Quest® Migration Manager for Exchange 8.15

Target Exchange 2019 Environment Preparation

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

Quest Software Inc.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

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

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.**

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

Migration Manager Target Exchange 2019 Environment Preparation
Updated - April 2020
Version - 8.15

Contents

Target Exchange 2019 Environment Preparation

Follow the steps that are described in the Preparation Overview topic to prepare your Exchange 2019 organization and its environment for being the target organization in the Exchange migration process conducted by Migration Manager for Exchange. For more information about Migration Manager for Exchange refer to the *Migration Manager for Exchange Overview*.

On some of steps you may need to coordinate the setup process with the administrator of the 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 2019 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 2019 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:
  a. The Directory Synchronization Agent (DSA) to access the target Active Directory domain
  b. The Migration Agent for Exchange (MAgE) to perform mailbox switch
- 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
- Install Microsoft Exchange Server MAPI Client and Collaboration Data Objects 1.2.1 version 6.5.8353.0 or later on agent hosts
- Create custom throttling policies

For public folder synchronization, the following additional steps are required:

- Prepare agent host for public folder synchronization agents
- Configure administrator mailboxes for public folder synchronization
- Create the Aelita EMW Recycle Bin public folder (optional)
- Configure public folder migration administrator mailboxes
- Create Outlook profiles for public folder synchronization
- Fine-tuning public folder synchronization agents to use Kerberos authentication (optional)

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 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 2019 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.

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 2019 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 2019 Organization Considerations

- The Migration Manager for Exchange console shows only those servers from target Exchange 2019 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 2019 organization. For information on Autodiscover for Exchange 2019, go to http://msdn.microsoft.com/en-us/library/exchange/jj900169.aspx.
- SSL certificates enabled on Exchange 2019 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 2019 Calendar Repair Assistant (CRA) should be disabled during the migration period.
- To migrate Recoverable Items subfolders the In-Place Hold and Litigation Hold features should be disabled on the target during the migration. Refer to User Guide for instructions on how to prepare your environment and enable this feature.

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:
  a. The Directory Synchronization Agent (DSA) to access the target Active Directory domain
  b. The Migration Agent for Exchange (MAgE) to perform mailbox switch

  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:

- The Directory Synchronization Agent (DSA) to access the target Active Directory domain
- The Migration Agent for Exchange (MAgE) to perform mailbox switch

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, 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)
- Permissions to log on to every mailbox involved in the migration by granting **Full Control** permission on a mailbox database
- 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.
- The **Mail Enabled Public Folders** management role
- Permissions to process public folders involved in the migration by granting **Full Control** permission on mailbox databases where those public folders reside.
- Permission to log on to public folder administrator mailbox by granting **Full Control** on it.

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

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

The default Exchange Account (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 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 Full Control on Mailbox Database

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

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

Granting 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 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 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 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
```

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 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**.

Setting Up Target Agent Host Account

This section describes how to set the required permissions for the Target 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 target agent host and to access the license server. The required privileges for the Target 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.
- The **db_owner** role on the SQL server where the database resides
- 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.

NOTE: Active Directory and Exchange accounts for mailbox or calendar synchronization and for public folder synchronization are set separately, and therefore may be different.

To set up the Target 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 Target Agent Host Account setup.

Changing the Default Target Agent Host Account

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

The default Target Agent 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. For that, go to the **Agent Management** node in the Migration Manager for Exchange Console, and use properties of the corresponding agent host server.

To go on using the default 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

The Target Agent Host Account should be a member of the local **Administrators** group on the agent host server and 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 Target Agents Host 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 Target Agent Host Account (in our example, **QMM_Trg_AH**).
5. 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**.

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**.

   i **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**.

Preparing the Target Exchange Environment for Exchange Migration

General steps

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

- Backing Up Exchange
- 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 Custom Throttling Policies

To prevent possible issues in an Exchange 2019 organization, you should create custom throttling policies, apply them to the Exchange Accounts and then restart the Microsoft Exchange Throttling Service. To do this, run the following cmdlets in Exchange Management Shell for each Exchange Account:

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

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

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

```
Restart-Service -Name MSExchangeThrottling
```

Configuring Transport Layer Security (TLS) Protocols

All servers involved into migration process must have at least one matching TLS protocol version enabled in order to communicate.

Microsoft Exchange 2019 by default uses TLS 1.2 only.

To ensure NativeMove requests can be handled successfully you should select one of the following options:

- Configure your source Exchange Server to use TLS 1.2

-OR-

- Configure your target Exchange Server to support TLS 1.0 or 1.1

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 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, you need to create an **Internet Send** connector and **Receive** connector on an Exchange Mailbox server that can be directly reached through the Internet.

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

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

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

Creating Send Connector

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

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

To create a Send connector using Exchange Admin Center

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

To create a Send connector using Exchange Management Shell

Run the following command:

```
new-SendConnector -Name 'QMM Send Connector' -Usage 'Custom' -AddressSpaces
'SMTP:*.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.
- *ServerNam*e is the Mailbox server name.

Modifying Default Receive Connector

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

To modify the default Receive connector using Exchange Admin Center

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

To modify the default Receive connector using Exchange Management Shell

Run the following command:

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

Where *ServerName* is the Mailbox server name.

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

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

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

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

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

Run the following command:

```
new-AcceptedDomain -Name '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.

Configuring Target DNS Server for Mail Forwarding

After you have completed setting up the target Exchange 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 server.

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

- *@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 Zon**e
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 serve**r 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