**Pre-Requisites**

Pre-Requisites For QMM AD

Before installing Migration Manager, make sure your environment meets the system requirements listed in the System Requirements and Access Rights document. In particular, check the requirements for the following computers:

• Migration Manager console

• Migration Manager database servers

• Active Directory Application Mode server

• Migration Manager agents’ servers

• Directory Synchronization Agent server

• Statistics Collection Agent server

• Statistics Portal server

• Domain controllers (source and target)

**DB Requirement For QMM AD**

**Active Directory Lightweight Directory Service Database**

The Active Directory Lightweight Directory Service (AD LDS) or Active Directory Application Mode (ADAM) database instance is used to store the migration project information, such as the domain pair configuration, migration and synchronization job configuration, resource processing tasks, and delegation information.

**SQL Configuration Database**

The SQL configuration database is used to store Exchange migration project information, such as the source and target Exchange organizations and the agent and job configuration.

**Licensing**

**Migration Manager for Active Directory**

The Migration Manager for Active Directory license specifies the maximum number of user accounts you can migrate and the maximum number of user accounts you can synchronize.

Directory synchronization agents obtain license information from the migration project partition stored in Active Directory Lightweight Directory Service (AD LDS) or Active Directory Application Mode (ADAM). Therefore, the agents must have access to the AD LDS or ADAM server and migration project partition. For more information, refer to the System Requirements and Access Rights document.

**Preparing the Source and Target Environments for Active Directory Migration**

Preparing the Source and Target Environments for Active Directory Migration

The suggested preparation steps as follows:

* [Establishing Trusts](https://support.quest.com/technical-documents/doc711904)
* [Configuring SID Filtering](https://support.quest.com/technical-documents/doc711905)
* [Checking Host Name Resolution](https://support.quest.com/technical-documents/doc711906)
* [Opening the Required Ports](https://support.quest.com/technical-documents/doc711907)
* [Configuring Windows 2008/2008 R2/2012 Firewall](https://support.quest.com/technical-documents/doc711908)
* [Number of NSPI Connections to a Windows 2008-based Domain Controller](https://support.quest.com/technical-documents/doc711909)

**Establishing Trusts**

Trusts between the source and target domains are not required for Active Directory or Exchange migration with Migration Manager. However, we recommend that you establish **two-way trusts** between each source and target domain that will participate in migration.

If the forest functional level in both source and target forests is set to Windows 2003 or higher, you can establish forest trust between the forest root domains.

Trusts make it possible to resolve objects’ security identifiers (SIDs), which in turn helps to distinguish objects and check that everything is going right. Trusts also help provide co-existence of two environments, including uninterrupted access to the resources for both switched users and users not yet switched.

For more information about the restrictions that apply and possible migration scenarios without having trusts established, refer to the Migration Manager Best Practices document.

**Configuring SID Filtering**

SID filtering is set on all trusts to prevent malicious users who have domain or enterprise administrator level access in a trusted forest from granting (to themselves or other user accounts in their forest) elevated user rights to a trusting forest.

SID filtering should be turned off only if you want target accounts to obtain all privileges of the source accounts for the period between account migration and resource processing. Otherwise, if you do not plan to use target accounts until resource processing will be completed, turning off SID filtering is not required.

|  |  |
| --- | --- |
| https://support.quest.com/technical-documents/image/ff7b29d3-7168-4795-9c30-a23c30be1942 | **Important:** Note that only **domain administrators** or **enterprise administrators** can modify SID filtering settings. |

**Disabling SID Filter Quarantining on External Trusts**

To disable SID filter quarantining for the trusting domain, type a command using the following syntax at a command-prompt:

Netdom trust TrustingDomainName /domain: TrustedDomainName /quarantine:No /usero: domainadministratorAcct /passwordo: domainadminpwd

To re-enable SID filtering, set the /quarantine: command-line option to Yes.

**Allowing SID History to Traverse Forest Trusts**

The default SID filtering applied to forest trusts prevents user resource access requests from traversing the trusts with the credentials of the original domain. If you want to enable users to use the credentials that were migrated from their original domain, you can allow SID history to traverse forest trusts by using the Netdom command.

