Quest

Quest® Migration Manager for Exchange 8.14

Target Exchange 2010 Environment Preparation (MAgE)

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.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at https://www.quest.com/legal.

Trademarks

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 for Exchange Target Exchange 2010 Environment Preparation (MAgE)
Updated - March 2019
Version - 8.14

Contents

Target Exchange 2010 Environment Preparation (MAgE)

Follow the steps that are described in the Preparation Overview topic to prepare your Exchange 2010 organization and its environment for being the target organization in the Exchange migration process conducted by Migration Manager for Exchange.

> **IMPORTANT:** This document covers the case when mailbox and calendar synchronization is performed using Migration Agent for Exchange. If you perform those types of synchronization using legacy agents then refer to the *Target Exchange 2010 Environment Preparation (Legacy)* document.

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

Preparation Overview

This section provides a short overview of the main steps that should be performed to set up your target Exchange 2010 organization and its environment for migration using Migration Manager for Exchange. These steps are described in detail in the related subtopics.

Setting up the target Exchange 2010 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 Manager for Exchange agents. 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:

- Target Active Directory Synchronization Account
  This account is used by the Directory Synchronization Agent (DSA) to access the target Active Directory domain
- Target Exchange Account
  This account is used by Migration Manager for Exchange agents installed on agent host to access the target Exchange server.
- Target Active Directory Account
  This account is used by Migration Manager for Exchange agents to access the target domain.
- Target Agent Host Account
  This account is used to install and run the Migration Manager for Exchange agents on agent host and to access the license server.

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 Target Exchange Environment for Exchange Migration

On this step you should perform common environment preparations:

- Back up Exchange
- Create the Aelita EMW Recycle Bin public folder (optional)
- Install Microsoft Exchange Server MAPI Client and Collaboration Data Objects 1.2.1 version 6.5.8353.0 or later on agent hosts (optional)
- Create administrator mailboxes for public folder synchronization
- Create custom throttling policies

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

Setting Up Connection with the Source Exchange Organization Using SMTP Connectors

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

1. Setting up the target Exchange 2010 organization for Internet mail flow between target and source Exchange organizations
2. Configuring target DNS server for mail forwarding
3. Testing the SMTP connectors (optional)

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

Prerequisites

Before starting the preparation of the target Exchange 2010 organization and its environment, make sure that you have the privileges to grant all of the following permissions to accounts.

NOTE: The list of permissions given below contains all required permissions for the accounts. However some of the permissions can be replaced with their equivalents. For more information, see the corresponding steps for each account.

Target Active Directory Synchronization Account

- Membership in the **Administrators** or **Domain Admins** group of the target domain.

Target Exchange Account

Mailbox and Calendar Synchronization

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

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

Public Folder Synchronization

- Membership in the local **Administrators** group on all target 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.
- Membership in the **Public Folder Management** group
- Permissions to process public folders involved in the migration by granting **Full Control** permission on public folder databases where those public folders reside.
- Permission to log on to public folder administrator mailbox by granting **Full Control** on it.

Target Active Directory Account

Mailbox and Calendar Synchronization

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

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 target Exchange servers involved in public folder synchronization reside.

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

Target Agent Host Account

- 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.
- 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.
- 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.

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 to Exchange 20102019 organization:

- 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.

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

Target Exchange 20102019 Organization Considerations

- The Migration Manager for Exchange console shows only those servers from target Exchange 20102019 organization that host the Mailbox role. This is required because only servers with actual data are considered for migration.
- The Exchange Autodiscover service must be properly configured and run in your Exchange 20102019 organization. For information on Autodiscover for Exchange 20102019, go to http://msdn.microsoft.com/en-us/library/exchange/jj900169.aspx.
- SSL certificates enabled on Exchange 20102019 Servers of the target 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 certificate to the Trusted Root Certification Authorities and Trusted Publisher lists.
- The Exchange 20102019 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 target Exchange servers. Migration Manager for Exchange allows you to use different administrative accounts for different purposes. Exchange data is migrated by Migration Manager for Exchange agents, which use the following accounts:

- Target Active Directory Synchronization Account
  This account is used by the Directory Synchronization Agent (DSA) to access the target Active Directory domain
  For more details, see Setting Up the Target Active Directory Synchronization Account.
- Target Exchange Account
  This account is used by Migration Manager for Exchange agents installed on agent host to access the target Exchange server.
  For more details, see Setting Up the Target Exchange Account.
- Target Active Directory Account
  This account is used by Migration Manager for Exchange agents to access the target domain.
  For more details, see Setting Up the Target Active Directory Account.
- Target Agent Host Account
  This account is used to install and run the Migration Manager for Exchange agents on agent host and to access the license server.
  For more details, see Setting Up Target Agent Host Account.

