

Quest® Migration Manager for Exchange 8.15

**Source and Target Exchange 2003
Environment Preparation**



© 2020 Quest Software Inc. ALL RIGHTS RESERVED.

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

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

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

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

Quest, the Quest logo, and Join the Innovation are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit <https://www.quest.com/legal/trademark-information.aspx>. All other trademarks and registered trademarks are property of their respective owners.

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 Source and Target Exchange 2003 Environment Preparation

Updated - March 2020

Version - 8.15

Contents

Source and Target Exchange 2003 Environment Preparation	4
Preparation Overview	4
Preparation Checklist	5
Prerequisites	6
Checking System Requirements	7
Setting Up Accounts and Required Permissions	8
Setting Up the Active Directory Synchronization Account	8
Setting Up the Exchange Account	9
Changing the Default Exchange Account	10
Granting Read Access to the Target Active Directory Domain (Target Exchange Environment Only)	10
Granting Membership in Server Local Administrators Group	10
Granting Full Control on Organizational Unit	11
Granting Full Control on Exchange Servers	11
Granting Full Control on the Microsoft Exchange System Objects Organizational Unit	12
Granting Modify Permissions	13
Setting Up the Active Directory Account	13
Changing the Default Active Directory Account	14
Granting Read Access to Active Directory Domain	14
Granting Full Control on Organizational Unit (For Target Exchange Environment Only)	15
Setting Up Agent Host Account	15
Changing the Default Agent Host Account	15
Granting Membership in the Local Administrators Group on the License Server	16
Preparing the Exchange Environment for Exchange Migration	16
Backing up Exchange	16
Create Aelita EMW Recycle Bin Public Folder (Optional)	17
Creating Mailboxes for Public Folder and Free/Busy Synchronization	17
Creating Administrator Mailboxes for Mailbox and Calendar Synchronization (Optional)	18
Configuring the NSPI Connection Limit	18
Connecting the Source and Target Exchange Organizations Using SMTP Connectors	19
Setting Up the SMTP Connectors	19
Forcing Exchange to Accept Redirected Mail as Inbound Mail	21
Modifying Name Resolution Parameters on the Bridgehead Servers in Exchange	22
Configuring DNS Servers for Mail Forwarding	22
Testing the SMTP Connectors (Optional)	23
About us	25
Technical support resources	25

Source and Target Exchange 2003 Environment Preparation

Follow the steps that are described in the [Preparation Checklist](#) topic to prepare your Exchange 2003 organization and its environment for Exchange migration process conducted by Migration Manager for Exchange.

i **NOTE:** This section contains information about preparing both source and target Exchange 2003 organizations.

Terminology Used

The following terms denote source and target Exchange 2003 environment servers and accounts, depending on the environment you are setting up using this guide.

Term	Source Environment	Target Environment
Exchange 2003 server	Source Exchange 2003 server	Target Exchange 2003 server
Active Directory Synchronization Account	Source Active Directory Synchronization Account	Target Active Directory Synchronization Account
Exchange Account	Source Exchange Account	Target Exchange Account
Active Directory Account	Source Active Directory Account	Target Active Directory Account
Agent Host Account	Source Agent Host Account	Target Agent Host Account

Preparation Overview

This section provides a short overview of the main steps that should be performed to set up your Exchange 2003 organization and its environment for migration using Migration Manager for Exchange.

Setting up the Exchange 2003 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:

- Active Directory Synchronization Account
This account is used by:
 - a. The Directory Synchronization Agent (DSA) to access the corresponding Active Directory domain
 - b. The Mail Source Agent (MSA) to perform mailbox switch

- **Exchange Account**
This account is used by Migration Manager for Exchange agents installed on agent host to access the Exchange server.
- **Active Directory Account**
This account is used by Migration Manager for Exchange agents to access the corresponding domain.
- **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.

i | **NOTE:** Throughout this guide each account is meant to be source or target regarding to the environment being set up.

