Quest® Archive Manager 5.9.6

Installation and Configuration Guide for Exchange

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 website (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 www.quest.com/legal.

Trademarks

Quest Software, Quest, and the Quest logo are trademarks and registered trademarks of Quest Software Inc. in the U.S.A. and other countries. For a complete list of Quest Software trademarks, please visit our website at www.quest.com/legal. All other trademarks, servicemarks, registered trademarks, and registered servicemarks are the property of their respective owners.

Legend

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

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

Archive Manager Installation and Configuration Guide for Exchange
Updated - February 2024
Software Version - 5.9.6

Contents

1

Deployment considerations for Exchange

Deployment models

Several different deployment options are available for Archive Manager, depending on organization size and type. The following information can be used to determine a basic specification for an Archive Manager solution, although each organization must be assessed for its own unique qualities and needs.

When estimating a configuration for a site, it is important to know:

- The number of sites and the number of users at each site
- The number of mail servers
- The bandwidth between each site

Single-site model

The single-site model is suitable for single-site organizations as well as for organizations with high-speed and low-use WAN connections.

Hardware sizing can be roughly estimated from the number of users. For detailed recommendations, see the Hardware recommendations chapter of this guide.

Sizing is also affected by the Archive Manager message policies applied to Exchange after Archive Manager is implemented. Specifically, hardware requirements will increase if messages are kept on the mail server for only short periods (for example, <15 days), since users will access the Archive Manager system far more extensively than if messages are kept 30 or 60 days.

NOTE: Large organizations and sites with comprehensive disaster recovery (DR) requirements need to consider clustering Microsoft SQL Server and Internet Information Services (IIS) if the archived information is deemed critical to the organization. The information within Archive Manager is a copy of current information and possibly all email information outside of the configured retention policy period; this may affect the requirements.

Multi-site model

The multi-site model can be used in organizations where WAN links are high speed and low utilization and the remote connected sites have 100 or fewer users.

To lower the bandwidth requirements even further from the default installation, Archive Manager can be configured to ‘Dataload’ email messages from the remote sites at preset times of the day.

If the remote sites already have email servers, the servers should be set up to journal locally in order to minimize bandwidth usage of the journaling process. In these cases, the Archive Manager Dataloader can be configured to retrieve the journaled messages from those sites overnight, thereby spreading network traffic over 24 hours instead of eight working hours.

Archive Manager provides the option of installing the Organizational form for ‘Stubbed’ messages. By not installing the form for Microsoft Outlook, the bandwidth requirements of Archive Manager are reduced further as email is not retrieved from the Archive Manager database when browsed via Microsoft Outlook; the email is retrieved only when a link in the message is selected.

Distributed model

The Archive Manager distributed model is best used when an organization has connected sites with more than 100 users at each, or low bandwidth connections with potentially fewer users.

To estimate the requirements of different site configurations, see the Hardware recommendations chapter of this guide.

Mixed model

Archive Manager can also be run as a combination of the preceding models. This is useful, for example, when the distributed model is not applicable, as with a satellite site of 50 users with no email server, which does not require a dedicated Archive Manager server.

Archive Manager can be considered a "thin client" solution because it uses a web browser for access.

By choosing not to use the installable Microsoft Exchange ’organizational form,’ the bandwidth requirements for Archive Manager’s "clientless" stubbing of message content can also be reduced considerably over the default installation, making Archive Manager highly effective in low-bandwidth environments.

Exchange journaling

Microsoft Exchange includes optional journaling features that can help an organization meet compliance standards, but that are not installed by default. The Pre-installation preparations chapter in this Guide suggests that you enable Exchange Journaling, and you can refer to Microsoft’s documentation for installation and configuration information.

Archive Manager lets you configure MAPI data loaders to offload messages from Exchange Journal mailboxes into Archive Manager. The installation procedures in this Guide include steps to configure MAPI data loaders for use with Exchange Journal folders, or you can later refer to the *Data Loaders* chapter of the Archive Manager *Administration Guide* for the procedure.

