Quest

Quest® Migration Manager for Active Directory
8.14

Granular Account Permissions

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

Quest Software Inc.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

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

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at https://www.quest.com/legal.

Trademarks

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

Legend

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

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

Migration Manager for Active Directory Granular Account Permissions
Updated - September 2018
Version - 8.14

Contents

Overview

To synchronize or migrate objects with their attributes from source to target Active Directory domain, Directory Synchronization Agent works with source and target domains using accounts specified during domain pair creation. Those accounts must have a specific set of rights in order to access the domain objects and perform directory migration or synchronization. A generalized set of permissions suitable for most migration scenarios is described in Accounts Used by the Directory Synchronization Agent. It is the most easy and efficient way to grant all necessary permissions for source and target accounts. However, if the requirements are too excessive and for security reasons you cannot grant such high privileges to the accounts, this document provides the minimum required set of rights that the source and target accounts must have.

This document also describes minimum required permissions for accounts used by Active Directory Processing Wizard (ADPW) and Exchange Processing Wizard (EPW).

Account Migration and Directory Synchronization

During account migration or directory synchronization DSA connects to the source and target Active Directory domains and to the source and target Microsoft Exchange information stores (if necessary). For that it uses source and target Active Directory accounts. These accounts are specified on the **Select Source Domain** and the **Select Target Domain** tab in the **Domain Pair Properties** dialog. The following sections provide minimum required permissions for the source and target Active Directory accounts.

In case you plan to perform the following operations that cannot be performed using granular account permissions described in this document:

- Migration of passwords
- Migration of SID History
- Undo of changes made by migration sessions

  you must do one of the following:

  - grant source and target Active Directory synchronization accounts permissions according to Accounts Used by the Directory Synchronization Agent
  - use preinstalled service as described in Using Preinstalled Service Feature to limit the source and target Active Directory synchronization account rights in accordance with least privilege principle.

Source Active Directory Synchronization Account Permissions

Source Active Directory synchronization account must have the following permissions in the source domain:

1. The **Replicate Directory Changes** permission on a domain naming context in case you perform directory synchronization from a Windows 2000 domain.
2. If you plan to merge or replace security descriptors, the **Manage auditing and security log** privilege must be granted for the source account in the source Domain Controllers Policy. This privilege is not required if security descriptors configured to be skipped.

TIP: Alternatively, if you perform migration (but not the synchronization), you can set the **SDFlagsSearch** registry parameter instead of granting the **Manage auditing and security log** privilege. For more information on the **SDFlagsSearch**, see the following KB articles: KB Article 59357, KB Article 78252 and KB Article 26334.
Caution: Setting this registry parameter will cause SACL to be wiped out for target objects after migration.

3. If you plan to create mail- or mailbox-enabled objects on target, source account must have the **Write proxyAddresses** permission on source objects. For details on types of target objects, see *Specify Exchange Options* in Configuring the Synchronization Job.
4. If you plan to migrate passwords or SID History the source account should be member of **Administrators** group or preinstalled service feature should be used as described in Using Preinstalled Service Feature in accordance with least privilege principle.
5. For performing mailbox switch using Migration Manager for Exchange, source account must have the **Write proxyAddresses** and **Write targetAddress** permissions on source objects.
6. If you plan to disable source user mailboxes or reconnect them to disabled target accounts, grant source account the following permissions:
    - Permissions to **Write** the **msExchMasterAccountSid**, **msExchUserAccountControl**, **msExchRecipientDisplayType** and **msExchRecipientTypeDetails** attributes
    - The **Manage auditing and security log** and **Restore files and directories** privileges in the source Domain Controllers Policy
    - The **Modify permissions** and **Modify owner** permissions on the source objects
    - The **Read All Properties** and **List content** permissions on the Exchange organization using the following script in Exchange Management Shell:
      `Get-OrganizationConfig | Add-ADPermission -User <SourceAccount> -AccessRights "ListChildren, ReadProperty"`
    - The **Modify permissions** and **Administer Information Store** permissions on the Exchange mailbox store where mailboxes reside using the following script in Exchange Management Shell:
      `Get-MailboxDatabase | Add-ADPermission -User <SourceAccount> -ExtendedRights ms-Exch-Store-Admin -AccessRights WriteDacl`

NOTE: The **Administer Information Store** permission is required only for Microsoft Exchange 2010 or lower.

For more details on disabling source accounts, see *Specify Object Processing Options* of Creating a Migration Session.

Target Active Directory Synchronization Account Permissions

Target Active Directory synchronization account must have the following permissions in the target domain:

1. The **Create all child objects** (if during migration or synchronization any objects are planned to be created) and **Write all properties** permissions on the target domain (or specifically on the OUs where objects reside or will be created) for all objects included in the migration or synchronization process.

