One Identity Manager 8.1.2

Administration Guide for Connecting to Microsoft Exchange

One Identity Manager Administration Guide for Connecting to Microsoft Exchange
Updated - March 2020
Version - 8.1.2

Contents

Managing Microsoft Exchange environments

The key aspects of managing a Microsoft Exchange environment with One Identity Manager include the mapping of mailboxes, email users, email 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

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

- Microsoft Exchange server

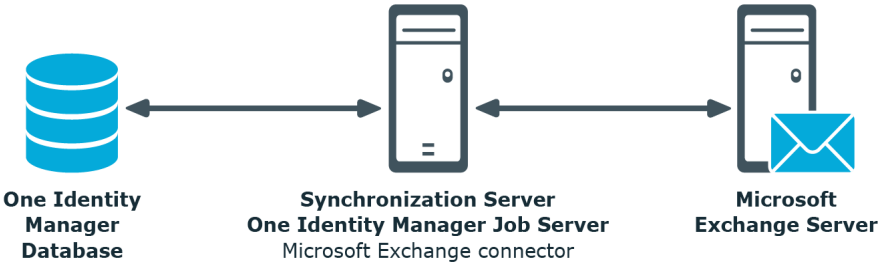
  The Microsoft Exchange server against which the Microsoft Exchange objects are synchronized. The synchronization server connects to this server in order to access the Microsoft Exchange objects.

- Synchronization server

  The synchronization server for synchronizing data between One Identity Manager and Microsoft Exchange. The One Identity Manager Service with the Microsoft Exchange connector is installed on this server. The synchronization server connects to the Microsoft Exchange server.

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

Figure 1: Architecture for synchronization



One Identity Manager users for managing Microsoft Exchange

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

Table 1: Users

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

User	Tasks
	accounts or groups. • Edit password policies for the target system. • Can add employees who have an other identity than the **Primary identity**. • Configure synchronization in the Synchronization Editor and define the mapping for comparing target systems and One Identity Manager. • Edit the synchronization's target system types and outstanding objects. • Authorize other employees within their area of responsibility as target system managers and create child application roles if required.
One Identity Manager administrators	• Create customized permissions groups for application roles for role-based login to administration tools in the Designer as required. • Create system users and permissions groups for non role-based login to administration tools in the Designer as required. • Enable or disable additional configuration parameters in the Designer as required. • Create custom processes in the Designer as required. • Create and configure schedules as required. • Create and configure password policies as required.

2

Setting up Microsoft Exchange synchronization

One Identity Manager supports synchronization with

- Microsoft Exchange 2010 Service Pack 3 or later
- Microsoft Exchange 2013 with Cumulative Update 23
- Microsoft Exchange 2016
- Microsoft Exchange 2019 with Cumulative Update 1

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

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

1. Prepare a user account with sufficient permissions for synchronization.
2. One Identity Manager parts for managing Microsoft Exchange systems are available if the **TargetSystem | ADS | Exchange2000** configuration parameter is set.
    - In the Designer, check if the configuration parameter is set. Otherwise, set the configuration parameter and compile the database.
    - Other configuration parameters are installed when the module is installed. Check the configuration parameters and modify them as necessary to suit your requirements.

3. Install and configure a synchronization server and declare the server as a Job server in One Identity Manager.
4. Check whether the domain trusts are entered correctly.
5. Enter the data for creating linked mailboxes within a resource forest.
6. Create a synchronization project with the Synchronization Editor.

Detailed information about this topic

- Users and permissions for synchronizing with Microsoft Exchange on page 11
- Setting up the synchronization server on page 13
- 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
- Disabling synchronization on page 39
- Recommendations for synchronizing Microsoft Exchange environments on page 27
- Customizing the synchronization configuration on page 30
- Configuration parameters for managing a Microsoft Exchange environment on page 135
- Default template for Microsoft Exchange 2010 on page 136
- Default project template for Microsoft Exchange 2013, Microsoft Exchange 2016, and Microsoft Exchange 2019 on page 137

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 at least the following authorizations for full synchronization of Microsoft Exchange objects with the supplied One Identity Manager default configuration.

User	Permissions
	• Member of the **View-only organization management** role group • Member of the **Public folder management** role group • Member of the **Recipient management** role group • The **Security Group Creation and Membership** role In Microsoft Exchange, create a new role group and assign the role and the user account to this role group. For more detailed information about managing permissions in Microsoft Exchange, see the Microsoft documentation.
User for creating linked mailboxes	The user account is required for adding linked mailboxes. The user account requires read access in Active Directory.
One Identity Manager Service user account	The user account for One Identity Manager Service requires permissions to carry out operations at file level. For example, assigning permissions and creating and editing directories and files. The user account must belong to the **Domain users** group. The user account must have the **Login as a service** extended user permissions. The user account requires access permissions to the internal web service. NOTE: If One Identity Manager Service runs under the network service (**NT Authority\NetworkService**), you can issue access permissions for the internal web service with the following command line call: `netsh http add urlacl url=http://<IP address>:<port number>/ user="NT AUTHORITY\NETWORKSERVICE"` The user account needs full access to the One Identity Manager Service installation directory in order to automatically update One Identity Manager. In the default installation, One Identity Manager is installed under: • `%ProgramFiles(x86)%\One Identity` (on 32-bit operating systems) • `%ProgramFiles%\One Identity` (on 64-bit operating systems)
User for accessing the One Identity Manager database	The **Synchronization** default system user is provided to execute synchronization with an application server.

Setting up the synchronization server

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

- Windows operating system

  The following versions are supported:

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

  NOTE: Take the target system manufacturer's recommendations into account.
- Windows Management Framework 4.0
- One Identity Manager Service, Microsoft Exchange connector
  - Install One Identity Manager components with the installation wizard.
    1. Select **Select installation modules with existing database**.
    2. Select the **Server | Job server | Microsoft Exchange** machine role.

IMPORTANT: The Microsoft Exchange One Identity Manager connector uses Windows PowerShell to communicate with the Microsoft Exchange server. For communication, extra configuration is required on the synchronization server and the Microsoft Exchange server. 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 recommended that you set up a Job server for each target system for performance reasons. This avoids unnecessary swapping of connections to target systems because a Job server only has to process tasks of the same type (re-use of existing connections).

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

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

machine roles.

- Configures the One Identity Manager Service.
- Starts the One Identity Manager Service.

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

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

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

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

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

       - OR -

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

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

          Syntax:

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

    NOTE: You can use the **Extended** option to make changes to other properties for the Job server. You can also edit the properties later with the Designer.
4. On the **Machine roles** page, select **Microsoft Exchange**.
5. On the **Server functions** page, select **Microsoft Exchange connector**.
6. On the **Service Settings** page, enter the connection data and check the One Identity

Manager Service configuration.

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

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

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

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

the user account, password and password confirmation.

- To change the install directory, names, display names, or description of the One Identity Manager Service, use the other options.

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

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

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

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

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 permits the execution of 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 ***** permits all connections. One Identity Manager uses the server's fully qualified domain name for the connection. You can limit the value.

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

1. Run Microsoft Exchange on the Windows PowerShell synchronization server.
2. Enter this command at the prompt:

   ```
   $creds = New-Object System.Management.Automation.PSCredential
   ("<domain>\<user>", (ConvertTo-SecureString "<password>" -AsPlainText -Force))
   ```

   - OR -

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

   This command finds the access data required for 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 command creates a remote session.

   NOTE: One Identity Manager establishes a connection to the fully qualified domain name of the Microsoft Exchange server. The server name must therefore be in the list configured with trusted hosts.
4. Enter this command at the prompt:

   ```
   Import-PsSession $session
   ```

   This command imports the remote session so that the connection can be accessed.
5. Test the functionality with any Microsoft Exchange command. For example, enter the following command at the prompt:

   ```
   Get-Mailbox
   ```

Testing Active Directory domain trusts

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

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

To enter the parent domain

1. In the Manager, select the **Active Directory | Domains** category.
2. Select the domain in the result list.

3. Select the **Change master data** task.
4. Enter the parent domain.
5. Save the changes.

   Implicit trusts are created automatically.

To test trusted domains

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

   This shows domains 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. In the Manager, select the **Active Directory | Domains** category.
2. Select the domain in the result list and run the **Change master data** task.
3. Enter the following information on the **Exchange** tab.

