Quest

Quest® Migration Manager for Exchange 8.14

Source Exchange 2016 Environment Preparation

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

Quest Software Inc.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

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

Legend

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

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

Migration Manager Source Exchange 2016 Environment Preparation
Updated - March 2019
Version - 8.14

Contents

Source Exchange 2016 Environment Preparation

Follow the steps that are described in the Preparation Overview topic to prepare your Exchange 2016 organization and its environment for being the source organization in the Exchange migration process conducted by Migration Manager for Exchange. For more information about Migration Manager for Exchange refer to the *Migration Manager for Exchange Overview*.

On some of steps you may need to coordinate the setup process with the administrator of the target Exchange organization.

Preparation Overview

This section provides a short overview of the main steps that should be performed to set up your source Exchange 2016 organization and its environment for migration using Migration Manager for Exchange. These steps are described in detail in the related subtopics.

Setting up the source Exchange 2016 organization consists of four main steps:

Checking the System Requirements

On this step make sure that your environment meets the minimal system requirements for Migration Agent for Exchange. For more details, see Checking System Requirements.

Setting Up Accounts and Required Permissions

On this step you should set up the accounts and required permissions for Exchange migration. There are four main types of accounts used by Migration Manager for Exchange agents:

- Source Active Directory Synchronization Account
- Source Exchange Account
- Source Active Directory Account
- Source Agent Host Account

You can simplify the setup by using a single account for all Migration Manager for Exchange processes. This account should have the permissions that are required for Migration Manager for Exchange console and all agents on every server that is involved in the migration.

For more details, see Setting Up Accounts and Required Permissions.

Preparing the Source Exchange Environment for Exchange Migration

On this step you should perform common environment preparations for mailbox and calendar synchronizations:

- Back up Exchange
- Install Microsoft Exchange Server MAPI Client and Collaboration Data Objects 1.2.1 version 6.5.8353.0 or later on agent hosts

- Create custom throttling policies
- Set Exchange Autodiscover URL (Optional)

On this step you should perform common environment preparations for public folder synchronization:

- Prepare agent host for public folder synchronization agents
- Configure administrator mailboxes for public folder synchronization
- Create Aelita EMW Recycle Bin public folder (optional)
- Prepare public folder mailboxes for public folder synchronization
- Create Outlook profiles for public folder synchronization
- Fine-Tuning the Public Folder Synchronization Agents to use Kerberos authentication (Optional)

For more details, see Preparing the Source Exchange Environment for Exchange Migration.

Setting Up Connection with the Target Exchange Organization Using SMTP Connectors

On this step you should set up the connection with the target Exchange organization using SMTP connectors. This task consists of three subtasks given below:

1. Setting up the source Exchange organization for Internet mail flow between source and target Exchange organizations
2. Configuring source DNS server for mail forwarding
3. Testing the SMTP connectors (optional)

For more details, see Setting Up Connection with the Target Exchange Organization Using SMTP Connectors.

Checking System Requirements

CAUTION: Any computer that does not meet the requirements should be upgraded before installing Migration Manager for Exchange components.

Migration Manager for Exchange uses the following Exchange-specific agents involved in the process of migration from Exchange 20102016 organization:

- Public Folder Source Agent (PFSA)
- Public Folder Target Agent (PFTA)
- Transmission Agent (NTA)
- Migration Agent for Exchange

Agents work on agent host servers. Agent host is a stand-alone server. It can be located in another forest.

NOTE: Agent hosts for mail and public folder synchronization must be different as additional software required for MAgE and for PFSA/PFTA to perform those synchronization types cannot be installed on the same computer.

For detailed information about system requirements for agent hosts, see the *Exchange Migration Agents* section of the System Requirements and Access Rights.

Source Exchange 2016 Organization Considerations

- The Exchange Autodiscover service must be properly configured and run in your Exchange organization. For information on Autodiscover for Exchange, go to https://msdn.microsoft.com/en-us/library/office/jj900169(v=exchg.150).aspx. Note that you may also need to manually configure the Autodiscover URLs for the migration project as described in Setting Exchange Autodiscover URL (Optional)
- SSL certificates enabled on Exchange Client Access Servers of the source organization should be signed by a trusted publisher. If you use self-signed certificates, you need to log on to each agent host under the Agent Host Account and add the certificate from CAS to the Trusted Root Certification Authorities and Trusted Publisher lists.
- If two-way calendar synchronization is planned to be utilized, then the Exchange 2016 Calendar Repair Assistant (CRA) should be disabled during the migration period.

Setting Up Accounts and Required Permissions

This section describes requirements for accounts working with the source Exchange servers. Migration Manager for Exchange allows you to use different administrative accounts for different purposes. The following accounts are used by Migration Manager:

- Source Active Directory Synchronization Account
  This account is used by the Directory Synchronization Agent (DSA) to access the source Active Directory domain

  For more details, see Setting Up the Source Active Directory Synchronization Account.
- Source Exchange Account

  For configuration details, see Setting Up the Source Exchange Account.
- Source Active Directory Account

  For configuration details, see Setting Up the Source Active Directory Account.
- Source Agent Host Account

  For configuration details, see Setting Up the Agent Host Account.

