One Identity Manager 8.0.3

Administration Guide for Connecting to Microsoft Exchange

Copyright 2019 One Identity LLC.

ALL RIGHTS RESERVED.

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

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

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

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

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

Patents

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

Trademarks

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

Legend

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

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

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

One Identity Manager Administration Guide for Connecting to Microsoft Exchange
Updated - March 2019
Version - 8.0.3

Contents

Managing Microsoft Exchange Environments

The key aspects of administrating a Microsoft Exchange system with One Identity Manager are mapping mailboxes, e-mail users, e-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.

Architecture Overview

The following servers are used for managing a Microsoft Exchange system in One Identity Manager:

- Microsoft Exchange server

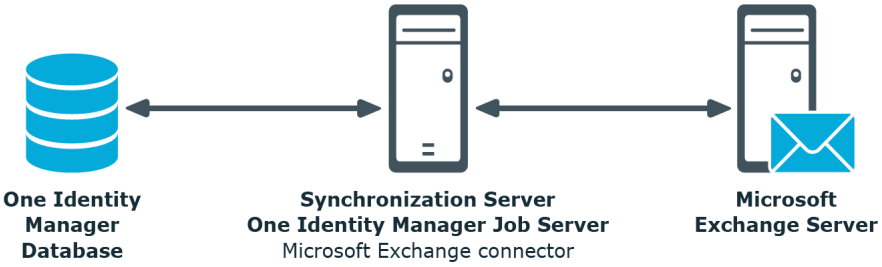
  Microsoft Exchange server against which Microsoft Exchange objects are executed. The synchronization server connects to this server in order to access Microsoft Exchange objects.

- Synchronization server

  The synchronization server for synchronizing the One Identity Manager database with the Microsoft Exchange system. The One Identity Manager Service is installed on this server with the Microsoft Exchange connector. 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 the administration of Microsoft Exchange.

Table 1: Users

User	Task
Target system administrators	Target system administrators must be assigned to the application role **Target system | Administrators**. Users with this application role: • Administrate application roles for individual target systems types. • Specify the target system manager. • Set up other application roles for target system managers if required. • Specify which application roles are conflicting for target system managers • Authorize other employee to be target system administrators. • Do not assume any administrative tasks within the target system.
Target system managers	Target system managers must be assigned to the application role **Target systems | Exchange** or a sub application role. Users with this application role: • Assume administrative tasks for the target system. • Create, change or delete target system objects, like user accounts or groups.

User	Task
	• Edit password policies for the target system. • Prepare for adding to the IT Shop. • Configure synchronization in the Synchronization Editor and defines the mapping for comparing target systems and One Identity Manager. • Edit the synchronization's target system types and outstanding objects. • Authorize other employees within their area of responsibility as target system managers and create child application roles if required.
One Identity Manager administrators	• Create customized permissions groups for application roles for role-based login to administration tools in the Designer, as required. • Create system users and permissions groups for non-role based login to administration tools, as required. • Enable or disable additional configuration parameters in the Designer, as required. • Create custom processes in the Designer, as required. • Create and configures schedules, as required. • Create and configure password policies, as required.

2

Setting up Microsoft Exchange Synchronization

One Identity Manager supports synchronization with Microsoft Exchange 2010 Service Pack 3 or later, Microsoft Exchange 2013 Service Pack 1 or later and Microsoft Exchange 2016.

One Identity Manager is responsible for synchronizing data between the Microsoft Exchange database and the One Identity Manager Service. Synchronization prerequisites are:

- 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 Active Directory client domain are entered to create linked mailboxes within a Microsoft Exchange resource forest topology

To load Microsoft Exchange objects into the One Identity Manager database

1. Prepare a user account with sufficient permissions for synchronization.
2. One Identity Manager parts for managing Microsoft Exchange systems are available if the configuration parameter "TargetSystem\ADS\Exchange2000" is set.
    - Check whether the configuration parameter is set in the Designer. Otherwise, set the configuration parameter and compile the database.
    - Other configuration parameters are installed when the module is installed. Check the configuration parameters and modify them as necessary to suit your requirements.
3. Install and configure a synchronization server and declare the server as 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 11
- Setting Up the Synchronization Server on page 12
- Configuring Participating Servers for Remote Access through Windows PowerShell on page 16
- Testing Active Directory Domain Trusts on page 17
- Extensions for Creating Linked Mailboxes in a Microsoft Exchange Resource Forest on page 18
- Creating a Synchronization Project for initial Synchronization of a Microsoft Exchange Environment on page 19
- Deactivating Synchronization on page 37
- Recommendations for Synchronizing Microsoft Exchange on page 27
- Customizing Synchronization Configuration on page 30
- Appendix: Configuration Parameters for Managing Microsoft Exchange on page 127
- Default Template for Microsoft Exchange 2010 on page 128
- Default Template for Microsoft Exchange 2013 and Microsoft Exchange 2016 on page 129

Users and Permissions for Synchronizing with Microsoft Exchange

The following users are involved in synchronizing One Identity Manager with Microsoft Exchange.

Table 2: Users for Synchronization

User	Permissions
User for accessing Microsoft Exchange	You must provide a user account with the following permissions for full synchronization of Microsoft Exchange objects with the supplied One Identity Manager default configuration. • Member in role group "View only organization management" • Member in role group "Public folder management" • Member in role group "Recipient management"
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	The user account for the One Identity Manager Service requires access rights to carry out operations at file level (issuing user

User	Permissions
user account	rights, adding directories and files to be edited). The user account must belong to the group "Domain Users". The user account must have the extended access right "Log on as a service". The user account requires access rights to the internal web service. NOTE: If the One Identity Manager Service runs under the network service (NT Authority\NetworkService), you can issue access rights for the internal web service with the following command line call: `netsh http add urlacl url=http://<IP address>:<port number>/ user="NT AUTHORITY\NETWORKSERVICE"` The user account needs full access to the One Identity Manager Service installation directory in order to automatically update the One Identity Manager. In the default installation the One Identity Manager is installed under: • `%ProgramFiles(x86)%\One Identity` (on 32-bit operating systems) • `%ProgramFiles%\One Identity` (on 64-bit operating systems)
User for accessing the One Identity Manager database	The default system user "Synchronization" is available to run synchronization over an application server.

Setting Up the Synchronization Server

To setup synchronization with a Microsoft Exchange environment a server has to be available that has the following software installed on it:

- Windows operating system

  Following versions are supported:

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

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

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

- Windows Installer
- Windows Management Framework 4.0
- One Identity Manager Service, Microsoft Exchange connector
  - Install One Identity Manager components with the installation wizard.
    1. Select the option **Select installation modules with existing database**.
    2. Select the machine role **Server | Job server | Microsoft Exchange**.

IMPORTANT: The One Identity Manager Microsoft Exchange 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. For more information, see Configuring Participating Servers for Remote Access through Windows PowerShell on page 16.

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

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

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

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

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

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

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

      - OR -

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

   b. Enter the following data for the Job server.

      Table 3: Job Servers Properties

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

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

4. Specify which job server roles to include in One Identity Manager on the **Machine role** page. Installation packages to be installed on the Job server are found depending on the selected machine role.

   Select at least the following roles:

   - Microsoft Exchange

5. Specify the server's functions in One Identity Manager on the **Server functions** page. One Identity Manager processes are handled depending on the server function.

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

   Select the following server functions:

   - Microsoft Exchange connector

6. Check the One Identity Manager Service configuration on the **Service settings** page.

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

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

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

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

Table 4: Installation Data

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

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

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

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

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

Related Topics

- Configuring Participating Servers for Remote Access through Windows PowerShell on page 16

Configuring Participating Servers for Remote Access through Windows PowerShell

NOTE: 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 context menu **Run as Administrator**.
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 allows you to execute all Windows PowerShell commands (Cmdlets). 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 customizes the list of trusted hosts to activate 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 Windows PowerShell on the Microsoft Exchange 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 making 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 commands creates a remote session.

   NOTE: One Identity Manager creates a connection using the Microsoft Exchange server's fully qualified domain name. 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

In order to synchronize with a Microsoft Exchange system, 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. Select the category **Active Directory | Domains**.
2. Select the domain in the result list.
3. Select **Change master data** in the task view.
4. Enter the parent domain.
5. Save the changes.

   Implicit trusts are created automatically.

To test trusted domains

1. Select the category **Active Directory | Domains**.
2. Select the domain in the result list.
3. Select **Specify trust relationships in the task view**.

   This shows domains which trust the selected domain.

For more detailed 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 master data for a domain

1. Select the category **Active Directory | Domains**.
2. Select the domain in the result list and run the task **Change master data**.

3. Enter the following information on the **Exchange** tab.

Table 5: Master Data of a Domain for Creating Linked Mailboxes

Property	Description
User (linked mailbox)	User account used to create linked mailboxes.
Password	User account password.
Password confirmation	Confirmation of the user account password.
DC (linked mailbox)	Active Directory Domain controller for create linked mailboxes.

4. Save the changes.

Related Topics

- Users and Permissions for Synchronizing with Microsoft Exchange on page 11

Creating a Synchronization Project for initial Synchronization of a Microsoft Exchange Environment

Use the Synchronization Editor to configure synchronization between the One Identity Manager database and Microsoft Exchange. The following describes the steps for initial configuration of a synchronization project.

NOTE: Refer to the recommendations for setting up synchronization described in Recommendations for Synchronizing Microsoft Exchange on page 27.

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

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

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

Prerequisites for Setting Up a Synchronization Project

- 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 Active Directory client domain are entered to create linked mailboxes within a Microsoft Exchange resource forest topology

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

Table 6: Information Required for Setting up a Synchronization Project

Data	Explanation
Microsoft Exchange version	One Identity Manager supports synchronization with Microsoft Exchange 2010, Service Pack 3 or later, Microsoft Exchange 2013, Service Pack 1 or later and Microsoft Exchange 2016.
Server (fully qualified)	Fully qualified name (FQDN) of the Microsoft Exchange server against which the synchronization server connects to access Microsoft Exchange objects. Example: `Server.Doku.Testlab.dd`

User account and password for logging in	Fully qualified name (FQDN) of the user account and password for logging in on the Microsoft Exchange.
	Example:
	`user@domain.com`
	`domain.com\user`
	Make a user account available with sufficient permissions. For more information, see Users and Permissions for Synchronizing with Microsoft Exchange on page 11.