Table 3: Domain master data for generating linked mailboxes

Property	Description
User (linked mailboxes)	User account that is used to create linked mailboxes.
Password	Password for the user account.
Password retry	Repeat entry of the password for the user account.
DC (linked mailbox)	Active Directory domain controller for creating 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 Synchronization Editor to configure synchronization between the One Identity Manager database and Microsoft Exchange environment. The following describes the steps for initial configuration of a synchronization project.

NOTE: When setting up the synchronization, note the recommendations described under Recommendations for synchronizing Microsoft Exchange environments 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 Microsoft Exchange client domain are entered to create linked mailboxes within a Active Directory resource forest topology

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

Table 4: Information required for setting up a synchronization project

Data	Explanation
Microsoft Exchange	One Identity Manager supports synchronization with Microsoft Exchange 2010 Service Pack 3 or later, Microsoft Exchange 2013 with

<table>
<tr><th>Data</th><th>Explanation</th></tr>
<tr><td>version</td><td>Cumulative Update 23, Microsoft Exchange 2016, and Microsoft Exchange 2019 with Cumulative Update 1.</td></tr>
<tr><td>Server (fully qualified)</td><td>Fully qualified name (FQDN) of the Microsoft Exchange server to which the synchronization server connects to access Microsoft Exchange objects.
Example:
<code>Server.Doku.Testlab.dd</code></td></tr>
<tr><td>User account and password for logging in</td><td>Fully qualified name (FQDN) of the user account and password for logging in on the Microsoft Exchange.
Example:
<code>user@domain.com</code>
<code>domain.com\user</code>
Make a user account available with sufficient permissions. For more information, see Users and permissions for synchronizing with Microsoft Exchange on page 11.</td></tr>
<tr><td>Synchronization server for Microsoft Exchange</td><td>The One Identity Manager Service with the Microsoft Exchange connector must be installed on the synchronization server.
Table 5: Additional properties for the Job server<table><tr><th>Property</th><th>Value</th></tr><tr><td>Server function</td><td>Microsoft Exchange connector</td></tr><tr><td>Machine role</td><td>Server | Job server | Active Directory | Microsoft Exchange</td></tr></table>For more information, see Setting up the synchronization server on page 13.</td></tr>
<tr><td>One Identity Manager database connection data</td><td>Database server
Database
SQL Server login and password
Specifies whether integrated Windows authentication is used. This type of authentication is not recommended. If you decide to use it anyway, ensure that your environment supports Windows authentication.</td></tr>
<tr><td>Remote connection server</td><td>To configure synchronization with a target system, One Identity Manager must load the data from the target system. One Identity</td></tr>
</table>

Data	Explanation
	Manager communicates directly with the target system to do this. Sometimes direct access from the workstation, on which the Synchronization Editor is installed, is not possible. For example, because of the firewall configuration or the workstation does not fulfill the necessary hardware and software requirements. If direct access is not possible from the workstation, you can set up a remote connection. The remote connection server and the workstation must be in the same Active Directory domain. Remote connection server configuration: • One Identity Manager Service is started • **RemoteConnectPlugin** is installed • 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. TIP: The remote connection server requires the same configuration as the synchronization server (with regard to the installed software and entitlements). Use the synchronization as remote connection server at the same time, by simply installing the `RemoteConnectPlugin` as well. For more detailed information about setting up a remote connection, see the *One Identity Manager Target System Synchronization Reference Guide*.

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

- Executed in default mode
- Started from the Launchpad

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

To set up initial synchronization project for Microsoft Exchange

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

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

2. Select the **Target system type Microsoft Exchange** entry and click **Start**.

   This starts the Synchronization Editor's project wizard.

3. Select the connector on the **Select target system** page.
    - To synchronize a Microsoft Exchange 2010 environment, select the **Microsoft Exchange 2010 connector**.
    - To synchronize a Microsoft Exchange 2013 environment, select the **Microsoft Exchange 2013 connector**.
    - To synchronize a Microsoft Exchange 2016 environment, select the **Microsoft Exchange 2016 connector**.
    - To synchronize a Microsoft Exchange 2019 environment, select the **Microsoft Exchange 2019 connector**.
4. On the **System access** page, specify how One Identity Manager can access the target system.
    - If access is possible from the workstation on which you started the Synchronization Editor, do not change any settings.
    - If access is not possible from the workstation on which you started the Synchronization Editor, you can set up a remote connection.

      Enable the **Connect using remote connection server** option and select the server to be used for the connection under **Job server**.
5. Enter the information about the Microsoft Exchange server on the **Select Microsoft Exchange server** page to which the synchronization server connects to access Microsoft Exchange objects.
    a. Under **Server**, enter the fully qualified name (FQDN) of the Microsoft Exchange server. To check the data, click **DNS query**.

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

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

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

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

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

       NOTE: Microsoft Exchange does not support this authentication type by default. You must configure support for this method in Microsoft Exchange. In addition, an SSL connection is used to authenticate using the **Basic** method.
6. Enter login data on the **Enter connection credentials** page to connect to Microsoft Exchange.

Table 6: Connection data to the Microsoft Exchange

Property	Description

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

Password	Password for the user account.

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 the recipients of the Microsoft Exchange organization, select the **Entire organization** option (recommended). As a prerequisite, the trusted domains of the Active Directory domains must be declared in One Identity Manager.
   - Select the **Only recipients of the following domain** option to synchronize recipients with specific domains and select a domain. The target system domain is listed as a minimum.
8. On the **One Identity Manager Connection** tab, test the data for connecting to the One Identity Manager database. The data is loaded from the connected database. Reenter the password.

   NOTE: If you use an unencrypted One Identity Manager database and have not yet saved any synchronization projects to the database, you need to enter all connection data again. This page is not shown if a synchronization project already exists.
9. The wizard loads the target system schema. This may take a few minutes depending on the type of target system access and the size of the target system.
10. On the **Restrict target system access** page, specify how system access should work. You have the following options:

Table 7: Specify target system access

Option	Meaning
Read-only access to target system.	Specifies that a synchronization workflow is only to be set up for the initial loading of the target system into the One Identity Manager database. The synchronization workflow has the following characteristics: • Synchronization is in the direction of **One Identity Manager**.

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

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

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

    a. Click to add a new Job server.

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

    c. Click **OK**.

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

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

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

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

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

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

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

    NOTE: If you do not want the synchronization project to be activated immediately,

disable the **Activate and save the new synchronization project automatically** option. In this case, save the synchronization project manually before closing the Synchronization Editor.

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

To configure the content of the synchronization log

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

   NOTE: Some content generates a particularly large volume of log data. The synchronization log should only contain data required for troubleshooting and other analyses.
7. Click **OK**.

To synchronize on a regular basis

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

To start initial synchronization manually

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

Related topics

- Setting up the synchronization server on page 13
- Users and permissions for synchronizing with Microsoft Exchange on page 11
- Testing Active Directory domain trusts on page 17

- Displaying synchronization results on page 26
- Recommendations for synchronizing Microsoft Exchange environments on page 27
- Customizing the synchronization configuration on page 30
- Default template for Microsoft Exchange 2010 on page 136
- Default project template for Microsoft Exchange 2013, Microsoft Exchange 2016, and Microsoft Exchange 2019 on page 137

Displaying synchronization results

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

To display a synchronization log

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

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

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

To display a provisioning log

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

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

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

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

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

Synchronization logs are stored for a fixed length of time.

To modify the retention period for synchronization logs

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

Recommendations for synchronizing Microsoft Exchange environments

The following scenarios for synchronizing Microsoft Exchange are supported.

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

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

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

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

For more information, see Creating a synchronization project for initial synchronization of a Microsoft Exchange environment on page 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, email contacts) are synchronized from the given Active Directory domain in the Microsoft Exchange organization.

The following synchronization project configuration is recommended in this case:

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

1. Set up the synchronization project for synchronizing the entire Microsoft Exchange infrastructure.

- Select the recipient **Complete organization**.
- Customize the synchronization workflow.
  - Disable synchronization steps of all schema types representing recipients. These are:

    Mailbox

    MailContact

    MailUser

    DistributionList

    DynamicDistributionList

    MailPublicFolder

  - Check that all schema types, not representing recipients, are synchronized. These are:

    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.
   - Select the recipient scope **Only recipients of the following domain** and select a domain of the Microsoft Exchange organization.