NOTE: The default Exchange and Active Directory Accounts for mailbox and calendar synchronization are specified when you create a corresponding synchronization job. To change it, use properties of the corresponding mailbox or calendar synchronization job.

Setting Up the Source Active Directory Synchronization Account

This section describes how to set the required permissions for the Source Active Directory Synchronization Account. This account is used by the Directory Synchronization Agent (DSA) to access the source Active Directory domain

The required privilege level for the Source Active Directory Synchronization Account is membership in the **Domain Admins** group of the source domain.

CAUTION: If for some reason you cannot grant such privileges to the Source Active Directory Synchronization Account, then refer to the *System Requirements and Access Rights* document for the list of minimal required permissions.

To grant the necessary permission to the Source Active Directory Synchronization Account, perform the following:

1. On the source domain controller in the **Active Directory Users and Computers** snap-in, click **Users**, then in the right pane right-click **Domain Admins** and click **Properties**.
2. Go to the **Members** tab, click **Add** and select the Source Active Directory Synchronization Account.
3. Close the dialog boxes by clicking **OK**.

Setting Up the Source Exchange Account

This section describes how to set the required permissions for the Source Exchange Account used by Migration Manager for Exchange agents. This account is used for the following:

- Working with source Exchange mailboxes and public folders (used by Migration Agent for Exchange, Public Folder Source Agent and Public Folder Target Agent)
- Moving mailboxes

Mailbox and Calendar Synchronizations

The following permissions are required for source Exchange account used by Migration Agent for Exchange during mailbox or calendar synchronization:

- **Read** access to the source domain (including all descendant objects)
- **Read** permission for the Microsoft Exchange container in the **Configuration** partition of source Active Directory (including all descendant objects)
- The **ApplicationImpersonation** management role
- The **Move Mailboxes** management role
- The **Mail Recipients** management role

TIP: The **Read** permission for the Microsoft Exchange container is required only if you plan to add the source Exchange organization using the **Add Source Organization Wizard** under this account.

To set up the Source Exchange Account, perform the steps described in the related subtopics.

NOTE: Note that the steps are given only as an example of a possible Source Exchange Account setup.

Public Folder Synchronization

The following permissions are required for source Exchange account used by PFSA and PFTA during public folder synchronization:

- Membership in the local **Administrators** group on all source Exchange servers involved in the migration. If a server is a domain controller, the account should be added to the domain local **Administrators** group of the domain.
- The **Mail Enabled Public Folders** management role

- Permissions to process public folders involved in the migration by granting **Full Control** permission on mailbox databases where those public folders reside.
- Permission to log on to public folder administrator mailbox by granting **Full Control** on it.

NOTE: Exchange account used for public folder synchronization must be mailbox-enabled to be able obtaining source public folder hierarchy.

To set up the Source Exchange Account, perform the steps described in the related subtopics.

NOTE: Note that the steps are given only as an example of a possible Source Exchange Account setup.

Changing Default Exchange Account

Mailbox and calendar synchronization

The default Exchange Account for mailbox and calendar synchronization is specified when you create a corresponding synchronization job. To change it, use properties of the corresponding mailbox or calendar synchronization job.

Public folder synchronization

The default Exchange Account for public folder synchronization (initially displayed on the **Connection** page of the Exchange server **Properties**) is set when you add the source or target organization to the migration project (see the *Registering Source and Target Organizations* section of the *Migration Manager for Exchange User Guide* for details). If necessary, you can change the default Exchange Account for public folder synchronization by clicking **Modify** on the **General** | **Connection** page in the properties of the corresponding server in the Migration Manager for Exchange Console.

To go on using the default Exchange Account for Exchange migration, grant the permissions required for Exchange migration to this account (see the next steps).

Granting Read Access to Active Directory Domain

To grant this permission to an account, complete the following steps:

1. In the **Active Directory Users and Computers** snap-in, right-click the domain name, and then click **Properties**.
2. On the **Security** tab, click **Add** and select the account.
3. Select the account, and then check the **Allow** box for the **Read** permission in the **Permissions** box.
4. Click the **Advanced** button. In the **Advanced Security Settings** dialog box, select the account you specified on step 2, and click **Edit**.
5. In the **Permission Entry** dialog box, select **This object and all descendant (child) objects** from the **Apply to** drop-down list.
6. Close the dialog boxes by clicking **OK**.

Granting Read Permission for Microsoft Exchange Container

To grant this permission to an account, complete the following steps:

1. From the **Start** menu, select **Run**. In the **Run** dialog box, type **ADSIEdit.msc**. Click **OK**.
2. In the **ADSIEdit** snap-in, open the **CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<…>,DC=<…>** container.
3. Right-click the **Microsoft Exchange** container and select **Properties**.
4. In the **Properties** dialog box, click the **Security** tab.
5. On the **Security** tab, click **Add** and select the account to which you wish to assign permissions.
6. Select the account name, and then enable the **Allow** option for the **Read** permission in the **Permissions** box.
7. Click the **Advanced** button. In the **Advanced Security Settings** dialog box, select the account you specified on step 5 and click **Edit**.
8. In the **Permission Entry** dialog box, select **This object and all child (descendant) objects** from the **Apply onto** drop-down list.
9. Close the dialog boxes by clicking **OK**.

