Quest® Migration Manager 8.15

System Requirements and Access Rights

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.**

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

Migration Manager System Requirements and Access Rights
Updated - October 2023
Version - 8.15

Contents

Migration Manager Console

Requirement	Details
Platform	One of the following: - AMD 64 - Intel EM64T
Memory	1 GB or more
Hard Disk Space	Minimum 300 MB
Operating System	One of the following: - Microsoft Windows Server 2019 - Microsoft Windows Server 2016
Additional Software	All of the following: - Microsoft .NET Framework 3.5 Service Pack 1 - Microsoft .NET Framework 4.5.2 or later - For processing messages in Exchange 2010 or earlier using EPW: version 6.5.8353.0 or later of Microsoft Exchange Server MAPI Client and Collaboration Data Objects 1.2.1 Limitation: neither Microsoft Outlook nor Exchange Server 2003 Management Tools must be installed Additional software in case of public folders migration to Microsoft Exchange 2013: - Shared Components of Migration Manager for Exchange Additional software for Microsoft SQL Server processing if TLS 1.0 is disabled: - Microsoft OLE DB Driver for SQL Server. The driver can be downloaded from Microsoft Download Center.

Migration to Microsoft Office 365

Migration Manager supports migrating users from Active Directory to Microsoft Office 365 and their mailboxes from the on-premises Exchange organization to Microsoft Exchange Online. However, in that migration scenario the following requirements apply to the Migration Manager components:

Migration Manager for Active Directory (Microsoft Office 365) Console

Requirement	Details
Platform	One of the following: • Intel x86 • AMD 64 • Intel EM64T
Operating System	One of the following: • Microsoft Windows Server 2019 • Microsoft Windows Server 2016
Additional Software	All of the following: • Microsoft .NET Framework 4.5 or later • Microsoft PowerShell 3.0 • Microsoft Online Services Sign-In Assistant for IT Professionals RTW*

* To get Microsoft Online Services Sign-In Assistant, go to https://support.quest.com/migration-manager-for-ad/kb/332933/download-links-for-office-365-sign-in-assistant-for-migration-manager-for-ad-and-exchange-to-o365

Migration Manager for Exchange Console

Requirement	Details
Platform	One of the following: • Intel x86 • AMD 64

Requirement	Details
	- Intel EM64T
Operating System	One of the following: - Microsoft Windows Server 2019 - Microsoft Windows Server 2016
Additional Software	All of the following: - Microsoft PowerShell 3.0 - Microsoft .NET Framework 3.5 Service Pack 1 - Microsoft .NET Framework 4.5.2 or later - Microsoft Online Services Sign-In Assistant for IT Professionals RTW* For specific cases only: - Version 6.5.8353.0 or later of Microsoft Exchange Server MAPI Client and Collaboration Data Objects 1.2.1. MAPI CDO now is only required for scenarios where MAPI is used: **migration scenarios where legacy Exchange agents are used**, and **migration by MAgE from Exchange 2007 or earlier**. MAPI CDO is optional for Native Move migration by MAgE scenarios. Source mailbox statistics will be only available with MAPI CDO. For all other supported scenarios, MAPI CDO is no longer needed. **Limitation:** neither Microsoft Outlook nor Exchange Server 2003 Management Tools must be installed. - **For environments where the TLS version 1.2 is the only enabled for Migration Manager for Exchange Database Server**: - Microsoft ODBC Driver for SQL Server, version 17, on all computers running Migration Manager console. Required version of ODBC Driver for SQL Server can be downloaded from Microsoft Download Center.

* To get Microsoft Online Services Sign-In Assistant, go to https://support.quest.com/migration-manager-for-ad/kb/332933/download-links-for-office-365-sign-in-assistant-for-migration-manager-for-ad-and-exchange-to-o365.

License Server

The computer where Migration Console is installed also usually hosts the Migration Manager license server. The license server depends on the Remote Registry service. Please make sure that the Remote Registry service startup type is set to **Automatic** on the license server computer.

Migration Manager Database Servers

Active Directory Lightweight Directory Services Server

This server is required to store the migration project information.

Requirement	Details
Platform	One of the following: • Intel x86 • AMD 64 • Intel EM64T
Operating System	For AD LDS: • Microsoft Windows Server 2019 • Microsoft Windows Server 2016
Additional Software	Active Directory Application Mode (ADAM) or Active Directory Lightweight Directory Services (AD LDS) instance running on the server.

ℹ **NOTE:** You can install AD LDS from the **Redist\AD LDS** folder on the Migration Manager CD.

Migration Manager for Exchange Database Server

Supported SQL Servers

Migration Manager can work with the following Microsoft SQL server versions:

- Microsoft SQL Server 2008
- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2012
- Microsoft SQL Server 2014
- Microsoft SQL Server 2016
- Microsoft SQL Server 2017
- Microsoft SQL Server 2019

> **IMPORTANT:** For environments where the TLS version 1.2 is the only enabled for Migration Manager for Exchange Database Server, the following additional software is required:
>
> Microsoft ODBC Driver for SQL Server, version 17, on all computers running Migration Manager console and on Statistics Collection Agent host. Required version of ODBC Driver for SQL Server can be downloaded from Microsoft Download Center.

Processor Requirements

A processor for the database server must be an **Intel® Xeon® E5-2650 v2** or a similar-performance processor. Number of cores for the processor can be estimated using the following formula:

```
[Number of cores] = 2 + (([Mail agents count] + [Calendar agents count]) x 0.03)
```

> **IMPORTANT:**
>
> - The minimum number of cores is 4.
> - This formula estimates number cores for physical processors. Required number of cores for virtual processors may need to be higher.

The following table contains recommended number of cores for migrations with different parameters.

	Mail agents	Calendar agents	Number of cores
Small migration	10	10	**4**
Medium migration	100	100	**8**
Large migration	250	250	**17**
Extra large migration	500	500	**32**

> **IMPORTANT:** Ensure that SQL Server Edition on the database server supports required number of cores.

Memory Requirements

To estimate the amount of RAM required for the database server, use the following formula:

```
[Amount of RAM] = ([Total number of mailboxes] x [Average number of messages in a
mailbox] * 1.28) / 10000000
```

> **IMPORTANT:** The minimum amount of RAM is 8 GB.

The following table contains required amount of RAM for migrations with different parameters.

	Number of mailboxes	Average number of messages	RAM Required
Small migration	1,000	20,000	**8 GB**
Medium migration	30,000	16,000	**64 GB**
Large migration	100,000	5,000	**64 GB**
Extra large migration	500,000	2,000	**128 GB**

> **IMPORTANT:** Ensure that operating system on the database server supports required amount of RAM.

Disk Space Requirements

Disk space required to store SQL database produced by Migration Manager for Exchange depends on a type of migration you plan to perform.

Migration to Microsoft Office 365 or Microsoft Exchange 2013/2016/2019

If you migrate to Microsoft Office 365 or Microsoft Exchange 2013/2016/2019 by means of Migration Agent for Exchange (MAgE), then to estimate the disk space that SQL database will take during the course of migration, use the following formula:

```
[SQL database size] = [Total number of mailboxes] x [Average number of messages in a
mailbox] x 1024 bytes [Size of information for single message] x 1.05 [Additional 5%
of size to store error messages]
```

For a sample migration that involves

- 100 mailboxes
- Around 30,000 messages per each mailbox

The resulting database size is calculated as follows:

```
[SQL database size] = 100 mailboxes x 30,000 messages x 1024 x 1.05 = 3,225,600,000
bytes ≈ 3GB
```

> **TIP:** To calculate total number of mailboxes and number of messages within them, use Quest MessageStats, or refer to the corresponding Microsoft documentation.

> **IMPORTANT:** If you plan to use express edition of Microsoft SQL Server, consider that database size may eventually exceed the allowed size limit. That limit is 4GB for SQL Server versions prior to 2008 R2 and 10GB for version 2008 R2 or later. For detailed information on differences between SQL Server editions, refer to the corresponding Microsoft documentation.

Other types of migration

If you are plan to perform any other type of migration supported by Migration Manager for Exchange, such as migration with legacy agents or native mailbox move, the database size does not exceed 4GB. Therefore any database servers stated above can be used as Migration Manager for Exchange Database Server including express editions.

Migration Manager Agent Servers

Directory Synchronization Agent Server

Requirement	Details
Platform	One of the following: • Intel x86 • AMD 64 • Intel EM64T
Operating System	One of the following: • Microsoft Windows Server 2019 • Microsoft Windows Server 2016

Directory Synchronization Agent depends on the Remote Registry service. Please make sure that the Remote Registry service startup type is set to **Automatic** on the Directory Synchronization Agent server.

Directory Migration Agent Server

Requirement	Details
Platform	One of the following: • Intel x86 • AMD 64 • Intel EM64T
Operating System	One of the following: • Microsoft Windows Server 2019 • Microsoft Windows Server 2016

Requirement	Details
Additional Software	All of the following: • Microsoft .NET Framework 4.5 or later • Microsoft PowerShell 3.0

Exchange Migration Agents Server

Migration Manager uses the following Exchange-specific agents:

- Public Folder Source Agent
- Public Folder Target Agent
- Mail Source Agent
- Mail Target Agent
- Calendar Synchronization Agent
- Free/Busy Synchronization Agent
- Transmission Agent
- Migration Agent for Exchange

Agents work on agent host servers.
Requirements and limitations for agent host servers:

- Multiple Exchange servers can be associated with a single agent host server.
- Agent host cannot be
    1. Microsoft Cluster Server (MSCS)
    2. Microsoft Cluster Server node
    3. Exchange Virtual Server
    4. Exchange 2003/2007 SCC cluster
    5. Exchange 2007 CCR cluster
- Agent host can be:
    1. An Exchange server itself, which is the default configuration. After you enumerate an Exchange organization all Exchange servers are registered as agent hosts for themselves (excluding Migration Agent for Exchange installations).
    2. Another Exchange server from the same Exchange organization.
    3. A stand-alone server. Agents hosts associated with Exchange Server version 2003, 2007, 2013, 2016 or 2019 can be located in another forest or workgroup. Agents hosts associated with Exchange Server 2010 must be located in the forest where the Exchange Server 2010 resides.

Legacy Migration Agents

For agent hosts associated with Exchange Server 2016, 2019, or Office 365 (public folder synchronization only)

The following requirements apply to agent hosts associated with Exchange Server 2016 or Office 365 which you plan to use for public folder synchronization. Requirements for agent host used for other types of synchronization are described in Migration Agent for Exchange (MAgE).

Requirement	Details
Platform	One of the following: • AMD 64 • Intel EM64T
Operating System	One of the following: • Microsoft Windows Server 2019 • Microsoft Windows Server 2016
Additional Software	All of the following: • Microsoft .NET Framework 3.5 Service Pack 1 • Microsoft Exchange Collaboration Data Objects must **not** be installed on the agent host • Microsoft Outlook 2013 32-bit or Microsoft Outlook 2016 32-bit version must be installed on the agent host. **NOTE:** The *MMEX_PFSA* and *MMEX_PFTA* profiles must be created as described in the *Creating Outlook Profiles for Public Folder Synchronization* of the following documents: ◦ Exchange 2016: *Target Exchange 2016 Preparation* document ◦ Office 365: *Migrating to Microsoft Office 365* document

IMPORTANT: The **Communicate with Exchange Server via Outlook MAPI** option must be selected on the **General | Connection** node in the properties of each agent host associated with Exchange Server 2016, 2019, or Office 365 on which PFSA or PFTA will be installed.

Migration Agent for Exchange (MAgE)

Requirements from the following tables apply to standalone servers acting as agent hosts for Migration Agent for Exchange (MAgE). Note that Migration Agent for Exchange cannot be installed on Exchange servers.