Synchronization server for Microsoft Exchange	The One Identity Manager Service with the Microsoft Exchange connector must be installed on the synchronization server. **Table 7: Additional Properties for the Job Server** **Property** / **Value** Server Function: Microsoft Exchange connector Machine role: Server/Job Server/Active Directory/Microsoft Exchange

Data	Explanation
	For more information, see Setting Up the Synchronization Server on page 12.
One Identity Manager Database Connection Data	SQL Server: • Database server • Database • Database user and password • Specifies whether Windows authentication is used. This type of authentication is not recommended. If you decide to use it anyway, ensure that your environment supports Windows authentication. Oracle: • Species whether access is direct or through the Oracle client Which connection data is required, depends on how this option is set. • Database server • Oracle instance port • Service name • Oracle database user and password • Data source (TNS alias name from `TNSNames.ora`)
Remote connection server	To configure synchronization with a target system, One Identity Manager must load the data from the target system. One Identity Manager communicates directly with target system to do this. Sometimes direct access from the workstation on which the Synchronization Editor is installed is not possible, because of the firewall configuration, for example, or because the workstation does not fulfill the necessary hardware and software requirements. If direct access to the workstation is not possible, you can set up a remote connection. The remote connection server and the workstation must be in the same Active Directory domain. Remote connection server configuration: • One Identity Manager Service is started • `RemoteConnectPlugin` is installed • Microsoft Exchange connector is installed The remote connection server must be declared as a Job server in One Identity Manager. The Job server name is required.

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

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

- In default mode
- Started from the launchpad

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

To set up initial synchronization project for Microsoft Exchange

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

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

2. Select the entry **Microsoft Exchange target system type**. Click **Run**.

   This starts the Synchronization Editor's project wizard.

3. Select the connector on the **Select target system** page.
   - Select **Microsoft Exchange 2010 connector** for synchronizing with Microsoft Exchange 2010.
   - Select **Microsoft Exchange 2013 connector** for synchronizing with Microsoft Exchange 2013.
   - Select **Microsoft Exchange 2016 connector** for synchronizing with Microsoft Exchange 2016.

4. Specify how the One Identity Manager can access the target system on the **System access** page.
   - If you have access from the workstation from which you started the Synchronization Editor, do not set anything.
   - If you do not have access from the workstation from which you started the Synchronization Editor, you can set up a remote connection.

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

5. Enter the information about the Microsoft Exchange server on the **Select Microsoft Exchange server** page against which the synchronization server connects to access Microsoft Exchange objects.
    a. Enter the fully qualified name (FQDN) in the Microsoft Exchange server in **Server**. To check the data, click **DNS query**.

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

    b. In **Max. concurrent connections**, enter the number of connection 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 utilize HTTPS for establishing the connection, set **Use SSL**.

        NOTE: Microsoft Exchange does not support this type of connection by default. You must configure support for HTTPS in your Microsoft Exchange.

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

    Table 8: Connection data to Microsoft Exchange

Property	Description

User name (user@-domain)	Fully qualified name (FQDN) of the user account for logging in.
	Example:
	`user@domain.com`
	`domain.com\user`

Password	User account password.

7. Specify on the **Recipient scope** page whether the recipient of any domain or complete Microsoft Exchange organization should be taken into account.
    - To synchronize Microsoft Exchange organization recipients, select the option **Entire organization** (recommended). As prerequisite the trusted Active Directory domains must be declared in One Identity Manager.
    - Select the option **Only recipients of the following domain** to synchronize recipients with specific domains and select a domain. The target system domain is listed as a minimum.

8. Verify the One Identity Manager database connection data on the **One Identity Manager connection** page. The data is loaded from the connected database. Reenter the password.

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

9. The wizard loads the target system schema. This may take a few minutes depending on the type of target system access and the size of the target system.

10. Specify how system access should work on the page **Restrict target system access**. You have the following options:

Table 9: Specifying Target System Access

Option	Meaning
Read-only access to target system.	Specifies whether a synchronization workflow should be set up to initially load the target system into the One Identity Manager database. The synchronization workflow has the following characteristics: • Synchronization is in the direction of "One Identity Manager". • Processing methods in the synchronization steps are only defined in synchronization direction "One Identity Manager".
Changes are also made to the target system.	Specifies whether a provisioning workflow should be set up in addition to the synchronization workflow to initially load the target system. The provisioning workflow displays the following characteristics: • Synchronization in the direction of the "target system" • Processing methods are only defined in the synchronization steps in synchronization direction "target system". • Synchronization steps are only created for such schema classes whose schema types have write access.

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

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

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

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

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

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

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

    The synchronization project is created, saved and enabled immediately.

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

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

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

To configure the content of the synchronization log

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

   NOTE: Certain content create a lot of log data.

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

6. Click **OK**.

To synchronize on a regular basis

1. Select the category **Configuration | Start up configurations**.
2. Select a start up configuration in the document view and click **Edit schedule...**.
3. Edit the schedule properties.

4. To enable the schedule, click **Activate**.
5. Click **OK**.

To start initial synchronization manually

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

Related Topics

- Setting Up the Synchronization Server on page 12
- Users and Permissions for Synchronizing with Microsoft Exchange on page 11
- Testing Active Directory Domain Trusts on page 17
- Show Synchronization Results on page 26
- Recommendations for Synchronizing Microsoft Exchange on page 27
- Customizing Synchronization Configuration on page 30
- Default Template for Microsoft Exchange 2010 on page 128
- Default Template for Microsoft Exchange 2013 and Microsoft Exchange 2016 on page 129

Show Synchronization Results

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

To display a synchronization log

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

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

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

To display a provisioning log.

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

3. Click in the navigation view toolbar.

   Logs for all completed provisioning processes are displayed in the navigation view.

4. Select a log by double-clicking on it.

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

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

Synchronization logs are stored for a fixed length of time.

To modify the retention period for synchronization logs

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

Recommendations for Synchronizing Microsoft Exchange

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, e-mail users, e-mail contacts) of the entire Microsoft Exchange organization are synchronized.

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

For more information, see Creating a Synchronization Project for initial Synchronization of a Microsoft Exchange Environment on page 19.

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, e-mail users, e-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 **Complete organization** in the recipient scope.
    - 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. There are:

          ActiveSyncMailboxPolicy

          DatabaseAvailabilityGroup

          MailboxDatabase

          ManagedFolderMailboxPolicy (Microsoft Exchange 2010)

          OfflineAddressBook

          Organization

          PublicFolder

          PublicFolderDatabase (Microsoft Exchange 2010)

          RetentionPolicy

          RoleAssingmentPolicy

          Server

          SharingPolicy

          AddressList

          GlobalAddressList

2. Set up the synchronization project for synchronizing recipient of an Active Directory domain.

- Check **Only recipients of the following domain** on the recipient scope page and select a Microsoft Exchange domain.
- Customize the synchronization workflow.
  - Disable synchronization steps of all schema types that do not represent recipients. These are:

    ActiveSyncMailboxPolicy

    DatabaseAvailabilityGroup

    MailboxDatabase

    ManagedFolderMailboxPolicy (Microsoft Exchange 2010)

    OfflineAddressBook

    Organization

    PublicFolder

    PublicFolderDatabase (Microsoft Exchange 2010)

    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.
   - Open the first synchronization project for synchronizing recipients in the Synchronization Editor.
   - Create a new base object for every domain. Use the wizards to attach a base object.

- Select the Microsoft Exchange connector in the wizard and declare the connection parameter. The connection parameters are saved in a special variable set.

  NOTE: Take note of the following when setting up the connection:

  - Select a Microsoft Exchange server in the domain as server if possible.
  - Select **Only recipients of the following domain** again in the recipient scope.

- Create a new start up configuration for each domain. Use the new variable sets in the start up configuration.
- 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.

Customizing Synchronization Configuration

You have used the Synchronization Editor to set up a synchronization project for initial synchronization with Microsoft Exchange. You can use this synchronization project to load Microsoft Exchange objects into the One Identity Manager database. When you manage mailboxes, e-mail users, e-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.

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

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

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

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

Detailed information about this topic

- How to Configure Microsoft Exchange Synchronization on page 31
- Updating Schemas on page 32

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

To create a synchronization configuration for synchronizing Microsoft Exchange

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

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

Updating Schemas

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

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

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

- A schema was changed by:
  - Changes to a target system schema
  - Customizations to the One Identity Manager schema
  - A One Identity Manager update migration
- A schema in the synchronization project was shrunk by:
  - Activating the synchronization project
  - Synchronization project initial save
  - Compressing a schema

To update a system connection schema

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

   - OR -

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

   This reloads the schema data.

To edit a mapping

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

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

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

Speeding Up Synchronization with Revision Filtering

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

Microsoft Exchange supports revision filtering for the schema types "Mailbox", "MailUser", "MailContact", "MailPublicFolder", "DistributionGroup" and "DynamicDistributionGroup". The underlying Active Directory objects' date of last change is used as revision counter (whenChanged).

IMPORTANT: The revision algorithm can only be enabled in synchronization projects created with version 8.0. If revisioning was enabled in old 7.x synchronization projects, modifications made directly in Microsoft Exchange are also not identified.

It is recommended, you set up the synchronization projects again using the 8.0 implemented synchronization project template.

Determining the revision is done when synchronization starts. Objects changed after this point are included with the next synchronization.

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

To permit revision filtering on a workflow

- Edit the workflow properties. Select the entry **Use revision filter** from **Revision filtering**.

To permit revision filtering for a start up configuration

- Edit the start up configuration properties. Select the entry **Use revision filter** from **Revision filtering**.

NOTE: Specify whether revision filtering will be applied when you first set up initial synchronization in the project wizard.

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

Post-Processing Outstanding Objects

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

Objects marked as outstanding:

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

Start target system synchronization to do this.

To post-process outstanding objects

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

   All tables assigned to the target system type Microsoft Exchange as synchronization tables are displayed in the navigation view.
2. Select the table whose outstanding objects you want to edit in the navigation view.