Granting ApplicationImpersonation Management Role

To grant the **ApplicationImpersonation** management role to the <*User*> (in our example, *LA\JohnSmith*), run the following cmdlet in Exchange Management Shell:

```
New-ManagementRoleAssignment -Role ApplicationImpersonation -User LA\JohnSmith
```

Granting Move Mailboxes Management Role

To grant the **Move Mailboxes** management role to the <*User*> (in our example, *LA\JohnSmith*), run the following cmdlet in Exchange Management Shell:

```
New-ManagementRoleAssignment -Role "Move Mailboxes" -User LA\JohnSmith
```

Granting Mail Recipients Management Role

To grant the **Mail Recipients** management role to the <*User*> (in our example, *LA\JohnSmith*), run the following cmdlet in Exchange Management Shell:

```
New-ManagementRoleAssignment -Role "Mail Recipients" -User LA\JohnSmith
```

Granting Membership in Local Administrators Group

To add an account to the local Administrators group on a server, perform the following:

1. Open the Computer Management snap-in (Click **Start | Run**, enter `compmgmt.msc` and then click **OK**).
2. In the left pane click **System Tools | Local Users and Groups | Groups**.
3. Right-click the **Administrators** group and click **Add to Group**.
4. Click **Add** and select the account.
5. Close the dialog boxes by clicking **OK**.

Granting Mail Enabled Public Folders Management Role

To grant the **Mail Enabled Public Folders** management role to the *<User>* (in our example, *LA\JohnSmith*), run the following cmdlet in Exchange Management Shell:

```
New-ManagementRoleAssignment -Role "Mail Enabled Public Folders" -User LA\JohnSmith
```

Granting Full Control on Mailbox Database

To grant the **Full Control** permission on a mailbox database to the *<User>* (in our example, *LA\JohnSmith*), run the following cmdlet in Exchange Management Shell:

```
Get-MailboxDatabase | Add-ADPermission -User LA\JohnSmith -AccessRights GenericAll -
ExtendedRights Receive-As
```

Granting Full Control on Public Folder Administrator Mailbox

To grant account the **Full Control** permission on a public folder administrator mailbox to the *<User>* (in our example, *LA\JohnSmith*), run the following cmdlet in Exchange Management Shell:

```
Add-MailboxPermission -Identity <Public_Folder_Migration_Administrator_Mailboxes> -
User LA\JohnSmith -AccessRights FullAccess
```

Setting Up the Source Active Directory Account

This section describes how to set the required permissions for the Source Active Directory Account used by Migration Manager for Exchange agents. This account is used for the following:

- Working with the source Active Directory
- Switching mailboxes

Mailbox and Calendar Synchronization

The following permissions are required for source Active Directory account used by Migration Agent for Exchange during mailbox or calendar synchronization:

- **Read** access to the source domain (including all descendant objects)
- **Read** permission for the **Microsoft Exchange** container in the **Configuration** partition of source Active Directory (including all descendant objects)

To set up the Source Active Directory Account, perform the steps described in the related subtopics.

NOTE: Note that these steps are given only as an example of a possible Source Active Directory Account setup.

Public Folder Synchronization

The following permissions are required for source Active Directory account used by PFSA and PFTA during public folder synchronization:

- The **Write proxyAddresses** permission on the **Descendant publicFolder objects** for the **Microsoft Exchange System Objects** organizational unit in all domains in which source Exchange servers involved in public folder synchronization reside.

  NOTE: Alternatively, you can grant the **Write** permission on that organizational unit.

To set up the Source Active Directory Account, perform the steps described in the related subtopics.

NOTE: Note that these steps are given only as an example of a possible Source Active Directory Account setup.

Changing Default Active Directory Account

CAUTION: This section is relevant to the public folder synchronization only. Active Directory Account for mailbox or calendar synchronization is specified during corresponding job configuration.

The default Source or Target Active Directory Account (initially displayed on the Associated domain controller page of the Exchange server's properties) is set when you add the source or target organization to the migration project (see the *Registering Source and Target Organizations* section of the **Migration Manager for Exchange User Guide** for details).

To change the Source or Target Active Directory Account, click **Modify** on the **General | Associated domain controller** page of the corresponding source (target) server properties in the Migration Manager for Exchange Console.

To go on using the default Source (Target) Active Directory Account for Exchange migration, grant the permissions required for Exchange migration to this account (see the next steps).

Granting Read Access to Active Directory Domain

To grant this permission to an account, complete the following steps:

1. In the **Active Directory Users and Computers** snap-in, right-click the domain name, and then click **Properties**.
2. On the **Security** tab, click **Add** and select the account.
3. Select the account, and then check the **Allow** box for the **Read** permission in the **Permissions** box.
4. Click the **Advanced** button. In the **Advanced Security Settings** dialog box, select the account you specified on step 2, and click **Edit**.
5. In the **Permission Entry** dialog box, select **This object and all descendant (child) objects** from the **Apply to** drop-down list.
6. Close the dialog boxes by clicking **OK**.