   If you want more granular permission assignment, grant the **Write** permissions to all non-skipped attributes as well as the following permissions:

IMPORTANT: The following attributes must not be skipped for directory synchronization: **name**, **cn**, **ou**, **displayName**, **objectCategory**, **objectSID**, **msExchMasterAccountSid**, **nTSecurityDescriptor**, and **msExchMailboxSecurityDescriptor**.

   1.1. Grant target account the **Create** permission for types of objects (for instance, users) you plan to create on target (if any).

1.2. The permission to **Write** service attributes specified on the **Object Matching** tab of the domain pair properties. By default, service attributes are **adminDescription**, **adminDisplayName**, **extensionAttribute14** and **extensionAttribute15**. For more details, see *Service Attributes* in Configuring a Domain Pair.

1.3. The **Write userAccountControl** permission for user, inetOrgPerson or computer objects and the **Write groupType** permission for group objects.

1.4. If you plan to create mail- or mailbox-enabled objects on target then target account must have permissions to **Write** attributes from the table below in the target domain when synchronizing objects of the user, inetOrgPerson, contact or group classes, regardless of whether those attributes are included or skipped.

OBJECT TYPE → ATTRIBUTE NAME ↓	user (inetOrgPerson)	contact	group
homeMDB	X*		
homeMTA	X*		
legacyExchangeDN	X	X	X
mail	X	X	X
mailNickname	X	X	X
msExchGroupDepartRestriction			X
msExchGroupJoinRestriction			X
msExchHomeServerName	X*		
msExchMailboxGuid	X**		
msExchMDBRulesQuota	X		
msExchModerationFlags			X
msExchPoliciesExcluded	X	X	X
msExchPoliciesIncluded	X	X	X
msExchProvisioningFlags			X
msExchRBACPolicyLink	X***		
msExchRecipientDisplayType	X	X	X
msExchRecipientTypeDetails	X	X	X
msExchResourceDisplay	X*		
msExchResourceMetaData	X*		
msExchResourceSearchProperties	X*		
msExchTransportRecipientSettingsFlags			X
msExchUMEnabledFlags2	X*		
msExchUserAccountControl	X*		
msExchVersion	X	X	X
protocolSettings	X*		
proxyAddresses	X	X	X

showInAddressBook	X	X	X
targetAddress	X	X	
textEncodedOrAddress	X	X	X

The following notation is used in the table:

X — any option except for **Users without mail options** is selected in **Exchange Options**
X* — only if **Mailbox-enabled users** option is selected in **Exchange Options** and source user is mailbox-enabled
X** — only if either **Mailbox-enabled users** or **Mail-enabled users for Native Move** option is selected in **Exchange Options**, and source user is mailbox-enabled

X*** — only if source user is mail-enabled, or the **Mailbox-enabled users** option is selected in **Exchange Options** and source user is mailbox-enabled

For details on possible Exchange options, see *Specify Exchange Options* in Configuring the Synchronization Job.

NOTE: If you plan to select the **Merge objects with corresponding contacts** option available on the **Specify Exchange Options** step, grant target account permission to delete corresponding contacts and to add objects to groups those contacts are members of.

1.5. If you plan to enable target accounts that are mailbox-enabled, grant target account permissions to **Write** the **msExchMasterAccountSid**, **msExchUserAccountControl**, **msExchRecipientDisplayType** and **msExchRecipientTypeDetails** attributes. For more details on enabling target accounts, see *Specify Object Processing Options* of Creating a Migration Session.

2. If you use the **Synchronize object deletions** option, grant target account permission to delete corresponding objects.
3. If you plan to migrate passwords or SID History the target account should be member of **Administrators** group or preinstalled service feature should be used as described in Using Preinstalled Service Feature in accordance with least privilege principle.
4. For updating security descriptors, the following permissions must be granted to the target account:
   - The **Manage auditing and security log** and **Restore files and directories** privileges in the target Domain Controllers Policy
   - The **Modify permissions** and **Modify owner** permissions on the target objects
5. For updating Microsoft Exchange mailbox permissions, the target account must have the following permissions:
   - The **Read All Properties** and **List content** permissions on the Exchange organization using the following script in Exchange Management Shell:
     ```
     Get-OrganizationConfig | Add-ADPermission -User <TargetAccount> -
     AccessRights "ListChildren, ReadProperty"
     ```
   - The **Modify permissions** and **Administer Information Store** permissions on the Exchange mailbox store where mailboxes reside using the following script in Exchange Management Shell:
     ```
     Get-MailboxDatabase | Add-ADPermission -User <TargetAccount> -
     ExtendedRights ms-Exch-Store-Admin -AccessRights WriteDacl
     ```

NOTE: The **Administer Information Store** permission is required only for Microsoft Exchange 2010 or lower.