Hardware Requirements

Requirement	Details
Platform	One of the following: • AMD 64 • Intel EM64T
Processor	2 GHz or higher (before Turbo Boost if applicable) Minimum: 1 CPU core per 2 MAgE instances Recommended: 1 CPU core per each MAgE instance
Memory (RAM)	Minimum: 0.8 GB per MAgE instances Recommended: 1.6 GB per MAgE instance
LAN Bandwidth	Minimum: 100 Mbps Recommended: 1 Gbps

TIP: Agent host server with maximum number of 20 MAgE instances running concurrently (10 for mailbox and 10 for calendar processing) must have:

- 10 CPU cores and 16 GB of RAM (minimum)
- 20 CPU cores and 32 GB of RAM (recommended)

Software Requirements

Requirement	Details
Operating System	One of the following: • Microsoft Windows Server 2019 • Microsoft Windows Server 2016
Additional Software	All of the following: • Microsoft .NET Framework 3.5 Service Pack 1 • Microsoft .NET Framework 4.5.2 or later For specific cases only: • Version 6.5.8353.0 or later of Microsoft Exchange Server MAPI Client and Collaboration Data Objects 1.2.1. MAPI CDO now is only required for scenarios where MAPI is used: **migration scenarios where legacy Exchange agents are used**, and **migration by MAgE from Exchange 2007 or earlier**. MAPI CDO is optional for Native Move migration by MAgE scenarios. Source mailbox statistics will be only available with MAPI CDO. For all other supported scenarios, MAPI CDO is no longer needed. **Limitation:** neither Microsoft Outlook nor Exchange Server 2003 Management Tools must be installed. **IMPORTANT:** Migration Manager for Exchange supports work with SQL Servers

Requirement	Details
	where the version 1.2 is the only enabled version of TLS, but the following additional software is required for this case: • Microsoft ODBC Driver for SQL Server, version 17, on all computers running Migration Manager console and on Statistics Collection Agent host. Required version of ODBC Driver for SQL Server can be downloaded from Microsoft Download Center. Additional software in case of migration to Microsoft Office 365: • Microsoft PowerShell 3.0 • Microsoft Online Services Sign-In Assistant for IT Professionals RTW*

* To get Microsoft Online Services Sign-In Assistant, go to https://support.quest.com/migration-manager-for-ad/kb/332933/download-links-for-office-365-sign-in-assistant-for-migration-manager-for-ad-and-exchange-to-o365.

IMPORTANT: Maximum number of MAgE instances per agent host is limited to 20: 10 for mailbox processing and 10 for calendar processing.

Statistics Portal Server

Requirement	Details
Platform	One of the following: • Intel x86 • AMD 64 • Intel EM64T
Operating System	One of the following: • Microsoft Windows Server 2019 • Microsoft Windows Server 2016
Additional Software	All of the following: • Microsoft .NET Framework 2.0 • Microsoft Internet Information Services • Microsoft Data Access Components (MDAC) 2.6 or later
Browser on Client Computer	Microsoft Internet Explorer 10.0 or 11.0 **NOTES:** • Scripts and frames must be enabled for Internet Explorer • Statistics Portal must be viewed in Compatibility View mode

Resource Updating Manager

Standalone Resource Updating Manager Console

Requirement	Details
Platform	One of the following: - Intel x86 - AMD 64 - Intel EM64T
Operating System	One of the following: - Microsoft Windows Server 2019 - Microsoft Windows Server 2016
Additional Software	All of the following: - Microsoft .NET Framework 2.0 Service Pack 1 - Microsoft PowerShell 2.0

Resource Updating Toolkit for PowerShell (PowerRUM)

Requirement	Details
Platform	One of the following: - Intel x86 - AMD 64 - Intel EM64T
Operating System	One of the following: - Microsoft Windows Server 2019 - Microsoft Windows Server 2016
Additional Software	All of the following: - Windows Management Framework 3.0

Requirement	Details
	- One of the following: - Migration Manager console - Standalone Resource Updating Manager console

Resource Updating Wizards

- Active Directory Processing Wizard
- Exchange Processing Wizard
- SMS Processing Wizard
- SQL Processing Wizard
- SharePoint Permissions Processing Wizard

Active Directory Processing Wizard

Requirement	Details
Platform	One of the following: • Intel x86 • AMD 64 • Intel EM64T
Operating System	One of the following: • Microsoft Windows Server 2019 • Microsoft Windows Server 2016
Additional Software	Microsoft .NET Framework 2.0

Exchange Processing Wizard

Requirement	Details
Platform	One of the following: • Intel x86 • AMD 64 • Intel EM64T
Operating System	One of the following: • Microsoft Windows Server 2019 • Microsoft Windows Server 2016
Additional Software	All of the following:

Requirement	Details
	• Microsoft .NET Framework 2.0 • **For processing messages in Exchange 2010 or earlier**: version 6.5.8353.0 or later of Microsoft Exchange Server MAPI Client and Collaboration Data Objects 1.2.1. **Limitation:** neither Microsoft Outlook nor Exchange Server 2003 Management Tools must be installed.

SMS Processing Wizard

Requirement	Details
Platform	One of the following: • Intel x86 • AMD 64 • Intel EM64T
Operating System	One of the following: • Microsoft Windows Server 2019 • Microsoft Windows Server 2016
Additional Software	Microsoft .NET Framework 2.0

SQL Processing Wizard

Requirement	Details
Platform	One of the following: • Intel x86 • AMD 64 • Intel EM64T
Operating System	One of the following: • Microsoft Windows Server 2019 • Microsoft Windows Server 2016
Additional Software	All of the following: • Microsoft .NET Framework 2.0 • Microsoft Data Access Components (MDAC) 2.7 or later

Requirement	Details
	Additional software for Microsoft SQL Server processing if TLS 1.0 is disabled: • Microsoft OLE DB Driver for SQL Server. The driver can be downloaded from Microsoft Download Center.

NOTE: SQL Processing Wizard does not require any SQL Server administrative tools to be installed on the computer on which it is run.

For a list of SQL server versions that can be processed, see SQL Servers.

Prerequisites

The following requirements must be met for a successful SQL Server update:

1. It is recommended that you run Resource Updating Manager before using SQL Processing Wizard. Otherwise, the wizard will not be able to update rights granted via membership in local groups.
2. It is recommended that you create a backup of the SQL Server before starting the SQL Processing Wizard.
3. The names of all the databases to be processed must conform to the standard Microsoft SQL naming requirements. Please see the Microsoft *SQL Server Books* online article *Rules for Regular Identifiers*, for details.
4. Processing errors will appear if the database to be processed is:
    - In Single User mode and there is already a connection to the database
    - In Read-only mode

1. To preserve the consistency of the SQL Server, the wizard will not update the server if any of the databases on the server is in the Suspend or Offline mode.
2. The login used to process the SQL Server versions 2000/2005 must be a member of the **sysadmin** role.

SharePoint Permissions Processing Wizard

Requirement	Details
Platform	One of the following: • Intel x86 • AMD 64 • Intel EM64T
Operating System	One of the following:

Requirement	Details
	- Microsoft Windows Server 2019 - Microsoft Windows Server 2016
Additional Software	- One of the supported Microsoft SharePoint Servers

Processed Platforms

- Active Directory Domain Controllers
- Source and Target Exchange Organizations
- Resource Updating Manager
- Systems Management Servers
- SQL Servers
- SharePoint Servers

Active Directory Domain Controllers

Domain controllers of the following Microsoft Windows Server versions can be used for Active Directory migration, synchronization and processing.

All AD Functional Levels supported by Microsoft for a Microsoft Windows Server operating system listed below are supported for migration from/to Domain controllers running on that same Operating System. For example, Windows Server 2016 functional levels are supported on Windows Server 2022, Windows Server 2019, and Windows Server 2016. For full details see Microsoft's documentation of Active Directory Domain Services Functional Levels in Windows Server on Microsoft Learn.

> **NOTE:** Windows Server 2003 functional levels are supported only on Windows Server 2016. That is, Microsoft does not support Windows Server 2003 functional levels on Windows Server 2019 or Windows Server 2022.

Requirement	Details
Platform	One of the following: • Intel x86 • AMD 64 • Intel EM64T
Operating System	One of the following: • Microsoft Windows Server 2022 (including Server Core) • Microsoft Windows Server 2019 (including Server Core) • Microsoft Windows Server 2016 (including Server Core)

> **IMPORTANT:** Attributes selected as DSA matching service attributes (**adminDisplayName** and **extensionAttribute15** by default) must be indexed in the Active Directory schema. Indexing is configured in the Active Directory Schema MMC snap-in, by the Index this attribute in the Active Directory option in the attribute properties.

Source and Target Exchange Organizations

On-Premises Migration

On-premises Exchange migration involves moving mailboxes (including calendars and free/busy status information) and public folders. The following table shows the supported paths for on-premises migration. For details about the specifics of mailbox, calendar and public folder synchronization, including handling of different Exchange versions, see the *Mailbox Migration Process* and *Calendar Synchronization Process* topics in the *Migration Manager for Exchange User Guide*.

Source Exchange Organization → **Target Exchange Organization** ↓	Microsoft Exchange 2003 Service Pack 2 or later	Microsoft Exchange 2007 Service Pack 2 or later	Microsoft Exchange 2010 Service Pack 2 Rollup 6 or later	Microsoft Exchange 2013 Cumulative Update 10 (CU10) or later	Microsoft Exchange 2016	**Microsoft Exchange 2019**
Microsoft Exchange 2003 Service Pack 2 or later	Yes	Yes	Yes	No	No	No
Microsoft Exchange 2007 Service Pack 2 or later	Yes	Yes	Yes	No	No	No
Microsoft Exchange 2010 Service Pack 2 Rollup 6 or later	Yes	Yes	Yes	Yes	Yes	No
Microsoft Exchange 2013 Cumulative Update 10 (CU10) or later	Yes	Yes	Yes	Yes	Yes	No
Microsoft Exchange 2016	Yes	Yes	Yes	Yes	Yes	No
Microsoft Exchange 2019	No	No	Yes	Yes	Yes	Yes

NOTE:

- Exchange clusters and Exchange database availability groups (DAGs) are supported.
- Native mailbox move from Exchange 2007 and earlier to Exchange 2016/2019 is not supported by Microsoft. See TIP: How to migrate Exchange 2007 to Exchange 2016/2019 via Native Move below for recommendations.

TIP: How to migrate Exchange 2007 to Exchange 2016/2019 via Native Move

In order to migrate Exchange 2007 to Exchange 2016/2019 via Native Move, use Exchange 2010 or Exchange 2013 as an intermediary migration step.

- Install Exchange 2010 or Exchange 2013 in your Exchange 2007 environment.
- Perform the migration from Exchange 2007.
- Migrate the resulting Exchange 2010 / 2013 to Exchange 2016/2019.

Cloud Migration

Mailbox, calendar and public folder synchronization to Microsoft Office 365 can be performed from the following Exchange versions:

- Microsoft Exchange 2019
- Microsoft Exchange 2016
- Microsoft Exchange 2013 Service Pack 1 or later
- Microsoft Exchange 2010 Service Pack 2 Rollup 6 or later
- Microsoft Exchange 2007 Service Pack 2 or later
- Microsoft Exchange 2003 Service Pack 2 or later

NOTE: Migration Manager also supports certain migration scenarios that involve hybrid deployments as migration destination. For detailed information, refer to the *Hybrid Migration Scenarios* section of *Migrating to Microsoft Office 365* document.

NOTE: Migration to Office 365 China tenants (operated by 21Vianet) and Office 365 Germany tenants (operated by T-Systems) is not supported.