- 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 the synchronization of recipients in the Synchronization Editor.
   - Create a new base object for every domain. Use the wizards to attach a base object.
     - In the wizard, select the Microsoft Exchange connector and enter the connection parameters. The connection parameters are saved in a

special variable set.

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

- If possible, select a Microsoft Exchange server that is in the domain.
- Select the **Only recipients of the following domain** recipient scope.

- Create a new start up configuration for each domain. In the start configuration, use the newly created variable sets.
- Run a consistency check.
- Activate the synchronization project.

4. Customize the synchronization schedule.

IMPORTANT: Set up the synchronization schedules such that the Microsoft Exchange infrastructure is synchronized before Microsoft Exchange recipients.

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

Customizing the synchronization configuration

Having used the Synchronization Editor to set up a synchronization project for initial synchronization of Microsoft Exchange, you can use the synchronization project to load Microsoft Exchange objects into the One Identity Manager database. When you manage mailboxes, email users, email 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 that contain the necessary information about the synchronization objects when synchronization starts. Variables can be implemented in base objects, schema classes, or processing method, for example.
- To specify which Microsoft Exchange objects and database objects are included in synchronization, edit the scope of the target system connection and the One Identity Manager database connection. To prevent data inconsistencies, define the same scope in both systems. If no scope is defined, all objects will be synchronized.
- Update the schema in the synchronization project if the One Identity Manager schema or target system schema has changed. Then you can add the changes to the mapping.

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

synchronization objects would be processed.

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

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

Detailed information about this topic

- Configuring Microsoft Exchange synchronization on page 31
- Updating schemas on page 32

Configuring Microsoft Exchange synchronization

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

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

Updating schemas

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

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

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

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

To update a system connection schema

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

   - OR -

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

   This reloads the schema data.

To edit a mapping

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

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

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

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.

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

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

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

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

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

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

  Variable: `CP_LocalServerRevisionMaxDifferenceInMinutes`

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

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

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

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

To permit revision filtering on a workflow

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

To permit revision filtering for a start up configuration

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

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, adjusting connections parameters and editing variables, 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.

Outstanding objects:

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

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

Start target system synchronization to do this.

To post-process outstanding objects

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

   All the synchronization tables assigned to the **Microsoft Exchange** target system type are displayed in the navigation view.
2. On the **Target system synchronization** form, in the **Table / object** column, open

the node of the table for which you want to post-process outstanding objects.

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

- The synchronization log has already been deleted.

  - OR -

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

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

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

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

TIP:

To display object properties of an outstanding object

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

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

3. Select the objects you want to rework. Multi-select is possible.
4. Click on one of the following icons in the form toolbar to execute the respective method.

Table 8: Methods for handling outstanding objects

Icon	Method	Description
	Delete	The object is immediately deleted from the One Identity Manager database. Deferred deletion is not taken into account. The **Outstanding** label is removed from the object. Indirect memberships cannot be deleted.
	Publish	The object is added to the target system. The **Outstanding** label is removed from the object. The method triggers the `HandleOutstanding` event. This runs a target system specific process that triggers the provisioning process for the object. Prerequisites: • The table containing the object can be published. • The target system connector has write access to the target

Icon	Method	Description
		system.
	Reset	The **Outstanding** label is removed for the object.

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

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

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

To disable bulk processing

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

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

To add custom tables to target system synchronization

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

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

Configuring the provisioning of memberships

Memberships, such as user accounts in groups, are saved in assignment tables in the One Identity Manager database. During provisioning of modified memberships, changes made

in the target system may be overwritten. This behavior can occur under the following conditions:

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

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

To allow separate provisioning of memberships

1. In the Manager, select the **Active Directory | Basic configuration data | Target system types** category.
2. Select **Microsoft Exchange** in the result list.
3. Select the **Configure tables for publishing** task.
4. Select the assignment tables that you want to set up for single provisioning. Multi-select is possible.
    - This option can only be enabled for assignment tables that have a base table with `XDateSubItem` or `CCC_XDateSubItem` column.
    - Assignment tables that are grouped together in a virtual schema property in the mapping must be marked identically.
5. Click **Enable merging**.
6. Save the changes.

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

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

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

To restore the default condition

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

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

Accelerating provisioning and single object synchronization

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

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

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

To configure load balancing

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

   All Job servers must access the same Microsoft Exchange organization as the synchronization server for the respective base object.
2. In the Synchronization Editor, assign a custom server function to the base object.

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

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

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

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

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

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

To use the synchronization server without load balancing.

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

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

Help for the analysis of synchronization issues

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

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

To generate a synchronization analysis report

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

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

Disabling synchronization

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

To prevent regular synchronization

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

   Now you can only start synchronization manually.

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

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

To deactivate the synchronization project

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

Related topics

- Creating a synchronization project for initial synchronization of a Microsoft Exchange environment on page 19

3

Basic data for managing an Microsoft Exchange environment

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

- Configuration parameter

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

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

  For more information, see Configuration parameters for managing a Microsoft Exchange environment on page 135.

- Account definitions

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

  For more information, see Setting up account definitions on page 42.

- 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 One Identity Manager. Assign the employees who are authorized to edit all Microsoft Exchange organizations in One Identity Manager to this application role.

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

For more information, see Target system managers on page 59.

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 yet have a user account in a target system, a new user account is created. This is done by assigning account definitions to an employee.

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

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

The following steps are necessary to implement an account definition:

- Creating an account definition
- Creating manage levels
- Creating a formatting rule for IT operating data
- Collecting 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. In the Manager, select the **Active Directory | Basic configuration data | Account definitions | Account definitions** category.
2. Select an account definition in the result list. Select the **Change master data** task.

   -OR-

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

Detailed information about this topic

- Master data for an account definition on page 43

Master data for an account definition

Enter the following data for an account definition:

Table 9: Master data for an account definition

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

Property	Description
	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. Option not set: the account definition assignment is not in effect. The associated user account is deleted.
Resource	Resource type for grouping account definitions.

Property	Description
type	
Spare field 01 - spare field 10	Additional company-specific information. Use the Designer to customize display names, formats, and templates for the input fields.

Creating manage levels

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

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

One Identity Manager supplies a default configuration for manage levels:

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

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

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

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

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

To assign manage levels to an account definition

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

   - OR -

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

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

To edit a manage level

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

   - OR -

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

Related topics

- Master data for manage levels on page 46

Master data for manage levels

Enter the following data for a manage level.

Table 10: Master data for manage levels

Property	Description
Manage level	Name of the manage level.
Description	Text field for additional explanation.
IT operating data overwrites	Specifies whether user account data formatted from IT operating data is automatically updated. Permitted values are: • **Never**: Data is not updated. • **Always**: Data is always updated.

Property	Description
	• **Only initially**: Data is only determined at the start.
Retain groups if temporarily disabled	Specifies whether user accounts of temporarily disabled employees retain their group memberships.
Lock user accounts if temporarily disabled	Specifies whether user accounts of temporarily disabled employees are locked.
Retain groups if permanently disabled	Specifies whether user accounts of permanently disabled employees retain group memberships.
Lock user accounts if permanently disabled	Specifies whether user accounts of permanently disabled employees are locked.
Retain groups on deferred deletion	Specifies whether user accounts of employees marked for deletion retain their group memberships.
Lock user accounts if deletion is deferred	Specifies whether user accounts of employees marked for deletion are locked.
Retain groups on security risk	Specifies whether user accounts of employees posing a security risk retain their group memberships.
Lock user accounts if security is at risk	Specifies whether user accounts of employees posing a security risk are locked.
Retain groups if user account disabled	Specifies whether disabled user accounts retain their group memberships.

Creating 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 automatically creating user accounts for an employee in the target system and modifying them.

- Microsoft Exchange mailbox database

To create a mapping rule for IT operating data

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

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

Table 11: Mapping rule for IT operating data

Property	Description
Column	User account property for which the value is set. In the menu, you can select the columns that use the `TSB_ITDataFromOrg` script in their template. For detailed information, see the *One Identity Manager Target System Base Module Administration Guide*.
Source	Specifies which roles to use in order to find the user account properties. You have the following options: • Primary department • Primary location • Primary cost center • Primary business roles NOTE: Only use the primary business role if the Business Roles Module is installed. • Empty If you select a role, you must specify a default value and set the **Always use default value** option.
Default value	Default value of the property for an employee's user account if the value is not determined dynamically from the IT operating data.
Always use default value	Specifies whether user account properties are always filled with the default value. IT operating data is not determined dynamically from a role.
Notify when applying the standard	Specifies whether email notification to a defined mailbox is sent when the default value is used. The **Employee - new user account with default properties created** mail template is used. To change the mail template, adjust the **TargetSystem | ADS | Exchange2000 | Accounts | MailTemplateDefaultValues** configuration parameter.