2

System requirements

Exchange messaging system

Microsoft Exchange, any of:

- Exchange Online
- 2019 CU1 - CU3
- 2019
- 2016 CU1 - CU14
- 2016
- 2013 CU1 - CU23
- 2013 SP1
- 2013
- 2010 SP3 RU5 - RU29

SQL Server

Enterprise or Standard edition, any of:

- Microsoft SQL Server, 32-bit or 64-bit version:
  - 2019
  - 2017
  - 2016 SP1- SP2
  - 2016

- 2014 SP1 - SP3
- 2014
- 2012 SP1 - SP4
- 2012

NOTE: Two Archive Manager databases should not be installed to the same SQL server instance. It is fine to install two Archive Manager databases to the same machine if the machine has two or more SQL Server instances running, and each will host a single Archive Manager database.

NOTE: If you are moving from one SQL server to another SQL server, the collation settings of the Aftermail_temp database and the Archive Manager database itself must match what existed when the Archive Manager database was first created. As long as the two settings are maintained as specified for Archive Manager, the SQL server that houses the Archive Manager database may have a different collation setting that may be needed for other purposes on that machine. The supported collation setting is: SQL_Latin1_General_CP1_CI_AS

NOTE: Use of the "sa" account for operational credentials during installation is not supported.

NOTE: Archive Manager supports AlwaysOn Availability Groups for SQL Server 2012 and later versions.

NOTE: Archive Manager supports TLS 1.2 for connections to SQL Server 2008 R2 SP3 and later versions.

NOTE: Make sure the compatibility level setting in your SQL Server is not lower than SQL Server 2008.

Active Directory services

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008
- Windows Server 2003

Archive Manager server operating system

Either:

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2 SP1 or RTM (will be deprecated in the next release)
- Windows Server 2008 SP2, 64-bit version (will be deprecated in the next release)

Please verify that your mail system requirements are supported on the desired operating system.

Prerequisites for servers running Archive Manager services and websites

Common prerequisites

Any prerequisites that are required for installation are installed automatically when you run the Archive Manager Setup Wizard to install Archive Manager. If you want to install the prerequisites software prior to running the installer, see the requirements below.

- Microsoft .NET Framework 3.5 SP1 must be pre-installed (before running the installer).
- Supported Archive Manager Server Operating System version. Please verify that your mail system requirements are supported on the desired operating system.
- Visual C++ 2012 Redistributable for Visual Studio 2012 Update 4: vcredist_x86.exe
- Visual C++ 2010 SP1 Redistributable Package: vcredist_x86.exe
- Microsoft .NET Framework 4.5.2
- SQL Native Client (sqlncli.msi). SQL Native Client 2005 or above is required.

To enable text-string searches and indexing of file attachments, you must install IFilters for the file types you want to search and index:

- Microsoft offers a free pack of IFilters for its Office 2010 file types at http://www.microsoft.com/en-us/download/details.aspx?id=17062, (link current as of this release). SP2 can be applied via Windows Update or downloaded at http://support.microsoft.com/kb/2687447. This Filter Pack includes IFilters for the following formats: .docx, .docm, .pptx, .pptm, .xlsx, .xlsm, .xlsb, .zip, .one, .vdx, .vsd, .vss, .vst, .vdx, .vsx, and .vtx.
- IFilters for earlier-version Office file extensions (.doc, .rtf, .xls, .ppt, etc.), and for .txt, .htm and .html files, are installed with Microsoft Windows, and so should already reside on the Archive Manager server. You can verify their installation, and track and manage your IFilters generally, with a third-party IFilter browser; several are available at little or no cost from independent vendors.
- Adobe bundles a copy of its PDF 32-bit iFilter with its free Adobe Reader 11 software, and offers a free PDF iFilter 64 11.0.01 as a separate download. It is recommended that you use Adobe version 11 PDF IFilters, or FoxIt IFilters.
- Installing Adobe Reader X uninstalls PDF iFilters, which then need to be reinstalled. For additional information, see www.adobe.com.

Prerequisites for servers running the Exchange Store Manager Service

- MAPI Support for Exchange Online:
  - Microsoft Outlook 2019 volume licensed (32-bit)
  - Microsoft Outlook 2013 SP1 (32-bit, requires KB3114941 and KB4022169)

- MAPI support for Exchange 2019, 2016, 2013 or 2010:
  - Microsoft Outlook 2019 volume licensed (32-bit)
  - Microsoft Outlook 2013 SP1 (32-bit, requires KB3114941 and KB4022169)
  - Microsoft Outlook 2013 (32-bit)

IMPORTANT: The update KB3114816 for Office and later versions (except KB3114941 and KB4022169) should NOT be installed for Outlook 2013 SP1 because they may crash the ESM service due to a bug from Microsoft.