Granting Read Permission for the Microsoft Exchange Container

To grant the **Read** permission for the Microsoft Exchange Container for the account, take the following steps:

1. From the **Start** menu, select **Run**. In the **Run** dialog box, type **ADSIEdit.msc**. Click **OK**.
2. In the **ADSIEdit** snap-in, open the **CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<…>,DC=<…>** container.
3. Right-click the **Microsoft Exchange** container and select **Properties**.
4. In the **Properties** dialog box, click the **Security** tab.
5. On the **Security** tab, click **Add** and select the account to which you wish to assign permissions.
6. Select the account name, and then enable the **Allow** option for the **Read** permission in the **Permissions** box.
7. Click the **Advanced** button. In the **Advanced Security Settings** dialog box, select the account you specified on step 5 and click **Edit**.
8. In the **Permission Entry** dialog box, select **This object and all child (descendant) objects** from the **Apply onto** drop-down list.
9. Close the dialog boxes by clicking **OK**.

Granting Write proxyAddresses Permission on Descendant PublicFolder Objects

To grant an account the **Write proxyAddresses** permission on the **Descendant publicFolder objects** for the **Microsoft Exchange System Objects** organizational unit, take the following steps:

1. In the **Active Directory Users and Computers** snap-in, right-click the **Microsoft Exchange System Objects** OU and click **Properties**.
   NOTE: If there is no Microsoft Exchange System Objects OU, you should select **View | Advanced Features** in the **Active Directory Users and Computers** snap-in.
2. On the **Security** tab, click **Advanced**, then click **Add** and specify the account. Then click **OK**.
3. On the **Object** tab of the **Permission Entry** dialog box , select **Descendant publicFolder objects** from the **Apply to** drop-down list.
4. Then open the **Properties** tab and select **Descendant publicFolder objects** again.
5. After that enable the **Allow** option for the **Write proxyAddresses** permission in the **Permissions** box.
6. Close the dialog boxes by clicking **OK**.

Setting Up the Agent Host Account

This section describes how to set the required permissions for the Agent Host Account used by Migration Manager for Exchange agents. This account is used to install and run Migration Manager for Exchange agents on agent hosts and to access the license server. The required privileges for the Agent Host Account are as follows:

- Membership in the local **Administrators** group on the license server (unless alternative credentials are used for the license server). If server is located in another trusted forest, the account should have local **Administrator** permissions on the license server
- Local **Administrator** permissions on the agent host server.

- Permission to create, read and write SCP in domain where agent host resides. The SCP object is located in the **CN=Exchange Migration Project,CN=QmmEx,CN=Migration Manager,CN=Quest Software,CN=System,DC=eternity,DC=<...> ,DC=<...>** Active Directory container.
- The **db_owner** role on the SQL server where the database resides. Note that this permission is required if you use **Windows authentication** option for connecting to SQL Server.

NOTE: By default each Exchange server is an agent host for itself. If you use the default agent host then to simplify the account setup process, you can grant these permissions to the Exchange Account and use it instead of the Agent Host Account.

To set up the Agent Host Account, perform the steps described in the related subtopics.

NOTE: Note that the steps are given only as an example of a possible Agent Host Account setup.

Changing the Default Source Agent Host Account

CAUTION: This section is relevant to the public folder synchronization only. Source Agent Host Account for mailbox or calendar synchronization is specified during corresponding job configuration.

The default Source Agent Host Account (initially displayed on the **Default Agent Host** page of the Exchange server **Properties**) is set when you add the source organization to migration project (see the *Registering Source and Target Organizations* section of the *Migration Manager for Exchange User Guide* for details).

If necessary, you can change the default Source Agent Host Account. For that, go to the **Agent Management** node in the Migration Manager for Exchange Console, and use properties of the corresponding agent host server.

To go on using the default Source Agent Host Account for Exchange migration, grant the permissions required for Exchange migration to this account (see the next steps).

Granting SCP Create, Read and Write Permissions

Grant the Agent Host Account permissions to **Create**, **Read** and **Write** Service Connection Point (SCP) object located in the **CN=Exchange Migration Project,CN=QmmEx,CN=Migration Manager,CN=Quest Software,CN=System,DC=eternity,DC=<...>,DC=<...>** container:

1. From the **Start** menu, select **Run**. In the **Run** dialog box, type **ADSIEdit.msc**. Click **OK**.

   NOTE: If you have a Windows 2003 domain controller, the ADSIEdit utility, which is part of the Windows 2003 Support Tools, may not be installed. In this case install the Support Tools by running the **Support\Tools\Suptools.msi** file located on the Windows 2003 CD.