Using Preinstalled Service Feature

The preinstalled service feature allows you to use Active Directory synchronization accounts that are domain members not included in **Administrators** group to migrate passwords and/or SID History. The preinstalled service must be also configured for environments where Microsoft Local Security Authority (LSA) protection is used. The preinstalled service feature is available starting from Quest Migration Manager for Active Directory version 8.14 with the Product Update 20180619.

To use this feature the following requirements should be met:

- Directory Synchronization Agent assigned for preinstalled service should be configured using the **EnablePreinstalledMode.ps1** script as described below.

  IMPORTANT:

  - Directory Synchronization Agent assigned for preinstalled service will not try to install binaries that should be installed to source and target DC under standard workflow. In case the existing Directory Synchronization Agent is used for multiple domain pairs, and preinstalled service feature will be used for part of them, Quest recommends to install and configure separate Directory Synchronization Agent assigned for preinstalled service feature usage only.
  - In case source or target Active Directory is based on multiple DC, the preferred DC must be specified in the Directory Synchronization Agent properties for source and target domains and configured to use preinstalled service feature.

    For details how to install and configure Directory Synchronization Agent see Agent Manager topic of *Quest Migration Manager for AD User Guide*.

- Both source and target DC should be configured to provide the preinstalled service using the **AllowAccess.ps1** script as described below.
- Source Active Directory synchronization account must have the permissions in the source domain as specified in Source Active Directory Synchronization Account Permissions.
- Target Active Directory synchronization account must have the permissions in the target domain as specified in Target Active Directory Synchronization Account Permissions.

Preinstalled service can be disabled when necessary as described in Disabling Preinstalled Service.

To configure source and target DC using AllowAccess.ps1 *script*

On the computer where Migration Manager is installed:

1. Extract **Switch Agent Mode.zip** located in %Program Files%\Quest Software\Migration Manager\Common\BIN\DeployDistr folder to the same location.
2. Copy the following files from %Program Files%\Common Files\Aelita Shared\ to the %Program Files%\Quest Software\Migration Manager\Common\BIN\DeployDistr\Switch Agent Mode folder:
   - aelagentms.exe
   - aelagentms64.exe
   - PwdHlp.dll
   - PwdHlp64.dll

   The compiled preinstalled service distributive is now available by network in \\QMM_host\DSASetup\.

On source and target DC:

3. Copy Switch Agent Mode folder containing preinstalled service distributive from \\QMM_host\DSASetup\ to the convenient folder on the source DC.

TIP: This folder also contains scripts that should be used in case you decide to disable preinstalled service later.

4. On source DC run the PowerShell session as administrator. You must select the 32-bit (x86) version of the PowerShell or 64-bit (x64) version depending on DC server bit version.
5. Execute the following commands:

```
cd "<full path to the folder used for preinstalled service distributive on the step 3 above>"
.\AllowAccess.ps1 <domainName> <userName>
```

Where domainName\userName is a source account, specified as Source Active Directory synchronization account for source domain when domain pair was configured.

6. Repeat the actions 3-5 for target domain, specifying Target Active Directory synchronization account for target domain accordingly.
7. Restart the source and target DC.

To configure the Directory Synchronization Agent using the EnablePreinstalledMode.ps1 script

1. Copy Switch Agent Mode folder containing preinstalled service distributive from \\QMM_host\DSASetup\ to the convenient folder.
2. Stop all synchronization jobs of the Directory Synchronization Agent that may be in progress on Quest Migration Manager console.
3. Open 32-bit (x86) version of the PowerShell prompt on the computer where Directory Synchronization Agent is hosted and execute the following commands:

```
cd "<full path to the folder used for preinstalled service distributive on step 1 above>"
.\EnablePreinstalledMode.ps1
```

4. Restart the synchronization jobs of the Directory Synchronization Agent that have been stopped on Quest Migration Manager Console on the step 2.

Disabling Preinstalled Service

To disable preinstalled service when necessary perform the following actions:

- Disable preinstalled service on a source and target DC
- Disable preinstalled service on a computer where Directory Synchronization Agent is hosted

All these actions should be performed to disable preinstalled service successfully.