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 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).
- Create administrator mailboxes for public folder and free/busy synchronization.
- Create administrator mailboxes for mailbox and calendar synchronization (optional)

For more details, see [Preparing the Exchange Environment for Exchange Migration](#).

Connecting the Source and Target Exchange Organizations Using SMTP Connectors

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

1. Setting up the SMTP connectors
2. Forcing Exchange to accept redirected mail as inbound mail
3. Modifying name resolution parameters on the bridgehead Servers in Exchange
4. Configuring DNS servers for mail forwarding
5. Testing the SMTP connectors (optional)

For more details, see [Connecting the Source and Target Exchange Organizations Using SMTP Connectors](#).

Preparation Checklist

This checklist will help you set up your Exchange 2003 organization and its environment properly. Make sure you have done all the steps below before completing the preparation.

Check	Step
<input type="checkbox"/>	Check the system requirements
<input type="checkbox"/>	Set up the Active Directory Synchronization Account
<input type="checkbox"/>	Set up the Exchange Account
<input type="checkbox"/>	Set up the Active Directory Account
<input type="checkbox"/>	Set up the Agent Host Account
<input type="checkbox"/>	Back up Exchange
<input type="checkbox"/>	Create the Aelita EMW Recycle Bin public folder (optional)
<input type="checkbox"/>	Create administrator mailboxes for public folder and free/busy synchronization
<input type="checkbox"/>	Create administrator mailboxes for mailbox and calendar synchronization (optional)
<input type="checkbox"/>	Configure the NSPI connection limit
<input type="checkbox"/>	Set up the SMTP connectors
<input type="checkbox"/>	Force Exchange to accept redirected mail as inbound mail
<input type="checkbox"/>	Modify name resolution parameters on the bridgehead servers in Exchange
<input type="checkbox"/>	Configure DNS servers for mail forwarding
<input type="checkbox"/>	Test the SMTP connectors (optional)

Prerequisites

Before starting the preparation of the Exchange 2003 organization and its environment, make sure that you have the privileges to grant all of the following permissions to accounts.

i **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.

Active Directory Synchronization Account

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

Exchange Account

- **Read** access to the target domain (for target Exchange environment only).
- Membership in the local **Administrators** group on all 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.
- **Full Control** permission on the organizational units (OUs) (and their child objects) where the synchronized objects are located.
- **Full control** permission on Exchange 2003 servers (including **Send As** and **Receive As** permissions).
- **Full Control** permission on the **Microsoft Exchange System Objects** organizational unit in all domains in which Exchange 2003 servers involved in public folder synchronization reside.

- Modify public folder replica list permission, **Modify public folder deleted item retention** permission, and **Modify public folder quotas** permission on the administrative groups where the Exchange 2003 servers involved in public folder synchronization reside.

Active Directory Account

- **Read** access to the corresponding domain.
- **Full Control** permission on the organizational units (OUs) (and their child objects) where the synchronized objects are located.

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.

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 migration process:

- Public Folder Source Agent
- Public Folder Target Agent
- Mail Source Agent (for source Exchange environment only)
- Mail Target Agent (for target Exchange environment only)
- Calendar Synchronization Agent
- Free/Busy Synchronization Agent
- Transmission Agent
- Migration Agent for Exchange

Agents work on agent host servers.

Agent host can be:

1. An Exchange server itself, which is the default configuration. After you enumerate an Exchange organization all Exchange servers are registered as agent hosts for themselves.
2. Another Exchange server from the same Exchange organization.
3. A stand-alone server. It can be located in another forest or workgroup.

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

! CAUTION: The private information store with administrator mailbox (the System Attendant mailbox used by default or custom administrator mailbox) should be mounted for each Exchange server where the mail, calendar, or free/busy synchronization agents are running.

Setting Up Accounts and Required Permissions

This section describes requirements for accounts working with the 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:

- Active Directory Synchronization Account
This account is used by:
 - a. The Directory Synchronization Agent (DSA) to access the corresponding Active Directory domain
 - b. The Mail Source Agent (MSA) to perform mailbox switch

For more details, see [Setting Up the Active Directory Synchronization Account](#).