4. Save the changes.

Related topics

- Collecting IT operating data on page 49

Collecting IT operating data

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

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

Example

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

Specify the effective IT operating data of department A for the 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 define IT operating data

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

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

Table 12: IT operating data

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

4. Save the changes.

Related topics

- Creating a formatting rule for IT operating data on page 47

Modify IT operating data

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

Prerequisites

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

  - OR -

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

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

To execute the template

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

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

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

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

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

Assigning account definitions to employees

Account definitions are assigned to company employees.

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

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

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

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

Prerequisites for indirect assignment of account definitions to employees

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

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

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

Detailed information about this topic

- Assigning account definitions to departments, cost centers, and locations on page 52
- Assigning an account definition to business roles on page 53
- Assigning account definitions to all employees on page 53
- Assigning account definitions directly to employees on page 54
- Assigning account definitions to a target system on page 57

Assigning account definitions to departments, cost centers, and locations

To add account definitions to hierarchical roles

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

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

   To remove an assignment

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

Related topics

- Assigning an account definition to business roles on page 53
- Assigning account definitions to all employees on page 53
- Assigning account definitions directly to employees on page 54

Assigning an account definition to business roles

Installed modules: Business Roles Module

To add account definitions to hierarchical roles

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

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

   To remove an assignment

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

Related topics

- Assigning account definitions to departments, cost centers, and locations on page 52
- Assigning account definitions to all employees on page 53
- Assigning account definitions directly to employees on page 54

Assigning account definitions to all employees

To assign an account definition to all employees

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

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

5. Save the changes.

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

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

Related topics

- Assigning account definitions to departments, cost centers, and locations on page 52
- Assigning an account definition to business roles on page 53
- Assigning account definitions directly to employees on page 54

Assigning account definitions directly to employees

To assign an account definition directly to employees

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

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

   To remove an assignment

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

Related topics

- Assigning account definitions to departments, cost centers, and locations on page 52
- Assigning an account definition to business roles on page 53
- Assigning account definitions to all employees on page 53

Assigning account definitions to system roles

Installed modules: System Roles Module

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

To add account definitions to a system role

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

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

   To remove an assignment

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

Adding account definitions in the IT Shop

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

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

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

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

To add an account definition to the IT Shop

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

   - OR -

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

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

To remove an account definition from individual IT Shop shelves

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

   - OR -

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

To remove an account definition from all IT Shop shelves

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

   - OR -

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

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

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

Related topics

- Master data for an account definition on page 43
- Assigning account definitions to departments, cost centers, and locations on page 52

- Assigning an account definition to business roles on page 53
- Assigning account definitions directly to employees on page 54
- Assigning account definitions to system roles on page 55

Assigning account definitions to a target system

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

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

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

To assign the account definition to a target system

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

Related topics

- Assigning account definitions to employees on page 51

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.

To delete an account definition

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

        In the **Remove assignments** pane, remove the business roles.
    d. Save the changes.
5. If the account definition was requested through the IT Shop, it must be canceled and removed from all IT Shop shelves.

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

To remove an account definition from all IT Shop shelves

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

   - OR -

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

b. Select an account definition in the result list.

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

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

e. Click **OK**.

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

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

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

   b. Select an account definition in the result list.

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

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

   e. Save the changes.

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

   a. In the Manager, select the domain in the **Active Directory | Domains** category.

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

   c. On the **General** tab, remove the assigned account definitions.

   d. Save the changes.

8. Delete the account definition.

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

   b. Select an account definition in the result list.

   c. Click to delete an account definition.

Target system managers

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

One Identity Manager to this application role.

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

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

Implementing application roles for target system managers

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

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

Table 13: Default application roles for target system managers

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

To initially specify employees to be target system administrators

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

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

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

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

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

To specify target system managers for individual Microsoft Exchange organizations

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

   - OR -

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

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

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

Related topics

- One Identity Manager users for managing Microsoft Exchange on page 8
- Microsoft Exchange organizations on page 64

4

Microsoft Exchange structure

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

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

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

Detailed information about this topic

Microsoft Exchange organizations

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

To edit organization master data

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

Table 14: 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	Type of synchronization through which the data is synchronized between the organization and One Identity Manager. You can no longer change the synchronization type once objects for this organization are present in

Property	Description
	One Identity Manager. When you create a organization with the Synchronization Editor, **One Identity Manager** is used. **Table 15: 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 59

Microsoft Exchange mailbox databases

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

To display mailbox database master data

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

To display the mailbox server of a mailbox database master data

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

Table 16: Mailbox database master data

Property	Description
Exchange organization	Name of the organization.
Name	Name of the mailbox database.
Administrative description	Administrative description of the mailbox database.
Master	Specifies where to find the mailbox database master. A server or a database availability group can be entered.
Master type	Type of mailbox database master.
Exchange database	Storage location of the server.
Store	Name of the storage group.
Public folder database	Name of the public folder database.
Offline address list	Name of the default offline address list.
Store deleted mailboxes [days]	Number of days the deleted mailboxes stay on the server before they are finally removed.
Store deleted objects [days]	Number of days the deleted objects (email message for example) remain on the server before being removed.
Warn at [KB]	Global setting for the maximum size of mailboxes in KB. If this size is exceeded the user is sent a warning that messages must be deleted in the archive mailbox.
Prohibit send at [KB]	Global setting for the size of mailboxes in KB above which, sending messages is prohibited. If this size is exceeded the user is sent a message that messages must be deleted in the archive mailbox. The user is not able to send more messages until the size of the mailbox has been reduced.
Prohibit transfer at [KB]	Global setting for the size of mailboxes in KB above which, sending, and receiving messages is prohibited.
Warning interval	Interval for warnings for mailbox databases.
Do not delete permanently	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. In the Manager, select the **Active Directory | Exchange system administration | <Organization> | Organization configuration | Address lists** category.
2. Select the address list in the result list.
3. Select the **Change master data** task.

Table 17: 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.
Email users	Specifies whether email users are permitted in the address list.
Email 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. In the Manager, select the **Active Directory | Exchange system administration | <Organization> | Organization configuration| Offline address lists** category.
2. Select the offline address list in the result list.
3. Select the **Change master data** task.

Table 18: 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.
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. In the Manager, select the **Active Directory | Exchange system administration | <organization> | Organization configuration | Public folders** category.
2. Select the public folder in the result list.
3. Select the **Change master data** task.

Table 19: 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. In the Manager, select the **Active Directory | Exchange system administration | <organization> | Organization configuration | Public folder database** category.
2. Select the public folder database in the result list.
3. Select the **Change master data** task.

Table 20: 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. In the Manager, select the **Active Directory | Exchange system administration | <organization> | Server configuration** category.
2. Select the server in the result list.
3. Select the **Change master data** task.

To display a mailbox server's mailbox database.

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

Table 21: Server master data

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

Microsoft Exchange data availability groups

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

To display a database availability group

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

Table 22: 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.

Share policies

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

To assign policies to mailboxes

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

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

   To remove an assignment

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

To display master data for a sharing policy

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

Table 23: 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. In the Manager, select the **Active Directory | Exchange system administration | <organization> | Policies | Retention policies** category.
2. Select the policy in the result list.

3. Select the **Assign mailboxes** task.
4. In the **Add assignments** pane, assign mailboxes.

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

   To remove an assignment

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

To display master data for a retention policy

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

Table 24: 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. In the Manager, select the **Active Directory | Exchange system administration | <organization> | Policies | Email policies** category.
2. Select the policy in the result list.
3. Select the **Assign mailboxes** task.
4. In the **Add assignments** pane, assign mailboxes.

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

To remove an assignment

- Select the mailbox and double-click .

5. Save the changes.

To display policy master data for a mobile email query

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

Table 25: 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.
Minimum password length	Minimum length of the password. Minimum number of characters the password must have.
Password cycle	Number of new passwords that a user has to use before an 'old' one can be reused.
Password expiry period	Length of time a password can be used before it expires.
Password restorable	Specifies whether a 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.