Exchange Servers

Migration Manager for AD supports the following Microsoft Exchange Server versions for Active Directory migration, synchronization and processing (by Active Directory Processing Wizard and by Exchange Processing Wizard):

- Microsoft Exchange Server 2019
- Microsoft Exchange Server 2016
- Microsoft Exchange Server 2013
- Microsoft Exchange Server 2010
- Microsoft Exchange Server 2003

Resource Updating Manager

1. Resource Updating Manager can update computers running one of the following operating systems:
    - Microsoft Windows Server 2019
    - Microsoft Windows Server 2016
    - Microsoft Windows 11
    - Microsoft Windows 10 (x86 and x64 editions)

    NOTE:

    - Resource Updating Manager does not support processing of Dynamic Access Control (DAC).
2. Resource Updating Manager supports processing of IIS up to version 10.0.

Systems Management Servers

The **SMS Processing Wizard** processes the following Systems Management Servers:

- Microsoft Systems Management Server 2003
- Microsoft System Center Configuration Manager 2007

SQL Servers

The **SQL Processing Wizard** processes the following SQL servers:

- Microsoft SQL Server 2000
- Microsoft SQL Server 2005
- Microsoft SQL Server 2005 Express
- Microsoft SQL Server 2008
- Microsoft SQL Server 2008 Express
- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2008 R2 Express
- Microsoft SQL Server 2012 Service Pack 1
- Microsoft SQL Server 2014
- Microsoft SQL Server 2016
- Microsoft SQL Server 2017
- Microsoft SQL Server 2019

NOTE: SQL Processing Wizard does not process aliases on Microsoft SQL Server 2008 or later.

SharePoint Servers

The **SharePoint Permissions Processing Wizard** processes the following SharePoint servers:

- Microsoft Windows SharePoint Services 3.0 Service Pack 1 (x86 or x64 version)
- Microsoft Office SharePoint Server 2007 (x86 or x64 version)
- Microsoft SharePoint Server 2010
- Microsoft SharePoint Server 2013
- Microsoft SharePoint Server 2016
- Microsoft SharePoint Server 2019

Additional Environment Security Configuration

- Firewalls and security requirements
- LDAP Signing Configuration Requirements
- RC4 Encryption

Firewalls and Security

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 the following ports are open on workstations, servers, routers, and firewalls: 135 and 137–139.

For the comprehensive list of port requirements for most of the Migration Manager components, refer to the *Migration Manager Required Ports* document.

NOTES

- For more detailed information on what ports and protocols Microsoft operating systems and programs require for network connectivity, refer to Microsoft Knowledge Base article 832017: Service overview and network port requirements for the Windows Server system.
- You can use the **DCDiag** and **NetDiag** utilities from **Windows Support Tools** to test network connectivity. To install Windows Support Tools, run **Setup.exe** from the **\SUPPORT\TOOLS** folder of Windows distributive CD. For more information about the utilities, refer to their online help and other documentation.

In Windows XP Service Pack 2, Microsoft introduced the Security Centre, which includes a client-side firewall application. The firewall is turned on by default and configured to filter the packets sent to the ports 137–139, and 445. These ports are used by the **File and Printer Sharing** service that must be installed and running on the computer to be updated.

IMPORTANT: In order to successfully update Windows XP Service Pack 2 and Windows Vista computers from Resource Updating Manager, the **File and Printer Sharing** service must be added to the firewall **Exceptions** list and ports 137–139 and 445 must be unblocked.

For more information on resource processing requirements, refer to *Migration Manager for Active Directory Resource Processing Guide*.

When granting the required permissions to the administrative accounts in Active Directory, you should also make sure that permissions inherited from the parent are not blocked at any level in your Active Directory.

LDAP Signing Configuration Requirements

If the **Domain controller: LDAP server signing requirement**s policy is set to **Require signing** at your Active Directory domain controllers, you must make sure the client **Network security: LDAP client signing requirements** policy is set to **Negotiate signing**, which is the default, or **Require signing**. This policy must never be set to **None** for the client as this would result in loss of connection with the server.

This requirement is applicable for the following components:

- Migration Manager Console
- Migration Manager for Active Directory (Microsoft Office 365) Console
- Directory Synchronization Agent Server
- Directory Migration Agent Server
- Standalone Resource Updating Manager Console
- Active Directory Processing Wizard
- Exchange Processing Wizard
- Migration Manager for Exchange Console
- Statistics Collection Agent Server
- Exchange Migration Agents Server (Legacy and MAgE)

RC4 Encryption

The RC4 encryption (Rivest Cipher 4 or RC4-HMAC) is an element of Microsoft Kerberos authentication that Quest migration products require to sync Active Directory passwords between Source and Target environments. Disabling the use of the RC4 protocol enabled makes password syncing between environments impossible.

Beginning on November 8, 2022 Microsoft recommended an out of band (OOB) patch be employed to set AES as the default encryption type. The enabling and disabling use of the RC4 encryption protocol has potential impact beyond the function of password syncing of Quest migration tooling and should be considered carefully.

Ports Used by General Migration Manager Components

This section describes ports required by Migration Manager components related to both Active Directory and Exchange migrations, as follows:

- Ports Used by Migration Manager Console
- Ports Used by ADAM/AD LDS Instance
- Ports Used by SQL Server
- Ports Used by Statistics Portal

Ports Used by Migration Manager Console

The following table lists ports required to be opened between Migration Manager Console and the other Migration Manager components so that Migration Manager Console is be able to communicate with those components properly:

Direction of Communication	Port	Protocol(s)	Communication with
Outbound	80	TCP/UDP	Statistics Portal and Microsoft Office 365
	443	TCP/UDP	Statistics Portal (if configured) and Microsoft Office 365
	389	TCP/UDP	Source and target domain controllers
	3268	TCP	Source and target global catalogs
	User-configured (default ports:389, 636, if available)	TCP/UDP	ADAM/AD LDS instance
	135	TCP/UDP	DSA server, all Exchange servers and agent hosts
	137	TCP/UDP	
	138	UDP	
	139	TCP	
	445	TCP/UDP	
	1024-65535	TCP/UDP	
	1433	TCP	SQL server (default SQL port)

Ports Used by ADAM/AD LDS Instance

The following table lists ports required to be opened between ADAM/AD LDS instance and the other Migration Manager components so that ADAM/AD LDS instance is be able to communicate with those components properly:

Direction of Communication	Port	Protocol(s)	Communication with
Inbound	User-configured (default ports:389, 636, if available)	TCP/UDP	Mail Source Agents, Directory Synchronization Agents, Calendar Synchronization Agents and Migration Manager Console

Ports Used by SQL Server

The following table lists ports required to be opened between SQL server and the other Migration Manager components so that SQL server is be able to communicate with those components properly:

Direction of Communication	Port	Protocol(s)	Communication with
Inbound	1433	TCP	Migration Manager Console, Statistics Collection Agent and Statistics Portal, Migration Agent for Exchange (MAgE)

Ports Used by Statistics Portal

The following table lists ports required to be opened between Statistics Portal and the other Migration Manager components so that Statistics Portal is be able to communicate with those components properly:

Direction of Communication	Port	Protocol(s)	Communication with
Inbound	80	TCP/UDP	Migration Manager Console or any web browser
	443	TCP/UDP	Migration Manager Console or any web browser (if configured)
	1024-65535	TCP/UDP	SQL server
Outbound	135	TCP/UDP	DSA server
	137	TCP/UDP	
	138	UDP	
	139	TCP	
	445	TCP/UDP	
	1024-65535	TCP/UDP	
	1433	TCP	SQL server (default SQL port)

Ports Used by Migration Manager for Exchange Components

This section describes ports required by Migration Manager components related to Exchange migration, as follows:

- Ports Used by Migration Manager for Exchange Console
- Ports Used by Migration Agent for Exchange (MAgE)
- Ports Used by Mail Source Agent (MSA)
- Ports Used by Mail Target Agent (MTA)
- Ports Used by Public Folder Source Agent (PFSA)
- Ports Used by Public Folder Target Agent (PFTA)
- Ports Used by Calendar Synchronization Agent (CSA)
- Ports Used by Transmission Agent (NTA)
- Ports Used by Free/Busy Synchronization Agent (FBSA)
- Ports Used by Statistics Collection Agent (SCA)
- Ports Used by Migration Attendant for Exchange

Ports Used by Migration Manager for Exchange Console

The following table lists ports required to be opened so that Migration Manager for Exchange Console is be able to communicate with all components properly:

Direction of Communication	Port	Protocol(s)	Communication with	Accounts
Outbound	80	TCP/UDP	Exchange servers, Microsoft Office 365, License Server	Exchange Account, Console Account, License Server Account
	443	TCP/UDP	Exchange servers and Microsoft Office 365	Exchange Account, Console Account
	389	TCP/UDP	Source domain controllers and Target domain controllers	Active Directory account, Active Directory

Direction of Communication	Port	Protocol(s)	Communication with	Accounts
				Synchronization account (Used by the Directory Synchronization Agent)
	3268	TCP/UDP	Source and target global catalog	Active Directory account
	User-configured (default ports: 389, 636, if available)	TCP/UDP	ADAM/AD LDS Instance	Auxiliary account
	1433	TCP	Database server	SQL configuration database account
	135	TCP/UDP	Exchange Servers, Agent Hosts	Exchange Account, Agent Host Account
	445	TCP/UDP		
	1024-65535	TCP/UDP		

Ports Used by Migration Agent for Exchange (MAgE)

> **NOTE:** During MAgE installation, the setup program automatically extends range of TCP ports for outbound communication on an agent host computer from default range to 1025-65535.

The following table lists ports required to be opened between Migration Agent for Exchange and the other Migration Manager components so that Migration Agent for Exchange is be able to communicate with components properly:

Direction of Communication	Port	Protocol(s)	Communication with	Accounts
Inbound	135	TCP/UDP	Migration Manager Console	Agent Host Account
	445	TCP/UDP		
	1024-65535	TCP/UDP		
Outbound	80	TCP/UDP	License Server	Agent Host Account (unless alternative credentials are used for the license server)
	User-configured (default ports:389, 636, if available)	TCP/UDP	ADAM/AD LDS Instance	Auxiliary account

Direction of Communication	Port	Protocol(s)	Communication with	Accounts
	1433	TCP	Database Server	SQL configuration database account
	53	TCP/UDP	Source domain controllers and Target domain controllers	Active Directory account Active Directory Synchronization account (Used by the Directory Synchronization Agent)
	88			
	135			
	389			
	445			
	3268			

The following table lists ports required to be opened to allow Exchange account process specific jobs by Migration Agent for Exchange

Job Type	Port	Protocol(s)	Communication with
Mail & Calendar (EWS)	80	TCP/UDP	Source Exchange servers and Target Exchange servers, Microsoft Office 365
	443		
Mail & Calendar (MAPI as source)	80	TCP/UDP	Source Exchange servers
	443		
	135		
	1024-65535		
	80	TCP/UDP	Target Exchange servers, Microsoft Office 365
	443		
Native Move	80	TCP/UDP	Source Exchange servers and Target Exchange servers
	443		
	135	TCP/UDP	Optional: Source Exchange server if mailbox’s statistics are needed.
Public Folders	443	TCP/UDP	Source Exchange servers and Target Exchange servers, Microsoft Office 365

Ports Used by Mail Source Agent (MSA)

The following table lists ports required to be opened between Mail Source Agent and the other Migration Manager components so that Mail Source Agent is be able to communicate with those components properly:

Direction of Communication	Port	Protocol(s)	Communication with
Inbound	135	TCP/UDP	Migration Manager Console and Statistics Collection Agent (SCA)
	137	TCP/UDP	
	138	UDP	
	139	TCP	
	445	TCP/UDP	
	1024-65535	TCP/UDP	
Outbound	389	TCP/UDP	Source and target domain controllers
	3268	TCP	Source and target global catalogs
	User-configured (default ports:389, 636, if available)	TCP/UDP	ADAM/AD LDS instance
	135	TCP/UDP	License server, source and target Exchange servers (CAS/MBX role) and source domain controllers
	137	TCP/UDP	Source and target Exchange servers (CAS/MBX role)
	138	UDP	
	139	TCP	
	445	TCP/UDP	
	1024-65535	TCP/UDP	Source and target Exchange servers (CAS/MBX role)
	1025	TCP	Source domain controllers