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

   TIP:

   To display object properties of an outstanding object

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

   b. Open the context menu and click **Show object**.
3. Select the objects you want to rework. Multi-select is possible.
4. Click one of the following icons in the form toolbar to execute the respective method.

Table 10: Methods for handling outstanding objects

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

Icon	Method	Description
		process for the object. Prerequisites: • The table containing the object can be published. • The target system connector has write access to the target system.
	Reset	The "outstanding" label is removed from the object.

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

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

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

To disable bulk processing

- Deactivate in the form toolbar.

You must customize synchronization to synchronize custom tables.

To add custom tables to the target system synchronization.

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

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

Configuring Memberships Provisioning

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

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

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

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

To allow separate provisioning of memberships

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

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

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

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

Help for Analyzing Synchronization Issues

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

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

To generate a synchronization analysis report

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

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

Deactivating Synchronization

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

To prevent regular synchronization

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

  Now you can only start synchronization manually.

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

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

To deactivate the loaded synchronization project

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

Related Topics

- Creating a Synchronization Project for initial Synchronization of a Microsoft Exchange Environment on page 19

3

Base Data for Managing Microsoft Exchange

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

- Configuration parameter

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

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

  For more information, see Appendix: Configuration Parameters for Managing Microsoft Exchange on page 127.

- Account definitions

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

  For more information, see Setting Up Account Definitions on page 40.

- Target system types

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

  For more information, see Post-Processing Outstanding Objects on page 34.

- Target system managers

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

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

For more information, see Target System Managers on page 57.

Setting Up Account Definitions

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

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

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

The following steps are necessary to implement an account definition:

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

Creating an Account Definition

To create a new account definition

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

   - OR -

   Click in the result list toolbar.

3. Enter the account definition's master data.
4. Save the changes.

Detailed information about this topic

- Master Data for an Account Definition on page 41

Master Data for an Account Definition

Enter the following data for an account definition:

Table 11: Master Data for an Account Definition

Property	Description
Account definition	Account definition name.
User account table	Table in the One Identity Manager schema which maps user accounts.
Target System	Target system to which the account definition applies.
Required account definition	Required account definitions. Define the dependencies between account definitions. When this account definition is requested or assigned, the required account definition is automatically requested or assigned with it. Enter the account definition of the associated Active Directory domain.
Description	Spare text box for additional explanation.
Manage level (initial)	Manage level to use by default when you add new user accounts.
Risk index	Value for evaluating the risk of account definition assignments to employees. Enter a value between 0 and 1. This property is only visible when the configuration parameter QER\CalculateRiskIndex is set. For more detailed information, see the One Identity Manager Risk Assessment Administration Guide.
Service item	Service item through which you can request the account definition in the IT Shop. Assign an existing service item or add a new one.
IT Shop	Specifies whether the account definition can be requested through the IT Shop. The account definition can be ordered by an employee over the Web Portal and distributed using a defined approval process. The account definition can still be directly assigned to employees and roles outside the IT Shop.

Property	Description
Only for use in IT Shop	Specifies whether the account definition can only be requested through the IT Shop. The account definition can be ordered by an employee over the Web Portal and distributed using a defined approval process. This means, the account definition cannot be directly assigned to roles outside the IT Shop.
Automatic assignment to employees	Specifies whether the account definition is assigned automatically to all internal employees. The account definition is assigned to every employee not marked as external, on saving. New employees automatically obtain this account definition as soon as they are added. IMPORTANT: Only set this option if you can ensure that all current internal employees in the database and all pending newly added internal employees obtain a user account in this target system. Disable this option to remove automatic assignment of the account definition to all employees. The account definition cannot be reassigned to employees from this point on. Existing account definition assignments remain intact.
Retain account definition if permanently disabled	Specifies the account definition assignment to permanently disabled employees. Option set: the account definition assignment remains in effect. The user account stays the same. Option not set: the account definition assignment is not in effect.The associated user account is deleted.
Retain account definition if temporarily disabled	Specifies the account definition assignment to temporarily disabled employees. Option set: the account definition assignment remains in effect. The user account stays the same. Option not set: the account definition assignment is not in effect.The associated user account is deleted.
Retain account definition on deferred deletion	Specifies the account definition assignment on deferred deletion of employees. Option set: the account definition assignment remains in effect. The user account stays the same. Option not set: the account definition assignment is not in effect.The associated user account is deleted.
Retain account definition on security risk	Specifies the account definition assignment to employees posing a security risk . Option set: the account definition assignment remains in effect. The user account stays the same.

Property	Description
	Option not set: the account definition assignment is not in effect.The associated user account is deleted.
Resource type	Resource type for grouping account definitions.
Spare field 01 - spare field 10	Additional company specific information. Use the Designer to customize display names, formats and templates for the input fields.

Setting Up Manage Levels

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

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

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

- Unmanaged

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

- Full managed

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

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

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

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

- Employee user accounts can be locked when they are disabled, deleted or rated as a security risk so that permissions are immediately withdrawn. If the employee is

reinstated at a later date, the user accounts are also reactivated.

- You can also define group membership inheritance. Inheritance can be discontinued if desired when, for example, the employee's user accounts are disabled and therefore cannot be members in groups. During this time, no inheritance processes should be calculated for this employee. Existing group memberships are deleted!

To assign manage levels to an account definition

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

   - OR -

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

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

To edit a manage level

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

   - OR -

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

Related Topics

- Master Data for a Manage Level on page 44

Master Data for a Manage Level

Enter the following data for a manage level.

Table 12: Master Data for a Manage Level

Property	Description
Manage level	Name of the manage level.

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

Creating a Formatting Rule for IT Operating Data

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

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

- Microsoft Exchange mailbox database

To create a mapping rule for IT operating data

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

Table 13: Mapping rule for IT operating data

Property	Description
Column	User account property for which the value is set.
Source	Specifies which roles to use in order to find the user account properties. You have the following options: • Primary department • Primary location • Primary cost center • Primary business roles NOTE: Only use the primary business role if the Business Roles Module is installed. • Empty If you select a role, you must specify a default value and set the option **Always use default value**.
Default value	Default value of the property for an employee's user account if the value is not determined dynamically from the IT operating data.
Always use default value	Specifies whether user account properties are always filled with the default value. IT operating data is not determined dynamically from a role.
Notify when applying the standard	Specifies whether email notification to a defined mailbox is sent when the default value is used. Use the mail template "Employee - new user account with default properties created". To change the mail template, modify the configuration parameter "TargetSystem\ADS\Exchange2000\Accounts\MailTemplateDefaultValues".

4. Save the changes.

Related Topics

- Determining IT Operating Data on page 47

Determining IT Operating Data

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

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

Example:

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

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

To specify IT operating data

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

Table 14: IT Operating Data

Property	Description
Organization/Business role	Department, cost center, location or business role for which the IT operating data is valid.
Effects on	IT operating data application scope. The IT operating data can be used for a target system or a defined account definition. ***To specify an application scope***

Property	Description
	a. Click → next to the text box. b. Select the table under **Table**, which maps the target system or the table TSBAccountDef for an account definition. c. Select the concrete target system or concrete account definition under **Effects on**. d. Click **OK**.
Column	User account property for which the value is set. Columns using the script template TSB_ITDataFromOrg in their template are listed. For more detailed information, see the One Identity Manager Target System Base Module Administration Guide.
Value	Concrete value which is assigned to the user account property.

3. Save the changes.

Related Topics

- Creating a Formatting Rule for IT Operating Data on page 45

Modifying IT Operating Data

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

Prerequisites

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

  - OR -

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

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

To execute the template

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

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

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

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

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

Assigning Account Definitions to Employees

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

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

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

Prerequisites for indirect assignment of account definitions to employees

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

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

Detailed information about this topic

- Assigning Account Definitions to Departments, Cost Centers and Locations on page 50
- Assigning Account Definitions to Business Roles on page 51
- Assigning Account Definitions to all Employees on page 51
- Assigning Account Definitions Directly to Employees on page 52
- Assigning Account Definitions to a Target System on page 54

Assigning Account Definitions to Departments, Cost Centers and Locations

To add account definitions to hierarchical roles

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

   - OR -

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

Related Topics

- Assigning Account Definitions to Business Roles on page 51
- Assigning Account Definitions to all Employees on page 51
- Assigning Account Definitions Directly to Employees on page 52

Assigning Account Definitions to Business Roles

Installed Modules: Business Roles Module

To add account definitions to hierarchical roles

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

   - OR -

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

Related Topics

- Assigning Account Definitions to Departments, Cost Centers and Locations on page 50
- Assigning Account Definitions to all Employees on page 51
- Assigning Account Definitions Directly to Employees on page 52

Assigning Account Definitions to all Employees

To assign an account definition to all employees

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

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

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

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

Related Topics

- Assigning Account Definitions to Departments, Cost Centers and Locations on page 50
- Assigning Account Definitions to Business Roles on page 51
- Assigning Account Definitions Directly to Employees on page 52

Assigning Account Definitions Directly to Employees

To assign an account definition directly to employees

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

   - OR -

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

Related Topics

- Assigning Account Definitions to Departments, Cost Centers and Locations on page 50
- Assigning Account Definitions to Business Roles on page 51
- Assigning Account Definitions to all Employees on page 51

Assigning Account Definitions to System Roles

Installed Modules: System Roles Module

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

To add account definitions to a system role

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

4. Assign system roles in **Add assignments**.

   - OR -

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

Adding Account Definitions in the IT Shop

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

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

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

To add an account definition to the IT Shop

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

   - OR -

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

To remove an account definition from individual IT Shop shelves

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

   - OR -

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

To remove an account definition from all IT Shop shelves

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

   - OR -

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

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

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

Related Topics

- Master Data for an Account Definition on page 41
- Assigning Account Definitions to Departments, Cost Centers and Locations on page 50
- Assigning Account Definitions to Business Roles on page 51
- Assigning Account Definitions Directly to Employees on page 52
- Assigning Account Definitions to System Roles on page 52

Assigning Account Definitions to a Target System

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

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

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

To assign the account definition to a target system

1. Select the domain in the category **Active Directory | Domains**.
2. Select **Change master data** in the task view.

3. Enter the account definition on the **Exchange** tab.
    a. Select the account definition for mailboxes from **Mailbox definition (initial)**.
    b. Select the account definition for contacts from **E-mail contact definition (initial)**.
    c. Select the account definition for e-mail users from **E-mail user definition (initial)**.
4. Save the changes.