Property	Description
Attachments download permitted	Specifies whether attachments are automatically downloaded.
Max. mail attachment size	Maximum size of mail attachment that can be automatically downloaded.
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. In the Manager, select the **Active Directory | Exchange system administration | <organization> | Policies | Folder management policies** category.
2. Select the policy in the result list.
3. Select the **Assign mailboxes** task.
4. In the **Add assignments** pane, assign mailboxes.

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

   To remove an assignment

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

To display master data for a folder management policy

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

Table 26: 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. In the Manager, select the **Active Directory | Exchange system administration | <organization> | Policies | Role assignment policies** category.
2. Select the policy in the result list.
3. Select the **Assign mailboxes** task.
4. In the **Add assignments** pane, assign mailboxes.

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

   To remove an assignment

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

To display master data for a role assignment policy

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

Table 27: 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. In the Manager, select the **Active Directory | Exchange system administration | <organization> | Policies | Outlook Web App mailbox policies** category.
2. Select the policy in the result list.
3. Select the **Assign mailboxes** task.
4. In the **Add assignments** pane, assign mailboxes.

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

   To remove an assignment

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

To display master data for a role assignment policy

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

5

Microsoft Exchange mailboxes

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

Table 28: Supported mailbox types

Mailbox type	Description
User mailbox	User mailboxes are assigned to Active Directory user accounts in a Microsoft Exchange organization.
Equipment mailbox	Equipment mailboxes are resource mailboxes used for planning resources, such as computers or laptops. This mailbox type can only be created for disabled user accounts.
Room mailbox	Room mailboxes are resource mailboxes used for planning meeting locations.
Linked mailbox	Linked mailboxes are assigned to Active Directory user accounts in a trusted domain. This makes the Microsoft Exchange organization available within a domain. Active Directory user accounts in a trusted domain without an Exchange structure can obtain a linked mailbox in this Microsoft Exchange organization. This mailbox type can only be created for disabled user accounts.
Shared mailbox	Shared mailboxes are mailboxes that are used by several users. This mailbox type can only be created for disabled user accounts.
Legacy mailbox	Legacy mailboxes are mailboxes from 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.
Linked	Linked room mailbox are used for planning meetings, for example, for

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

Detailed information about this topic

- Creating mailboxes on page 79
- Editing master data for mailboxes on page 80
- Receive restrictions for mailboxes on page 91
- Send permission for mailboxes on page 91
- Deactivating mailboxes on page 92
- Deleting and restoring mailboxes on page 93

Creating mailboxes

You always create mailboxes for Active Directory user accounts. 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, shared mailboxes and linked mailboxes can only be created for disabled user accounts.

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

1. In the Manager, select the **Active Directory | Mailboxes** category.
2. Click in the result list.
3. On the master data form, enter the master data for the mailbox.
4. Save the changes.

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

1. In the Manager, select the **Active Directory | User accounts** category.
2. In the result list, select the user account then select the **Change master data** task.

3. Select the **Create mailbox** task.
4. Enter the following information:
    - **Active Directory user account**: The user account is already selected.
    - **Exchange organization**: The exchange organization is already selected. Check the setting.
    - (Optional) **Mailbox database**: Name of the mailbox database. If empty, Microsoft Exchange decides which mailbox database is used.
    - **Alias**: Unique alias for further identification of the mailbox.
5. Save the changes.

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

Detailed information about this topic

- Mailbox general master data on page 81
- Calendar settings for mailboxes on page 84
- Limits for a mailbox on page 85
- Mailbox archive on page 86
- Mailbox retention on page 87
- Mailbox functions on page 88
- Booking resources on page 88

Related topics

- Editing master data for mailboxes on page 80
- Setting up account definitions on page 42
- Deactivating mailboxes on page 92
- Deleting and restoring mailboxes on page 93
- Deleting and restoring e-mail users on page 99

Editing master data for mailboxes

To edit a mailbox

1. In the Manager, select the **Active Directory | Mailboxes** category.
2. Select the mailbox in the result list and run the **Change master data** task.
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 81
- Calendar settings for mailboxes on page 84
- Limits for a mailbox on page 85
- Mailbox archive on page 86
- Mailbox retention on page 87
- Mailbox functions on page 88
- Booking resources on page 88

Related topics

- Setting up account definitions on page 42
- Deactivating mailboxes on page 92
- Deleting and restoring mailboxes on page 93

Mailbox general master data

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

Table 29: 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

Property	Description
	account definition are available in the menu.
Active Directory user account	Active Directory user account for which this mailbox is created.
Linked mailbox	External Active Directory user account that has access to the Exchange organization through this mailbox. A linked mailbox is only permitted for mailboxes with the **linked mailbox** mailbox type. The linked mailbox itself is disabled. Disabling in Active Directory is done by the One Identity Manager Service. After the next synchronization, the linked mailbox is also disabled in the One Identity Manager database.
Exchange organization	Name of the Microsoft Exchange organization.
Canonical name	Mailbox's canonical name. The canonical name is generated automatically.
Mailbox type	Type of mailbox. Available mailbox types are: **User**, **Room**, **Equipment**, **Linked**, **Legacy**, **Shared**, **Discovery**, and **Linked room**.
Alias	Unique alias for further identification of the mailbox.
Mailbox database	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

Property	Description
	organization message delivery in the Microsoft Exchange System Manager.
Send and forward	Specifies whether to send and forward messages. Set this option to send messages to alternative recipients and mailbox owners.
Alternative recipient	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 field. 2. Select the table under **Table** which maps the recipient. 3. Select the recipient under **Alternative recipient**. 4. Click **OK**.
Simple display name	Simple display name for systems that cannot interpret all the characters of normal display names.
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 42
- Share policies on page 71
- Folder administration policies on page 75

- Role assignment policies on page 76
- Deactivating mailboxes on page 92

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 30: 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. Permitted values are: • **Calender attendant disabled**: The calendar attendant is not activated. • **Calender attendant enabled**: The calendar attendant is activated. • **Resource booking attendant enabled**: The resource booking attendant is automatically enabled for mailboxes of type **Room**.
New meeting requests are marked with the status "tentative".	Specifies whether meeting requests are automatically entered in the calendar with the **Tentative** status.
Permit meeting requests from external senders	Specifies whether meeting requests from external senders are entered in the calendar.
Delete expired meeting requests	Specifies whether to automatically delete old meeting requests from the calendar.
Delete expired meeting requests	Specifies whether to automatically delete messages to other attendees about forwarded meetings. These messages are moved to the **Deleted items** folder.

Related topics

- Booking resources on page 88

Limits for a mailbox

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

Table 31: Limits for a mailbox

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

Property	Description
permanently before a backup is made	run.
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 in a mailbox 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. recov-erable 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 items 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 65

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 32: Archiving a mailbox

Property	Description
Archiving enabled	Specifies whether a personal archive is created for this mailbox. Set this option if you want to set up a personal archive for this mailbox.
Archive mailbox database	Name of the archive mailbox database.

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 33: 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 the **Start date** and **End date** fields.
Start date	Start date on which to stop retention actions.
End date	Date on which to end retention actions.
Litigation hold	Specifies whether mailbox retention is mandatory.
Website for litig-ation hold	Website or document with more information to keep the user informed, when the **Litigation hold** option is set. This data is displayed to the user in Outlook.
Comment for litig-ation hold	Additional comment with more information to keep the user informed, when the **Litigation hold** option is set. This data is displayed to the user in Outlook.

Related topics

- Retention policies on page 72

Mailbox functions

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

Table 34: 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 73

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 35: 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.

Property	Description
	Permitted values are: • **Calender attendant disabled**: the calendar attendant is not activated. • **Calender attendant enabled**: the calendar attendant is activated. • **Resource booking attendant enabled**: The resource booking attendant is automatically enabled for mailboxes of type **Room**.
Reject repeated meeting after max. planning period	Specifies whether booking series can be set up beyond the planning period.
Forward meeting requests	Specifies whether meeting requests are forwarded to the resource mailbox deputy managers. The deputy decides about the meeting request.
Max. booking window [days]	Maximum planning period for meeting request in days.
Max. duration [min]	Maximum time allowed booking the resource.
Max. conflicting instances	Maximum conflicts permitted for meeting series which overlap with other meetings. If the value is exceeded, the series request is denied.
Max. series conflicts [%]	Threshold in percent for the permitted conflicts of meetings series that overlap with other meetings. If this value is exceeded, the series request is denied.
Remove attach-ments from meeting requests	Specifies whether attachments are deleted from meeting requests.
Remove comments from meeting requests	Specifies whether message text is deleted from meeting requests.
Remove subject from meeting requests	Specifies whether the subject is deleted from meeting requests.
Only retain calendar meetings	Specifies whether elements that do not belong the calendar are deleted.
Add organizer's name to subject	Specifies whether the organizer's name is given in the meeting request subject field.