2. In the ADSIEdit snap-in, open the **CN=Exchange Migration Project,CN=QmmEx,CN=Migration Manager,CN=Quest Software,CN=System,DC=eternity,DC=<...>,DC=<...>** container
3. Right-click the SCP object and click **Properties**.
4. In the **Properties** dialog box, click the **Security** tab.
5. On the Security tab, click **Advanced**.
6. In the **Advanced Security Settings** dialog box, click **Add**.
7. In the **Select User**, **Computer**, or **Group** (or similar) dialog box, select the administrative account and click **OK**.

8. In the **Permission Entry** for dialog box, select **This object and all descendant (child) objects** from the **Apply onto** drop-down list.
9. Allow **Create**, **Read**and **Write** permissions for the Agent Host Account.
10. Close the dialog boxes by clicking **OK**.

Granting db_owner Role on SQL Server

To grant the **db_owner** role on the SQL Server for the Agent Host Account, take the following steps:

1. In **SQL Server Management Studio**, browse to the server that will be used by Migration Manager for Exchange, and select **Logins** from the server **Security** node.
2. Right-click Logins and click **New Login**.
3. On the General page of the **Login - New** dialog box, specify the account in the **Login** name field and select the Windows Authentication method.
4. On the **User Mapping** page of the **Login - New** dialog box, select the migration project database and then select **db_owner** database role for that database.
5. Close the dialog boxes by clicking **OK**.

Preparing the Source Exchange Environment for Exchange Migration

Perform the steps described in the related subtopics to ensure that your Exchange environment is ready for migration:

- Backing Up Exchange
- Installing the Microsoft Exchange Server MAPI Client and Collaboration Data Objects 1.2.1
- Creating Custom Throttling Policies
- Setting Exchange Autodiscover URL (Optional)

Additional steps for public folder synchronization

Preparation of Exchange 2016 organization for public folder synchronization is different from preparation of any earlier Exchange version. The main distinction is that public folder synchronization agents (PFSA and PFTA) communicate with Exchange 2016 Server via Outlook MAPI instead of Microsoft Exchange Server MAPI Client and CDO.

If you perform public folder synchronization with Exchange 2016 organization, take the following additional steps.

- Preparing Agent Host for Public Folder Synchronization Agents
- Configuring Administrator Mailboxes for Public Folder Synchronization
- Preparing Public Folder Mailboxes for Public Folder Synchronization
- Creating Aelita EMW Recycle Bin Public Folder (Optional)

- Creating Outlook Profiles for Public Folder Synchronization
- Fine-Tuning Public Folder Synchronization Agents to Use Kerberos Authentication (Optional)

Backing Up Exchange

Before implementing Migration Manager for Exchange in your production environment, back up your Exchange infrastructure. We recommend that Active Directory data be backed up at least twice a day during migration.

Transaction Log File Cleanup

When Migration Manager for Exchange synchronizes mail, for every megabyte of data migrated from the source to the target, a transaction log file of equal size is generated on the target Exchange server. Exchange-aware backup applications purge the transaction logs after the backup completes. By the time the backup finishes, all logged transactions have already been applied to the store and backed up to tape, making log cleaning safe.

Large transaction logs that are generated during mailbox migration quickly occupy free disk space. To work around this problem, perform one of the following:

- If a full backup strategy is implemented in the organization or there is no backup strategy at all, then circular logging may be enabled for unattended log deletion.
- If an incremental or differential backup strategy is already implemented in the organization, then make sure that logs are cleared automatically when backup process is finished. Do not enable circular logging in this case.

Note also that Microsoft recommends turning OFF circular logging on the Exchange server. For more information, refer to Microsoft Knowledge Base article 147524: XADM: How Circular Logging Affects the Use of Transaction Logs.

Installing the Microsoft Exchange Server MAPI Client and Collaboration Data Objects 1.2.1

Migration Manager for Exchange also requires Microsoft Exchange Server MAPI Client and Collaboration Data Objects 1.2.1 version 6.5.8353.0 or later to be installed on all computers where Migration Agent for Exchange instances will run.

Since the MAPI CDO setup package is not available for distribution, you should download it from the Microsoft Web site. At the moment of the last document update, the download link is http://www.microsoft.com/en-us/download/details.aspx?id=42040.

After installing the API, restart the computer.

Creating Custom Throttling Policies

To prevent possible issues in an Exchange 2016 organization, you should create custom throttling policies, apply them to the Exchange Accounts and then restart the Microsoft Exchange Throttling Service. To do this, run the following cmdlets in Exchange Management Shell for each Exchange Account:

```
New-ThrottlingPolicy <QMM_Exchange_Account_Throttling_Policy_Name>
```

```
Set-ThrottlingPolicy <QMM_Exchange_Account_Throttling_Policy_Name> -RCAMaxConcurrency
Unlimited -EWSMaxConcurrency Unlimited -EWSMaxSubscriptions Unlimited -
CPAMaxConcurrency Unlimited -EwsCutoffBalance Unlimited -EwsMaxBurst Unlimited -
EwsRechargeRate Unlimited -PowerShellMaxConcurrency Unlimited

Set-ThrottlingPolicyAssociation -Identity <QMM_Exchange_Account_Name> -
ThrottlingPolicy <QMM_Exchange_Account_Throttling_Policy_Name>

Restart-Service -Name MSExchangeThrottling
```

Preparing Agent Host for Public Folder Synchronization Agents

To perform public folder synchronization you will need one (or more) standalone agent host server associated with each source Exchange 2016 server.

