p>Variable: CP_UseLocalServerTimeAsRevision</p>
Max. time difference (local/re-	Revision filtering data

Setting	Meaning
mote) in minutes	<p>Maximum time difference in minutes between the synchronization server and the Microsoft Exchange server. If the time difference is more than 60 minutes, alter the value.</p> <p>Default: 60</p> <p>Variable: CP_LocalServerRevisionMaxDifferenceInMinutes</p>
Retry count	<p>Maximum number of reconnection attempts after an interrupted connection has been identified.</p> <p>Default: 30</p> <p>Variable: CP_MaxReconnectRetries</p>
Delay between retries	<p>Time delay between retry attempts in seconds.</p> <p>Default: 20</p> <p>Variable: CP_ReconnectIntervalInSeconds</p>
ConfigurationDomainController	<p>FQDN of the configuration domain controller to be used for reading Microsoft Exchange configuration information. For auto discovery, leave the value blank.</p> <p>Variable: CP_ConfigurationDomainController</p>
PreferredGlobalCatalog	<p>FQDN of the global catalog server for reading recipient information. For auto discovery, leave the value blank.</p> <p>Variable: CP_PREFERREDGlobalCatalog</p>
SetPreferredDomainControllers	<p>Comma-delimited list of domain controllers (FQDN) for reading information from Active Directory. For auto discovery, leave the value blank.</p> <p>Variable: CP_SetPreferredDomainControllers</p>
PreferredServer	<p>FQDN of the domain controller to be used for writing data. For auto discovery, leave the value blank.</p> <p>Variable: CP_PREFERREDServer</p>

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 57
 - add to IT Shop 71
 - assign automatically 70
 - assign to Active Directory domain 74
 - assign to all identities 70
 - assign to business role 69
 - assign to cost center 68
 - assign to department 68
 - assign to identities 67, 70
 - assign to location 68
 - assign to system roles 71
 - create 58
 - delete 74
 - edit 58
 - IT operating data 64-65
 - manage level 61-62
- Active Directory domain
 - account definition mail contact (initial) 74
 - account definition mail user (initial) 74
 - account definition mailbox (initial) 74
 - DC (linked mailbox) 22
 - trust 21
 - user (linked mailbox) 22
- architecture overview 8

B

- base object 37, 43

C

- calculation schedule 46
 - deactivate 47
- configuration parameter 172
- convert connection parameter 37

D

- direction of synchronization
 - direction target system 26, 35
 - in the Manager 26
- dynamic distribution group 148
 - add mail-enabled distribution groups 152
 - addressing 148
 - alias 148
 - condition 148
 - display name 148
 - expansion server 148
 - identifier 148
 - limit 148
 - mail acceptance 150
 - receive restriction 150
 - recipient type 148
 - send on behalf of 151