Setting Up the Target Active Directory Synchronization Account

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

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

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

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

1. On the target 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 Target Active Directory Synchronization Account (in our example, **QMM_Trg_DSA**).
3. Close the dialog boxes by clicking **OK**.

Setting Up the Target Exchange Account

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

- Working with target Exchange mailboxes and public folders (used by Migration Agent for Exchange, Public Folder Source Agent, and Public Folder Target Agent)
- Making the newly-created public folders mail-enabled (used by the public folder agents only: Public Folder Source Agent and Public Folder Target Agent)
- Moving mailboxes

Mailbox and Calendar Synchronization

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

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

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

Public Folder Synchronization

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

- Membership in the local **Administrators** group on all target 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.
- Membership in the **Public Folder Management** group
- Permissions to process public folders involved in the migration by granting **Full Control** permission on public folder databases where those public folders reside.
- Permission to log on to public folder administrator mailbox by granting **Full Control** on it.

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

NOTE: Note that the steps are given only as an example of a possible Target 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 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 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 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 Full Control on Public Folder Database

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

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

Granting Membership in Public Folder Management Group

To add an account to the **Public Folder Management** group in the Exchange 2010 organization, take the following steps:

1. In the **Active Directory Users and Computers** snap-in select the **Microsoft Exchange Security Groups** node.
2. In the right pane, right-click **Public Folder Management** group and click **Properties**.
3. On the **Members** tab click **Add** and select the account.
4. Close the dialog boxes by clicking **OK**.

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 Target Active Directory Account

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

- Working with the target Active Directory
- Switching mailboxes

Mailbox and Calendar Synchronization

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

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

The following permissions are required for target 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 target Exchange servers involved in public folder synchronization reside.

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

To set up the Target 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 Target 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**.

Granting Write permission on the Microsoft Exchange System Objects Organizational Unit

The account needs the Write permission on the Microsoft Exchange System Objects organizational unit (OU) in all domains in which Exchange servers involved in public folder synchronization reside.

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 **Add**, and select the account.
3. Select the account name, and then enable the **Allow** option for the **Write** 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 child (descendant) object**s from the **Apply onto** drop-down list.
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 Target Agent Host Account

The default Target Agents Host Account (initially displayed on the **Default Agent Host** page of the Exchange server Properties) is set when you add the target 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 Target Agent Host Account by clicking **Modify** on the **General | Default Agent Host** page of the corresponding target server properties in the Migration Manager for Exchange Console.

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

Granting Membership in the Local Administrators Group on the License Server

The Target Agent Host Account should be a member of the local **Administrators** group on the license server (unless alternative credentials are used for the license server).

CAUTION:

- **If license server is a domain controller, the account should be added to the domain local Administrators group of the domain.**
- **Local Administrator permissions are required on the license server if this license server is located in another trusted forest.**

To add the Agent Host Account to the local **Administrators** group on the license 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 Target Agent Host Account (in our example, **QMM_Src_AH**).
5. Close the dialog boxes by clicking **OK**.

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 Target 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
- Creating Aelita EMW Recycle Bin Public Folder (Optional)
- Installing the Microsoft Exchange Server MAPI Client and Collaboration Data Objects 1.2.1 (Optional)
- Creating Administrator Mailboxes for Public Folder Synchronization
- Creating Custom Throttling Policies

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.

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.

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

IMPORTANT:

This step should be performed only on agent hosts used by PFSA and PFTA to perform public folder synchronization.