- Exchange Account
This account is used by Migration Manager for Exchange agents installed on agent host to access the Exchange server.
For more details, see [Setting Up the Exchange Account](#).
- Active Directory Account
This account is used by Migration Manager for Exchange agents to access the corresponding domain.
For more details, see [Setting Up the Active Directory Account](#).
- 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 Agent Host Account](#).

Setting Up the Active Directory Synchronization Account

This section describes how to set the required permissions for the Active Directory Synchronization Account. This account is used by:

- The Directory Synchronization Agent (DSA) to access the corresponding Active Directory domain
- The Mail Source Agent (MSA) to perform mailbox switch

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

! CAUTION: If for some reason you cannot grant such privileges to the 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 Active Directory Synchronization Account, perform the following:

1. On the corresponding 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 Active Directory Synchronization Account.
3. Close the dialog boxes by clicking **OK**.

Setting Up the Exchange Account

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

In the source Exchange 2003 environment

- Working with the source Exchange mailboxes and public folders (used by the Mail Source/Target Agent, 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)
- Synchronizing Calendar information (used by the Calendar Synchronization Agent)
- Synchronizing free/busy data (optional) (used by the Free/Busy Synchronization Agent)
- Switching/Moving mailboxes

In the target Exchange 2003 environment

- Working with target Exchange mailboxes and public folders (used by the Mail Target Agent, 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)
- Synchronizing Calendar information (used by the Calendar Synchronization Agent)
- Synchronize free/busy data (optional) (used by the Free/Busy Synchronization Agent)
- Move mailboxes

The required privileges for the Exchange Account are as follows:

- **Read** access to the target domain (for target Exchange environment only).
- Membership in the local **Administrators** group on all 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.
- **Full Control** permission on the organizational units (OUs) (and their child objects) where the corresponding synchronized objects are located.
- **Full Control** permission on Exchange 2003 servers (including **Send As** and **Receive As** permissions).
- **Full Control** permission on the Microsoft Exchange System Objects organizational unit in all domains in which Exchange 2003 servers involved in public folder synchronization reside.
- **Modify public folder replica list** permission, **Modify public folder deleted item retention** permission, and **Modify public folder quotas** permission on the administrative groups where the Exchange 2003 servers involved in public folder synchronization reside.

To set up the Exchange Account, perform the following steps:

1. Change the default Exchange account.
2. Grant **Read** access to the target Active Directory domain (target Exchange environment only).

3. Grant membership in server local **Administrators** group.
4. Grant **Full Control** on organizational unit.
5. Grant **Full Control** on Exchange servers.
6. Grant **Full Control** on the Microsoft Exchange System Objects organizational unit.
7. Granting **Modify** permissions.

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

Changing the Default Exchange Account

The default Exchange Account (initially displayed on the Connection page of the Exchange server Properties) is set when you add 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 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.

Granting Read Access to the Target Active Directory Domain (Target Exchange Environment Only)

Exchange Account should have **Read** access to the target Active Directory.

To grant this permission to the Exchange 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 **Exchange Account**.
3. Select the **Exchange 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 child (descendant) objects** from the **Apply onto** drop-down list.
6. Close the dialog boxes by clicking **OK**.

Granting Membership in Server Local Administrators Group

The Exchange Account used by Migration Manager for Exchange agents should be a member of the local **Administrators** group on each Exchange server involved in the migration.

! | **CAUTION:** If the Exchange server is a domain controller, the account should be added to the domain local **Administrators** group of the domain.

To add the Exchange Account to the local **Administrators** group on each Exchange server involved in the migration, 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 **Exchange Account**.
5. Close the dialog boxes by clicking **OK**.

Granting Full Control on Organizational Unit

To work with the Active Directory objects, the Exchange Account needs the **Full Control** permission on the organizational units and their child objects that contain the objects to be synchronized. This permission should be set on the domain controller where the objects you need to synchronize are located.

