Quest

Quest® Migration Manager for Exchange 8.15

Source 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

Legend

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

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

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

Contents

Changing Default Exchange Account ... 3
Granting Read Access to Active Directory Domain ... 4
Granting Read Permission for Microsoft Exchange Container ... 4
Granting ApplicationImpersonation Management Role ... 4
Granting Move Mailboxes Management Role ... 4
Granting Mail Recipients Management Role ... 5
Granting Membership in Local Administrators Group ... 5
Granting Mail Enabled Public Folders Management Role ... 5
Granting Full Control on Mailbox Database ... 5
Granting Full Control on Public Folder Administrator Mailbox ... 5
Changing Default Active Directory Account ... 6
Granting Read Access to Active Directory Domain ... 6
Granting Read Permission for the Microsoft Exchange Container ... 6
Granting Write proxyAddresses Permission on Descendant PublicFolder Objects ... 7
Changing the Default Source Agent Host Account ... 7
Granting SCP Create, Read and Write Permissions ... 7
Granting db_owner Role on SQL Server ... 8
Backing Up Exchange ... 8
Creating Custom Throttling Policies ... 9
Setting Exchange Autodiscover URL (Optional) ... 9
Testing the SMTP Connectors (Optional) ... 10

About us ... **11**
Technical support resources ... 11

Changing Default Exchange Account

Mailbox and calendar synchronization

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

Public folder synchronization

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

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

Granting Read Access to Active Directory Domain

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

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

Granting Read Permission for Microsoft Exchange Container

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

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

Granting ApplicationImpersonation Management Role

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

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

Granting Move Mailboxes Management Role

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

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

Granting Mail Recipients Management Role

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

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

Granting Membership in Local Administrators Group

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

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

Granting Mail Enabled Public Folders Management Role

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

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

Granting Full Control on Mailbox Database

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

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

Granting Full Control on Public Folder Administrator Mailbox

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

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

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**.

Changing the Default Source Agent Host Account

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

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

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

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

Granting SCP Create, Read and Write Permissions

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

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

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

2. In the ADSIEdit snap-in, open the **CN=Exchange Migration Project,CN=QmmEx,CN=Migration Manager,CN=Quest Software,CN=System,DC=eternity,DC=<...>,DC=<...>** container
3. Right-click the SCP object and click **Properties**.
4. In the **Properties** dialog box, click the **Security** tab.
5. On the Security tab, click **Advanced**.
6. In the **Advanced Security Settings** dialog box, click **Add**.
7. In the **Select User**, **Computer**, or **Group** (or similar) dialog box, select the administrative account and click **OK**.
8. In the **Permission Entry** for dialog box, select **This object and all descendant (child) objects** from the **Apply onto** drop-down list.
9. Allow **Create**, **Read**and **Write** permissions for the Agent Host Account.
10. Close the dialog boxes by clicking **OK**.

Granting db_owner Role on SQL Server

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

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

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
```

Setting Exchange Autodiscover URL (Optional)

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

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

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

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

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

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

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