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 Manager for Exchange agents 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 Administrator Mailboxes for Public Folder Synchronization

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

The administrative mailbox selected for public folder synchronization should reside in a private mailbox database located on the same server as the public folder database. The mailbox database should be also associated with that public folder database. To set this association, in **Exchange Management Console** open properties of the mailbox database and specify the public database as **Default public folder database** on the **Client Settings** tab.

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.**

Creating Custom Throttling Policies

To prevent possible issues in an Exchange 2010 Service Pack 1 or later 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 PowerShell commands for each Exchange Account:

```
New-ThrottlingPolicy <QMM_Exchange_Account_Throttling_Policy_Name>

Set-ThrottlingPolicy <QMM_Exchange_Account_Throttling_Policy_Name> -
PowerShellMaxConcurrency <MaxConcurrency>

Set-ThrottlingPolicy <QMM_Exchange_Account_Throttling_Policy_Name> –EWSMaxConcurrency
$null –EWSPercentTimeInAD $null –EWSPercentTimeinCAS $null –EWSPercentTimeInMailboxRPC
$null –EWSMaxSubscriptions $null –EWSFastSearchTimeoutInSeconds $null –
EWSFindCountLimit $null

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

Restart-Service -Name MSExchangeThrottling
```

where *MaxConcurrency* is the number of Migration Agent for Exchange (MAgE) instances simultaneously working with Exchange 2010 server, multiplied by the value of 5.

NOTE: To ensure stable operation of MAgE agents when working with Microsoft Exchange 2010, you should increase the number of permitted user connections. For that, change the value for the **MaxSessionsPerUser** parameter using the client throttling policies, as follows:

1. On the computer that hosts the Microsoft Exchange CAS server, in **%Program Files%\Microsoft\Exchange Server\V14\Bin**, open the **microsoft.exchange.addressbook.service.exe.config** file in a text editor.
2. Change the value of the **MaxSessionsPerUser** parameter to **100000**.
3. Save and close the file.
4. Restart the Address Book service.

Setting Up Connection with the Source Exchange Organization Using SMTP Connectors

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

For more details, see the related topics:

- Setting up Target Exchange 2010 Organization for Internet Mail Flow between Target and Source Exchange Organizations
- Configuring Target DNS Server for Mail Forwarding
- Testing the SMTP Connectors (Optional)

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

You need to establish Internet mail flow between the target and the source Exchange organizations. For that, one of the following methods can be used:

- Establishing Internet mail flow directly through a Hub Transport server.
- Establishing Internet mail flow through a subscribed Edge Transport server.

Establishing Internet Mail Flow Directly Through a Hub Transport Server

If you choose this option, you need to create an **Internet Send** connector and **Receive** connector on an Exchange 2010 Hub Transport server that can be directly reached through the Internet.

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

1. Create a Send connector (to send email from source Exchange 2010 organization to the Internet) on the Hub Transport 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 on the Hub Transport server.

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

NOTE: For information about configuring Receive connectors in Exchange 2010 organization, refer to the following Microsoft Knowledge Base articles:

- Allow Anonymous Relay on a Receive Connector
- Configure the Receive connector as externally secured

Creating Send Connector

To create a Send connector, you can use either Exchange Management Console or Exchange Management Shell.

To create a Send connector using Exchange Management Console

1. Open the Exchange Management Console. Select **Organization Configuration** | **Hub Transport**.
2. In the action pane, click **New Send Connector**. The **New SMTP Send Connector** wizard runs.
3. When prompted, in the **Name** field, type a unique name for the connector, for example, "**QMM Send Connector.**" From the **Select the intended use for this Send connector** drop-down list, select **Custom**, and then click **Next**.
4. On the **Address space** page, click **Add**. In the dialog box displayed, specify the address space you want to use for mail redirection from source to target (target to source) organization (for example, ***.target.local** or ***.source.local**), select the **Include all subdomains** option, click **OK** and then click **Next**.
5. On the **Network settings** page, select **Use Domain Name System (DNS) "MX" records to route mail automatically**. Select the **Use the External DNS Lookup settings on the transport server** option.
6. Next, on the **Source Server** page, click **Add**. In the dialog box displayed, select one or more **Hub Transport** servers in your organization, click **OK** and then click **Next**.
7. Finally, on the **New Connector** page, click **New**, and then on the **Completion** page, click **Finish**.