Such agent host must meet the following specific requirements:

- Outlook 2013 32-bit or Outlook 2016 32-bit version must be installed on the agent host.
- The agent host must be used only for PFSA and PFTA to work with source Exchange 2016. No other agents can be installed on it.

NOTE: For complete set of requirements, see *Exchange Migration Agents Server* in the System Requirements and Access Rights document.

Later when configuring migration in Migration Manager for Exchange console, after you register that agent host (s), open its **Properties**, go to the **General | Connection** node and select the **Communicate with Exchange Server via Outlook MAPI** option. Then select the agent host as **Default Agent Host** in the **Properties** of an Exchange 2016 server.

Creating Aelita EMW Recycle Bin Public Folder (Optional)

NOTE: If you skip this step, the **Aelita EMW Recycle Bin** folder will be created automatically by PFTA during public folder synchronization.

If you plan to perform public folder synchronization using Migration Manager Public Folder agents, you should create a special public folder called **Aelita EMW Recycle Bin.**

This folder will help prevent data loss in case of accidental public folder deletion. When a public folder is deleted in one of the environments, the public folder synchronization agents move the corresponding folder in the other environment to the **Aelita EMW Recycle Bin** folder, if it exists, instead of permanently deleting the folder. You can use this folder to check whether important information has been deleted, and restore any data deleted by mistake.

CAUTION: Only deleted public folders will be put into the Aelita EMW Recycle Bin. If you delete a message from a public folder, it will be destroyed permanently in both the Source and Target Exchange organizations.

Configuring Administrator Mailboxes for Public Folder Synchronization

Public folder migration administrator mailboxes should be created on all Exchange 2016 servers involved in public folder synchronization. These mailboxes will be used to access the public folder tree when creating public folder synchronization jobs.

> **CAUTION: The administrator mailbox specified for the synchronization job should not be changed during the synchronization process.**
>
> **The administrator mailboxes should not be included in mailbox or calendar synchronization jobs.**

After you created public folder migration administrator mailboxes, take the following steps:

1. Ensure that the Exchange 2016 organization has primary hierarchy mailbox (which is the first created public folder mailbox in organization). If there are no public folder mailboxes yet, create one. It will automatically become primary hierarchy mailbox.
2. After that associate public folder migration administrator mailbox specified for the public folder synchronization with the primary hierarchy mailbox. To do this, run the following cmdlet in Exchange Management Shell:

```
Set-Mailbox –Identity <Public_Folder_Migration_Administrator_Mailboxes> -
DefaultPublicFolderMailbox <Primary_Hierarchy_Mailbox>
```

> **CAUTION: The mailbox database and root public folder specified for the synchronization job should not be renamed during the synchronization process.**

Preparing Public Folder Mailboxes for Public Folder Synchronization

1. Ensure that the size of public folder data to be migrated does not exceed the size limit for the primary hierarchy mailbox. If public folder content in the source organization is larger than the limit in the target organization, to migrate it you will need to perform specific steps including creation of additional secondary hierarchy mailboxes in your target Exchange 2016 organization. For detailed instructions, see *Appendix B. Migrating Large Public Folders to Exchange 2013 or Higher* of *Migration Manager for Exchange User Guide*.
   TIP: For general information on public folders in Exchange 2016, see https://technet.microsoft.com/en-en/library/mt577271(v=exchg.160).aspx.
2. For each public folder mailbox consider adjusting the *Recoverable Items* quota according to the needs of your Exchange 2016 organization (by default, the limit is 30 GB per mailbox). If the quota limit is exceeded for a public folder mailbox, deletions of content in the source public folders will not be synced to that target public folder mailbox anymore.
   To change the quota value for a public folder mailbox, invoke the following cmdlet:

   ```
   Set-Mailbox -Identity PFMailbox –PublicFolder -RecoverableItemsQuota 50GB
   ```

Creating Outlook Profiles for Public Folder Synchronization

To synchronize public folders with Exchange 2016 organization, you need to create special Outlook profiles on the agent host associated with Exchange 2016 where you plan to install PFSA and PFTA.

For that, log on to agent host under the Agent Host Account, open **Start | Control Panel | Mail (32-bit)** and click **Show Profiles**. You must create two profiles: one named *MMEX_PFSA* and the other — *MMEX_PFTA*. To create each profile, take the following steps:

1. Click **Add** and then specify the profile name (either *MMEX_PFSA* or *MMEX_PFTA*, respectively). Click **OK**.
2. Specify the administrator mailbox you plan to use for public folder synchronization.
3. Click **Next** and wait until wizard connects to the mailbox. If prompted for credentials, specify Source Exchange Account credentials and select the **Remember my credentials** option.
4. Select the **Change account settings** option and click **Next**.
5. Clear the **Use Cached Exchange Mode** option.
6. Click **Finish** to complete the wizard.