Other considerations:

- When Exchange 2019, 2016 or 2013 works with Outlook 2019 or Outlook 2013 SP1 (32-bit, with KB3114941 and KB4022169 installed), and MAPI over HTTP is enabled on both ends:
  - The ESM service account must have full access permissions to the exported mailboxes. To grant full access, run the following command at the PowerShell command prompt on the Exchange server:

    ```
    Add-MailboxPermission -Identity <mailboxIdentity> -User <your Archive Manager user or group> -AccessRights FullAccess -InheritanceType All -AutoMapping $false
    ```

  - For the MAPI Journal Data Loader, the data loader service user account must have full access permissions to the journal mailbox.
- For the Exchange Store Manager (ESM), the service user account must have **Receive As** and **View Information Store Status** permissions to the mail store from which the ESM will export mailboxes.
- For the MAPI Journal Data Loader, the data loader service user account must have **Receive As** and **View Information Store Status** permissions to the mail store that contains the journal mailbox.
- In a parent/child domain configuration, if you are installing Archive Manager in the child domain, you must create two accounts: an Exchange Store Manager account in the child domain for the Archive Manager installation, and another Exchange Store Manager account in the parent domain.

Prerequisites for servers running the Lync Store Manager Service

NOTE: Archive Manager only supports archived conversations from Lync servers configured with the **Lync Server Archiving databases** option. Archive Manager does not support **Archiving using Microsoft Exchange integration**.

Install the corresponding administrative tools based on the Skype/Lync servers you want to archive.

IMPORTANT: Only one of the administrative tools can be installed per Archive Manager Services server. To support a mixed environment, you must run multiple instances of the Archive Manager Services server running instances of the Lync Store Manager Service.

- Install Skype for Business Server 2019 or 2015, Administrative Tools

  Please refer to the following for specific instructions: https://technet.microsoft.com/en-us/library/dn933921.aspx.
- Install Microsoft Lync Server 2013, Administrative Tools

  Please refer to the following for specific instructions: https://technet.microsoft.com/en-us/library/gg398665.aspx.
- Install Microsoft Lync Server 2010, Administrative Tools

  Please refer to the following for specific instructions: https://technet.microsoft.com/en-us/library/gg398665(v=ocs.14).aspx.

- PowerShell 3.0 or later versions.

Prerequisites for servers running the Active Directory Connector Service

- Microsoft Graph Powershell (for working with Office 365 only): Please install it with the Administrator Account, or Archive Manager Application Pool's identity. For more information about the accounts, see Archive Manager rights and permissions.
- ExchangeOnlineManagement (for working with Office 365 only): Please install it with the Administrator Account, or ADC Service Account. For more information about the accounts, see Archive Manager rights and permissions.
- PowerShell 3.0 or later versions

Prerequisites for servers running Archive Manager websites

- Microsoft Internet Information Services (IIS) version 10, 8.5, 8.0, 7.5 or 7.0.

  Certain role services are required to be manually selected and installed on the web server in order for the Archive Manager Website to run correctly. These roles include: Common HTTP Features; Static Content ; ASP.net; ASP; Basic Authentication; Windows Authentication; IIS Management Tools and Scripts; and IIS Management Console.
- Microsoft ASP.NET (component of Windows, any supported Windows version).
- Microsoft Graph Powershell (for working with Office 365 only): Please install it with the Administrator Account, or Archive Manager Application Pool's identity. For more information about the accounts, see Archive Manager rights and permissions.
- ExchangeOnlineManagement (for working with Office 365 only): Please install it with the Administrator Account, or Archive Manager Application Pool's identity. For more information about the accounts, see Archive Manager rights and permissions.
- PowerShell 3.0 or later versions.

The API web service endpoint can be configured to use Windows Authentication or Anonymous Authentication. When using Anonymous Authentication, the web service application performs security checks and authenticates the client using Basic Authentication (plain text user password authentication). When using Windows Authentication, IIS handles the authentication and provides the web service application with a confirmation of the authentication attempt.