Ports Used by Mail Target Agent (MTA)

The following table lists ports required to be opened between Mail Target Agent and the other Migration Manager components so that Mail Target Agent is be able to communicate with those components properly:

Direction of Communication	Port	Protocol(s)	Communication with
Inbound	135	TCP/UDP	Migration Manager Console, Statistics Collection Agent (SCA) and Transmission Agent
	137	TCP/UDP	
	138	UDP	
	139	TCP	
	445	TCP/UDP	
	1024-65535	TCP/UDP	Migration Manager Console, Statistics Collection Agent (SCA), Transmission Agent
Outbound	389	TCP/UDP	Target domain controllers
	3268	TCP	Target global catalogs
	135	TCP/UDP	Target Exchange servers (CAS/MBX role)
	137	TCP/UDP	
	138	UDP	
	139	TCP	
	445	TCP/UDP	
	1024-65535	TCP/UDP	Target Exchange servers (CAS/MBX role)

Ports Used by Public Folder Target Agent (PFTA)

The following table lists ports required to be opened between Public Folder Target Agent and the other Migration Manager components so that Public Folder Target Agent is be able to communicate with those components properly:

Direction of Communication	Port	Protocol(s)	Communication with
Inbound	135	TCP/UDP	Migration Manager Console, Statistics Collection Agent (SCA) and Transmission Agent (NTA)
	137	TCP/UDP	
	138	UDP	
	139	TCP	
	445	TCP/UDP	
	1024-65535	TCP/UDP	Migration Manager Console, Statistics Collection Agent (SCA), Transmission Agent (NTA)

Direction of Communication	Port	Protocol(s)	Communication with
Outbound	389	TCP/UDP	Source and target domain controllers
	3268	TCP	Source and target global catalogs
	80	TCP/UDP	Target Exchange servers (CAS/MBX role)
	135	TCP/UDP	
	137	TCP/UDP	
	138	UDP	
	139	TCP	
	445	TCP/UDP	
	1024-65535	TCP/UDP	

Ports Used by Public Folder Source Agent (PFSA)

The following table lists ports required to be opened between Public Folder Source Agent and the other Migration Manager components so that Public Folder Source Agent is be able to communicate with those components properly:

Direction of Communication	Port	Protocol(s)	Communication with
Inbound	135	TCP/UDP	Migration Manager Console and Statistics Collection Agent (SCA)
	137	TCP/UDP	
	138	UDP	
	139	TCP	
	445	TCP/UDP	
	1024-65535	TCP/UDP	Migration Manager Console, Statistics Collection Agent (SCA)

Direction of Communication	Port	Protocol(s)	Communication with
Outbound	389	TCP/UDP	Source and target domain controllers
	3268	TCP	Source and target global catalogs
	135	TCP/UDP	Source Exchange servers (CAS/MBX role)
	137	TCP/UDP	
	138	UDP	
	139	TCP	
	445	TCP/UDP	
	1024-65535	TCP/UDP	
	135	TCP/UDP	Source domain controllers
	1025	TCP	

Ports Used by Calendar Synchronization Agent (CSA)

The following table lists ports required to be opened between Calendar Synchronization Agent and the other Migration Manager components so that Calendar Synchronization Agent is be able to communicate with those components properly:

Direction of Communication	Port	Protocol(s)	Communication with
Inbound	135	TCP/UDP	Migration Manager Console and Statistics Collection Agent (SCA)
	137	TCP/UDP	
	138	UDP	
	139	TCP	
	445	TCP/UDP	
	1024-65535	TCP/UDP	Migration Manager Console, Statistics Collection Agent (SCA)

Direction of Communication	Port	Protocol(s)	Communication with
Outbound	389	TCP/UDP	Source and target domain controllers
	3268	TCP	Source and target global catalogs
	User-configured (default ports:389, 636, if available)		ADAM/AD LDS instance
	135	TCP/UDP	License server, source and target Exchange servers (CAS/MBX role) and source domain controllers
	137	TCP/UDP	Source and target Exchange servers (CAS/MBX role)
	138	UDP	
	139	TCP	
	445	TCP/UDP	
	1024-65535	TCP/UDP	Source and target Exchange servers (CAS/MBX role)
	1025	TCP	Source domain controllers

Ports Used by Transmission Agent (NTA)

The following table lists ports required to be opened between Transmission Agent and the other Migration Manager components so that Transmission Agent is be able to communicate with those components properly:

Direction of Communication	Port	Protocol(s)	Communication with
Inbound	135	TCP/UDP	Migration Manager Console and Statistics Collection Agent (SCA)
	137	TCP/UDP	
	138	UDP	
	139	TCP	
	445	TCP/UDP	
	1024-65535	TCP/UDP	Migration Manager Console, Statistics Collection Agent (SCA)

Direction of Communication	Port	Protocol(s)	Communication with
Outbound	135	TCP/UDP	Target agent hosts
	137	TCP/UDP	
	138	UDP	
	139	TCP	
	445	TCP/UDP	
	1024-65535	TCP/UDP	

Ports Used by Free/Busy Synchronization Agent (FBSA)

The following table lists ports required to be opened between Free/Busy Synchronization Agent and the other Migration Manager components so that Free/Busy Synchronization Agent is be able to communicate with those components properly:

Direction of Communication	Port	Protocol(s)	Communication with
Inbound	135	TCP/UDP	Migration Manager Console and Statistics Collection Agent (SCA)
	137	TCP/UDP	
	138	UDP	
	139	TCP	
	445	TCP/UDP	
	1024-65535	TCP/UDP	Migration Manager Console, Statistics Collection Agent (SCA)
Outbound	389	TCP/UDP	Source and target domain controllers
	3268	TCP	Source and target global catalogs
	135	TCP/UDP	Source and target Exchange servers (CAS/MBX role)
	137	TCP/UDP	
	138	UDP	
	139	TCP	
	445	TCP/UDP	
	1024-65535	TCP/UDP	Source and target Exchange servers (CAS/MBX role)
	135	TCP/UDP	Source domain controllers
	1024	TCP	

Ports Used by Statistics Collection Agent (SCA)

The following table lists ports required to be opened between Statistics Collection Agent and the other Migration Manager components so that Statistics Collection Agent is be able to communicate with those components properly:

Direction of Communication	Port	Protocol(s)	Communication with
Inbound	135	TCP/UDP	Migration Manager Console
	137	TCP/UDP	
	138	UDP	
	139	TCP	
	445	TCP/UDP	
	1024-65535	TCP/UDP	Migration Manager Console, Statistics Collection Agent (SCA)
Outbound	135	TCP/UDP	Source and target agent hosts
	137	TCP/UDP	
	138	UDP	
	139	TCP	
	445	TCP/UDP	
	1024-65535	TCP/UDP	
	1433	TCP	SQL server (default SQL Port)

Ports Used by Migration Attendant for Exchange

The following table lists ports required to be opened between Migration Attendant for Exchange and the other Migration Manager components so that Migration Attendant for Exchange is be able to communicate with those components properly:

Direction of Communication	Port	Protocol(s)	Communication with
Inbound	135	TCP/UDP	Source/target agent hosts
	137	TCP/UDP	
	138	UDP	
	139	TCP	
	445	TCP/UDP	
	1024-65535	TCP/UDP	
Outbound	135	TCP/UDP	Source/target Exchange servers (CAS/MBX role)
	137	TCP/UDP	
	138	UDP	
	139	TCP	
	445	TCP/UDP	
	1024-65535	TCP/UDP	

Ports Used by Migration Manager for Active Directory Components

This section describes ports required by Migration Manager components related to Active Directory migration, as follows:

- Ports Used by Directory Synchronization Agent (DSA)
- Ports Used by Migration Manager for Active Directory (Microsoft Office 365) Console
- Ports Used by Directory Migration Agent (DMA)

Ports Used by Directory Synchronization Agent (DSA)

The following table lists ports required to be opened between Directory Synchronization Agent and the other Migration Manager components so that Directory Synchronization Agent is be able to communicate with those components properly:

Direction of Communication	Port	Protocol(s)	Communication with
Inbound	3389	TCP/UDP	Migration Manager Console (port is used during DSA installation only)
	1024-65535	TCP/UDP	Migration Manager Console (port may be used while troubleshooting)
Outbound	User-configured (default ports:389, 636, if available)	TCP/UDP	ADAM/AD LDS instance
	3268	TCP	Source and target global catalogs
	389	TCP/UDP	Source and target domain controllers
	137	TCP/UDP	
	138	UDP	
	139	TCP	
	445	TCP/UDP	
	135	TCP/UDP	
	1024-65535	TCP/UDP	Source and target domain controllers, target Exchange servers

Ports Used by Migration Manager for Active Directory (Microsoft Office 365) Console

The following table lists ports required to be opened between Migration Manager for Active Directory (Microsoft Office 365) console and the other Migration Manager components so that Directory Synchronization Agent is be able to communicate with those components properly:

Direction of Communication	Port	Protocol(s)	Communication with
Inbound	1000	TCP/UDP	Directory Migration Agent instances
Outbound	User-configured (default ports:389, 636, if available)	TCP/UDP	ADAM/AD LDS instance
	389	TCP/UDP	Source domain controllers
	3268	TCP	Source global catalogs
	User-configured (default port:1001)	TCP/UDP	Directory Migration Agent instances
	80	TCP/UPD	Microsoft Office 365
	443	TCP/UPD	

NOTE: The list of permissions given below contains all required permissions for the accounts. However some of the permissions can be replaced with their equivalents. For more information, see the corresponding steps for each account.

Ports Used by Directory Migration Agent (DMA)

The following table lists ports required to be opened between Directory Migration Agent and the other Migration Manager components so that Directory Synchronization Agent is be able to communicate with those components properly:

Direction of Communication	Port	Protocol(s)	Communication with
Inbound	User-configured (default port:1001)	TCP/UPD	Migration Manager for Active Directory (Microsoft Office 365) console

Direction of Communication	Port	Protocol(s)	Communication with
Outbound	User-configured (default ports:389, 636, if available)	TCP/UPD	ADAM/AD LDS instance
	389	TCP/UDP	Source domain controllers
	3268	TCP	Source global catalogs
	1000	TCP/UPD	Migration Manager for Active Directory (Microsoft Office 365) console
	80	TCP/UPD	Microsoft Office 365
	443	TCP/UPD	

Ports Used by Resource Updating Manager

The following sections provide a comprehensive list of port requirements for Resource Updating Manager (abbreviated to RUM). The list of required ports depends on the way you process resources:

1. Processing Resources with Agents
2. Processing Resources Remotely (without Agents)

i **TIP:** For information on Resource Updating Manager, refer to the *Resource Update* section of the *Migrating Manager for Active Directory User Guide* document.