To ensure that logon to created profiles through Outlook can be performed correctly, run Outlook 2013 and select the *MMEX_PFSA* (*MMEX_PFTA*) profile. If no error messages, credential prompts or any other message boxes that require user response appear, then profile is created properly and therefore can be used by PFSA and PFTA to perform public folder synchronization.

NOTE: Make sure that no issues related to certificate validation occur when you run Outlook. For instance, if you use self-signed certificates for Exchange 2016 Servers, you need to log on to each agent host under the Agent Host Account and add certificate from to the **Trusted Root Certification Authorities** and **Trusted Publisher** lists.

Fine-Tuning Public Folder Synchronization Agents to Use Kerberos Authentication (Optional)

During public folder synchronization, agents establish PowerShell session with source or target Exchange Server to process mail-enabled public folders. If only Kerberos authentication is available in the environment, then force each deployed PFSA or PFTA to use Kerberos authentication as follows:

1. Locate *CONFIG.INI* file of an agent.
2. Add the following line to the INI file and save the file:
   `PSForceUseKerberos=1`
3. Restart the agent.

Setting Exchange Autodiscover URL (Optional)

Migration Agent for Exchange uses the Exchange Autodiscover service to query certain properties of mailboxes being migrated. In order to submit queries to the Autodiscover service, MAgE needs to know its URL. In most cases, the agent automatically gets the Autodiscover URLs for both the source and target organizations. However, you may experience situations when automatically discovering the URL fails or returns the incorrect URL.

When the correct URL cannot be obtained, an error will be generated causing the synchronization job to fail. Errors in the log file with the following exceptions indicate problems with obtaining the proper Autodiscover URL:

- **AutodiscoverLocalException**: The Autodiscover service couldn't be located.
- **ServiceRequestException**: The request failed. The remote server returned an error: (401) Unauthorized.
- **ServiceRemoteException**: Invalid user: 'Joe.User@contoso.com'.
- **AutodiscoverDeploymentIdMismatchException**: The User Deployment ID returned from Autodiscover does not match the expected value.

If you encounter any of the above exceptions, you need to manually configure the Autodiscover URL for the source or target organizations (or both) . The Autodiscover URL can be configured using the Set-MMExOrganizationProperties cmdlet from the MMExPowerShell module. Below is an example how to use the cmdlet:

```
Set-MMExOrganizationProperties -FQDN source.contoso.com -AutodiscoverUrl
https://autodiscover.source.contoso.com/autodiscover/autodiscover.svc
```

TIP: For information how to use the MMExPowerShell.psm1 module, see Configuring Migration Project Settings Using PowerShell.

Setting Up Connection with the Target Exchange Organization Using SMTP Connectors

This section describes how to set up a connection with the target Exchange organization using SMTP connectors. On this step you may need to coordinate with the administrator of the target Exchange organization to set up the connection properly.

For more details, see the related topics:

- Setting up Source Exchange Organization for Internet Mail Flow between Source and Target Exchange Organizations
- Configuring Source DNS Server for Mail Forwarding
- Testing the SMTP Connectors (Optional)

Setting up Source Exchange Organization for Internet Mail Flow between Source and Target Exchange Organizations

You need to establish Internet mail flow between the source and the target Exchange organizations. For that, you need to create an **Internet Send** connector and **Receive** connector on an Exchange Mailbox server that can be directly reached through the Internet.

To establish mail flow to and from the Internet through a Mailbox server, follow these steps:

1. Create a Send connector (to send email from source Exchange organization to the Internet) on the Mailbox server.
2. Modify the default Receive connector for the source domain to accept anonymous e-mail from the Internet
3. Add the e-mail domain used for redirection to the list of accepted domains.

Each step is explained in further detail in the related subtopics.

Creating Send Connector

To create a Send connector, you can use either Exchange Admin Center (EAC) or Exchange Management Shell.

NOTE: For additional information, refer to the Create a Send Connector for Email Sent to the Internet TechNet article.

To create a Send connector using Exchange Admin Center

1. In the **Exchange Admin Center**, navigate to **Mail flow > Send** connectors, and then click **Add +.**
2. In the **New send connector** wizard, specify a name for the send connector, for example, *QMM Send Connector*, and then select **Custom** for the **Type**. Click **Next**.
3. Verify that MX record associated with recipient domain is selected. Then select the Use the external DNS lookup settings on servers with transport roles. Click Next.
4. Under **Address** space, click **Add +**. In the **Add domain** window, make sure SMTP is listed as the **Type**. For **Fully Qualified Domain Name (FQDN)**, specify the address space you want to use for mail redirection from source to target organization (for example, **.target.local*). Click **Save**.
5. Make sure **Scoped send connector** is not selected, and then click **Next**.
6. For **Source server**, click **Add +**. In the S**elect a Server** window, select one or more Mailbox servers in your organization and click **Add**. After you've selected the server, click **OK**.
7. Click **Finish**.

To create a Send connector using Exchange Management Shell

Run the following command:

```
new-SendConnector -Name 'QMM Send Connector' -Usage 'Custom' -AddressSpaces
'SMTP:*.target.local;1' -IsScopedConnector $false -DNSRoutingEnabled $true -
UseExternalDNSServersEnabled $true -SourceTransportServers 'ServerName'
```

where:

- **.target.local* is the address space you want to use for mail redirection from source to target organization.
- *ServerName* is the Mailbox server name.