To allow SID history credentials to traverse a trust relationship between two forests, type a command using the following syntax at a command-prompt:

Netdom trust TrustingDomainName /domain: TrustedDomainName /enablesidhistory:Yes /usero: domainadministratorAcct /passwordo: domainadminpwd

To re-enable the default SID filtering setting across forest trusts, set the /enablesidhistory: command-line option to No.

For more information about configuring SID filtering refer to the Microsoft article available at <https://technet.microsoft.com/en-us/library/cc755321(v=ws.10).aspx>.

**Checking Host Name Resolution**

**DNS Name Resolution**

Make sure that DNS is configured and functioning properly in your environment.

The following computers' DNS names must be successfully resolved to IP addresses from the servers running the Directory Synchronization Agents and Migration Manager console:

* Source and target servers
* Server on which the AD LDS or ADAM project partition is located
* Server hosting the SQL configuration database

**NetBIOS Name Resolution**

Since the agents installed on agent hosts communicate with Exchange servers and with each other, agent hosts and Exchange servers must be able to resolve each other’s NetBIOS names to IPv4 addresses. In other words, each server must be able to “see” the other servers by NetBIOS.

Windows Internet Naming Service (WINS) is usually used to resolve servers’ NetBIOS names to IP addresses. If WINS is not configured in your environment, host files can be used instead.

Check the host NetBIOS name resolution and make sure that the servers’ NetBIOS names can be resolved from the console as well.

**Opening the Required Ports on Servers, Routers, and Firewalls**

Since the Migration Manager agents are installed and updated from the console over RPC and the agents transfer data directly between source and target servers over RPC as well, RPC traffic must be allowed over the routers separating the subnets.

Make sure that ports 135, 137, 138, and 139 are open on the following machines:

* Source and target servers
* Routers separating the subnets
* Firewalls

|  |  |
| --- | --- |
| https://support.quest.com/technical-documents/image/ff7b29d3-7168-4795-9c30-a23c30be1942 | Note: For the comprehensive list of port requirements for most of the Migration Manager components, refer to the *Migration Manager–Required Ports* document. |

**Configuring Windows Server 2008/2008 R2/2012 Firewall**

Windows Server 2008, Windows Server 2008 R2 and Windows Server 2012 have built-in firewall that is enabled by default. To migrate passwords and SIDHistory, you need to modify the firewall settings on a target domain controller and create a new inbound rule. This is also required for proper operation of the Undo Wizard.

* To create a new rule on an x86 target domain controller, run the following command (Windows Server 2008 only):

netsh advfirewall firewall add rule name="Migration Manager Agent" dir=in action=allow program="%SystemRoot%\System32\AelAgentMS.exe"

* To create a new rule on an x64 target domain controller, run the following command:

netsh advfirewall firewall add rule name="Migration Manager Agent" dir=in action=allow program="%SystemRoot%\System32\AelAgentMS64.exe"

|  |  |
| --- | --- |
| https://support.quest.com/technical-documents/image/ff7b29d3-7168-4795-9c30-a23c30be1942 | Note: Alternatively, you can create a new rule using the New Inbound Rule Wizard. To run the wizard:   1. Open the **Server Manager** console on a target domain controller. 2. Navigate to **Configuration | Windows Firewall with Advanced security | Inbound Rules** in the console tree. 3. Click **New Rule**. |
| https://support.quest.com/technical-documents/image/128bc0ee-6329-42ca-bb13-683d2b845ab8 | **Caution:** In case of two-way directory synchronization, you should perform the same actions on the source domain controller. |

**Number of NSPI Connections to a Windows 2008-based Domain Controller**

A Name Service Provider Interface (NSPI) connection from a MAPI client to a Windows Server 2008-based domain controller may fail with the following error code that is returned from the server: «MAPI\_E\_LOGON\_FAILED».

This behavior occurs because Windows Server 2008 only allows for a default maximum of 50 concurrent NSPI connections per user to any domain controller. Additional NSPI connections are rejected with a MAPI\_E\_LOGON\_FAILED error code.

Note Windows Server 2003 and earlier versions of Microsoft Windows operating systems do not exhibit this behavior. The change of behavior in Windows Server 2008 is intended to protect domain controllers against clients that open too many NSPI connections without then closing the connections. Too many connections such as these can result in resource depletion.

For more information about how to modify registry settings to allow for additional NSPI connections, see the following Microsoft KB article: <http://support.microsoft.com/kb/949469>.