To grant the required permissions to the account, perform the following steps:

1. In the **Active Directory Users and Computers** snap-in, right-click the OU where the objects are located, and click **Properties**.
2. On the **Security** tab, click **Add**, and select the **Exchange Account**.

i | **NOTE:** If there is no **Security** tab, you should select **View | Advanced Features** in the **Active Directory Users and Computers** snap-in.

3. Select the account name, and then enable the **Allow** option for the **Full Control** 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) objects** from the **Apply onto** drop-down list.
6. Close the dialog boxes by clicking **OK**.

Granting Full Control on Exchange Servers

The Exchange Account should have the Full Control permission on Exchange servers in the Exchange 2003 organization, including the **Send As** and **Receive As** permissions.

To grant the required permissions to the account, do one of the following:

- If an Active Directory Connector (ADC) has previously been installed in the Active Directory domain, add the account to the **Exchange Services** group. This is a local domain security group created when you install ADC.
- Grant an account access to all mailboxes in the entire organization by completing the following steps:
 - a. Start **Exchange System Manager**.
 - b. Open the organization's **Properties**.
 - c. Open the **Security** tab.

i | **NOTE:** By default, you are not allowed to modify security on the organization object, and the **Security** tab is not displayed. Refer to the *Enabling the Security Tab* section below for instructions on how to enable the **Security** tab on the organization object.

- d. Select the Full Control permission for the account.

CAUTION: The explicit denial of rights to administrators is set on the organization object by denying the **Receive As** and **Send As** rights. If the account is an **Exchange Administrator** or belongs to the **Enterprise Admins** or **Domain Admins** groups, it will still not be able to access mailboxes, because the denial to the group will take precedence over the grant of permissions to the individual account.

Alternatively, if you do not want to enable the **Security** tab on the organization object, you can grant the account access to every single server by completing the following steps:

1. Start the **Exchange System Manager**.
2. Open the server's **Properties**.
3. Click the **Security** tab.
4. Select the **Full Control** or the **Send As** and **Receive As** permissions for the account.

After you change permissions, you may need to log off and log on again. You should wait for about 10 minutes for the directory cache to expire. If you have multiple domain controllers in the forest, it may also be necessary to wait for directory replication to complete.

Enabling the Security Tab

To force the display of the Security tab on the organization objects, you must add a registry key, as follows:

1. Click **Run** on the **Start Menu** and type `regedit` to start **Registry Editor**.
2. Locate the following registry key on the local machine: **HKEY_CURRENT_USER\Software\Microsoft\Exchange\ExAdmin**
3. On the **Edit** menu, click **Add Value**, and then add the following registry value:
Value name: ShowSecurityPage
Data type: REG_DWORD
Value: 1
4. Quit Registry Editor.

This change takes effect immediately; you do not need to restart Exchange System Manager. This change affects only the user currently logged on.

CAUTION: An incorrectly modified registry cannot be undone and may cause serious problems with the operating system. We recommend that only advanced users modify the registry.

Granting Full Control on the Microsoft Exchange System Objects Organizational Unit

The Exchange Account used by Migration Manager for Exchange agents needs the **Full Control** permission on the Microsoft Exchange System Objects organizational unit (OU) in all domains in which Exchange 2003 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 **Exchange Account**.
3. Select the account name, and then enable the **Allow** option for the **Full Control** 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) objects** from the **Apply onto** drop-down list.
6. Close the dialog boxes by clicking **OK**.

Granting Modify Permissions

The Exchange Account used by Migration Manager for Exchange agents needs the following permissions:

- **Modify public folder replica list** permission
- **Modify public folder deleted item retention** permission
- **Modify public folder quotas** permission

To grant the required permissions to the account, perform the following:

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

i **NOTE:** If you have a Windows 2003 domain controller, the ADSIEdit utility, which is a 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=Administrative Groups,CN=<ExchangeOrganizationName>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<...>,DC=<...>** container.
3. For each administrative group in the container, right-click the **CN=<AdministrativeGroupName>** container and select **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 Exchange account and click **OK**.
8. In the **Permission Entry** for dialog box, select **This object and all child (descendant) objects** from the **Apply onto** drop-down list.
9. Allow the **Modify public folder replica list** permission, **Modify public folder deleted item retention** permission and **Modify public folder quotas** permissions for the administrative account.
10. Close the dialog boxes by clicking **OK**.

