Quest® Migration Manager for Exchange 8.15

Granular Account Permissions for Exchange 2010 to 2010 Migration

Migration Manager for Exchange Granular Account Permissions for Exchange 2010 to 2010 Migration
Updated - January 2020
Version - 8.15

Contents

Overview

This document describes minimal set of permissions required for mailbox, calendar and public folder synchronization from a source Exchange 2010 organization to a target Exchange 2010 organization using Migration Manager for Exchange.

> **i** | **NOTE:** Permissions required for native mailbox move are out of scope of this document.

For general information on account permissions required for Migration Manager for Exchange operation, refer to System Requirements and Access Rights document.

> **i** | **IMPORTANT:** Permissions in this document are sufficient for a successful migration only if the following requirements are met:
>
> 1. User accounts used by Migration Manager for Exchange agents are members of the **Domain Users** group. Membership in that group is gained automatically when a user is created in a domain.
>
> 2. Default group permissions of the **Domain Users** group are not modified.
>
> 3. Permissions for Active Directory Synchronization accounts are granted according to Accounts Used by the Directory Synchronization Agent. Those accounts are used for switching mailboxes during mailbox synchronization.

Source Exchange 2010 Permissions

Exchange Account
Active Directory Account

Exchange Account

Mailbox and Calendar Synchronization

The following permissions are required for source Exchange account used by MSA and CSA during legacy mailbox or calendar synchronization:

Permission	How to Grant
Read access to the source domain (including all descendant objects)	Link
Membership in the local **Administrators** group on all source Exchange servers involved in the migration. If a server is a domain controller, the account should be added to the domain local **Administrators** group of the domain.	Link
Read permission for the Microsoft Exchange container in the **Configuration** partition of source Active Directory (including all descendant objects)	Link

Permissions to process every mailbox involved in the migration by granting
 	
  1. **Full Control** permission on a mailbox database
 	
  2. **Full Control** permission on an associated public folder database
	Link: Mailbox database
	Link: Public folder database

> **i** | **NOTE:** If you have any Exchange 2010 Service Pack 2 servers in the source Exchange organization, the Address Book Policy (ABP) assigned to the account must include Global Address List (GAL) containing all recipients of the source Exchange organization.

> **i** | **TIP:** The **Read** permission for the Microsoft Exchange container is required only if this account is used as Active Directory account as well and you plan to add the source Exchange organization using the **Add Source Organization Wizard** under this account.

Public Folder Synchronization

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

Permission	How to Grant
Membership in the local **Administrators** group on all source Exchange servers involved in the migration. If a server is a domain controller, the account should be added to the domain local Administrators group of the domain.	Link
Membership in the **Public Folder Management** group	Link

Migration Manager for Exchange 8.15 Granular Account Permissions for Exchange
2010 to 2010 Migration
Source Exchange 2010 Permissions

5

Permission	How to Grant
Permissions to process public folders involved in the migration by granting **Full Control** permission on public folder databases where those public folders reside.	Link

Active Directory Account

Mailbox and Calendar Synchronization

The following permissions are required for source Active Directory account used by MSA and CSA during legacy mailbox or calendar synchronization:

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

> **i** **IMPORTANT:** If migration is performed in the child domain, ensure that Active Directory account has the **Read** access to the parent (root) domain as well.

Public Folder Synchronization

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

Permission	How to Grant
The **Write proxyAddresses** permission on the **Descendant publicFolder objects** for the **Microsoft Exchange System Objects** organizational unit in all domains in which source Exchange servers involved in public folder synchronization reside. **NOTE:** Alternatively, you can grant the **Write** permission on that organizational unit.	Link

Migration Manager for Exchange 8.15 Granular Account Permissions for Exchange
2010 to 2010 Migration
Source Exchange 2010 Permissions

6

Target Exchange 2010 Permissions

Exchange Account
Active Directory Account

Exchange Account

Mailbox and Calendar Synchronization

The following permissions are required for target Exchange account used by MSA, MTA and CSA during legacy mailbox or calendar synchronization:

Permission	How to Grant
Read access to the target domain (including all descendant objects)	Link
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.	Link
Read permission for the **Microsoft Exchange** container in the **Configuration** partition of target Active Directory (including all descendant objects)	Link
Permissions to process every mailbox involved in the migration by granting 1. **Full Control** permission on a mailbox database 2. **Full Control** permission on an associated public folder database	Link: Mailbox database Link: Public folder database
The **Move Mailboxes** management role	Link

> **i** **NOTE:** If you have any Exchange 2010 Service Pack 2 servers in the target Exchange organization, the Address Book Policy (ABP) assigned to the account must include Global Address List (GAL) containing all recipients of the target Exchange organization.

> **i** **TIP:** The **Read** permission for the Microsoft Exchange container is required only if this account is used as Active Directory account as well and 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:

Permission	How to Grant
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.	Link

Migration Manager for Exchange 8.15 Granular Account Permissions for Exchange 2010 to 2010 Migration
Target Exchange 2010 Permissions

7

Permission	How to Grant
Membership in the **Public Folder Management** group	Link
Permissions to process public folders involved in the migration by granting **Full Control** permission on public folder databases where those public folders reside.	Link

Active Directory Account

Mailbox and Calendar Synchronization

The following permissions are required for target Active Directory account used by MSA, MTA and CSA during legacy mailbox or calendar synchronization:

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

> **i** **IMPORTANT:** If migration is performed in the child domain, ensure that Active Directory account has the **Read** access to the parent (root) domain as well.

Public Folder Synchronization

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

Permission	How to Grant
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.	Link

Migration Manager for Exchange 8.15 Granular Account Permissions for Exchange
2010 to 2010 Migration
Target Exchange 2010 Permissions

8

How to Grant Required Permissions

This section contains reference information how to grant an account the following permissions:

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**.

Read Permission for the 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.

Migration Manager for Exchange 8.15 Granular Account Permissions for Exchange
2010 to 2010 Migration
How to Grant Required Permissions

9

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**.

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
```

Full Control on Public Folder Database

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

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

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
```

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**.

Migration Manager for Exchange 8.15 Granular Account Permissions for Exchange
2010 to 2010 Migration
How to Grant Required Permissions

10

4. Click **Add** and select the account.

5. Close the dialog boxes by clicking **OK**.

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**.

Membership in Public Folder Management Group

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

1. In the **Active Directory Users and Computers** snap-in select the **Microsoft Exchange Security Groups** node.

2. In the right pane, right-click **Public Folder Management** group and click **Properties**.

3. On the **Members** tab click **Add** and select the account.

4. Close the dialog boxes by clicking **OK**.

Migration Manager for Exchange 8.15 Granular Account Permissions for Exchange
2010 to 2010 Migration
How to Grant Required Permissions

11

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