Modifying Default Receive Connector

To modify the default Receive connector for the source Exchange organization to receive mail from the Internet, you can use either Exchange Admin Center or Exchange Management Shell.

To modify the default Receive connector using Exchange Admin Center

1. In the Exchange Admin Center, navigate to **Mail flow > Receive connectors**.
2. Select the appropriate Mailbox server from the list of servers.
3. Then select the **Default <Server Name>** connector and click **Edit**.
4. In the **Default <Server Name>** window, go to **Security**.
5. In **Permission groups**, select **Anonymous users** to add anonymous permissions.
6. Click **Save**.

To modify the default Receive connector using Exchange Management Shell

Run the following command:

```
Set-ReceiveConnector -PermissionGroups 'AnonymousUsers, ExchangeUsers,
ExchangeServers, ExchangeLegacyServers' -Identity 'ServerName\Default ServerName'
```

Where *ServerName* is the Mailbox server name.

Adding E-mail Domain Used for Redirection to the List of Accepted Domains

To add a new Accepted domain, you can use either Exchange Admin Center or Exchange Management Shell.

To add a domain to Accepted Domains list using Exchange Admin Center

1. In the Exchange Admin Center, navigate to **Mail flow > Accepted domains**, and then click **Add +**.
2. In the **Name** field, specify the accepted domain, such as *source.local*.
3. In the **Accepted domain** field, specify the SMTP namespace for which the Exchange organization will accept e-mail messages, such as **.source.local*.
4. Then select the **Authoritative Domain. E-mail is delivered to a recipient in this Exchange organization** option.
5. Click **Save**.

To add a domain to Accepted Domains list using Exchange Management Shell

Run the following command:

```
new-AcceptedDomain -Name 'source.local' -DomainName '*.source.local' -DomainType
'Authoritative'
```

where **.source.local* is the address space you want to use for mail redirection from the target to the source organization.

Configuring Source DNS Server for Mail Forwarding

After you have completed setting up the source Exchange 2016 organization for Internet mail flow between source and target Exchange organizations, you should also add the Mail Exchanger (MX) record for the source domain to the DNS server. This is necessary to forward the mail (redirected to the additional SMTP addresses added by the Directory Synchronization Agent) to the source Exchange server.

We will use the following additional address space given as example on the previous steps:

- *@source.local*—to redirect mail from target to source mailboxes. A secondary SMTP address will be added to each source mailbox by the Directory Synchronization Agent according to this template.

To set MX record for the source domain

1. In the DNS snap-in, connect to the target DNS server and browse to the **Forward Lookup Zones** container.
2. Right-click the **Forward Lookup Zones** and select **New Zone**
3. In the **New Zone** wizard, select the **Primary zone** to be created.
4. Type local for the Zone name and complete the wizard.
5. Right-click the zone object local again, and click **New Mail Exchanger** on the shortcut menu.
6. In the **New Resource Record** dialog box, type **target** for the **Host or child domain**.
7. Click **Browse** and select the **Exchange server** in the source domain to which mail sent to the *@source.local* domain will be redirected.
8. Click **OK**.

Testing the SMTP Connectors (Optional)

After both source and target Exchange organizations have been set up for Internet mail flow as well as both source and target DNS servers have been configured for mail forwarding, it is recommended to test the connection between the source and the target organizations.

> **CAUTION: This step should be performed in coordination with the administrator of the Exchange organization.**

To test the SMTP connectors:

1. Create test mailboxes on the source and target Exchange servers. In this example, both mailboxes will be called **mbx1**.
2. Set the same primary SMTP address for both mailboxes.
3. In this example the primary address for both mailboxes will be **mbx1@Westland.Exchange.com**.
4. Set additional addresses for both mailboxes.

5. In this example additional address for the source mailbox will be **mbx1@source.local**, and **mbx1@target.local** for the target mailbox.
6. Create a contact on the source Exchange server and point it to the additional SMTP address of the target Exchange mailbox (**mbx1@target.local**).
7. Create a contact on the target Exchange server and point it to the additional SMTP address of the source mailbox (*mbx1@source.local*).
8. Open the test source mailbox and send a message to the source contact.
9. Open the test target mailbox and make sure that the message has arrived.
10. From the test target mailbox, send a message to the target contact, and make sure the e-mail has reached the source test mailbox.

About us

Quest provides software solutions for the rapidly-changing world of enterprise IT. We help simplify the challenges caused by data explosion, cloud expansion, hybrid datacenters, security threats, and regulatory requirements. We are a global provider to 130,000 companies across 100 countries, including 95% of the Fortune 500 and 90% of the Global 1000. Since 1987, we have built a portfolio of solutions that now includes database management, data protection, identity and access management, Microsoft platform management, and unified endpoint management. With Quest, organizations spend less time on IT administration and more time on business innovation. For more information, visit www.quest.com.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.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
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product