Processing Resources with Agents

RUM Console

The following table lists ports required to be opened between RUM Console and the components specified in the table so that RUM Console may communicate with those components properly:

Direction of Communication	Port	Protocol(s)	Communication with
Outbound	User-configured (default ports:389, 636, if available)	TCP/UDP	ADAM/AD LDS instance
	389		Source and target domain controllers
	3268		Source and target global catalogs

RUM Controller

The following table lists ports required to be opened between RUM Controller and the other Migration Manager components so that RUM controller is be able to communicate with those components properly:

Direction of Communication	Port	Protocol(s)	Communication with
Inbound	445	TCP/UDP	RUM Agent
	1024-65535		

Direction of Communication	Port	Protocol(s)	Communication with
Outbound	389	TCP/UDP	Source and target domain controllers
	3268		Source and target global catalogs
	User-configured (default ports:389, 636, if available)		ADAM/AD LDS instance
	135-139		RUM Agent
	1024-65535		
	53		DNS Server

RUM Agent

The following table lists ports required to be opened between RUM agent and the other Migration Manager components so that RUM agent is be able to communicate with those components properly:

Firewall State	Direction of Communication	Port	Protocol(s)	Communication with
Disabled	Inbound	1024-65535	TCP/UDP	RUM Controller
	Outbound	389		Source and target domain controllers
		3268		Source and target global catalogs
		53		DNS Server
		135-139		RUM Controller
		445		
		1024-65535		
Enabled	Outbound	389	TCP/UDP	Source and target domain controllers
		3268		Source and target global catalogs
		53		DNS Server
		135-139		RUM Controller
		445		
		1024-65535		

Processing Resources Remotely (without Agents)

RUM Console

The following table lists ports required to be opened between RUM console and the other Migration Manager components so that RUM console is be able to communicate with those components properly:

Direction of Communication	Port	Protocol(s)	Communication with
Outbound	User-configured (default ports:389, 636, if available)	TCP/UDP	ADAM/AD LDS instance
	389		Source and target domain controllers
	3268		Source and target global catalogs

RUM Controller

The following table lists ports required to be opened between RUM Controller and the other Migration Manager components so that RUM controller is be able to communicate with those components properly:

Direction of Communication	Port	Protocol(s)	Communication with
Outbound	389	TCP/UDP	Source and target domain controllers
	3268		Source and target global catalogs
	User-configured (default ports:389, 636, if available)		ADAM/AD LDS instance
	135-139		Workstation processed
	1024-65535		
	53		DNS Server

Workstation

The following table lists ports required to be opened between each workstation you plan to process with RUM and RUM Controller so that they may be processed successfully:

Direction of Communication	Port	Protocol(s)	Communication with
Inbound	135-139 1024-65535	TCP/UDP	RUM Controller

Accounts Required for Migration Manager Operation

Migration Manager account

Description	Where Specified	Rights and Permissions
The account under which the administrator is logged on when Migration Manager is started. This account is used to connect to ADAM/AD LDS and open the migration project. (The appropriate users should be delegated rights within the project to open and work with the project).	At administrator's logon	Membership in the local **Administrators** group on the console machine. If there are cluster servers in the source or target Exchange organizations, the Migration Manager account must: • Be a member of the local **Administrators** group on each cluster node. • Have **Full Control** rights over the cluster.

ADAM/AD LDS administrative account

Description	Where Specified	Rights and Permissions
Is used to connect to ADAM/AD LDS and create a new migration project.	During ADAM/AD LDS instance installation. Later, when you first start Migration Manager, specify this account in the **Open Project Wizard**.	After ADAM/AD LDS instance installation, this account is granted **Full Control** rights over the whole ADAM/AD LDS instance. The user who creates the project is automatically granted **Full Control** rights in the project and can later delegate rights within the project to other users. **NOTE:** Delegated users will have rights only within the ADAM/AD LDS project partition, but no rights to manage the ADAM/AD LDS instance.

SQL configuration database account

Description	Where Specified	Rights and Permissions
Is used to: • Create the SQL configuration database when a migration project is created • Access the SQL configuration database	In the **Open Project Wizard**	**Database Creator** role on the SQL server where the configuration database will be created

ℹ **NOTE:** Database creator server role is required only if project database has not been created and you are planning to create it. In case the project database has been created, server role **dbcreator** is no longer required. Database role **db_owner** is enough to work with existing project database. You can grant this permission directly to the SQL configuration database account, or through the security group that can also be used for Agent Host accounts.

Auxiliary account

Description	Where Specified	Rights and Permissions
Is used by different Migration Manager components to retrieve information from ADAM/AD LDS	During Migration Manager setup, or in the **Open Project Wizard**	Membership in the local **Administrators** group on the console machine. **IMPORTANT NOTES**: This account must not be changed during migration. Account password must not expire or be changed during migration.

Accounts Used by the Directory Synchronization Agent

The following accounts are used by the Directory Synchronization Agent (DSA) to connect to the domains.

> **TIP:** The DSA account permissions provided below are high level permissions that can be easily and quickly granted. However, if they are too elevated and thus cannot be granted in your environment , take a look at minimum required permissions for DSA accounts in Migration Manager for Active Directory Granular Account Permissions.

Source Active Directory Synchronization account

Description	Where Specified	Rights and Permissions
Is used: • By the DSA to connect to the source Active Directory domain • By the Mail Source Agent (MSA) to perform mailbox switch (related to Migration Manager for Exchange)	You specify this account when you create and configure a domain pair.	Membership in the **Administrators** group. You can use account that is not a member of **Administrators** group in case Preinstalled Service feature is configured and enabled.

Target Active Directory Synchronization account

Description	Where Specified	Rights and Permissions
Is used: • By the DSA to connect to the target Active Directory domain • By the Mail Source Agent (MSA) to perform mailbox switch (related to Migration Manager for Exchange)	You specify this account when you create and configure a domain pair.	Membership in the **Administrators** group. You can use account that is not a member of **Administrators** group in case Preinstalled Service feature is configured and enabled.

Source Accounts Used by Migration Manager for Exchange Agents

NOTE: Each computer on which Migration Manager for Exchange agents run must have DCOM **Access** and **Launch** permissions. These permissions are acquired by the agent through server's local **Administrators** group membership.

Accounts for Exchange 2003 Server

Exchange account

Used To	Where Specified	Rights and Permissions
• Work with source Exchange mailboxes and public folders (used by the Mail Source Agent, Public Folder Source Agent, and Public Folder Target Agent) • Mail-enable the newly-created public folders(used by the public folder agents only: Public Folder Source Agent and Public Folder Target Agent) • Synchronize Calendar information (used by the Calendar Synchronization Agent) • Synchronize free/busy data (optional) (used by the Free/Busy Synchronization Agent) • Switch mailboxes	On the **General>Connection** page of the source Exchange server **Properties** in the Migration Manager Console	• 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. • **Full Control** permission on the organizational units (OUs) (and their child objects) where the source synchronized objects are located. • **Full Control** permission on source Exchange 2003 servers (including the **Send As** and **Receive As** permissions).

Used To	Where Specified	Rights and Permissions
		• **Full Control** permission on the **Microsoft Exchange System Objects** organizational unit in all domains in which source Exchange 2003 servers involved in public folder synchronization reside. • **Modify public folder replica list** permission, **Modify public folder deleted** item retention permission, and **Modify public folder quotas** permission on the administrative groups where the source Exchange 2003 servers involved in public folder synchronization reside

Active Directory account

Used To	Where Specified	Rights and Permissions
Work with the source Active Directory	On the **General>Associateddomain controller** page of the source Exchange server **Properties** in the Migration Manager Console	• **Read** access to the source domain **NOTE:** If migration is performed in the child domain, ensure that Active Directory account has the **Read** access to the parent (root) domain as well.

To learn how to grant rights and permissions required for this account, refer to the *Exchange 2003 Environment Preparation* document.

Accounts for Exchange 2007 Server

Exchange account

Used To	Where Specified	Rights and Permissions
• Work with source Exchange mailboxes and public folders (used by the Mail Source Agent, Public Folder Source Agent, and Public Folder Target Agent) • Mail-enable the newly-created public folders(used by the public folder agents only: Public Folder Source Agent and Public Folder Target Agent) • Synchronize Calendar information (used by the Calendar Synchronization Agent) • Synchronize free/busy data (optional) (used by the Free/Busy Synchronization Agent) • Switch mailboxes	On the **General>Connection** page of the source Exchange server **Properties** in the Migration Manager Console	• 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. • **Full Control** permission on the organizational units (OUs) (and their child objects) where the source synchronized objects are located. • **Full Control** permission on source Exchange 2007 servers (including the **Send As** and **Receive As** permissions). • **Full Control** permission on the **Microsoft Exchange System Objects** organizational unit in all domains in which source Exchange 2007 servers involved in public folder synchronization reside. • **Exchange Public Folder Administrator** role.

Active Directory account

Used To	Where Specified	Rights and Permissions
Work with the source Active Directory	On the **General>Associated domain controller** page of the source Exchange server **Properties** in the Migration Manager Console	• **Read** access to the source domain • **Read** permission for the **Microsoft Exchange** container in Active Directory

To learn how to grant rights and permissions required for this account, refer to the *Source Exchange 2007 Preparation* document.

Accounts for Exchange 2010 Server

TIP: If you plan to migrate to Exchange 2010 or Exchange 2013 organization, take a look at minimum required permissions for accounts in the Granular Account Permissions for Exchange 2010 to 2010 Migration and Granular Account Permissions for Exchange 2010 to 2013 Migration documents, respectively.

Exchange account

Used To	Where Specified	Rights and Permissions
• Work with source Exchange mailboxes and public folders (used by the Mail Source Agent, Public Folder Source Agent, and Public Folder Target Agent) • Mail-enable the newly-created public folders(used by the public folder agents only: Public Folder Source Agent and Public Folder Target Agent) • Synchronize Calendar information (used by the Calendar Synchronization Agent) • Synchronize free/busy data (optional) (used by the Free/Busy Synchronization Agent) • Switch mailboxes	On the **General>Connection** page of the source Exchange server **Properties** in the Migration Manager Console	• 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. • **Full Control** permission on the organizational units (OUs) (and their child objects) where the source synchronized objects are located. • **Full Control** permission on source Exchange 2010 servers (including the **Send As** and **Receive As** permissions). • **Full Control** permission on source Exchange 2010 organization • Membership in the **Public Folder Management** group. • Permissions to log on to every mailbox involved in the migration. • Membership in the **Recipient Management** group. • The **ApplicationImpersonation** management role for migration to Exchange 2013 (or higher) or Office 365

Used To	Where Specified	Rights and Permissions
		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.

Active Directory account

Used To	Where Specified	Rights and Permissions
Work with the source Active Directory	On the **General>Associated domain controller** page of the source Exchange server **Properties** in the Migration Manager Console	- **Read** access to the source domain - **Read** permission for the **Microsoft Exchange** container in Active Directory **NOTE**: If migration is performed in the child domain, ensure that Active Directory account has the **Read** access to the parent (root) domain as well.

To learn how to grant rights and permissions required for this account, refer to the *Source Exchange 2010 Preparation* document.

Accounts for Exchange 2013 Server

Exchange account

Used To	Where Specified	Rights and Permissions
- Work with source Exchange mailboxes and public folders (used by the Migration Agent for Exchange, Public Folder Source Agent, and Public Folder Target Agent)	On the **General>Connection** page of the source Exchange server **Properties** in the Migration Manager Console	- **Read** access to the source domain - **Full Control** permission on Exchange 2013 mailboxes - The **Mail Enabled Public Folders** management role

Used To	Where Specified	Rights and Permissions
- Mail-enable the newly-created public folders (used by the public folder agents only: Public Folder Source Agent and Public Folder Target Agent) - Move mailboxes		- Membership in the local **Administrators** group on all source Exchange servers involved in the public folder synchronization. If a server is a domain controller, the account should be added to the domain local **Administrators** group of the domain. - Membership in the **Recipient Management** group - The **ApplicationImpersonation** management role for migration to Exchange 2013 (or higher) or Office 365

Active Directory account

Used To	Where Specified	Rights and Permissions
- Work with the source Active Directory	On the **General>Associateddomain controller** page of the source Exchange server **Properties** in the Migration Manager Console	- **Read** access to the source domain - **Read** permission for the Microsoft Exchange container in the source Active Directory - **Write** permission on the **Microsoft Exchange System Objects** organizational unit in all domains in which source Exchange 2013 servers involved in public folder synchronization reside

To learn how to grant rights and permissions required for this account, refer to the *Source Exchange 2013 Preparation* document.

Accounts for Exchange 2016/2019 Server

Exchange account

Used To	Where Specified	Rights and Permissions
- Work with source Exchange mailboxes - Move mailboxes	When creating a calendar or mailbox synchronization job. To change it, use properties of the corresponding synchronization job.	- **Read** access to the source domain (including all descendant objects) - **Read** permission for the **Microsoft Exchange** container in the **Configuration** partition of source Active Directory (including all descendant objects) - The **ApplicationImpersonation** management role **TIP:** The **Read** permission for the Microsoft Exchange container is required only if you plan to add the source Exchange organization using the **Add Source Organization Wizard** under this account.