Property	Description
Remove "private" flag from accepted meeting	Specifies whether the **Private** status is deleted from meeting requests.
Mark meeting requests as "Tentative"	Specifies whether meeting requests are marked with **Tentative** status in the calendar. If this option is disabled, meeting requests are marked with the **Free** status.
Inform organizer about declined meeting request	Specifies whether the organizer is sent information when a meeting request is declined because of conflicts.
Send additional information about rejected request	Specifies whether additional information is sent in response to a meeting request. Enter the additional information in the **Additional information** input field.
Additional data	Additional information for responding to meeting requests.
Booking permissions for everyone	Specifies whether meeting requests conforming to policy are automatically approved for all users. If this option is not set, use **Assign booking permissions** to specify individual users who can send requests conforming to policy, which are automatically approved.
Out-of-policy request permissions for everyone	Specifies whether all user can send meeting requests that do not conform to policy. These requests are decided by the mailbox deputy. If this option is not set, use **Assign out-of-policy meeting request permission** to specify individual users who can send requests which are policy non-conform.
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 **Booking permissions for everyone** is set. If this option is not set, use **Assign in-policy meeting request permissions** to specify individual users who can send requests which are policy non-conform.
Allow conflicts	Specifies whether conflicting meeting requests are allowed.
Allow reoccurring requests	Specifies whether a series of meetings is allowed.
Request only possible during working hours	Specifies whether the resource can be booked during working hours or outside them, as well.
Resource capacity	Resource capacity, for example, the number of seats in a meeting room.

Related topics

- Send permission for mailboxes on page 91

Receive restrictions for mailboxes

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

To customize mail acceptance for mailboxes

1. In the Manager, select the **Active Directory | Mailboxes** category.
2. Select a mailbox in the result list.
3. Select the **Assign mail acceptance** task to define which recipients can accept messages.

   - OR -

   Select the **Assign mail rejection** task to define which recipients can reject messages.
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 group
   - Mailboxes
   - Email users
   - Email contacts
5. In the **Add assignments** pane, assign recipients.

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

   To remove an assignment
   - Select the recipient and double-click ✓.
6. Save the changes.

Send permission for mailboxes

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

To customize send permission for mailboxes

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

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

    To remove an assignment

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

Deactivating mailboxes

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

Scenario:

- Mailboxes are managed through account definitions.

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

Scenario:

- Mailboxes are not managed through account definitions.

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

- If the configuration parameter is set, mailboxes for an 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. In the Manager, select the **Active Directory | Mailboxes** category.
2. Select a mailbox in the result list.
3. Select the **Change master data** task.
4. Set **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. In the Manager, select the **Active Directory | Mailboxes** category.
2. Select a mailbox in the result list.
3. Select the **Change master data** task.
4. Set the **Mailbox is disabled** option on the **General** tab.
5. Save the changes.

Related topics

- Creating an account definition on page 42
- Creating manage levels on page 45
- Deleting and restoring mailboxes on page 93

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

To restore a mailbox

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

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

Configuring deferred deletion

By default, mailboxes are finally deleted from the database after 30 days. During this period you have the option to reactivate the mailboxes. A restore is not possible once deferred deletion has expired. In the Designer, you can set an alternative delay on the `EX0MailContact` table.

Related topics

- Deactivating mailboxes on page 92

Email users and email contacts

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

Detailed information about this topic

Creating email users

Enter email 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 email 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 email 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

1. In the Manager, select the **Active Directory | E-mail user** category.
2. Click in the result list.
3. On the master data form, enter the master data for the user.
4. Save the changes.

To create an email user for an Active Directory user account manually

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

Related topics

- Master data for email users on page 97
- Editing master data for email users on page 96
- Setting up account definitions on page 42
- Deleting and restoring e-mail users on page 99
- Deleting and restoring mailboxes on page 93

Editing master data for email users

To edit an email user.

1. In the Manager, select the **Active Directory | E-mail user** category.
2. Select the email user in the result list and run the **Change master data** task.

3. Edit the email user's master data.
4. Save the changes.

Related topics

- Master data for email users on page 97
- Setting up account definitions on page 42
- Deleting and restoring e-mail users on page 99

Master data for email users

Table 36: General data of an email user

Property	Description
Employee	Employee to use the email user. An employee is already entered if the email user was generated by an account definition. If you create the email user manually, you can select an employee in the menu.
Account definition	Account definition through which the email user was created. Use the account definition to automatically populate email user master data and to specify a manage level for the email user. One Identity Manager finds the IT operating data of the assigned employee and uses it to populate the corresponding fields in the email user. NOTE: The account definition cannot be changed once the email user has been saved.
Manage level	Manage level with which the email 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 email user is created.
Exchange organization	Name of the organization.
Canonical name	Canonical name of the email 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 email 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 email 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 email 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 email 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 email user is visible in address books. Set this option if you want to prevent the email 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 email user.
Simple display	Simple display name for systems that cannot interpret all the characters of normal display names.
Distinguished name	Email user's distinguished name.

Related topics

- Setting up account definitions on page 42

Receive restrictions for email users

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

To customize mail acceptance for email users

1. In the Manager, select the **Active Directory | E-mail user** category.
2. Select the email user in the result list.
3. Select the **Assign mail acceptance** task to define which recipients can accept messages.

   - OR -

   Select the **Assign mail rejection** task to define which recipients can reject messages.
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 group
   - Mailboxes
   - Email users
   - Email contacts
5. In the **Add assignments** pane, assign recipients.

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

   To remove an assignment
   - Select the recipient and double-click .
6. Save the changes.

Deleting and restoring e-mail users

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

To delete an email user

1. In the Manager, select the **Active Directory | E-mail user** category.
2. Select the email user in the result list.

3. Click to delete the e-mail user.
4. Confirm the security prompt with **Yes**.

To restore an email user

1. In the Manager, select the **Active Directory | E-mail user** category.
2. Select the email user in the result list.
3. Click in the result list.

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

Configuring deferred deletion

By default, email users are finally deleted from the database after 30 days. During this period you have the option to reactivate the email users. A restore is not possible once deferred deletion has expired. In the Designer, you can set an alternative delay on the `EX0MailUser` table.

Creating email contacts

Enter email contacts for Active Directory contacts.

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

- In order to create email 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

1. In the Manager, select the **Active Directory | E-mail contacts** category.
2. Click in the result list.
3. On the master data form, enter the master data for the contact.
4. Save the changes.

To create an email contact for an Active Directory contact manually

1. In the Manager, select the **Active Directory | Contacts** category.
2. In the result list, select the contact then select the **Change master data** task.
3. Select the **Create mail contact** task.
4. Enter the following information:

- **Active Directory contact**: the contact is already selected.
- **Exchange organization**: the exchange organization is already selected. Check the setting.
- **Destination address type**: Target address type of the email address.
- **Destination address**: E-mail address to which the messages should be forwarded.
- **Alias**: Unique alias for further identification of the e-mail contact.

5. Save the changes.

Related topics

- Editing master data for email contacts on page 101
- Master data for email contacts on page 101
- Deleting and restoring email contacts on page 104

Editing master data for email contacts

To edit an email contact

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

Related topics

- Creating email contacts on page 100
- Master data for email contacts on page 101
- Deleting and restoring email contacts on page 104

Master data for email contacts

Table 37: General data of an email contact

Property	Description
Employee	Employee to use the email contact. An employee is already entered if the e-mail contact was generated by an account definition. If you create the email contact manually, you can select an employee in the menu.

Property	Description
Account definition	Account definition through which the email contact was created. Use the account definition to automatically populate email contact master data and to specify a manage level for the email contact. One Identity Manager finds the IT operating data of the assigned employee and uses it to populate the corresponding fields in the email contact. NOTE: The account definition cannot be changed once the email contact has been saved.
Manage level	Manage level with which the email contact is created. Select a manage level from the menu. You can only specify the manage level can if you have also entered an account definition. All manage levels of the selected account definition are available in the menu.
Active Directory contact	Active Directory contact for whom the email is created.
Exchange organization	Name of the organization.
Canonical name	Canonical name of the email 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 email 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 email 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 email 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.