Related Topics

- Assigning Account Definitions to Employees on page 49

Deleting an Account Definition

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

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

To delete an account definition

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

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

b. Select an account definition in the result list.

c. Select **Assign organizations**.

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

e. Save the changes.

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

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

b. Select an account definition in the result list.

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

Remove business roles from **Remove assignments**.

d. Save the changes.

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

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

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

b. Select an account definition in the result list.

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

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

e. Save the changes.

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

a. Select the domain in the category **Active Directory | Domains**.

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

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

d. Save the changes.

8. Delete the account definition.

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

b. Select an account definition in the result list.

c. Click , to delete the account definition.

Target System Managers

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

Implementing Application Roles for Target System Managers

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

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

Table 15: Default Application Roles for Target System Managers

User	Task
Target System Managers	Target system managers must be assigned to the application role **Target systems | Exchange** or a sub application role. Users with this application role: • Assume administrative tasks for the target system. • Create, change or delete target system objects, like user accounts or groups. • Edit password policies for the target system. • Prepare for adding to the IT Shop. • Configure synchronization in the Synchronization Editor and defines the mapping for comparing target systems and One Identity Manager. • Edit the synchronization's target system types and outstanding objects. • Authorize other employees within their area of responsibility as target system managers and create child application roles if required.

To initially specify employees to be target system administrators

1. Log in to the Manager as One Identity Manager administrator (application role **Base role | Administrators**)

2. Select the category **One Identity Manager Administration | Target systems | Administrators**.
3. Select **Assign employees** in the task view.
4. Assign the employee you want and save the changes.

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

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

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

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

To define target system managers for individual Microsoft Exchange organizations.

1. Login to the Manager as target system manager.
2. Select the category **Active Directory | Exchange system administration**.
3. Select **Change master data** in the task view.
4. Select the application role on the **General** tab in the **Target system manager** menu.

   - OR -

   Click next to the **Target system manager** menu to create a new application role.
   - Enter the application role name and assign the parent application role **Target system | Exchange**.
   - Click **OK** to add the new application role.
5. Save the changes.
6. Assign the application role to employees, who are authorized to edit the in One Identity Manager.

Related Topics

- One Identity Manager Users for Managing Microsoft Exchange on page 8
- Microsoft Exchange Organization on page 61

4

Microsoft Exchange Structure

Structure elements in Microsoft Exchange that are not server dependent, are matched by each Microsoft Exchange Server. This effects 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 effects 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 Organization

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

To edit organization master data

1. Select the category **Active Directory | Exchange system administration**.
2. Select the organization from the result list.
3. Select **Change master data** in the task view.
4. Save the changes.

Table 16: Organization Master 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 works in mixed or single mode.
Target system manager	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. 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.
Synchronized by	NOTE: You can only specify the synchronization type when adding a new organization. No changes can be made after saving. "One Identity Manager" is used when you create a organization

Property	Description
	with the Synchronization Editor. Type of synchronization through which the data is synchronized between the organization and One Identity Manager. **Table 17: 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 on page 57

Microsoft Exchange Mailbox Databases

Mailbox data is stored in the mailbox database (messages received, attachments, folders, documents).

To display mailbox database master data

1. Select the category **Active Directory | Exchange system administration | <organization> | Organization configuration | Mailbox databases**.
2. Select a mailbox database in the result list.
3. Select **Change master data** in the task view.

To display the mailbox server of a mailbox database master data

1. Select the category **Active Directory | Exchange system administration | <organization> | Organization configuration | Mailbox databases**.
2. Select a mailbox database in the result list.
3. Select **Change master data** in the task view.

Table 18: Mailbox Database Master Data

Property	Description
Exchange organization	Name of the organization.
identifier	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	Specifies whether objects are allowed to be deleted after a final backup is run.

Property	Description
before a backup is made	
Journal recipient	All messages sent using the mailbox database are logged in this mailbox or distribution group.
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.

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, email users, email 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 master data

1. Select the category **Active Directory | Exchange System administration | <organization> | Organization configuration | Address lists**.
2. Select the address list in the result list.
3. Select **Change master data** in the task view.

Table 19: Address List Master Data

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

Property	Description
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.
E-mail users	Specifies whether email users are permitted in the address list.
E-mail contacts	Specifies whether email 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 master data of an offline address list

1. Select the category **Active Directory | Exchange System administration | <organization> | Organization configuration | Offline address lists**.
2. Select the offline address list in the result list.
3. Select **Change master data** in the task view.

Table 20: Offline Address List Master 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.
Server	Microsoft Exchange server where the offline address list is stored.
Supports Outlook	Information about which Outlook versions are supported.
Calculation schedule	Update interval for the offline address list.

Microsoft Exchange Public Folders

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

To display public folder master data

1. Select the category **Active Directory | Exchange system administration | <organization> | Organization configuration | Public folders**.
2. Select the public folder in the result list.
3. Select **Change master data** in the task view.

Table 21: Public Folder Master 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	Path to the public folder.
Read state per user	Specifies whether users can show information about read and unread messages.

To display master data for a public folder

1. Select the category **Active Directory | Exchange system administration | <organization> | Organization configuration | Public folder database**.
2. Select the public folder database in the result list.
3. Select **Change master data** in the task view.

Table 22: Master 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.
Master server	If this is a copy of the database, the server on which the original copy is to be found is entered here.

Property	Description
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 master data

1. Select the category **Active Directory | Exchange system administration | <organization> | Server configuration.**
2. Select the server in the result list.
3. Select **Change master data** in the task view.

To display a mailbox server's mailbox database.

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

Table 23: Server Master Data

Property	Description
Exchange organization	Name of the organization.
Active Directory computer	Computer on which the Microsoft Exchange server is installed.
Server	Name of the server.
Distinguished name	Distinguished name of the server.
Function	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. Select the category **Active Directory | Exchange system administration | <organization> | Organization configuration | Database availability groups**.
2. Select the database availability group in the result list.
3. Select **Change master data** in the task view.

Table 24: Database Availability Group Master 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.

Sharing 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. Select the category **Active Directory | Exchange system administration | <organization> | Policies | Share policies**.
2. Select the policy from the result list.
3. Select **Assign mailboxes** in the task view.
4. Assign mailboxes in **Add assignments**.

   - OR -

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

To display master data for a sharing policy

1. Select the category **Active Directory | Exchange system administration | <organization> | Policies | Share policies**.
2. Select the policy from the result list.
3. Select **Change master data** in the task view.

Table 25: Sharing Policy Master Data

Property	Description
Exchange organization	Name of the organization.
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 the 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. Select the category **Active Directory | Exchange system administration | <organization> | Policies | Retention policies**.
2. Select the policy from the result list.
3. Select **Assign mailboxes** in the task view.

4. Assign mailboxes in **Add assignments**.

   - OR -

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

To display master data for a retention policy

1. Select the category **Active Directory | Exchange system administration | <organization> | Policies | Retention policies**.
2. Select the policy from the result list.
3. Select **Change master data** in the task view.

Table 26: Retention Policy Master Data

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

Policies for Mobile Email Queries

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

To assign policies to mailboxes

1. Select the category **Active Directory | Exchange system administration | <organization> | Policies | Email policies**.
2. Select the policy from the result list.
3. Select **Assign mailboxes** in the task view.
4. Assign mailboxes in **Add assignments**.

   - OR -

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

To display policy master data for a mobile email query

1. Select the category **Active Directory | Exchange system administration | <organization> | Policies | Email policies**.
2. Select the policy from the result list.
3. Select **Change master data** in the task view.

Table 27: Email Policy Master Data

Property	Description
Exchange organization	Name of the organization.
Name	Name of the 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.
Encrypt password	Specifies whether device encryption is required.
Simple passwords allowed	Specifies whether a simple password is allowed.
Min. 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 restore 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 blocked.
Lock if inactive for [min]	Number of minutes without activity before the device is locked.
Attachments download permitted	Specifies whether attachments are automatically downloaded.
Max. mail attachment size	Maximum size of mail attachment that can be automatically downloaded.

Property	Description
Default	Specifies whether this is the default policy.

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. Select the category **Active Directory | Exchange system administration | <organization> | Policies | Folder management policies**.
2. Select the policy from the result list.
3. Select **Assign mailboxes** in the task view.
4. Assign mailboxes in **Add assignments**.

   - OR -

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

To display master data for a folder management policy

1. Select the category **Active Directory | Exchange system administration | <organization> | Policies | Folder management policies**.
2. Select the policy from the result list.
3. Select **Change master data** in the task view.

Table 28: Master 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. Select the category **Active Directory | Exchange system administration | <organization> | Policies | Role assignment policies**.
2. Select the policy from the result list.
3. Select **Assign mailboxes** in the task view.
4. Assign mailboxes in **Add assignments**.

   - OR -

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

To display master data for a role assignment policy

1. Select the category **Active Directory | Exchange system administration | <organization> | Policies | Role assignment policies**.
2. Select the policy from the result list.
3. Select **Change master data** in the task view.

Table 29: Role Assignment Policy Master 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.

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. Select the category **Active Directory | Exchange system administration | <organization> | Policies | Outlook Web App mailbox policies**.
2. Select the policy in the result list.
3. Select **Assign mailboxes** in the task view.
4. Assign mailboxes in **Add assignments**.

   - OR -

Remove mailboxes from **Remove assignments**.

5. Save the changes.

To display master data for a role assignment policy

1. Select the category **Active Directory | Exchange system administration | <organization> | Policies | Outlook Web App mailbox policies**.
2. Select the policy in the result list.
3. Select **Change master data** in the task view.

5

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 30: 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. This mailbox type can only be created for disabled user accounts.
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.
Legacy mailbox	Legacy mailboxes are mailboxes from previous 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 mail, which is used as target mailbox for searches through eDiscovery in Microsoft Exchange, is created by default. These mailboxes are loaded into One Identity Manager by synchronization and cannot be edited.