Setting Up the Active Directory Account

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

In the source Exchange 2003 environment

- Working with the source Active Directory

In the target Exchange 2003 environment

- Working with the target Active Directory
- Re-homing mailboxes
- Switching mailboxes and synchronize mailboxes in Remote Users Collections (Mail Source Agent, Mail Target Agent)

The required permissions for the Active Directory Account are as follows:

- **Read** access to the corresponding domain.
- **Full Control** permission on the organizational units (OUs) (and their child objects) where the synchronized objects are located.

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

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

Changing the Default Active Directory Account

The default Active Directory Account (initially displayed on the **Associated domain controller** page of the Exchange server's properties) is set when you add 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 Active Directory Account, click *Modify* on the **General | Associated domain** controller page of the corresponding server properties in the Migration Manager for Exchange Console.

To go on using the default Active Directory Account for Exchange migration, grant the permissions required for Exchange migration to this account.

Granting Read Access to Active Directory Domain

The Active Directory Account used by Migration Manager for Exchange agents needs **Read** access to the corresponding domain to work with servers and Active Directory.

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

1. On the corresponding domain controller in the **Active Directory Users and Computers** snap-in, right-click the domain name, and then click **Properties** on the shortcut menu.
2. On the **Security** tab, click **Add** and select the account to which you wish to assign permissions.

i | **NOTE:** If there is no Security tab, you should select **View | Advanced Features** in the **Active Directory Users and Computers** snap-in.

3. Select the account name, and then enable the **Allow** option 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 child (descendant) objects** from the **Apply onto** drop-down list. Close the dialog boxes by clicking **OK**.

Granting Full Control on Organizational Unit (For Target Exchange Environment Only)

To work with the target Active Directory objects, the Active Directory Account needs the **Full Control** permission on the organizational units and their child objects that contain the objects to be synchronized. This permission should be set on the domain controller where the objects you need to synchronize are located.

To grant the required permissions to the account, perform the following steps:

1. In the **Active Directory Users and Computers** snap-in, right-click the OU where the objects are located, and click **Properties**.
2. On the **Security** tab, click **Add**, and select the **Active Directory Account**.
i | **NOTE:** If there is no **Security** tab, you should select **View | Advanced Features** in the **Active Directory Users and Computers** snap-in.
3. Select the account name, and then enable the **Allow** option for the **Full Control** 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) objects** from the **Apply onto** drop-down list.
6. Close the dialog boxes by clicking **OK**.

Setting Up 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 the agent host 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.

i | **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 Agents Host Account.

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

i | **NOTE:** Note that these steps are given only as an example of a possible Agent Host Account setup.

Changing the Default Agent Host Account

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

To go on using the default Agent Host Account for Exchange migration, grant the permissions required for Exchange migration to this account.

Granting Membership in the Local Administrators Group on the License Server

The 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 Agents 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 Agent Host Account.
5. Close the dialog boxes by clicking **OK**.

Preparing the 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](#)
- [Create Aelita EMW Recycle Bin Public Folder \(Optional\)](#)
- [Creating Mailboxes for Public Folder and Free/Busy Synchronization](#)
- [Creating Administrator Mailboxes for Mailbox and Calendar Synchronization \(Optional\)](#)
- [Configuring the NSPI Connection Limit](#)

Backing up Exchange

Before implementing Migration Manager 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 and public folders, 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. 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, "XDAM: How Circular Logging Affects the Use of Transaction Logs."

Create Aelita EMW Recycle Bin Public Folder (Optional)

! CAUTION: If you skip this step, you must manually turn off using the Aelita EMW Recycle Bin folder during public folder synchronization (set the UseRecycleBin parameter to 0). See the Use Fine-Tuning the Agents section of the Migration Manager for Exchange User Guide for details.