Property	Description
Max. receiving size [KB]	Maximum size for message in KB that an email 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 email contact is visible in address books. Set this option if you want to prevent the email 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**.
Sender authentication required	Specifies whether authentication data is requested from senders. Set this option to prevent anonymous senders mailing the email contact.
Simple display	Simple display name for systems that cannot interpret all the characters of normal display names.
Distinguished name	Email contact's distinguished name.

Related topics

- Setting up account definitions on page 42

Receive restrictions for email contacts

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

To customize mail acceptance for e-mail contacts

1. In the Manager, select the **Active Directory | E-mail contacts** category.
2. Select the email contact in the result list.
3. Select the **Assign mail acceptance** task to define which recipients can accept messages.

   - OR -

   Select the **Assign mail rejection** task to define which recipients can reject messages.
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 group
- Mailboxes
- Email users
- Email contacts

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

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

   To remove an assignment

   - Select the recipient and double-click .

6. Save the changes.

Deleting and restoring email 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. In the Manager, select the **Active Directory | E-mail contact** category.
2. Select the email contact in the result list.
3. Delete the email contact with .
4. Confirm the security prompt with **Yes**.

To restore an email contact

1. In the Manager, select the **Active Directory | E-mail contact** category.
2. Select the email contact in the result list.
3. Click the **Undo delete** button in the result list toolbar.

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

Configuring deferred deletion

By default, email 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 deferred deletion has expired. In the Designer, you can set an alternative delay on the `EX0MailContact` table.

Mail-enabled distribution groups

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

Detailed information about this topic

Creating mail-enabled distribution groups

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

To create a mail-enabled distribution group

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

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

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

Related topics

- Editing master data for mail-enabled distribution groups on page 106
- Master data for mail-enabled distribution groups on page 107

Editing master data for mail-enabled distribution groups

To edit a mail-enabled distribution group

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

Related topics

- Master data for mail-enabled distribution groups on page 107

Master data for mail-enabled distribution groups

Table 38: 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.
Report to owner	Specifies whether the delivery reports are sent to the message owner.
Automatically	Specifies whether changes to recipient's email addresses are automat-

Property	Description
update based on recipient policy	ically updated based on incoming settings.
Only limit messages from authen-ticated users	Specifies whether authentication data is requested from senders. Set this option if only messages from authenticated users are permitted.
Out-of-office message to sender	Set this option if the message sender should receive out-of-office messages.
Add to group	Specifies how members can join the mail-enabled distribution group. Permitted values are: • **Open**: Members can be added to the group without approval. • **Closed**: Only mail-enabled distribution group administrators can add members to the group. Requests to be added to the group are automatically denied. • **Owner approval**: Requests to be added to the group can be made and are approved by the mail-enabled distribution group administrators.
Leave group	Use this option to specify how members can leave the distribution group. Permitted values are: • **Open**: Members can leave the group without approval. • **Closed**: Members can only leave the group with administrator approval. Requests to leave the group are automatically denied.
Distribution group moder-ation	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. Permitted values are: • **Do not notify**: The sender is not notified. • **Only notify senders in your exchange organization**: Only internal senders receive a notification. • **Notify all senders**: Internal and external senders receive notification.

Receive restrictions for mail-enabled distribution groups

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

To modify mail acceptance for mail-enabled distribution groups

1. In the Manager, select the **Active Directory | Mail-enabled distribution groups** category.
2. Select the mail-enabled distribution group in the result list.
3. Select the **Assign mail acceptance** task to define which recipients can accept messages.

   - OR -

   Select the **Assign mail rejection** task to define which recipients can reject messages.
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 group
   - Mailboxes
   - Email users
   - Email contacts
5. In the **Add assignments** pane, assign recipients.

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

   To remove an assignment
   - Select the recipient and double-click .
6. Save the changes.

Send permission for mail-enabled distribution groups

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

To modify the send permission for mail-enabled distribution groups

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

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

    To remove an assignment

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

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. In the Manager, select the **Active Directory | Mail-enabled distribution groups** category.
2. Select the mail-enabled distribution group in the result list.
3. Select the **Assign administrators** task.
4. Select the table which contains the administrators from the menu at the top of the form. You have the following options:
    - Active Directory user accounts
    - Active Directory groups
5. Assign administrator roles in **Add assignments**.

    - OR -

    Remove administrator roles 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. In the Manager, select the **Active Directory | Mail-enabled distribution groups** category.
2. Select the mail-enabled distribution group in the result list and run the **Assign dynamic distribution groups** task.
3. 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 118

Extensions for moderated distribution groups

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

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

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

To specify moderators for mail-enabled distribution groups

1. In the Manager, select the **Active Directory | Mail-enabled distribution groups** category.
2. Select the mail-enabled distribution group in the result list.
3. Select the **Assign moderators** task.
4. Select the table which contains the user from the menu at the top of the form. You have the following options:

- Mailboxes
- Email contacts
- Email users

5. Assign moderators in **Add assignments**.

   - OR -

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

To exclude users from moderation

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

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

   To remove an assignment
   - Select the user and double-click .
6. Save the changes.

Deleting mail-enabled distribution groups

To delete a mail-enabled distribution group

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

The members of a dynamic distribution group are not fixed but are determined using a filter criteria. Dynamic distribution groups are loaded into One Identity Manager through synchronization and can only be edited to a limited extent in One Identity Manager.

Detailed information about this topic

- Master data for dynamic distribution groups on page 114
- Receive restrictions for dynamic distribution groups on page 116
- Send permissions for dynamic distribution groups on page 117
- Adding a dynamic distribution group to mail-enabled distribution groups on page 118

Master data for dynamic distribution groups

To display a dynamic distribution group

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

Table 39: 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.
Email 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. In the Manager, select the **Active Directory | Exchange system administration | <Organization> | Recipient configuration | Dynamic distribution groups** category.
2. Select the dynamic distribution list in the result list.
3. Select the **Assign mail acceptance** task to define which recipients can accept messages.

   - OR -

   Select the **Assign mail rejection** task to define which recipients can reject messages.

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 group
    - Mailboxes
    - Email users
    - Email contacts
5. In the **Add assignments** pane, assign recipients.

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

    To remove an assignment
    - Select the recipient and double-click ✓.
6. Save the changes.

Send permissions for dynamic distribution groups

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

To modify the send permission for dynamic distribution groups

1. In the Manager, select **Active Directory | Exchange system administration | <Organization> | Recipient configuration | Dynamic distribution groups** category.
2. Select the dynamic distribution list in the result list.
3. Select the **Assign send authorizations** task.
4. Select the table which contains the user from the menu at the top of the form. You have the following options:
    - Mail-enabled distribution groups
    - Mailboxes
    - Email users
5. In the **Add assignments** pane, assign users.

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

    To remove an assignment
    - Select the user and double-click ✓.
6. Save the changes.

Adding 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. In the Manager, select the **Active Directory | Exchange system administration | <Organization> | Recipient configuration | Dynamic distribution groups** category.
2. Select the dynamic distribution group in the result list and run the **Assign distribution groups** task.
3. 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 111

Mail-enabled public folders

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

To display mail-enabled public folders

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

To display mail acceptance for mail-enabled public folders

1. In the Manager, select the **Active Directory | Exchange system administration | <organization> | Recipient configuration | Mail-enabled public folders** category.
2. Select the mail-enabled distribution group in the result list.
3. Select the **Assign mail acceptance** task to display which recipients can accept messages.

   - OR -

   Select the **Assign mail rejection** task to display which recipients can reject messages.

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

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

Table 40: Mail-enabled public folder master data

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

Extensions for supporting Exchange hybrid environments

NOTE:

This function is only available if the module Exchange hybrid is installed.