To disable preinstalled service on a source and target DC

1. On source DC run the PowerShell session as administrator. You must select the 32-bit (x86) version of the PowerShell or 64-bit (x64) version depending on DC server bit version.
2. Execute the following commands:

   ```
   cd "<full path to the folder on this DC used for preinstalled service distributive on step 1 above>"
   .\DisableAccess.ps1
   ```

3. Repeat these actions for target domain, specifying Target Active Directory synchronization account for target domain accordingly.
4. Restart the source and target DC.
5. Optionally, you can remove the following files from the **%Systemroot%\System32** on the source and target DC:

   on computers running 32-bit Microsoft Windows

   - aelagentms.exe
   - PwdHlp.dll

   on computers running 64-bit Microsoft Windows

   - aelagentms64.exe
   - PwdHlp64.dll

To disable preinstalled service on a computer where Directory Synchronization Agent is hosted

1. Stop all synchronization jobs of the Directory Synchronization Agent that may be in progress on Quest Migration Manager console.
2. Open 32-bit (x86) version of the PowerShell prompt on the computer where Directory Synchronization Agent is hosted and execute the following commands:

   ```
   cd "<full path to the folder on this machine specified for preinstalled service distributive when Directory Synchronization agent was configured>"
   .\DisablePreinstalledMode.ps1
   ```

3. Restart the synchronization jobs of the Directory Synchronization Agent that have been stopped on Quest Migration Manager Console.

Active Directory Processing

Account under which Active Directory Processing Wizard (ADPW) performs Active Directory processing must have the following permissions:

1. For processing Group membership grant account the **Write Members** permission on group objects.

2. For processing Linked attributes grant account permissions to **Write** corresponding linked attributes for processed objects.

3. For processing Active Directory permissions, the following permissions must be granted to the account:

   - The **Manage auditing and security log** and **Restore files and directories** privileges in the Domain Controllers Policy
   - The **Modify permissions** and **Modify owner** permissions on processed objects

4. For processing Default schema permissions grant account the **Write defaultSecurityDescriptor** permission on **classSchema** objects inside schema naming context.

5. For processing Exchange mailbox permissions, the account must have the following permissions:

   - The **Write msExchMailboxSecurityDescriptor** and Write **msExchMasterAccountSid** permissions on processed objects.
   - The **Read All Properties** and **List content** permissions on the Exchange organization using the following script in Exchange Management Shell:
     ```
     Get-OrganizationConfig | Add-ADPermission -User <ServiceAccount> -AccessRights "ListChildren, ReadProperty"
     ```
   - The **Administer Information Store** and **Modify** permissions on the Exchange mailbox store where mailboxes reside using the following script in Exchange Management Shell:
     ```
     Get-MailboxDatabase | Add-ADPermission -User <ServiceAccount> -ExtendedRights ms-Exch-Store-Admin -AccessRights WriteDacl
     ```

> **NOTE:** The **Administer Information Store** permission is required only for Microsoft Exchange 2010 or lower.

6. For processing the Other Exchange permissions, the following permissions must be granted to the account:

   - The **Manage auditing and security log** and **Restore files and directories** privileges in the Domain Controllers Policy
   - The **Read permissions**, **Modify permissions** and **Modify owner** permissions on objects inside the Exchange configuration container
   - The **Read All Properties** and **List content** permissions on the Exchange configuration container using the following script in Exchange Management Shell:
     ```
     Add-ADPermission -Identity (Get-OrganizationConfig).Identity.Parent -User <ServiceAccount> -AccessRights "ListChildren, ReadProperty"
     ```

- The **Write msExchAdmins** permission for **msExchOrganizationContainer** and **msExchAdminGroup** objects
- The **Write msExchChatAccess** permission for **msExchChatChannel**, **msExchChatNetwork** and **msExchChatProtocol** objects
- The **Write msExchUserLink** permission for **msExchRoleAssignment** objects

Exchange Server Processing

Account under which Exchange Processing Wizard performs Exchange servers processing must have the following permissions:

1. **Read All Properties** and **List content** permissions on the Exchange organization. To grant these permissions to the account, use the following script in Exchange Management Shell:

```
Get-OrganizationConfig | Add-ADPermission -User <ServiceAccount> -AccessRights
"ListChildren, ReadProperty"
```

2. To process client permissions of mailboxes, grant the **ApplicationImpersonation** management role.

3. To perform public folder processing:

- The account must be mailbox-enabled
- For Exchange 2010 servers:
  - Grant membership in the **Public Folder Management role** group (Mail Enabled Public Folders, Public Folders roles) for processing client and administrative permissions of public folders
- For Exchange 2013 or later servers:
  - Account must have the **ReadItems**, **EditOwnedItems**, **EditAllItems**, **FolderOwner**, **FolderContact**, and **FolderVisible** on the public folders to be processed.

    -OR-

  - Grant **FullAccess** on a mailbox where public folders are located using the following script: `Get-Mailbox "PublicFolderMailbox" -PublicFolder | Add-MailboxPermission -User "ServiceAccount" -AccessRights "FullAccess"`

About us

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 www.quest.com/contact.

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