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**. Replicate this folder to all the public folder servers involved in the public folder synchronization process.

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.

Creating Mailboxes for Public Folder and Free/Busy Synchronization

Administrator mailboxes should be created on all Exchange 2003 servers involved in public folder and free/busy synchronization. These mailboxes will be used to access the public folder tree and the Schedule+ Free/Busy folder when creating public folder and free/busy synchronization jobs.

The administrative mailbox selected for public folder synchronization should be hosted on the same server as the public database. This public database should be associated with the mailbox database where the administrative mailbox resides. For that, 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 Administrator Mailboxes for Mailbox and Calendar Synchronization (Optional)

Mailbox and calendar synchronization agents access the migrated mailboxes via the administrator mailbox. By default, the Microsoft System Attendant mailbox is used as the administrator mailbox on Exchange 2003 servers. However, in some cases it is necessary to create custom administrator mailboxes and use them instead of the Microsoft System Attendant mailbox.

Configuring the NSPI Connection Limit

i | **IMPORTANT:** This step must be performed only if you have any Windows Server 2008 or later domain controllers acting as Global Catalog.

By default, the maximum number of simultaneous Name Service Provider Interface (NSPI) connections equals to 50 per user for Windows Server 2008 or later domain controllers. Therefore, to avoid possible issues related to exceeding that value, you may need to increase the NSPI connection limit on all Windows Server 2008 or later domain controllers acting as Global Catalog. The recommended limit value equals the number of agent instances working simultaneously multiplied by 5.

To change the default connection limit for a domain controller, take the following steps:

1. Click **Start**, click **Run**, type **regedit**, and then click **OK**.
2. Locate and then click the following registry subkey:
`HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NTDS`
3. Click the **Parameters** key.
4. On the **Edit** menu, point to **New**, and then click **DWORD Value**.
5. Type **NSPI max sessions per user**, and then press **Enter**.
6. Double-click **NSPI max sessions per user**, type the appropriate maximum number of the NSPI connections, and then click **OK**.
7. Restart the computer or restart Active Directory Domain Services.

For additional information, see the following Microsoft Support articles:

- [Error: "Trying to connect to Microsoft Exchange Server" results in MAPI_E_LOGON_FAILED](#)
- [NSPI connection to a Windows-based domain controller causes MAPI client applications to fail and returns a "MAPI_E_LOGON_FAILED" error message](#)

Connecting the Source and Target Exchange Organizations Using SMTP Connectors

To ensure that users do not lose their mail during the migration period, and to make the migration from source Exchange organization to target smooth, Migration Manager establishes mail redirection between the source and the target Exchange servers.

Accordingly, Migration Manager requires the source and target Exchange organizations be connected using SMTP connectors.

For more details, see the related topics:

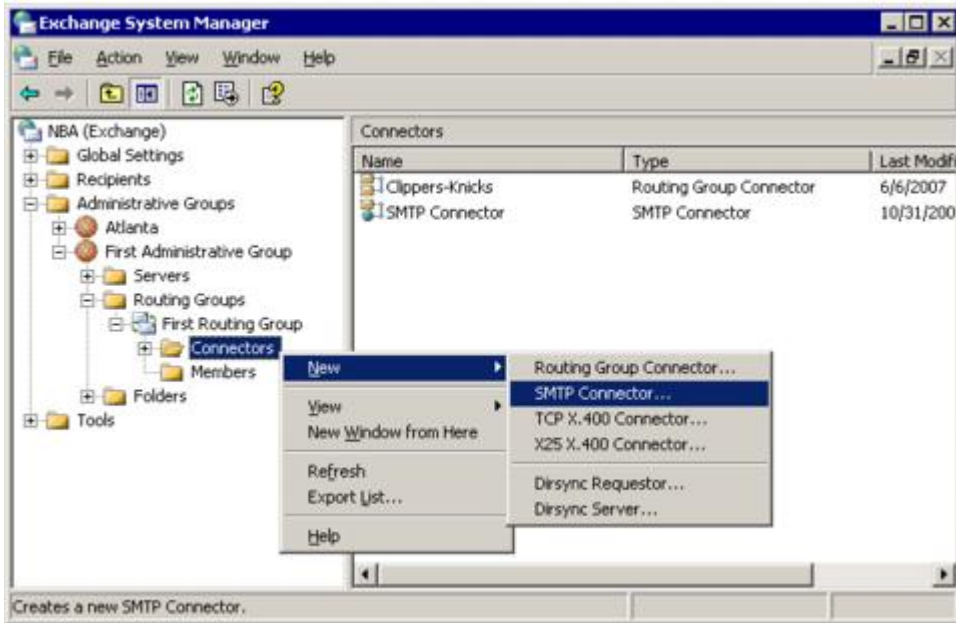
- [Setting Up the SMTP Connectors](#)
- [Forcing Exchange to Accept Redirected Mail as Inbound Mail](#)
- [Modifying Name Resolution Parameters on the Bridgehead Servers in Exchange](#)
- [Configuring DNS Servers for Mail Forwarding](#)
- [Testing the SMTP Connectors \(Optional\)](#)