Detailed information about this topic

- Entering Master Data for Mailboxes on page 76
- Disabling Mailboxes on page 87
- Deleting and Restoring Mailboxes on page 88
- Receive Restrictions for Mailboxes on page 89
- Permission "Send on behalf of" for Mailboxes on page 90

Entering Master Data for Mailboxes

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

NOTE: Equipment mailboxes, room 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 employees.

- In order to create mailboxes through account definitions, the employee 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.
- In this case, some of the master data described in the following is mapped through templates from employee master data.

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

1. Select the category **Active Directory | User accounts**.
2. Select the user account in the result list and run **Create mailbox** in the task view.
3. Save the changes.

To edit a mailbox

1. Select the category **Active Directory | Mailboxes**.
2. Select the mailbox in the result list and run the task **Change master data**.
3. Edit the mailbox's master data.
4. 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

- Mailbox General Master Data on page 77
- Calendar Settings for Mailboxes on page 80
- Limits for a Mailbox on page 81
- Mailbox Archive on page 82
- Mailbox Retention on page 83
- Mailbox Functions on page 84
- Booking Resources on page 84

Related Topics

- Setting Up Account Definitions on page 40
- Deleting and Restoring E-Mail Users on page 96

Mailbox General Master Data

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

Table 31: Mailbox General Master Data

Property	Description
Employee	Employee using the mailbox. An employee is already entered if the mailbox was generated by an account definition. If you create the mailbox manually, you can select an employee in the menu.
Account definition	Account definition through which the mailbox was created. Use the account definition to automatically populate mailbox master data and to specify a manage level for the mailbox. One Identity Manager finds the IT operating data of the assigned employee and uses it to populate the corresponding fields in the mailbox. NOTE: The account definition cannot be changed once the mailbox has been saved.
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 for which this mailbox is created.

Property	Description
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 mailbox type "linked mailbox". The linked mailbox itself is disabled. Disabling in One Identity Manager Service is done by the Active Directory. 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. The mailbox type is specified when a mailbox is added and cannot be changed afterward. Available mailbox types are: user, room, equipment, linked, legacy, share and discovery.
Alias	Unique alias for further identification of the mailbox.
Mailbox database	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 employee depending on the mailbox manage level. This data is optional. If empty, Microsoft Exchange decides which mailbox database is used.
Automatically update based on recipient policy	Specifies whether changes to recipient's email addresses are automatically updated based on incoming settings.
Proxy addresses	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). Use the following syntax to set up other proxy addresses: `Address type: new email address`
Sender authentication required	Specifies whether authentication data is requested from senders. Set this option to prevent anonymous senders mailing to the mailbox.
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.

Property	Description
Alternative recipient	Alternative recipient to which messages from this mailbox are forwarded. You can either enter an alternative recipient, a recipient group or a receive folder. ***To specify an alternative recipient*** 1. Click → next to the text box. 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.
Folder policy	Mailbox policy for folder administration.
Role assign-ment 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.
Mailbox is locked	Specifies whether the mail box is locked.
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.
Distinguished name	Active Directory user account's distinguished name.
Distinguished Exchange name	Mailbox's distinguished name.

Related Topics

- Setting Up Account Definitions on page 40
- Sharing Policies on page 68
- Folder Administration Policies on page 72
- Role Assignment Policies on page 72
- Disabling Mailboxes on page 87

Calendar Settings for 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 data on the **Calendar** tab.

Table 32: Mailbox Calendar Settings

Property	Description
Enable Calendar Attendant	Specifies whether the Calendar Attendant is enabled for mailboxes. Other settings become available once the Calendar Attendant is enabled. **Table 33: Permitted Values** **Value** / **Meaning** Disable Calendar Attendant — The Calendar Attendant is not enabled. Enable Calendar Attendant — The Calendar Attendant is enabled. Enable Resource Booking Attendant — The Resource Booking Attendant is automatically enabled for mailboxes of type "room mailbox".
New meeting requests are marked with the status "tentative".	Specify whether meeting requests are marked with the state "Tentative" in the calendar.
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 message are moved to the "Deleted objects" folder.

Related Topics

- Booking Resources on page 84

Limits for a Mailbox

Enter the following master data on the **Limits** tab.

Table 34: 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 [KB]	Used disk space in KB. 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 size [KB]	Maximum size for message in KB that a mailbox 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.
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	Specifies whether objects are allowed to be deleted after a final backup is run.

Property	Description
permanently before a backup is made	
Max. number subfolders	Maximum number of subfolders allowed in a mailbox. This property is available from Microsoft Exchange Server 2013 or later.
Warn at [subfolder]	Number of subfolders which can be created before the user is sent a warning. This property is available from Microsoft Exchange Server 2013 or later.
Max. folder levels	Maximum number of levels in the mailbox folder structure. This property is available from Microsoft Exchange Server 2013 or later.
Warn at [folder levels]	Number of folder levels which can be created before the user is sent a warning. This property is available from Microsoft Exchange Server 2013 or later.
Max. recoverable items	Maximum number of messages allowed in a folder in the "Recoverable items" folder. This property is available from Microsoft Exchange Server 2013 or later.
Warn at [recoverable items]	Number of item a folder in the "Recoverable items" folder can contain before a warning is sent to the user. This property is available from Microsoft Exchange Server 2013 or later.

Related Topics

- Microsoft Exchange Mailbox Databases on page 62

Mailbox Archive

You can configure personal archives with which users can save messages in an archive mailbox.

Enter the following master data on the **Archive** tab.

Table 35: 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.

Property	Description
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.

Mailbox Retention

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

Table 36: Mailbox Retention Master Data

Property	Description
Retention policy	Retention policy applying to this mailbox.
Retention hold during this period	Specifies whether retention is temporary stopped 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 **Start date** and **End date**.
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 option **Litigation hold** 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 option **Litigation hold** is set. This data is displayed to the user in Outlook.

Related Topics

- Retention Policies on page 69

Mailbox Functions

Enter the following master data on the **Functions** tab.

Table 37: Mailbox Functions

Property	Description
Outlook Web Access enabled	Specifies whether the function for Microsoft Office Outlook Web App is enabled. Office Outlook Web App allows mailbox access over the web browser.
Mobile access	Specifies whether mobile devices can access the mailbox.
Email policy	Mailbox policy for mobile email queries. Mailbox policies for mobile email queries contain settings that come into effect when data is accessed in the Microsoft Exchange organization with mobile devices through the synchronization protocol Exchange ActiveSync.
MAPI enabled	Specifies whether the function for MAPI access is enabled. MAPI allows mailbox access through a MAPI client, like Outlook.
POP3 enabled	Specifies whether the function for POP3 access is enabled.
IMAP4 enabled	Specifies whether the function for IMAP4 access is enabled.

Related Topics

- Policies for Mobile Email Queries on page 70

Booking Resources

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

Enter the following master data on the **Resources** tab.

Table 38: Master Data for Booking Resources

Property	Description
Enable Calendar Attendant	Specifies whether the Resource Booking Attendant is enabled for device mailboxes and room mailboxes so that booking requests can be processed automatically.

<table>
<tr><th>Property</th><th>Description</th></tr>
<tr><td></td><td>Table 39: Permitted Values
<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>Disable Calendar Attendant</td><td>The Calendar Attendant is not enabled.</td></tr>
<tr><td>Enable Calendar Attendant</td><td>The Calendar Attendant is enabled.</td></tr>
<tr><td>Enable Resource Booking Attendant</td><td>The Resource Booking Attendant is automatically enabled for device and room mailboxes.</td></tr>
</table></td></tr>
<tr><td>Reject repeated meeting after max. planning period</td><td>Specifies whether booking series can be set up beyond the planning period.</td></tr>
<tr><td>Forward meeting requests</td><td>Specifies whether meeting requests are forwarded to the resource mailbox deputy managers. The deputy decides about the meeting request.</td></tr>
<tr><td>Max. booking window [days]</td><td>Maximum planning period for meeting request in days.</td></tr>
<tr><td>Max. duration [min]</td><td>Maximum time allowed booking the resource.</td></tr>
<tr><td>Max. conflicting instances</td><td>Maximum conflicts permitted for meeting series which overlap with other meetings. If the value is exceeded, the series request is denied.</td></tr>
<tr><td>Max. series conflicts [%]</td><td>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.</td></tr>
<tr><td>Remove attachments from meeting requests</td><td>Specifies whether attachments are deleted from meeting requests.</td></tr>
<tr><td>Remove comments from meeting requests</td><td>Specifies whether message text is deleted from meeting requests.</td></tr>
<tr><td>Remove subject from meeting requests</td><td>Specifies whether the subject is deleted from meeting requests.</td></tr>
<tr><td>Only retain calendar meetings</td><td>Specifies whether elements that do not belong the calendar are deleted.</td></tr>
</table>

Property	Description
Add organizer's name to subject	Specifies whether the organizer's name is given in the meeting request subject field.
Remove "private" flag from accepted meeting	Specifies whether the state "Private" is deleted from meeting requests.
Mark meeting requests as "Tentative"	Specifies whether meeting requests are marked with the state "Tentative" in the calendar. If this option is disabled, meeting requests are marked with the state "Free".
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 input field **Additional information**.
Additional information	Additional information for responding to meeting requests.
Booking permissions for everyone	Specifies whether meeting requests conforming to policy are automatically approved for all users. If this option is not set, use the task **Assign booking permissions** to specify individual users who can send requests conforming to policy, which are automatically approved.
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 the task **Assign out-of-policy meeting request permission** to specify individual users who can send requests which are policy non-conform.
Booking permissions for everyone	Specifies whether all users can send booking requests that conform to policy. These requests are decided by the mailbox delegate unless the option **Booking permissions for everyone** is set. If this option is not set, use the task **Assign in-policy meeting request permissions** 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.

Property	Description
Resource capacity	Resource capacity, for example, the number of seats in a meeting room.

Related Topics

- Permission "Send on behalf of" for Mailboxes on page 90

Disabling Mailboxes

Table 40: Configuration Parameters for Disabling Mailboxes

Configuration parameter	Meaning
QER\Person\TemporaryDeactivation	When this parameter is set, the employee's user accounts are locked when the employee is temporarily or permanently disabled.