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

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

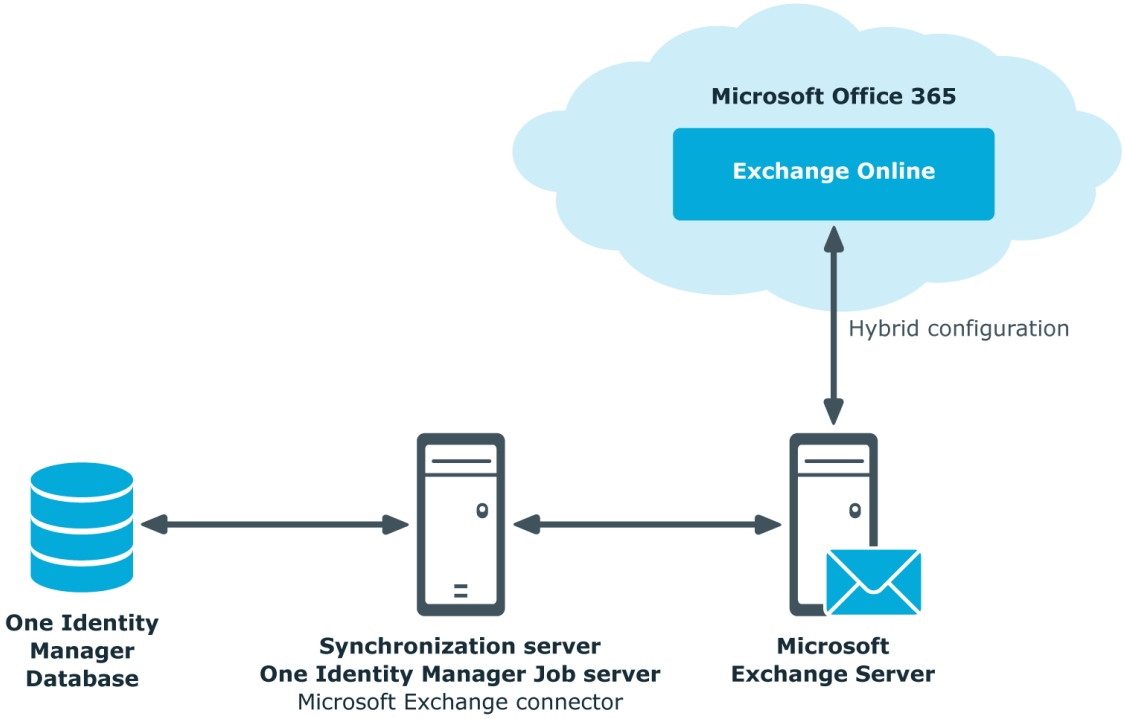
There are the following different types of remote mailboxes:

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

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

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

Figure 2: Architecture for synchronization



Detailed information about this topic

- Advice for synchronizing remote mailboxes on page 122
- Advice for migrating mailboxes on page 123
- Editing remote mailboxes on page 127

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 (if possible, according to Exchange Online)
- In One Identity Manager, the connection between the local Exchange Organization (`EX0Organization`) and the corresponding Azure Active Directory tenant (`AAD0rganization`) must be defined.

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

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

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

Related topics

- Creating a synchronization project for initial synchronization of a Microsoft Exchange environment on page 19
- Default project template for Microsoft Exchange on page 136

Advice for migrating mailboxes

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

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

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

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

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

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

   - Select the mailbox and switch to the Active Directory user account overview. Here you can see whether the user account is connected with a local mailbox and a remote mailbox.

2. Delete the outstanding mailbox.

   - In the Manager, in the **Active DirectoryTarget system synchronization: Exchange** category, select the mailbox in the `EX0Mailbox` table and execute the **Delete** method for 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 exists in One Identity Manager 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. Delete the account definition for local mailboxes belonging to 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.

Creating remote mailboxes

To create a remote mailbox

1. In the Manager, select the **Active Directory | Remote mailboxes** category.
2. Click  in the result list.
3. On the master data form, enter the master data for the mailbox.
4. Save the changes.

To create a mailbox for an Active Directory user account manually

1. In the Manager, select the **Active Directory | User accounts** category.
2. In the result list, select the user account then select the **Change master data** task.
3. Select the **Create remote mailbox** task.
4. Enter the following information:
   - **Active Directory user account**: The user account is already selected.
   - **Exchange organization**: The exchange organization is already selected. Check the setting.
   - **Alias**: Unique alias for further identification of the mailbox.
5. Click **OK**.

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

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

To display remote mailboxes without Exchange licenses

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

Related topics

- Editing remote mailboxes on page 127
- General master data of a remote mailbox on page 127
- Information about remote configuration on page 129
- Information about cloud-based archive mailboxes on page 130
- Receive restrictions for remote mailboxes on page 130
- Extensions for moderated remote mailboxes on page 131

Editing remote mailboxes

To edit a mailbox

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

Related topics

- General master data of a remote mailbox on page 127
- Information about remote configuration on page 129
- Information about cloud-based archive mailboxes on page 130
- Receive restrictions for remote mailboxes on page 130
- Extensions for moderated remote mailboxes on page 131

General master data of a remote mailbox

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

Table 41: 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 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. You can choose from the following options: **Remote user**, **Remote room**, **Remote equipment** and **Remote shared**.
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	Specifies whether authentication data is requested from senders. Set this option to prevent anonymous senders mailing to the mailbox.

Property	Description
required	
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`
Sending message to	Specifies how senders are notified when they send messages to moderated mailbox. Permitted values are: • **Do not notify**: the sender is not notified. • **Only notify senders in your exchange organization**: Only internal senders receive a notification. • **Notify all senders**: Internal and external senders receive notification.
Distinguished name	Mailbox's distinguished name.

Information about remote configuration

The following information about remote configuration is mapped 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 42: Archiving a mailbox

Property	Description
Archiving enabled	Specifies whether a personal archive is created for this mailbox. Set this option if you want to set up a personal archive for this mailbox.
Archive name	Name of the archive.
Archive state	Status of the archive mailbox. This property is available from Microsoft Exchange Server 2013 or later.

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. In the Manager, select the **Active Directory | Remote mailboxes** category.
2. Select a mailbox in the result list.
3. Select the **Assign mail acceptance** task to define which recipients can accept messages.

   - OR -

   Select the **Assign mail rejection** task to define which recipients can reject messages.
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 group
   - Mailboxes
   - Email users

- Email contacts
- Remote mailbox

Extensions for moderated remote mailboxes

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

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

To specify moderators for a mailbox

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

   - OR -

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

To exclude users from moderation

1. In the Manager, select the **Active Directory | Remote mailboxes** category.
2. Select a mailbox in the result list.
3. Select the **Exclude from moderation** task.
4. Select the table which contains the user from the menu at the top of the form. You have the following options:
   - Mail-enabled distribution groups
   - Dynamic distribution group
   - Mailboxes

- Remote mailbox
- Email users
- Email contacts

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

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

   To remove an assignment

   - Select the user and double-click ✓.

6. Save the changes.

11

Error handling

Possible errors when synchronizing an Exchange hybrid environment

Problem

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

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

Cause

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

Solution

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

Problem

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

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

Cause

The Microsoft Exchange Module has already been updated. Therefore, the Microsoft Exchange connector recognizes the extensions for synchronizing Exchange hybrid. The

Exchange Hybrid Module was not installed.

Solution

If you want to synchronize Exchange hybrid

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

Configuration parameters for managing a Microsoft Exchange environment

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

Table 43: Configuration parameters for managing a Microsoft Exchange environment

Configuration parameter	Meaning
TargetSystem | ADS | Exchange2000	Preprocessor relevant configuration parameter for controlling the database model components for the administration of the Microsoft Exchange target system. If the parameter is set, the target system components are available. Changes to this parameter require the database to be recompiled.
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. The **Employee - new user account with default properties created** mail template is used.
TargetSystem | ADS | Exchange2000 | DefaultAddress	The configuration parameter contains the recipient's default email address for sending notifications about actions in the target system.

Appendix B

Default project template for Microsoft Exchange

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

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

Detailed information about this topic

- Default template for Microsoft Exchange 2010 on page 136
- Default project template for Microsoft Exchange 2013, Microsoft Exchange 2016, and Microsoft Exchange 2019 on page 137

Default template for Microsoft Exchange 2010

The template uses mappings for the following schema types.

Table 44: 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 project template for Microsoft Exchange 2013, Microsoft Exchange 2016, and Microsoft Exchange 2019

The template uses mappings for the following schema types.

Table 45: Mapping Microsoft Exchange 2013, Microsoft Exchange 2016, and Microsoft Exchange 2019 schema types to tables in the One Identity Manager schema.

Schema type in Microsoft Exchange	Table in the One Identity Manager schema
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 and other inquiries, such as licensing, support, and renewals, visit https://www.oneidentity.com/company/contact-us.aspx.

Technical support resources

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

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

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

Index

I

J

L

M

O

P

R

S

T

U