Active Directory account

Used To	Where Specified	Rights and Permissions
- Work with the source Active Directory - Switch mailboxes	When creating a calendar or mailbox synchronization job. To change it, use properties of the corresponding synchronization job.	- **Read** access to the source domain (including all descendant objects) - **Read** permission for the **Microsoft Exchange** container in the **Configuration** partition of source Active Directory (including all descendant objects)

To learn how to grant rights and permissions required for this account, refer to the *Source Exchange 2016 Preparation*, *Source Exchange 2019 Preparation*, *Target Exchange 2016 Preparation*, or *Target Exchange 2019 Preparation*documents depending on your environment.

Target Accounts Used by Migration Manager for Exchange Agents

ℹ **NOTE:** Each computer on which Migration Manager for Exchange agents run must have DCOM Access and Launch permissions. These permissions are acquired by the agent through server's local **Administrators** group membership.

- Accounts for Exchange 2003 Server
- Accounts for Exchange 2007 Server
- Accounts for Exchange 2010 Server (Legacy)
- Accounts for Exchange 2010 Server (MAgE)
- Accounts for Exchange 2013 Server
- Accounts for Exchange 2016/2019 Server

Accounts for Exchange 2003 Server

Exchange account

Used To	Where Specified	Rights and Permissions
• Work with target Exchange mailboxes and public folders (used by the Mail Target Agent, Public Folder Source Agent, and Public Folder Target Agent) • Mail-enable the newly-created public folders (used by the public folder agents only: Public Folder Source Agent and Public Folder Target Agent) • Synchronize Calendar information (used by the Calendar Synchronization Agent) • Synchronize free/busy data (optional) (used by the Free/Busy Synchronization Agent) • Move mailboxes	On the **General>Connection** page of the target Exchange server **Properties** in the Migration Manager Console	• **Read** access to the target domain. • 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. • **Full Control** permission on the organizational units (OUs) (and their child objects) where the target synchronized objects are located.

Used To	Where Specified	Rights and Permissions
		- **Full Control** permission on target Exchange 2003 servers (including the **Send As** and **Receive As** permissions). - **Full Control** permission on the **Microsoft Exchange System Objects** organizational unit in all domains in which target Exchange 2003 servers involved in public folder synchronization reside. - **Modify public folder replica list** permission, **Modify public folder deleted** item retention permission, and **Modify public folder quotas** permission on the administrative groups where the target Exchange 2003 servers involved in public folder synchronization reside

Active Directory account

Used To	Where Specified	Rights and Permissions
- Work with the target Active Directory - Re-home mailboxes - Switch mailboxes and synchronize mailboxes in Remote Users Collections (Mail Source Agent, Mail Target Agent)	On the **General>Associateddomain controller** page of the target Exchange server **Properties** in the Migration Manager Console	- **Read** access to the target domain - **Full Control** rights on the OUs (and their child objects) where the target synchronized objects are located. **NOTE**: If migration is performed in the child domain, ensure that Active Directory account has the **Read** access to the parent (root) domain as well.

To learn how to grant rights and permissions required for this account, refer to the *Exchange 2003 Environment Preparation* document.

Accounts for Exchange 2007 Server

Exchange account

Used To	Where Specified	Rights and Permissions
• Work with target Exchange mailboxes and public folders (used by the Mail Target Agent, Public Folder Source Agent, and Public Folder Target Agent) • Mail-enable the newly-created public folders (used by the public folder agents only: Public Folder Source Agent and Public Folder Target Agent) • Synchronize Calendar information (used by the Calendar Synchronization Agent) • Synchronize free/busy data (optional) (used by the Free/Busy Synchronization Agent) • Move mailboxes	On the **General>Connection** page of the target Exchange server **Properties** in the Migration Manager Console	• **Read** access to the target domain. • 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. • **Full Control** permission on the organizational units (OUs) (and their child objects) where the target synchronized objects are located. • **Full Control** permission on target Exchange 2007 servers (including the **Send As** and **Receive As** permissions). • **Full Control** permission on the **Microsoft Exchange System Objects** organizational unit in all domains in which target Exchange 2007 servers involved in public folder synchronization reside. • **Exchange Public Folder Administrator** role.

Active Directory account

Used To	Where Specified	Rights and Permissions
• Work with the target Active Directory	On the **General>Associateddomain controller** page of the target	• **Read** access to the target domain

Used To	Where Specified	Rights and Permissions
• Re-home mailboxes • Switch mailboxes and synchronize mailboxes in Remote Users Collections (Mail Source Agent, Mail Target Agent)	Exchange server **Properties** in the Migration Manager Console	• **Full Control** rights on the OUs (and their child objects) where the target synchronized objects are located. • **Read** permission for the **Microsoft Exchange** container in Active Directory **NOTE**: If migration is performed in the child domain, ensure that Active Directory account has the **Read** access to the parent (root) domain as well.

To learn how to grant rights and permissions required for this account, refer to the *Target Exchange 2007 Preparation* document.

Accounts for Exchange 2010 Server (Legacy)

TIP: If you plan to migrate from Exchange 2010 organization, take a look at minimum required permissions for accounts in the *Granular Account Permissions for Exchange 2010 to 2010 Migration* and *Granular Account Permissions for Exchange 2010 to 2013 Migration* documents, respectively.

Exchange account

Used To	Where Specified	Rights and Permissions
• Work with target Exchange mailboxes and public folders (used by the Mail Target Agent, Public Folder Source Agent, and Public Folder Target Agent) • Mail-enable the newly-created public folders (used by the public folder agents only: Public Folder Source Agent and Public Folder Target Agent) • Synchronize Calendar information (used by the Calendar Synchronization Agent)	On the **General>Connection** page of the target Exchange server **Properties** in the Migration Manager Console	• **Read** access to the target domain. • 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.

Used To	Where Specified	Rights and Permissions
- Synchronize free/busy data (optional) (used by the Free/Busy Synchronization Agent) - Move mailboxes		- **Full Control** permission on the organizational units (OUs) (and their child objects) where the target synchronized objects are located. - **Full Control** permission on the **Microsoft Exchange System Objects** organizational unit in all domains in which target Exchange 2010 servers involved in public folder synchronization reside. - **Full Control** permission on target Exchange 2010 organization - Membership in the **Public Folder Management** group. - Permissions to log on to every mailbox involved in the migration. - Membership in the **Recipient Management** group. **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.

Active Directory account

Used To	Where Specified	Rights and Permissions
- Work with the target Active Directory - Re-home mailboxes - Switch mailboxes and synchronize mailboxes in Remote Users Collections (Mail Source Agent, Mail Target Agent)	On the **General>Associateddomain controller** page of the target Exchange server **Properties** in the Migration Manager Console	- **Read** access to the target domain - **Full Control** rights on the OUs (and their child objects) where the target synchronized objects are located.

Used To	Where Specified	Rights and Permissions
		- **Read** permission for the **Microsoft Exchange** container in Active Directory **NOTE**: If migration is performed in the child domain, ensure that Active Directory account has the **Read** access to the parent (root) domain as well.

To learn how to grant rights and permissions required for this account, refer to the *Target Exchange 2010 Preparation (Legacy)* document.

Accounts for Exchange 2010 Server (MAgE)

Exchange account

Used To	Where Specified	Rights and Permissions
- Work with target Exchange mailboxes and public folders (used by Migration Agent for Exchange, Public Folder Source Agent, and Public Folder Target Agent) - Make the newly-created public folders mail-enabled (used by the public folder agents only: Public Folder Source Agent and Public Folder Target Agent) - Move mailboxes	On the **General>Connection** page of the target Exchange server **Properties** in the Migration Manager Console	For mailbox and calendar synchronization: - **Read** access to the target domain (including all descendant objects) - **Read** permission for the **Microsoft Exchange** container in the **Configuration** partition of target Active Directory (including all descendant objects) - The **Move Mailboxes** management role - The **Mail Recipients** management role - The **ApplicationImpersonation** management role **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. For public folder synchronization:

Used To	Where Specified	Rights and Permissions
		- 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. - Membership in the **Public Folder Management** group - Permissions to process public folders involved in the migration by granting **Full Control** permission on public folder databases where those public folders reside.

Active Directory account

Used To	Where Specified	Rights and Permissions
- Work with the target Active Directory - Switch mailboxes	On the **General>Associateddomain controller** page of the target Exchange server **Properties** in the Migration Manager Console	For mailbox and calendar synchronization: - **Read** access to the target domain (including all descendant objects) - **Read** permission for the **Microsoft Exchange** container in the **Configuration** partition of target Active Directory (including all descendant objects) For public folder synchronization: - 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.

To learn how to grant rights and permissions required for this account, refer to the *Target Exchange 2010 Preparation (MAgE)* document.

Accounts for Exchange 2013 Server

Exchange account

Used To	Where Specified	Rights and Permissions
• Work with target Exchange mailboxes and public folders (used by the Migration Agent for Exchange, Public Folder Source Agent, and Public Folder Target Agent) • Mail-enable the newly-created public folders (used by the public folder agents only: Public Folder Source Agent and Public Folder Target Agent) • Move mailboxes	On the **General>Connection** page of the target Exchange server **Properties** in the Migration Manager Console	For mailbox and calendar synchronization: • **Read** access to the target domain (including all descendant objects) • **Read** permission for the **Microsoft Exchange** container in the **Configuration** partition of target Active Directory (including all descendant objects) . This is required only if you plan to add the target Exchange organization using the **Add Target Organization Wizard** under this account. • Permissions to log on to every mailbox involved in the migration by granting **Full Control** permission on a mailbox database • The **Move Mailboxes** management role • The **Mail Recipients** management role • The **ApplicationImpersonation** management role For public folder synchronization: • 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.

Used To	Where Specified	Rights and Permissions
		- The **Mail Enabled Public Folders** management role - Permissions to process public folders involved in the migration by granting **Full Control** permission on mailbox databases where those public folders reside.

Active Directory account

Used To	Where Specified	Rights and Permissions
- Work with the target Active Directory - Re-home mailboxes - Switch mailboxes (Migration Agent for Exchange)	On the **General>Associateddomain controller** page of the target Exchange server **Properties** in the Migration Manager Console	For mailbox and calendar synchronization: - **Read** access to the target domain (including all descendant objects) - **Read** permission for the **Microsoft Exchange** container in the **Configuration** partition of target Active Directory (including all descendant objects) For public folder synchronization: - 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.

To learn how to grant rights and permissions required for this account, refer to the *Target Exchange 2013 Preparation* document.

Accounts for Exchange 2016 Server

Exchange account

Used To	Where Specified	Rights and Permissions
• Work with target Exchange mailboxes and public folders (used by the Migration Agent for Exchange, Public Folder Source Agent, and Public Folder Target Agent) • Mail-enable the newly-created public folders (used by the public folder agents only: Public Folder Source Agent and Public Folder Target Agent) • Move mailboxes	On the **General>Connection** page of the target Exchange server **Properties** in the Migration Manager Console	For mailbox and calendar synchronization: • **Read** access to the target domain (including all descendant objects) • **Read** permission for the **Microsoft Exchange** container in the **Configuration** partition of target Active Directory (including all descendant objects) . This is required only if you plan to add the target Exchange organization using the **Add Target Organization Wizard** under this account. • Permissions to log on to every mailbox involved in the migration by granting **Full Control** permission on a mailbox database • The **Move Mailboxes** management role • The **Mail Recipients** management role • The **ApplicationImpersonation** management role For public folder synchronization: • 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. • The **Mail Enabled Public Folders** management role

Used To	Where Specified	Rights and Permissions
		- Permissions to process public folders involved in the migration by granting **Full Control** permission on mailbox databases where those public folders reside. - Permission to log on to public folder administrator mailbox by granting **Full Control** on it. **NOTE:** Exchange account used for public folder synchronization must be mailbox-enabled to be able obtaining target public folder hierarchy.