How you disabled and delete an employee's mailboxes depends on the type of mailbox administration.

Scenario:

- Mailboxes are managed through account definitions.

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

Scenario:

- Mailboxes are not managed through account definitions.

The behavior depends on the configuration parameter "QER\Person\TemporaryDeactivation".

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

To lock a mailbox when the configuration parameter is not set

1. Select the category **Active Directory | Mailboxes**.
2. Select a mailbox in the result list.

3. Select **Change master data** in the task view.
4. Set the option **Mailbox is disabled** on the **General** tab.
5. Save the changes.

Scenario:

- Mailboxes not linked to employees.

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

1. Select the category **Active Directory | Mailboxes**.
2. Select a mailbox in the result list.
3. Select **Change master data** in the task view.
4. Set the option **Mailbox is disabled** on the **General** tab.
5. Save the changes.

Related Topics

- Creating an Account Definition on page 40
- Setting Up Manage Levels on page 43
- Deleting and Restoring Mailboxes on page 88

Deleting and Restoring Mailboxes

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

To delete a mailbox

1. Select the category **Active Directory | Mailboxes**.
2. Select a mailbox in the result list.
3. Delete the mailbox using .
4. Confirm the security prompt with **Yes**.

To restore a mailbox

1. Select the category **Active Directory | Mailboxes**.
2. Select a mailbox in the result list.
3. Click **Undo delete** in the result list toolbar.

When you delete a mailbox, the option **Do not display in address lists** is enabled and the mailbox is no longer shown in address books. Furthermore, the settings **Use default**

database values, **Max. send size [KB]**, **Max. receiving size [KB]**, **Prohibit transfer at [KB]** and **Prohibit send at [KB]** are reset so that no email messages can be received or send with this mailbox.

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 the delete delay has expired. You can configure an alternative deletion delay on the table `EX0MailBox` in the Designer.

Related Topics

- Disabling Mailboxes on page 87

Receive Restrictions for Mailboxes

NOTE: Assignments **Assign mail acceptance** and **Assign mail rejection** 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 mailboxes

1. Select the category **Active Directory | Mailboxes**.
2. Select a mailbox in the result list.
3. Select **Assign mail acceptance** in the task view to establish from which recipients messages are accepted.

   - OR -

   Select **Assign mail rejection** in the task view to specify from which recipients messages are not accepted.
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
   - E-mail users
   - Email contacts
5. Assign recipients in **Add assignments**.

   - OR -

   Remove recipients from **Remove assignments**.
6. Save the changes.

Permission "Send on behalf of" for Mailboxes

Use the send permission "Send on behalf of" to specify which users can send messages on behalf of the mailbox owner.

To modify the permission "Send on behalf of" for mailboxes

1. Select the category **Active Directory | Mailboxes**.
2. Select a mailbox in the result list.
3. Select **Assign send authorizations** in the task view.
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
    - E-mail users
5. Assign users in **Add assignments**.

    - OR -

    Remove users from **Remove assignments**.
6. Save the changes.

E-Mail Users and E-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 Active Directory user accounts (e-mail users) and mail-enabled Active Directory contacts (e-mail contacts) in One Identity Manager.

Detailed information about this topic

Entering Master Data for E-Mail Users

Enter e-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 an e-mail user for this user account.

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

- In order to create e-mail users through account definitions, employees 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.
- In this case, some of the master data described in the following is mapped through templates from employee master data.

To create an e-mail user for an Active Directory user account manually

1. Select the category **Active Directory | User accounts**.
2. Select the user account in the result list and run **Create e-mail user** in the task view.
3. Save the changes.

To edit an e-mail user.

1. Select the category **Active Directory | E-mail users**.
2. Select the e-mail user in the result list and run the task **Change master data**.
3. Edit the email user's master data.
4. Save the changes.

Table 41: General Data of an E-Mail User

Property	Description
Employee	Employee to use the e-mail user. An employee is already entered if the e-mail user was generated by an account definition. If you create the e-mail user manually, you can select an employee in the menu.
Account definition	Account definition through which the e-mail user was created. Use the account definition to automatically populate e-mail user master data and to specify a manage level for the e-mail user. The One Identity Manager finds the IT operating data of the assigned employee and uses it to populate the corresponding fields in the e-mail user. NOTE: The account definition cannot be changed once the e-mail user has been saved.
Manage level	Manage level with which the e-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.
Active Directory account	Active Directory user account for which the e-mail user is created.
Exchange organization	Name of the organization.
Canonical name	Canonical name of the e-mail user. 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

Property	Description
	type (SMTP, X400).
Alias	Unique alias for further identification of the e-mail user.
Automatically update based on recipient policy	Specifies whether changes to recipient's email addresses are automatically updated based on incoming settings.
Proxy addresses	Other email addresses for the e-mail user. You can also add other mail connectors (for example, CCMail, MS) in addition to the standard address type (SMTP, X400). Use the following syntax to set up other proxy addresses: `Address type: new email address`
Max. send size [KB]	Maximum size for message in KB that an e-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 an e-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 e-mail user is visible in address books. Set this option if you want to prevent the e-mail user from being displayed in address books. This option applies to all address books.
Use MAPI-RTF	Specifies whether the e-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 e-mail user.
Simple display	Simple display name for systems that cannot interpret all the characters of normal display names.
Distinguished name	E-mail user's distinguished name.

Related Topics

- Setting Up Account Definitions on page 40
- Deleting and Restoring Mailboxes on page 88

Entering Master Data for E-Mail Contacts

Enter e-mail contacts for Active Directory contacts.

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

- In order to create e-mail contacts through account definitions, employees 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.
- In this case, some of the master data described in the following is mapped through templates from employee master data.

To create an e-mail contact for an Active Directory contact manually

1. Select the contact in the result list and run **Create e-mail contact** in the task view.
2. Save the changes.

To edit an e-mail contact

1. Select the category **Active Directory | E-mail contacts**.
2. Select the e-mail contact in the result list and run the task **Change master data**.
3. Edit the email contact's master data.
4. Save the changes.

Table 42: General Data of an E-Mail Contact

Property	Description
Employee	Employee to use the e-mail contact. An employee is already entered if the e-mail contact was generated by an account definition. If you create the e-mail contact manually, you can select an employee in the menu.
Account definition	Account definition through which the e-mail contact was created. Use the account definition to automatically populate e-mail contact master data and to specify a manage level for the e-mail contact. The One Identity Manager finds the IT operating data of the assigned employee and uses it to populate the corresponding fields in the e-mail contact. NOTE: The account definition cannot be changed once the e-mail contact has been saved.
Manage level	Manage level with which the e-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

Property	Description
	account definition are available in the menu.
Active Directory contact	Active Directory contact for whom the e-mail is created.
Exchange organization	Name of the organization.
Canonical name	Canonical name of the e-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 e-mail contact.
Automatically update based on recipient policy	Specifies whether changes to recipient's email addresses are automatically updated based on incoming settings.
Proxy addresses	Other email addresses for the e-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 an e-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 an e-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 e-mail contact is visible in address books. Set this option if you want to prevent the e-mail contact from being displayed in address books. This option applies to all address books.
Use MAPI-RTF	Specifies whether the e-mail contact can receive messages in MAPI format. Available options are "Never", "Always" and "Use default settings".

Property	Description
Sender authentication required	Specifies whether authentication data is requested from senders. Set this option to prevent anonymous senders mailing the e-mail contact.
Simple display	Simple display name for systems that cannot interpret all the characters of normal display names.
Distinguished name	E-mail contact's distinguished name.

Related Topics

- Disabling Mailboxes on page 87
- Setting Up Account Definitions on page 40

Deleting and Restoring E-Mail Users

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

To delete an e-mail user

1. Select the category **Active Directory | E-mail users**.
2. Select the e-mail user in the result list.
3. Delete the e-mail user with .
4. Confirm the security prompt with **Yes**.

To restore an e-mail user

1. Select the category **Active Directory | E-mail users**.
2. Select the e-mail user in the result list.
3. Click **Undo delete** in the result list toolbar.

When you delete an e-mail user, the option **Do not display in address lists** is enabled and the e-mail user is no longer shown in address books.

Configuring Deferred Deletion

By default, e-mail users are finally deleted from the database after 30 days. During this period you have the option to reactivate the e-mail users. A restore is not possible once the delete delay has expired. You can configure an alternative deletion delay on the table `EX0MailUser` in the Designer.

Deleting and Restoring E-Mail Contacts

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

To delete an e-mail contact

1. Select the category **Active Directory | E-mail contacts**.
2. Select the e-mail contact in the result list.
3. Delete the e-mail contact with .
4. Confirm the security prompt with **Yes**.

To restore an e-mail contact

1. Select the category **Active Directory | E-mail contacts**.
2. Select the e-mail contact in the result list.
3. Click **Undo delete** in the result list toolbar.

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

Configuring Deferred Deletion

By default, e-mail contacts are finally deleted from the database after 30 days. During this period you have the option to reactivate the e-mail contacts. A restore is not possible once the delete delay has expired. You can configure an alternative deletion delay on the table `EX0MailContact` in the Designer.

Receive Restrictions for E-Mail Users

NOTE: Assignments **Assign mail acceptance** and **Assign mail rejection** 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 e-mail users

1. Select the category **Active Directory | E-mail users**.
2. Select the e-mail user in the result list.
3. Select **Assign mail acceptance** in the task view to establish from which recipients messages are accepted.

   - OR -

Select **Assign mail rejection** in the task view to specify from which recipients messages are not accepted.

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
   - E-mail users
   - Email contacts
5. Assign recipients in **Add assignments**.

   - OR -

   Remove recipients from **Remove assignments**.
6. Save the changes.

Receive Restrictions for E-Mail Contacts

NOTE: Assignments **Assign mail acceptance** and **Assign mail rejection** 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 e-mail contacts

1. Select the category **Active Directory | E-mail contacts**.
2. Select the e-mail contact in the result list.
3. Select **Assign mail acceptance** in the task view to establish from which recipients messages are accepted.

   - OR -

   Select **Assign mail rejection** in the task view to specify from which recipients messages are not accepted.
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
   - E-mail users
   - Email contacts
5. Assign recipients in **Add assignments**.