To install Migration Manager, either click Migration Manager and its components on the CD menu or start the Suite\AeCDSuiteLauncher.exe setup program, and then follow the wizard’s instructions.

|  |  |
| --- | --- |
| https://support.quest.com/technical-documents/image/ff7b29d3-7168-4795-9c30-a23c30be1942 | Note: For security reasons, all network protocols may be disabled by default in SQL Server 2005 and SQL Server Express 2005 or later, which causes trouble with connecting to a project. For details on enabling the network protocols, refer to SQL Server documentation.  To avoid connectivity problems, you should enable all network protocols in SQL Server if you plan to install MAgE agents on the agent hosts that are located separately from the SQL Server host. |

***To install Migration Manager:***

1. When prompted, specify your name and company. Click **Licenses** to verify your license information in the dialog displayed: browse for a valid license file, and then click Close.
2. Next, on the **Select Features** step, select the components you want to install and specify the installation folder.
3. On the next step, you are prompted to select the product installation scenario. Possible options are **Express** or **Advanced**.

**Express** means that setup will do the following:

* Install all the components that are permitted by the license file.
* Install all other required components, such as the AD LDS or ADAM instance, SQL Server or SQL Server Express instance (for Exchange migrations only), and the Directory Synchronization Agent.
* Configure the project.
* If IIS is installed on the computer, Statistics Portal will be automatically installed and configured as well.

**Advanced** is recommended if you plan to manually install AD LDS or ADAM, SQL Server or SQL Server Express (for Exchange migrations only), and the Directory Synchronization Agent, as well as configure the project by running the Open Project Wizard (described in the Opening a Migration Project topic). Only the basic product components (selected in Select Features step) will be installed automatically.

|  |  |
| --- | --- |
| https://support.quest.com/technical-documents/image/ff7b29d3-7168-4795-9c30-a23c30be1942 | Note: When selecting the setup scenario, consider the following:  By default, SQL Server Express is installed with only Windows (AD-integrated) authentication allowed; however, Statistics Portal required basic SQL authentication. To provide for SQL authentication method, you can do either of the following:  Use the **Express** setup scenario (proper configuration will be applied automatically).  After running the Advanced setup, install SQL Server Express using the special installation wizard from Migration Manager CD Autorun, and then use the Microsoft SQL Server Management tools (Enterprise Manager), or edit the registry as described in Microsoft Knowledge Base article 319930 at <http://support.microsoft.com/kb/319930/>. |

If you select the **Advanced** setup scenario, you will be taken to step 7 of this procedure.

1. On the **Set Account for ADAM Access** step, specify the auxiliary account that various Migration Manager components will use to access the AD LDS or ADAM database.
2. This account does not require any particular rights in the domain; ordinary domain user rights are sufficient. However, this account must be a member of the computer local Administrators group on the computer running the Migration Manager console. Note that this account will be granted Full Admin rights in the project database.
3. On the **MSDE setup** step, specify the password for the **sa** account that will be used to install and configure the local SQL Server database.
4. Next, the setup checks for third-party software required for Migration Manager (for example, Microsoft Message Queuing). If some required components are missing, setup will notify you and attempt to install these components from the installation CD. To install these components automatically, click **Next**; alternatively, you can install them manually and after that restart the setup program.
5. After all the required components are installed, the setup wizard is ready to install the features you have selected (and configure the product if the Express setup scenario is running). Click **Next** and wait for the installation to complete.

**Downloading MAPI CDO**

Migration Manager also requires version 6.5.8353.0 or later of Microsoft Exchange Server MAPI Client and Collaboration Data Objects 1.2.1 to be installed on the following computers:

* Where Migration Manager agents will run (that is, Exchange 2007 and 2010 Servers and agent hosts)
* Where the Migration Manager console is installed

Since the MAPI CDO setup package is not available for distribution, you should download it from the Microsoft Web site. At the moment of the last document update, the download link is <http://www.microsoft.com/en-us/download/details.aspx?id=42040>.

|  |  |
| --- | --- |
| https://support.quest.com/technical-documents/image/128bc0ee-6329-42ca-bb13-683d2b845ab8 | **Caution:** This package cannot be installed on a system on which any version of Microsoft Outlook or Microsoft Exchange Server 2003 or earlier is installed. |