E

- Exchange Hybrid 155
 - remote mailbox 160-161
 - synchronization 156, 170

I

IT operating data

change 66

IT Shop shelf

assign account definition 71

J

Job server 79

edit 16-17

load balancing 44

L

load balancing 44

log file 53

M

mail-enabled distribution group 137

Active Directory group 139

addressing 139

administrator 144

alias 139

assign dynamic distribution
group 146

create 137

delete 147

display name 139

edit 138

expansion server 139

join 139

leave 139

limit 139

mail acceptance 141

moderate 139, 144

moderator 144

receive restriction 141

mail-enabled public folder 153

mail contact 123

account definition 74, 131

Active Directory contact 131

addressing 131

alias 131

create 130

deferred deletion 135

delete 135

destination address 131

display name 131

edit 131

identity 131

limit 131

mail acceptance 134

manage level 131

receive restriction 134

restore 135

mail user 123

account definition 74, 125

Active Directory user account 125

addressing 125

alias 125

create 123

deferred deletion 129

delete 129

destination address 125

display name 125

edit 125

identity 125

limit 125

mail acceptance 128

manage level 125

- receive restriction 128
- restore 129
- mailbox
 - account definition 74, 106
 - Active Directory user account 106
 - address book policy 101, 106
 - addressing 106
 - alias 106
 - alternative recipient 106
 - archive size 112
 - book 114
 - Calendar Attendant 109, 114
 - calendar setting 109
 - connected mailbox 106
 - create 103
 - deactivate 106, 120
 - deferred deletion 121
 - delete 121
 - discovery mailbox 102
 - display name 106
 - edit 105
 - equipment mailbox 102, 114
 - folder policy 98, 106
 - functions 113
 - identity 106
 - limit 110
 - linked mailbox 102
 - mail acceptance 116
 - mailbox database 106
 - mailbox type 102, 106
 - manage level 106
 - migrate 157
 - mobile device policy 97, 113
 - Outlook Web App mailbox policy 106
 - personal archive 112
 - receive restriction 116
 - Resource Attendant 114
 - resource mailbox 102, 114
 - restore 121
 - retention policy 96, 112
 - role assignment policy 99-100, 106
 - room mailbox 102, 114
 - set up 102
 - shared mailbox 102
 - sharing policy 95, 106
 - size 110
 - user mailbox 102
- mailbox permissions
 - full access 36, 119
 - send as 36, 118
 - send on behalf of 117
- membership
 - modify provisioning 42
- Microsoft Exchange connector 8
- Microsoft Exchange organization
 - application roles 9
 - hierarchical address book 87
 - target system manager 9, 77, 86
- Microsoft Exchange server 8
 - configure 20
 - remote access 20
- Microsoft Exchange structure 85
 - address book policy 101
 - address list 90
 - database availability group 94
 - hierarchical address book 87
 - mailbox database 88
 - mailbox server 93
 - mobile device policy 97
 - offline address list 90

- organizations 86
- Outlook Web App mailbox policy 100
- policy for folder admin 98
- public folder 92
- retention policy 96
- role assignment policy 99
- sharing policy 95

N

- NLog 53

O

- object
 - delete immediately 49
 - outstanding 49
 - publish 49
- offline mode 54
- outstanding object 49

P

- project template 173
- provisioning
 - accelerate 44
 - members list 42

R

- remote mailbox
 - account definition 157, 162
 - Active Directory user account 162
 - alias 162
 - archive mailbox 165
 - Azure Active Directory user account 164

- create 160
- edit 161
- equipment mailbox 162
- Exchange Online mailbox 164
- identity 162
- license 160
- mail acceptance 165
- manage level 162
- Microsoft Exchange organization 162
- moderate 162, 166
- remote configuration 164
- room mailbox 162
- SMTP address 164
- user login name 162
- user mailbox 162
- without license 160
- reset revision 53
- reset start up data 53
- revision filter 40

S

- schema
 - changes 39
 - shrink 39
 - update 39
- server 79
- single object synchronization 43, 48
 - accelerate 44
- start up configuration 37
- synchronization
 - accelerate 40
 - authorizations 14
 - calculation schedule 46
 - configure 26, 34
 - connection parameter 26, 34

- Exchange Hybrid 156, 170
- Microsoft Exchange 12
- prevent 47
- scope 34
- set up 12
- simulate 53
- start 26, 46
- synchronization project
 - create 26
- user 14
- variable 34
- workflow 26, 35
- synchronization analysis report 53
- synchronization configuration
 - customize 34-35
- synchronization log 47, 53
 - contents 33
 - create 33
- synchronization project
 - create 26, 28
 - deactivate 47
 - project template 173
- synchronization server 8, 79
 - configure 16, 20
 - install 16-17
 - Job server 16-17
 - remote access 20
- synchronization workflow
 - create 26, 35
- synchronize single object 48
- system connection
 - change 37
 - enabled variable set 38

T

- target system
 - not available 54
- target system manager 77
- target system synchronization 49
- template
 - IT operating data, modify 66

U

- user account
 - apply template 66

V

- variable set 37
 - active 38