- OR -

Remove recipients from **Remove assignments**.

6. Save the changes.

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

Entering Master Data for 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 for an Active Directory group

1. Select the category **Active Directory | Groups | Universal groups**.
2. Select the group in the result list and run the task **Create mail-enabled distribution group**.
3. Save the changes.

To edit a mail-enabled distribution group

1. Select the category **Active Directory | Mail-enabled distribution groups**.
2. Select the mail-enabled distribution group in the result list and run **Change master data** in the task view.
3. Edit the mail-enabled distribution group's master data.
4. Save the changes.

Table 43: Mail-Enabled Distribution Group Master 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.
Expansion server	Server on to which to expand the mail-enabled distribution group.
Proxy addresses	Email addresses for the mail-enabled distribution group. You can also add other mail connectors (for example, CCMail, MS) in addition to the standard address type (SMTP, X400). Use the following syntax to set up other proxy addresses: `Address type: new email address`
Do not display in address list	Specifies whether the mail-enabled distribution group is visible in address books. Set this option if you want to prevent the mail-enabled distribution group from being displayed in address books. This option applies to all address books.
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.

Property	Description
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 incoming settings.
Only limit messages from authenticated users	Specifies whether authentication data is requested from senders. Set this option if only messages from authenticated users are permitted.
Out-of-office message to sender	Set this option if the message sender should receive out-of-office messages.
Add to group	Specifies how members can join the mail-enabled distribution group.

Table 44: Permitted Values

Value	Meaning
Open	Members can be added to the group without approval.
Closed	Only mail-enabled distribution group administrator can be added 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 administrator.

Leave group	Use this option to specify how members can leave the distribution group.

Table 45: Permitted Values

Value	Meaning
Open	Members can leave the group without approval.
Closed	The group can only be left with administrator approval. Requests to leave the group are automatically denied.

Distribution group moderation	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.
Sending message to	Specifies how senders are notified when they send messages to moderated distribution groups.

Property	Description

Table 46: Permitted Values

Value	Meaning
Do not notify	No message is sent.
Only notify senders in your exchange organization	Only internal sender receive notification.
Notify all senders	Internal and external sender receive notification.

Receive Restrictions for Mail-Enabled Distribution Groups

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

To modify mail acceptance for mail-enabled distribution groups

1. Select the category **Active Directory | Mail-enabled distribution groups**.
2. Select the mail-enabled distribution group in the result list.
3. Select **Assign mail acceptance** in the task view to establish from which recipients messages are accepted.

   - OR -

   Select **Assign mail rejection** in the task view to specify from which recipients messages are not accepted.
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
   - E-mail users
   - Email contacts
5. Assign recipients in **Add assignments**.

   - OR -

   Remove recipients from **Remove assignments**.
6. Save the changes.

Permission "Send on behalf of" for Mail-Enabled Distribution Groups

Use the send permission "Send on behalf of" to specify which users can use the mailbox to send messages.

To customize the permission "Send on behalf of" for mail-enabled distribution groups

1. Select the category **Active Directory | Mail-enabled distribution groups**.
2. Select the mail-enabled distribution group in the result list.
3. Select **Assign send authorizations** in the task view.
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
    - E-mail users
5. Assign users in **Add assignments**.

    - OR -

    Remove users from **Remove assignments**.
6. Save the changes.

Assigning Administrators for 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. Select the category **Active Directory | Mail-enabled distribution groups**.
2. Select the mail-enabled distribution group in the result list.
3. Select **Assign administrators** in the task view.
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. Assign the administrators in **Add assignments**.

   - OR -

   Remove the call types in **Remove assignments**.
6. Save the changes.

Adding Dynamic Distribution Groups to a Mail-Enabled Distribution Group

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. Select the category **Active Directory | Mail-enabled distribution groups**.
2. Select the mail-enabled distribution group in the result list and run **Assign dynamic distribution groups** in the task view.
3. Assign dynamic distribution groups in **Add assignments**.

   - OR -

   Remove dynamic distribution lists from **Remove assignments**.
4. Save the changes.

Related Topics

- Adding a Dynamic Distribution Group to Mail-Enabled Distribution Groups on page 112

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. Select the category **Active Directory | Mail-enabled distribution groups**.
2. Select the mail-enabled distribution group in the result list.
3. Select **Assign moderators** in the task view.
4. Select the table which contains the user from the menu at the top of the form. You have the following options:
    - Mailboxes
    - Email contacts
    - E-mail users
5. Assign moderators in **Add assignments**.

    - OR -

    Remove organization assignments **Remove assignments**.
6. Save the changes.

To exclude users from moderation

1. Select the category **Active Directory | Mail-enabled distribution groups**.
2. Select the mail-enabled distribution group in the result list.
3. Select **Exclude from moderation** in the task view.
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
    - E-mail users
    - Email contacts
5. Assign moderators in **Add assignments**.

    - OR -

    Remove organization assignments **Remove assignments**.
6. Save the changes.

Deleting Mail-Enabled Distribution Groups

To delete a mail-enabled distribution group

1. Select the category **Active Directory | Mail-enabled distribution groups**.
2. Select the mail-enabled distribution group in the result list.
3. Delete the mail-enabled distribution group using  .
4. Confirm the security prompt with **Yes**.

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

8

Dynamic Distribution Group

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

- Master Data for Dynamic Distribution Groups on page 108
- Receive Restrictions for Dynamic Distribution Groups on page 110
- Permission "Send on behalf of" for Dynamic Distribution Groups on page 111
- Adding a Dynamic Distribution Group to Mail-Enabled Distribution Groups on page 112

Master Data for Dynamic Distribution Groups

To display a dynamic distribution group

1. Select the category **Active Directory | Exchange system administration | <organization> | Recipient configuration | Dynamic distribution groups**.
2. Select the dynamic distribution list in the result list.
3. Select **Change master data** in the task view.

Table 47: Dynamic Distribution List Master Data

Property	Description
Exchange organization	Name of the organization.
Expansion server	Server on to which to expand the dynamic distribution group.

Property	Description
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.
E-mail users	Specifies whether e-mail users are permitted in the dynamic distribution group.
Email contacts	Specifies whether e-mail contacts are permitted in the dynamic distribution group.
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 distri-

Property	Description
	bution 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 incoming settings.
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.

Receive Restrictions for Dynamic Distribution Groups

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

To modify mail acceptance for dynamic distribution groups

1. Select the category **Active Directory | Exchange system administration | <organization> | Recipient configuration | Dynamic distribution groups**.
2. Select the dynamic distribution list in the result list.
3. Select **Assign mail acceptance** in the task view to establish from which recipients messages are accepted.

   - OR -

   Select **Assign mail rejection** in the task view to specify from which recipients messages are not accepted.

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
    - E-mail users
    - Email contacts
5. Assign recipients in **Add assignments**.

    - OR -

    Remove recipients from **Remove assignments**.
6. Save the changes.

Permission "Send on behalf of" for Dynamic Distribution Groups

Use the send permission "Send on behalf of" to specify which users can use the mailbox to send messages.

To customize the permission "Send on behalf of" for dynamic distribution groups

1. Select the category **Active Directory | Exchange system administration | <organization> | Recipient configuration | Dynamic distribution groups**.
2. Select the dynamic distribution list in the result list.
3. Select **Assign send authorizations** in the task view.
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
    - E-mail users
5. Assign users in **Add assignments**.

    - OR -

    Remove users from **Remove assignments**.
6. Save the changes.

Adding a Dynamic Distribution Group to Mail-Enabled Distribution Groups

As from Microsoft Exchange Server 2010, you can add dynamic distribution groups to mail-enabled distribution groups.

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

1. Select the category **Active Directory | Exchange system administration | <organization> | Recipient configuration | Dynamic distribution groups**.
2. Select the dynamic distribution group in the result list and run **Assign distribution groups** in the task view.
3. Assign the dynamic distribution group to mail-enabled distribution groups in **Add assignments**.

   - OR -

   Remove the dynamic distribution group assignments from mail-enabled distribution groups in **Remove assignments**.
4. Save the changes.

Related Topics

- Adding Dynamic Distribution Groups to a Mail-Enabled Distribution Group on page 105

Mail-enabled Public Folders

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

To display mail-enabled public folders

1. Select the category **Active Directory | Exchange system administration | <organization> | Receive configuration | Mail-enabled public folder**.
2. Select the mail-enabled distribution group in the result list.
3. Select **Change master data** in the task view.

To display mail acceptance for mail-enabled public folders

1. Select the category **Active Directory | Exchange system administration | <organization> | Receive configuration | Mail-enabled public folder**.
2. Select the mail-enabled distribution group in the result list.
3. Select **Assign mail acceptance** in the task view to display recipients from whom messages are accepted.

   - OR -

   Select **Assign mail rejection** in the task view to display recipients from whom messages are not accepted.

To customize the permission "Send on behalf of" for mail-enabled public folders

1. Select the category **Active Directory | Exchange system administration | <organization> | Receive configuration | Mail-enabled public folder**.
2. Select the mail-enabled distribution group in the result list.
3. Select **Assign send authorizations** in the task view.

Table 48: Mail-Enabled Public Folder Master Data

Property	Description
Exchange organization	Name of the organization.

Property	Description
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.

10

Extensions for Supporting Exchange hybrid

NOTE: This function is only available if the module Exchange Hybrid Module is installed.