Setting Up the SMTP Connectors

Create SMTP connectors between the bridgehead servers of your source and target Exchange organizations by taking the following steps:

1. In Exchange System Manager, right-click the **Connectors** node, select **New**, and then select **SMTP Connector**.

i **NOTE:** The following is an example of connector configuration for a source Exchange 2003 server.

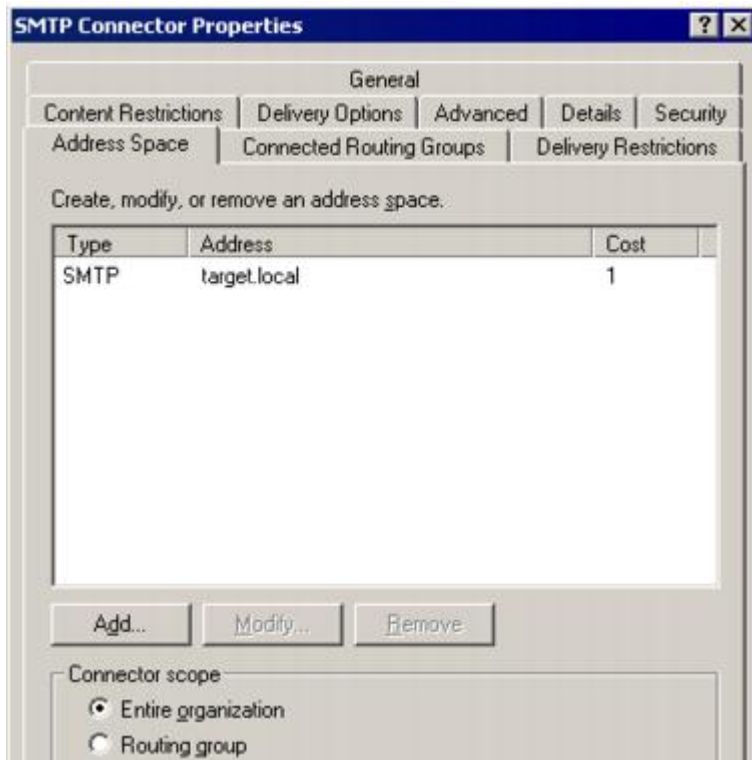


2. Go to the **General** tab of the new connector's properties, and click **Add** to specify the name for the connector and local bridgehead server. Select the **Use DNS to route to each address space on this connector** option to use DNS to route mail to the address spaces specified for this connector.



3. When Migration Manager for Exchange is configured to use SMTP for mail redirection, mail is forwarded to additional SMTP addresses generated by the Directory Synchronization Agent and based on the address templates you provide when setting up the directory synchronization jobs.

Go to the **Address Space** tab and click **Add** to add a new address space. It is recommended that you use the same SMTP prefix that was specified in the **Target SMTP address** template in the directory synchronization settings.