Active Directory account

Used To	Where Specified	Rights and Permissions
- Work with the target Active Directory - Re-home mailboxes - Switch mailboxes (Migration Agent for Exchange)	On the **General>Associateddomain controller** page of the target Exchange server **Properties** in the Migration Manager Console	For mailbox and calendar synchronization: - **Read** access to the target domain (including all descendant objects) - **Read** permission for the **Microsoft Exchange** container in the **Configuration** partition of target Active Directory (including all descendant objects) For public folder synchronization: - 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.

To learn how to grant rights and permissions required for this account, refer to the *Target Exchange 2016 Preparation* document.

Accounts for Target Exchange 2019 Server

Exchange account

Used To	Where Specified	Rights and Permissions
• Work with target Exchange mailboxes (used by the Migration Agent for Exchange) • Move mailboxes	On the **General>Connection** page of the target Exchange server **Properties** in the Migration Manager Console	For mailbox and calendar synchronization: • **Read** access to the target domain (including all descendant objects) • **Read** permission for the **Microsoft Exchange** container in the **Configuration** partition of target Active Directory (including all descendant objects). This is required only if you plan to add the target Exchange organization using the **Add Target Organization Wizard** under this account. • Permissions to log on to every mailbox involved in the migration by granting **Full Control** permission on a mailbox database • The **Move Mailboxes** management role • The **Mail Recipients** management role • The **ApplicationImpersonation** management role

Active Directory account

Used To	Where Specified	Rights and Permissions
• Work with the target Active Directory • Re-home mailboxes • Switch mailboxes (Migration Agent for Exchange)	On the **General>Associateddomain controller** page of the target Exchange server **Properties** in the Migration Manager Console	For mailbox and calendar synchronization: • **Read** access to the target domain (including all descendant objects)

Used To	Where Specified	Rights and Permissions
		- **Read** permission for the **Microsoft Exchange** container in the **Configuration** partition of target Active Directory (including all descendant objects) **NOTE:** Alternatively, you can grant the **Write** permission on that organizational unit.

To learn how to grant rights and permissions required for this account, refer to the *Target Exchange 2019 Preparation* document.

Agent Host Account Used by Legacy Migration Manager for Exchange Agents

Used To	Where Specified	Rights and Permissions
• Install and run Migration Manager for Exchange agents on the agent host • Access the license server	Agent host account is specified when registering an agent host. It can be changed in **Properties** of the agent host in the Migration Manager Console. **NOTE**: Agents installed automatically on the specified default agent host during creation of a synchronization job, use the default agent host account. The default agent host account can be changed on the **General>Default agent host** page of the Exchange server **Properties**. Changing the account also affects all agents already installed on the default agent host.	• Membership in the local **Administrators** group on the license server (unless alternative credentials are used for the license server). If server is located in another trusted forest, the account should have local **Administrator** permissions on the license server. • Local **Administrator** permissions on the agent host server.

To learn how to grant rights and permissions required for this account, refer to dedicated Exchange environment preparation documents.

Agent Host Account Used by Migration Agent for Exchange (MAgE)

Used To	Where Specified	Rights and Permissions
• Run the Migration Agent for Exchange service • Read and write Service Connection Point (SCP) • Access the SQL database if **Windows authentication** is selected in migration project properties	During the Migration Agent for Exchange setup in the Migration Manager for Exchange console	• Local **Administrator** permissions on the agent host server where the corresponding MAgE instance is installed • Membership in the local **Administrators** group on the license server (unless alternative credentials are used for the license server). If server is located in another trusted forest, the account should have local **Administrator** permissions on the license server • In case **Windows authentication** is selected in the migration project settings: the **db_owner** role on the SQL server where the database resides • Permission to create, read and write SCP in domain where agent host resides. The SCP object is located in the `CN=Exchange Migration Project,CN=QmmEx,CN=Migration Manager,CN=Quest Software,CN=System,DC=eternity,DC=<...>,DC=<...>` Active Directory container.

To learn how to grant rights and permissions required for this account, refer to the *Setting Up Source Agent Host Account* section of the *Source Exchange 2013 Preparation* document.

Accounts Used for Migrating to Microsoft Office 365

- Accounts Required for Migration Manager for Active Directory Operation
- Accounts Required for Migration Manager for Exchange Operation

Accounts Required for Migration Manager for Active Directory Operation

Console account

Used To (By)	Where Specified	Rights and Permissions
The account under which the administrator is logged on when Migration Manager for Active Directory (Microsoft Office 365) console is started. This account is used to connect to ADAM/AD LDS and open the migration project. The appropriate users should have Full Control permission in ADAM/AD LDS.	At administrator's logon	Membership in the local **Administrators** group on the computer where Migration Manager for Active Directory (Microsoft Office 365) console is installed.

ADAM/AD LDS administrative account

Used To (By)	Where Specified	Rights and Permissions
Connect to ADAM/AD LDS and create a new migration project	During ADAM/AD LDS instance installation	After ADAM/AD LDS instance installation, this account is granted **Full Control** permission over the whole ADAM/AD LDS instance.

Agent service account

Used To (By)	Where Specified	Rights and Permissions
By the Directory Migration Agent to run	In Migration Manager for Active Directory (Microsoft Office 365) console when installing a DMA instance. This account can be later changed by modifying the DMA instance settings.	**Full Control** permission in ADAM/AD LDS project.

Active Directory account

Used To (By)	Where Specified	Rights and Permissions
By the Directory Migration Agent to connect to the source Active Directory domain	In Migration Manager for Active Directory (Microsoft Office 365) console when creating and configuring a domain pair or a connection.	Membership in the **Domain Admins** group. If this is not possible, or in case you use a single administrative account for source and target domains: • **Full Control** permissions on the Domain partition via ADSIEdit (ensure those permission are propagated/inherited) • **Read** permissions on the Configuration partition via ADSIEdit (ensure those permission are propagated/inherited) Note that a **Domain Admin** account should not be used as an Exchange account as it conflicts with the default Exchange security model (**Domain Admins** group has **Deny** for **Send As** and **Receive As**).

Office 365 administrative account

Used To (By)	Where Specified	Rights and Permissions
By the Directory Migration Agent to access Microsoft Office 365	In Migration Manager for Active Directory (Microsoft Office 365) console when creating and configuring a domain pair or a connection.	The **Exchange Administrator**, **User Management Administrator** user roles, **ApplicationImpersonation** and **Mail Recipients** roles in Microsoft Office 365. **IMPORTANT**: An Exchange Online license must be assigned to this account. This account must have the default UPN suffix <tenant_name>.onmicrosoft.com.

Accounts Required for Migration Manager for Exchange Operation

Exchange account

Used To (By)	Where Specified	Rights and Permissions
Access local mailboxes and mail during migration to Microsoft Office 365	On the **General>Connection** page of the source Exchange server **Properties** in the Migration Manager for Exchange console	See the Source Accounts Used by Migration Manager for Exchange Agents topic.

Active Directory account

Used To (By)	Where Specified	Rights and Permissions
Work with the source Active Directory	On the **General>Associated domain controller** page of the source Exchange server **Properties** in the Migration Manager for Exchange console	See the Source Accounts Used by Migration Manager for Exchange Agents topic.

Office 365 administrative account

Used To (By)	Where Specified	Rights and Permissions
By Migration Agent for Exchange to access the corresponding Microsoft Office 365 tenant	For mailbox and calendar synchronization: during an Office 365 mailbox migration or calendar synchronization collection creation in the Migration Manager for Exchange console	• **User Management Administrator** account • **ApplicationImpersonation** role • **Mail Recipients** role • Microsoft Exchange Online license • Default UPN
By legacy Migration Manager for Exchange agents to synchronize public folders with Office 365	For public folder synchronization: when adding Office 365 tenant in the Migration Manager for Exchange console	• **User Management Administrator** account • **ApplicationImpersonation** role • **Mail Recipients** role • Microsoft Exchange Online license • Default UPN • The account should be associated with the primary hierarchy public folder mailbox • The account should be granted by **Owner** permissions on all public folders

NOTE: Rights and permissions for the agent host account used by Migration Agent for Exchange (MAgE) are listed in Agent Host Account Used by Migration Agent for Exchange (MAgE) topic.

Refer to the Migrating to Microsoft Office 365 document for more details.

Account Required for Migration Manager to Access Tenant Data

Migration Manager for Active Directory (Office 365) uses Microsoft Graph API to access Azure Active Directory. Administrative consent is required in order to grant the "Quest Migration Manager for Active Directory" application access to the tenant data.

Microsoft Graph account

Used To (By)	Where Specified	Rights and Permissions
Grant the application access to the tenant data.	Consent can be granted at the time of adding a Migration Pair or in advance using this hyperlink https://login.microsoftonline.com/###-####-###-####/adminconsent?client_id=8edd986e-2f01-4f62-84d2-34576b05fc01 where ###-#####-###-##### must be replaced with an actual tenant id (which can be obtained via the Azure Admin console).	• **Global Administrator** or **Privileged Role Administrator** role • Once the Application has been granted access, the Migration Manager service account can function with the following minimal set of roles: • For Matching only: **Exchange Administrator** role • For Migration, the following minimal set of roles: **Exchange Administrator**, **Directory Readers**, **Directory Writers**

Accounts Used by RUM Agent Service

Migration Manager RUM Agent service account

Used To (By)	Where Specified	Rights and Permissions
Run the Migration Manager RUM Agent service on the computers to be processed	For Migration Manager RUM agents installed using the Resource Updating Manager console, the **Project | Manage Domains Credentials** option should be used. If the account is not specified, the **Local System** account (default) is used. When creating agents setup to deploy agents using Group Policy or SMS, specify this account using the **Project | Create Agent Setup** option in the Resource Updating Manager console menu. If the account is not specified, the **Local System** account (default) is used.	You can use either the **Local System** account (default) or a specified account. If you specify an account explicitly, make sure that it has sufficient privileges to create and remove computer accounts as part of the move operation. One way to do this is to give the account administrative rights in both the source and target domains (membership in the **Domain Admins** group of the source domain and in the domain local **Administrators** group of the target domain, or vice versa). However, if you prefer privileges to be more granular, you can give the account the following specific permissions: • **Create All Child Objects** on the target domain object • **Delete All Child Objects** on the source domain object **IMPORTANT**: If computer running Migration Manager RUM Controller Service (in fact, computer running Migration Manager console) and computers running Migration Manager RUM Agent Service (workstations and servers to be processed) are located in different domains of different forests without trusts established between them then you should specify account for Migration Manager RUM Agent service account explicitly. The **Local System** account (default) cannot be used.

Accounts Used by RUM Controller Service

Migration Manager RUM Controller service account

Used To (By)	Where Specified	Rights and Permissions
• Run the Migration Manager RUM Controller Service on the console computer • Access a computer to install or uninstall the Resource Updating Agent (only if no other account is explicitly specified for domain using the **Project | Manage Domains Credentials** option in the Resource Updating Manager console menu)	**Project | Manage Controller Credentials** option in the Resource Updating Manager console menu.	• Must be a member of the local **Administrators** group on the computer running the Resource Updating Manager. • Must have **Full Admin** access rights on ADAM/AD LDS database.

Local account

Used To (By)	Where Specified	Rights and Permissions
This account must be created only if computer running Migration Manager RUM Controller Service (in fact, computer running Migration Manager console) and computers running Migration Manager RUM Agent Service (workstations and servers to be processed) are located in different domains of different forests without trusts established between them.	On computer running Migration Manager RUM Controller Service. Create local account with the same name and password as Migration Manager RUM Agent service account has.	Must be a member of the local **Administrators** group on the computer running the Resource Updating Manager.

