

Quest® Migration Manager for Exchange 8.14

**Granular Account Permissions for  
Exchange 2010 to 2013 Migration**



**© 2017 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.

# Contents

<b>Overview</b> .....	<b>4</b>
<b>Source Exchange 2010 Permissions</b> .....	<b>5</b>
Exchange Account .....	5
Active Directory Account .....	6
<b>Target Exchange 2013 Permissions</b> .....	<b>7</b>
Exchange Account .....	7
Active Directory Account .....	8
<b>How to Grant Required Permissions</b> .....	<b>9</b>
Read Access to Active Directory Domain .....	9
Read Permission for the Microsoft Exchange Container .....	9
Full Control on Mailbox Database .....	10
Full Control on Public Folder Database .....	10
Move Mailboxes Management Role .....	10
Mail Recipients Management Role .....	10
Mail Enabled Public Folders Management Role .....	11
ApplicationImpersonation Management Role .....	11
Membership in Local Administrators Group .....	11
Write proxyAddresses Permission on Descendant PublicFolder Objects .....	11
Membership in Public Folder Management Group .....	12
<b>About us</b> .....	<b>13</b>
Contacting Quest .....	13
Technical support resources .....	13

# 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 2013 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.

# 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 Migration Agent for Exchange during mailbox or calendar synchronization:

Permission	How to Grant
<b>Read</b> access to the source domain (including all descendant objects)	<a href="#">Link</a>
<b>Read</b> permission for the Microsoft Exchange container in the <b>Configuration</b> partition of source Active Directory (including all descendant objects)	<a href="#">Link</a>
Permissions to process every mailbox involved in the migration by granting <ol style="list-style-type: none"><li>1. <b>Full Control</b> permission on a mailbox database</li><li>2. <b>Full Control</b> permission on an associated public folder database</li></ol>	<a href="#">Link: Mailbox database</a> <a href="#">Link: Public folder database</a>
The <b>ApplicationImpersonation</b> management role	<a href="#">Link</a>

**i** **TIP:** The **Read** permission for the Microsoft Exchange container is required only if you plan to add the source Exchange organization in 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 <b>Administrators</b> 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.	<a href="#">Link</a>
Membership in the <b>Public Folder Management</b> group	<a href="#">Link</a>
Permissions to process public folders involved in the migration by granting <b>Full Control</b> permission on public folder databases where those public folders reside.	<a href="#">Link</a>

# Active Directory Account

## Mailbox and Calendar Synchronization

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

Permission	How to Grant
<b>Read</b> access to the source domain (including all descendant objects)	<a href="#">Link</a>
<b>Read</b> permission for the <b>Microsoft Exchange</b> container in the <b>Configuration</b> partition of source Active Directory (including all descendant objects)	<a href="#">Link</a>

**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 <b>Write proxyAddresses</b> permission on the <b>Descendant publicFolder objects</b> for the <b>Microsoft Exchange System Objects</b> organizational unit in all domains in which source Exchange servers involved in public folder synchronization reside.	<a href="#">Link</a>

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

# Target Exchange 2013 Permissions

[Exchange Account](#)  
[Active Directory Account](#)

## Exchange Account

### Mailbox and Calendar Synchronization

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

Permission	How to Grant
<b>Read</b> access to the target domain (including all descendant objects)	<a href="#">Link</a>
<b>Read</b> permission for the <b>Microsoft Exchange</b> container in the <b>Configuration</b> partition of target Active Directory (including all descendant objects)	<a href="#">Link</a>
Permissions to log on to every mailbox involved in the migration by granting <b>Full Control</b> permission on a mailbox database	<a href="#">Link</a>
The <b>Move Mailboxes</b> management role	<a href="#">Link</a>
The <b>Mail Recipients</b> management role	<a href="#">Link</a>
The <b>ApplicationImpersonation</b> management role	<a href="#">Link</a>

**i** **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:

Permission	How to Grant
Membership in the local <b>Administrators</b> 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 <b>Administrators</b> group of the domain.	<a href="#">Link</a>
The <b>Mail Enabled Public Folders</b> management role	<a href="#">Link</a>
Permissions to process public folders involved in the migration by granting <b>Full Control</b> permission on mailbox databases where those public folders reside.	<a href="#">Link</a>

# Active Directory Account

## 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:

Permission	How to Grant
<b>Read</b> access to the target domain (including all descendant objects)	<a href="#">Link</a>
<b>Read</b> permission for the <b>Microsoft Exchange</b> container in the <b>Configuration</b> partition of target Active Directory (including all descendant objects)	<a href="#">Link</a>

## 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 <b>Write proxyAddresses</b> permission on the <b>Descendant publicFolder objects</b> for the <b>Microsoft Exchange System Objects</b> organizational unit in all domains in which target Exchange servers involved in public folder synchronization reside. <b>NOTE:</b> Alternatively, you can grant the <b>Write</b> permission on that organizational unit.	<a href="#">Link</a>



# How to Grant Required Permissions

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

- Read Access to Active Directory Domain
- Read Permission for the Microsoft Exchange Container
- Full Control on Mailbox Database
- Full Control on Public Folder Database
- Move Mailboxes Management Role
- Mail Recipients Management Role
- Mail Enabled Public Folders Management Role
- ApplicationImpersonation Management Role
- Membership in Local Administrators Group
- Write proxyAddresses Permission on Descendant PublicFolder Objects
- Membership in Public Folder Management Group

## 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.
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
```

## 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
```

# 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
```

# 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
```

# 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**.

# 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**.

## We are more than just a name

We are on a quest to make your information technology work harder for you. That is why we build community-driven software solutions that help you spend less time on IT administration and more time on business innovation. We help you modernize your data center, get you to the cloud quicker and provide the expertise, security and accessibility you need to grow your data-driven business. Combined with Quest's invitation to the global community to be a part of its innovation, and our firm commitment to ensuring customer satisfaction, we continue to deliver solutions that have a real impact on our customers today and leave a legacy we are proud of. We are challenging the status quo by transforming into a new software company. And as your partner, we work tirelessly to make sure your information technology is designed for you and by you. This is our mission, and we are in this together. Welcome to a new Quest. You are invited to Join the Innovation™.

## Our brand, our vision. Together.

Our logo reflects our story: innovation, community and support. An important part of this story begins with the letter Q. It is a perfect circle, representing our commitment to technological precision and strength. The space in the Q itself symbolizes our need to add the missing piece — you — to the community, to the new Quest.

## Contacting Quest

For sales or other inquiries, visit <https://www.quest.com/company/contact-us.aspx> or call +1-949-754-8000.

## 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