4. Configure other options if needed and click **OK**. This example shows the other options keeping their default values.

Forcing Exchange to Accept Redirected Mail as Inbound Mail

Migration Manager for Exchange provides for uninterrupted user collaboration using the technology of mail redirection between the source and target organizations. Additional SMTP addresses are used for mail redirection. These addresses are automatically added by the Directory Synchronization Agent.

For mail redirection to work, the mail destined to the additional addresses must be accepted as inbound mail. For that, create a recipient policy to make the Exchange organization responsible for all mail delivery to the specified addresses.

Creating a Recipient Policy

To make Exchange consider the redirected mail to be inbound mail and search for the recipients in Active Directory, configure your recipient policy as follows:

1. In Exchange System Manager, expand **Recipients** in the left-hand pane tree, and then right-click the **Recipient Policies** node and create a new policy.
2. In the **New Policy** dialog box that opens, make sure only the **E-Mail Addresses** option is selected.
3. Provide a name for the new policy and leave the list of filter rules blank.
4. Add a new SMTP entry. In the **Address** field, type the address space that you plan to specify for the source or target Exchange organization when setting up the directory synchronization job (for example, **@source.local** or **@target.local**, respectively).
5. Verify that the **This Exchange Organization is responsible for all mail delivery to this address** check box is selected. Then click **OK**.

Modifying Name Resolution Parameters on the Bridgehead Servers in Exchange

To provide for zero-impact migration, recipients of the redirected mail must be resolved to the corresponding directory objects whose addresses are contained in the Global Address List (GAL). To make Exchange resolve SMTP addresses into the directory objects, modify the name resolution parameters on the bridgehead servers in the Exchange organization.

Turn on the **Resolve Anonymous E-mail** option on each Exchange 2003 bridgehead server, as follows:

1. In Exchange 2003 System Manager, expand **Servers** node, and then expand the server's node.
2. Expand the Protocols node, and then expand the **SMTP** node.
3. Right-click the **SMTP virtual server** and then click **Properties**.
4. In the **Properties** dialog box, go to the **Access** tab. Click **Authentication**, and then select the **Resolve anonymous E-mail** check box.
5. Repeat this procedure for each Exchange 2003 bridgehead server.

For more details, refer to the [Resolve Anonymous Senders Functionality in Microsoft Exchange 2003](#) Microsoft Knowledge Base article.

Configuring DNS Servers for Mail Forwarding

After you have configured the SMTP connection between the source and target Exchange organizations, you should also add the MX (Mail Exchanger) records for the source and target domains to the DNS. This is necessary to forward the mail (redirected to the additional SMTP addresses added by the Directory Synchronization Agent) to the source and target SMTP bridgeheads.

i | **NOTE:** Alternatively, instead of creating MX records in DNS, you can configure SMTP connectors to redirect mail to the source and target SMTP bridgeheads correspondingly.

As an example, we will use the following additional address spaces:

- **@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.
- **@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 Mail Exchanger (MX) record for the source domain:

1. In the DNS snap-in, connect to the source 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 newly-created zone object local, and click **New Mail Exchanger** on the shortcut menu.
6. In the **New Resource Record** dialog, type **source** 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**.

To set the Mail Exchanger (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 newly-created zone object local, and click **New Mail Exchanger** on the shortcut menu.
6. In the **New Resource Record** dialog, 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.

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
In this example the primary address for both mailboxes will be **mbx1@Westland.Exchange.com**.
3. Set additional addresses for both mailboxes.
In this example additional address for the source mailbox will be **mbx1@source.local**, and **mbx1@target.local** for the target mailbox.
4. Create a contact on the source Exchange server and point it to the additional SMTP address of the target Exchange mailbox (**mbx1@target.local**).

5. Create a contact on the target Exchange server and point it to the additional SMTP address of the source mailbox (**mbx1@source.local**).
6. Open the test source mailbox and send a message to the source contact.
7. Open the test target mailbox and make sure that the message has arrived.
8. 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