NOTE: You cannot move mailboxes between local Microsoft Exchange and Exchange Online with One Identity Manager. Microsoft offers migration scenarios for moving mailboxes. For detailed 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

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

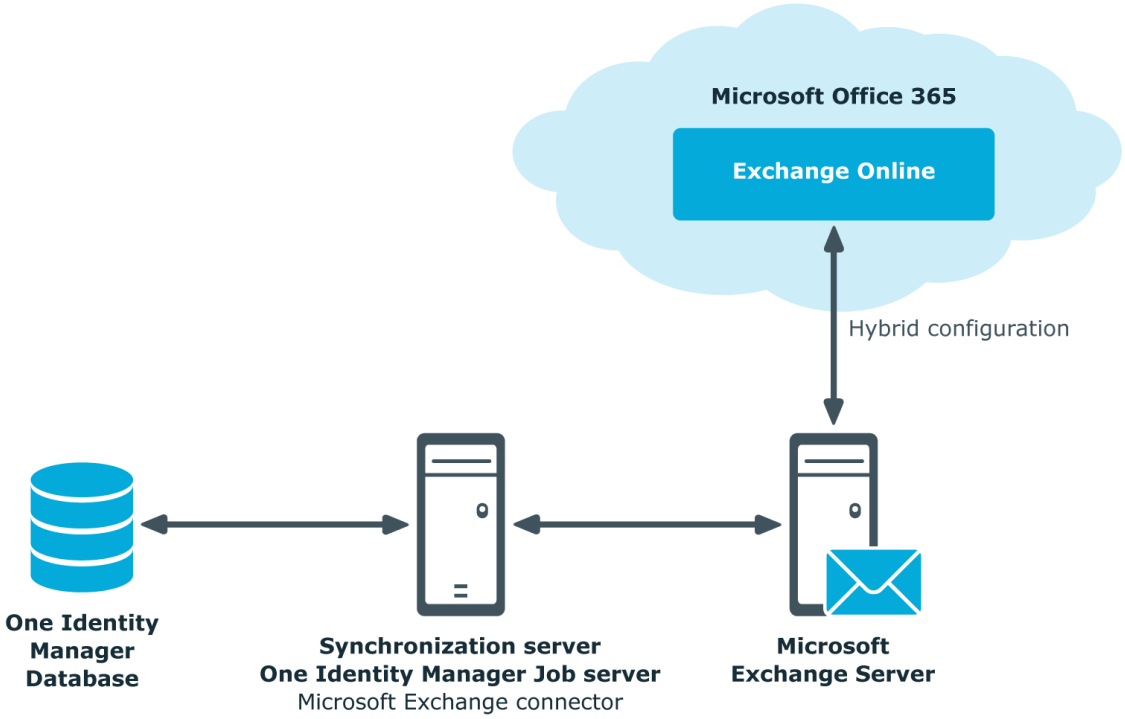
NOTE:

The following modules must be present to support Exchange hybrid environments.

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

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 116
- Advice for Migrating Mailboxes on page 117
- Editing Remote Mailboxes on page 120

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 for is recommended for synchronizing the target systems.
  1. Azure Active Directory
  2. Local Active Directory (in parallel with Azure Active Directory possible)
  3. Exchange Online
  4. Local Microsoft Exchange (after Exchange Online if possible).
- The connection between local Exchange (`EX0Organization`) and the corresponding Azure Active Directory tenant (`AADOrganization`) in One Identity Manager must be set up.

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

Related Topics

- Creating a Synchronization Project for initial Synchronization of a Microsoft Exchange Environment on page 19
- Appendix: Default Project Template for Microsoft Exchange on page 128

Advice for Migrating Mailboxes

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

Synchronizing Microsoft Exchange after moving a mailbox from local Microsoft Exchange to Exchange Online 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 category **Active Directory | Troubleshooting | Mailboxes migrated to Exchange Online**.

   - 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.

   - Select the mailbox in the table `EX0Mailbox` in the category **Active Directory | target system synchronization: Exchange** and select "Delete" in the toolbar to delete the mailbox.

     For more information, see Post-Processing Outstanding Objects on page 34.

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 1

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 employees.

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. Ensure that the remote mailbox in One Identity Manager exists and is connected to the Active Directory user account.
   b. Delete the outstanding local mailbox in One Identity Manager.

c. Assign the account definition for remote mailboxes to the employee.

d. Remove the account definition for local mailboxes from the employee.

Example 2

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 employees through it's 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 employee until the mailbox has been successfully migrated.

   - Configure a dynamic role for this parallel structure, to include all employees who:
     - 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 employees 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 employees who:
     - 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.

Editing Remote Mailboxes

To edit a mailbox

1. Select the category **Active Directory | Remote mailboxes** in the Manager.
2. Select the remote mailbox in the result list and run the task **Change master data**.
3. Edit the remote mailbox's master data.
4. Save the changes.

NOTE: After creating a remote mailbox, a corresponding mailbox is not added in Exchange Online until the next time you synchronize your Azure Active Directory tenant in Azure Active Directory Connect. 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 type "Remote user mailbox" have been created by Azure Active Directory or Exchange Online internal processes, an appropriate Exchange license must be assigned for resulting the Azure Active Directory user account,

To display remote mailboxes without Exchange licenses

- Select the category **Active Directory | Exchange system administrators | <organization> | Recipient configuration | Remote mailboxes | Remote user | Without assigned license** in the Manager.

Related Topics

- General Master Data of a Remote Mailbox on page 120
- Information about Remote Configuration on page 122
- Information about Cloud-based Archive Mailboxes on page 122
- Receive Restrictions for Remote Mailboxes on page 123
- Extensions for Moderated Remote Mailboxes on page 123

General Master Data of a Remote Mailbox

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

Table 49: General Master Data of a Remote Mailbox

Property	Description
Employee	Employee using the mailbox. An employee is already entered if the mailbox was generated by an account definition. If you create the

Property	Description
	mailbox manually, you can select an employee in the menu.
Account definition	Account definition through which the mailbox was created. Use the account definition to automatically populate mailbox master data and to specify a manage level for the mailbox. One Identity Manager finds the IT operating data of the assigned employee and uses it to populate the corresponding fields in the mailbox. NOTE: The account definition cannot be changed once the mailbox has been saved.
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 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. The following are available: remote user mailbox, remote room mailbox and remote equipment mailbox.
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.
Sending message to	Specifies how senders are notified when they send messages to moderated mailbox.

Property	Description
	Table 50: Permitted Value **Value** / **Meaning** Do not notify / No message is sent. Only notify senders in your exchange organization / Only internal sender receive notification. Notify all senders / Internal and external sender receive notification.
Distinguished name	Mailbox's distinguished name.

Information about Remote Configuration

The following information about remote configuration is mapped on the **Remote** tab.

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 master data about a cloud-based archive mailbox is mapped on the **Archive** tab.

Table 51: 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.

Property	Description
Archive state	Status of the archive.

Receive Restrictions for Remote Mailboxes

NOTE: Assignments **Assign mail acceptance** and **Assign mail rejection** 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 mailboxes

1. Select the category **Active Directory | Remote mailboxes**.
2. Select a mailbox in the result list.
3. Select **Assign mail acceptance** in the task view to establish from which recipients messages are accepted.

   - OR -

   Select **Assign mail rejection** in the task view to specify from which recipients messages are not accepted.
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
   - E-mail users
   - Email contacts
   - Remote mailboxes

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. Select the category **Active Directory | Remote mailboxes**.
2. Select a mailbox in the result list.
3. Select **Assign moderators** in the task view.
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
    - Email contacts
    - E-mail users
5. Assign moderators in **Add assignments**.

    - OR -

    Remove organization assignments **Remove assignments**.
6. Save the changes.

To exclude users from moderation

1. Select the category **Active Directory | Remote mailboxes**.
2. Select a mailbox in the result list.
3. Select **Exclude from moderation** in the task view.
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
    - E-mail users
    - Email contacts
5. Assign moderators in **Add assignments**.

    - OR -

    Remove organization assignments **Remove assignments**.
6. Save the changes.

11

Troubleshooting

Possible Errors Synchronizing Exchange hybrid

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 (EX 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 another 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 other 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 19.

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

Appendix: Configuration Parameters for Managing Microsoft Exchange

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

Table 52: Configuration Parameter for Managing a Microsoft Exchange Environment

Configuration parameter	Meaning
TargetSystem\ADS\Exchange2000	Preprocessor relevant configuration parameter for controlling the database model components for the administration of the target system Microsoft Exchange. If the parameter is set, the target system components are available. Changes to the parameter require recompiling the database.
TargetSystem\ADS\Exchange2000\Accounts	This configuration parameter permits configuration of recipient data.
TargetSystem\ADS\Exchange2000\Accounts\ MailTemplateDefaultValues	This configuration parameter contains the mail template used to send notifications if default IT operating data mapping values are used for automatically creating a user account. Use the mail template "Employee - new user account with default properties created".
TargetSystem\ADS\Exchange2000\DefaultAddress	The configuration parameter contains the recipient's default email address for sending notifications about actions in the target system.

Appendix: Default Project Template for Microsoft Exchange

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

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

Detailed information about this topic

- Default Template for Microsoft Exchange 2010 on page 128
- Default Template for Microsoft Exchange 2013 and Microsoft Exchange 2016 on page 129

Default Template for Microsoft Exchange 2010

The template uses mappings for the following schema types.

Table 53: Mapping Microsoft Exchange 2010 schema types to tables in the One Identity Manager schema.

Schema type in Microsoft Exchange	Table in the One Identity Manager schema
ActiveSyncMailboxPolicy	EX0ActiveSyncMBPolicy
CalendarProcessing	EX0Mailbox
DatabaseAvailabilityGroup	EX0DAG

Schema type in Microsoft Exchange	Table in the One Identity Manager schema
DistributionGroup	EX0DL
DynamicDistributionGroup	EX0DynDL
ExchangeServer	EX0Server
GlobalAdressList	EX0AddrList
LocalAddressList	EX0AddrList
Mailbox	EX0Mailbox
MailboxDatabase	EX0MailboxDatabase
Mailboxstatistics	EX0Mailbox
MailContact	EX0MailContact
MailPublicFolder	EX0MailPublicFolder
MailUser	EX0MailUser
ManagedFolderMailboxPolicy	EX0ManagedFolderPolicy
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

Default Template for Microsoft Exchange 2013 and Microsoft Exchange 2016

The template uses mappings for the following schema types.

Table 54: Mapping Microsoft Exchange 2013 and Microsoft Exchange 2016 schema types to tables in the One Identity Manager schema.

Schema type in Microsoft Exchange	Table in the One Identity Manager schema
CalendarProcessing	EX0Mailbox
DatabaseAvailabilityGroup	EX0DAG
DistributionGroup	EX0DL
DynamicDistributionGroup	EX0DynDL
ExchangeServer	EX0Server
GlobalAdressList	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

About us

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

Contacting us

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

Technical support resources

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

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

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

Index

I

J

M

O

P

R

S

T

U