To create a Send connector using Exchange Management Shell

Run the following command for the source Exchange organization:

```
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 Hub Transport server name.

Run the following command for the target Exchange organization:

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

where:

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

Modifying Default Receive Connector

To modify the default Receive connector for the source or target Exchange 2007/2010 organization to receive mail from the Internet, you can use either Exchange Management Console or Exchange Management Shell.

To modify the default Receive connector using Exchange Management Console

1. Run Exchange Management Console. Select the **Server Configuration | Hub Transport** node.
2. In the **Hub Transport** pane select the appropriate Hub Transport server.
3. On the **Receive Connectors** tab, select the **Default <Server Name>** connector. In the **Actions** pane, click **Properties** for this connector.
4. In **Default <Server Name> Properties** dialog box, open the **Permission Groups** tab.
5. Select **Anonymous Users** to add anonymous permissions.
6. Click **OK** to apply the settings.

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 Hub Transport server name.

Adding E-mail Domain Used for Redirection to the List of Accepted Domains on Hub Transport Server

To add a new Accepted domain on a computer that has the Hub Transport server role installed, you can use either Exchange Management Console or Exchange Management Shell.

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

1. Run the Exchange Management Console and select the **Organization Configuration** | **Hub Transport** node.
2. In the **Actions** pane, click **New Accepted Domain**. This will start the **New Accepted Domain** wizard.
3. On the first page, provide the following information:
    - **Name**—Specify the accepted domain in the user interface, such as **source.local** (target.local).
    - **Accepted Domain**—Specify the SMTP namespace for which the Exchange organization will accept e-mail messages, such as ***.source.local** (***.target.local**).

4. Select the **Authoritative Domai**n. **E-mail is delivered to a recipient in this Exchange organization** option for the accepted domain type.
5. Click **New**.
6. On the **Completion** page, click **Finish**.

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

Run the following command for the source Exchange organization:

```
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.

Run the following command the target Exchange organization:

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

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

Establishing Internet Mail Flow through a Subscribed Edge Transport Server

The second option for establishing Internet mail flow between the target and the source Exchange organizations (or between the source and the target Exchange organizations) is to subscribe the **Edge Transport** server to an Active Directory site. The connectors that establish mail flow to the Internet are created automatically when you subscribe an Edge Transport server to an Active Directory site by using the Edge Subscription process.

Before you begin this procedure, verify that the following prerequisites are met:

- Authoritative domains are configured on the Hub Transport server.
- E-mail address policies are configured on the Hub Transport server.
- Network communications over the secure LDAP port 50636/TCP are enabled through the firewall separating your perimeter network from the Exchange organization.

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

1. Export the Edge Subscription file from the Edge Transport server.
2. Import the Edge Subscription file on the Hub Transport server.
3. Force EdgeSync synchronization to begin on the Hub Transport server.

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

Export the Edge Subscription file from the Edge Transport Server

1. Run the following command on the Edge Transport server, providing the complete file path of the Edge Subscription file that you are creating.
   ```
   New-EdgeSubscription -FileName "C:\EdgeSubscriptionInfo.xml"
   ```
2. Copy the resulting XML file to the Hub Transport server.

Import the Edge Subscription file on the Hub Transport Server

On the Hub Transport server, run the following command:

```
New-EdgeSubscription -filename "C:\EdgeSubscriptionInfo.xml" -
CreateInternetSendConnector $true -CreateInboundSendConnector $true -site "Site-Name"
```

Where Site-Name is the name of Active Directory site where the Hub Transport server is located.

Force EdgeSync Synchronization

To force EdgeSync synchronization, run the following command from the Exchange Management Shell on the Hub Transport server:

```
Start-EdgeSynchronization
```

Configuring Target DNS Server for Mail Forwarding

After you have completed setting up the target Exchange 2007/2010 organization for Internet mail flow between target and source Exchange organizations, you should also add the Mail Exchanger (MX) record for the target 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 target Exchange 2007/2010 server.

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

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

To set MX record for the target 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 target domain to which mail sent to the *@target.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