Account Used by Statistics Collection Agent Service

Statistics Collection Agent service account

Description	Where Specified	Rights and Permissions
Used to start and run the Statistics Collection Agent service on the server where the agent is installed	During Statistics Collection Agent setup	• Member of the local **Administrators** group on the server where the agent is installed • **Log on as a service** right enabled on the server on which the agent is installed. To verify that this right is granted, do the following: 1. Start the **Local Security Settings** snap-in. 2. In the left pane, select **User Rights Assignment** under the **Local Policies** node. 3. Double-click the **Log on as a service** right in the right pane. Verify that the Statistics Collection Agent service account is in the list of accounts that are granted the right. If it is not, add it.

NOTE: The Statistics Collection Agent service account can be changed on the **Server** page of the **Statistics Collection Agent Properties** dialog box.

Accounts Used by Statistics Portal Accounts

The account used to configure the Statistics Portal from the **Open Project Wizard** must be a member of local **Administrators** group on the IIS server on which the portal is installed.

Statistics Portal account to connect to ADAM/AD LDS project partition

Description	Where Specified	Rights and Permissions
Used to connect to ADAM/AD LDS	When you configure Statistics Portal (create a new portal configuration)	Requires **Full Control** rights in the project.

Statistics Portal account to connect to the SQL configuration database

Description	Where Specified	Rights and Permissions
Used to connect to the SQL configuration database to read the statistical information	When you configure Statistics Portal (create a new portal configuration)	At least the **db_datareader** role on the configuration database. **IMPORTANT**: Only SQL Server authentication is supported for this operation by the Statistics Portal Server. AD-integrated authentication (Windows authentication) is not supported.

IMPORTANT: To see statistical information on a particular directory or Exchange synchronization job or on a resource processing task, a user must be delegated at least the **Reader** role at the Migration Project, Directory Migration, or domain pair node in the migration project, regardless of whether a delegated migration task for that user has been created. For more information on Migration Manager delegation model, refer to the *Delegating Migration Tasks* section of the ***Migration Manager for Active Directory User Guide***.

Accounts and Rights Required for Active Directory Migration Tasks

Migration Manager for Active Directory requires administrative access for the source and target domains, processed servers, and workstations.

Migration Manager for Active Directory allows you to use different administrative accounts to access domains and computers involved in migration. For directory migration and synchronization Migration Manager uses the source and the target Active Directory accounts to access the source and the target domains, respectively.

The table below shows what privileges each account must have. To learn how to set these permissions, please see Appendix. How to Set the Required Permissions for Active Directory Migration and Exchange environment preparation documents.

Directory migration

Accounts Involved	Requirements	How To Grant
Source and target Active Directory accounts	Administrative access to each source and target domain involved in Active Directory migration	We recommend that you to create a **new user account** for the migration activities in each source and target domain instead of using an existing one. Add these accounts to the domain's local **Administrators** group in the corresponding domains. For details, see Appendix. How to Set the Required Permissions for Active Directory Migrationand dedicated Exchange environment preparation documents.. **NOTE**: If you have established two-way trusts between each source and target domain or forest trust, you can grant this single account administrative access to each source and target domain. **IMPORTANT**: This powerful account must be maintained closely and should be deleted after the project is complete. It is recommended that this account be owned by one individual and one backup individual (or as few individuals as possible).

Distributed resource update

Accounts Involved	Requirements
The account used to update a computer	Member of the computer's local Administrators group
Migration Manager RUM Controller Service account	• Member of the local **Administrators** group on the computer running the Resource Updating Manager • **Full Admin** access rights on the ADAM/AD LDS database access rights on the ADAM/AD LDS database

Exchange update

Full Exchange Administrator role for the Exchange organization

Intraforest mailbox reconnection

Accounts Involved	Requirements
The account that the DSA uses to connect to the source domain	**Full Control** for the Exchange store where the reconnected mailboxes reside

SMS update

Accounts Involved	Requirements
The account used to process the SMS server	Administrative rights to all SMS classes

SQL update

Accounts Involved	Requirements
Account used to process SQL server	Member of the **sysadmin** role

SharePoint permissions processing

Accounts Involved	Requirements	How To Grant
The account used to reassign SharePoint permissions after migration	For SharePoint versions prior to 2010: • Member of the SharePoint administration group on SharePoint server • Member of the local **Administrators** group on the computer running the SharePoint permissions processing For SharePoint 2010:	How to specify the SharePoint administration group: 1. On the server that is running SharePoint Products, click **Start**, point to **Administrative Tools**, and then click **SharePoint Central Administration**. 2. Under **Security Configuration**, click **Set SharePoint administration group**. 3. In the **Group account name** box, type the domain group you want to allow to administer. 4. Click **OK**.

• Member of the **Farm Administrators** group on SharePoint server • **Full Control** permission on **User Profile Service Application** • Member of the local **Administrators** group on the computer running the SharePoint permissions processing	For more information about Central Administrator group for SharePoint, see the following Microsoft KB article: Managing the SharePoint Administration Group. How to add user account to the **Farm Administrators** group: 1. On the server that is running SharePoint Products, click **Start**, point to **Administrative Tools**, and then click **SharePoint Central Administration**. 2. Under **Security** click **Manage the farm administrators group**. 3. Expand the **New** menu, and then click **Add Users**. 4. On the **Add Users** page, in the **Add Users** section, specify user accounts which should be added to the **Farm Administrators** group. 5. Click **OK**. How to grant user account the **Full Control** permission on **User Profile Service Application**: 1. On the server that is running SharePoint Products, click **Start**, point to **Administrative Tools**, and then click **SharePoint Central Administration**. 2. Click **Application Management**. 3. Then click **Manage service applications**. 4. Select **User Profile Service Application**. 5. Click **Permission** and grant the **Full Control** permission to desired user account. 6. After that, click **Administrators** and grant the **Full Control** permission to the user account.

Accounts and Rights Required for Exchange Migration Tasks

This section lists the tasks that will be performed during Exchange migration, and names the required accounts.

Migration Manager for Exchange agents work with different servers on the network. They create and modify Exchange and Active Directory objects and work with mailboxes and public folders. To accomplish all these tasks, the agents must have the appropriate permissions.

Migration Manager for Exchange allows you to use different administrative accounts for different purposes. Exchange data is migrated by the Exchange agents, which use the Exchange and Active Directory accounts.

Enumerate source and target Exchange organizations (added to the migration project)

Accounts Involved	Requirements	How To Grant
Account intended to enumerate organizations (specified while adding source and target organizations to migration project; see the *Registering Source and Target Organizations* section of the *Migration Manager for Exchange User Guide* for details) **NOTE**: This account will be set by default as the **Exchange account**, **Active Directory account** and **Agent Host account** for all the Exchange servers in the registered organization for subsequent migration. If you do not want to change the Exchange account after the organization is registered for each server, grant this account the permissions required for Exchange migration.	**Read** access to Active Directory (sufficient to read the Exchange configuration)	To grant an account this permission, complete the following steps: 1. In the **Active Directory Users and Computers** snap-in, right-click the domain name, and then click **Properties** on the shortcut menu. 2. On the **Security** tab, click **Add** and select the account to which you wish to assign permissions. 3. Select the account name, and then enable **Allow** option for the **Read** permission in the **Permissions** box. 4. Click the **Advanced** button. In the **Advanced Security Settings** dialog, select the account you specified in step 2 and click **Edit**. 5. In the **Permissions Entry** dialog, select **This object and all child (descendant) objects** from the **Apply onto** drop-down list, and click **OK**. 6. Close the dialog boxes by clicking **OK**.

Migrate Exchange data (using Migration Manager for Exchange agents)

Accounts Involved	Requirements	How To Grant
Exchange and Active Directory accounts (source and target)	Rights and permissions sufficient to create and modify Exchange and Active Directory objects, to work with mailboxes and public folders, etc.	You can create a single administrative account that has all the required permissions. For step-by-step instructions on creating such an account, please see dedicated Exchange environment preparation documents.

Using the Exchange Processing Wizard with Exchange 2010 or Later

This section is relevant only for scenarios where migration to or from Exchange 2010 or later is a part of Active Directory migration.

- Processing Mailboxes and Public Folders
- Processing Mailbox and Public Folder Contents

Processing Mailboxes and Public Folders

Access to mailboxes and public folders

Rights and Permissions	Where Specified

The account should be a member of the **Domain Admins** or **Enterprise Admins** group (See the note below the table)
Alternatively, if you want to avoid granting such broad privileges, make the account a member of the **Organization Management** and **Public Folder Management** roles.
	To assign the roles to the account (<*User*>), run the following commands in the Exchange Management Shell:
	`Add-RoleGroupMember "Organization Management" -Member <User>`
	`Add-RoleGroupMember "Public Folder Management" -Member <User>`

Exchange impersonation (step 1)

Rights and Permissions	Where Specified
The **ApplicationImpersonation** role enables the Exchange processing user account to impersonate other users.	To enable the account (<*User*>) to impersonate all users in an organization, run the following in the Exchange Management Shell: `New-ManagementRoleAssignment -Name <AssignmentName> -Role ApplicationImpersonation -User <User>` See http://msdn.microsoft.com/en-us/library/bb204095.aspx for more details related to enabling Exchange impersonation, such as limiting the scope of users.

Exchange impersonation (step 2)

Rights and Permissions	Where Specified

In addition to enabling Exchange impersonation for an account, give it the necessary access privileges by granting the **ms-Exch-EPI-May-Impersonate** extended right.	To give the account (*<User>*) the right to impersonate all users on all Client Access Servers, run the following in the Exchange Management Shell:
	`Get-ExchangeServer | where {$_.IsClientAccessServer -eq $TRUE} | ForEach-Object {Add-ADPermission -Identity $_.distinguishedname -User ((Get-User -Identity <User>) | select-object).identity -extendedRight ms-Exch-EPI-Impersonation}`
	To give the account (*<User>*) permission to impersonate all accounts on all MailboxDatabases, run the following in the Exchange Management Shell:
	`Get-MailboxDatabase | ForEach-Object {Add-ADPermission -Identity $_.DistinguishedName -User <User> -ExtendedRights ms-Exch-EPI-May-Impersonate}`
	See http://msdn.microsoft.com/en-us/library/bb204095%28EXCHG.80%29.aspx for more details related to granting Exchange impersonation rights, such as narrowing the scope of accounts, servers and databases.

IMPORTANT: Since membership in the **Domain Admins** or **Enterprise Admins** group denies **Send As** and **Receive As** permissions, you cannot continue using single administrative account. In this case it is advised to create separate processing service account.

Processing Mailbox and Public Folder Contents

Operation	Rights and Permissions	Where Specified
Message sending	**Send A**s extended right.	Run the following in the Exchange Management Shell: `Add-ADPermission "Mailbox" -User <User> -Extendedrights "Send As"`
Message processing in other users' mailboxes	Full mailbox access rights.	Run the following in the Exchange Management Shell: `Add-MailboxPermission "Mailbox" -User <User> -AccessRights FullAccess`

Appendix. How to Set the Required Permissions for Active Directory Migration

This section will help you to set the permissions that are required by Migration Manager for Active Directory.

Set Administrative Access to Source and Target Domains

Migration Manager for Active Directory requires administrative access to each source and target domain involved in Active Directory migration.

We recommend that you to create a new user account for the migration activities in each source and target domain instead of using an existing one.

To grant the account administrative access to the Active Directory domain, add the account to the domain’s local **Administrators** group as follows:

1. In the **Active Directory Users and Computers** snap-in, right-click the user and select **Properties**.
2. Go to the **Member Of** tab and click **Add** to make the user a member of the domain local **Administrators** group.

If you have established two-way trusts between each source and target domain or forest trust, you can grant this single account administrative access to each source and target domain. This powerful account must be maintained closely and should be deleted after the project is complete. It is recommended that this account be owned by one individual and one backup individual (or as few individuals as possible).

About us

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Office 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now. 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