When Archive Manager works in a pure Office 365 environment,

- Please do not change the authentication mode to Windows Authentication because no on-premises Windows logins will be archived by Archive Manager in this scenario.
- Users who have MFA (Multi-Factor Authentication) enabled in Office 365 cannot log in to the Archive Manager website, unless you have added the Archive Manager servers to Trusted IPs.

Prerequisites for Office 365 on-premise journaling

Archive Manager can archive emails for Office 365 through Journaling. This is set up in the following two steps:

1 Setup on-premise journaling for Office 365 users with a local Exchange email address.

2 Setup Archive Manager MAPI Data Loader for journal email address.

To setup on-premise journaling for Office 365:

1 Prepare a local Exchange email address as the journal email address.

2 Go to https://login.microsoftonline.com.

3 Login with your administrative account.

4 On the top left corner, click **View all my apps** to launch the view.

5 Select **Admin** to open the Admin center (preview) page. (Or under the text **Collaborate with Office Online**, select **Admin**).

6 Click the **Admin centers** menu in the left menu list to view all the apps.

7 Select **Exchange** to open the Exchange admin center page.

8 Click the **compliance management** menu in the left menu list to open the compliance management page.

9 Select the **journal rules** tab to open the journal rules view.

10 Delete any existing rule.

11 Click the **+** button to open the Journal Rule wizard.

12 In the **Send journal reports to:** textbox, enter the email address you prepared at the beginning of the procedure. Fill in other information as necessary and click **Save** to create the journal rule.

Once the journal rule is created, each message sent to/from users in the Office 365 tenant will have an envelope journal report sent to the email address you specified in the journal rule.

To setup Archive Manager MAPI Data Loader for journal email address, see Adding MAPI data loaders for Exchange Journal mailboxes on page 47.

After configuring the MAPI Data Loader, all messages in the journal email address will be exported by the MAPI Data Loader and loaded by the File System Data Loader to Archive Manager database.

Attachment store types

Some attachment store types are deprecated in Archive Manager for new installations. Existing customers on deprecated file storage types are fully supported till next release**.**

TIP: A full or nearly full attachment store can dramatically slow loading of the Archive Manager website due to disk-read bottlenecks. A minimum buffer of 300 MB free space on all attachment store volumes is recommended to preempt such performance issues.

Table 1. External store types

External storage type	Support status
File System	Supported.
NetApp SnapLock 7.2.4	Supported.
EMC Centera 4.2.1, 4.2, 4.1, 4.0, 3.1.4, or EMC Atmos 2.0	Supported.
Caringo CAStor 6.5.4	Supported.
Hedvig Distributed Storage Platform Version 3.7.1	Supported.

Client workstation

Stubbed message reconstruction using the Outlook Form requires the following:

- Microsoft Outlook for Office 365 ProPlus, **or**
- Microsoft Outlook 2019, **or**
- Microsoft Outlook 2016, 64-bit or 32-bit, running on Windows 10, 8.1, 8, or 7 SP1, **or**
- Microsoft Outlook 2013, 64-bit or 32-bit, running on Windows 10, 8.1, 8, or 7, **or**
- Microsoft Outlook 2010, 64-bit or 32-bit, running on Windows 10, 8, 7, or Vista SP1

The Offline Client requires the following:

- Microsoft Outlook for Office 365 ProPlus, **or**
- Microsoft Outlook 2019, **or**
- Microsoft Outlook 2016, 64-bit or 32-bit, running on Windows 10, 8.1, 8, or 7 SP1, **or**
- Microsoft Outlook 2013, 64-bit or 32-bit, running on Windows 10, 8.1, 8, or 7, **or**
- Microsoft Outlook 2010, 64-bit or 32-bit, running on Windows 10, 8, 7, or Vista SP1, **and**
- Windows Installer 3.1 or later (only for installation).
- Microsoft .NET Framework Version 4.5.2 and 3.5 SP1.
- Microsoft SQL Server Compact 4.0
- Visual Studio 2010 Tools for Office Runtime
- MSXML 6.0 SP1

The Search Exporter requires the following:

- Microsoft Outlook for Office 365 ProPlus, 32-bit, **or**
- Microsoft Outlook 2019, 32-bit only, **or**
- Microsoft Outlook 2016, 32-bit only, running on Windows 10, 8.1, 8, or 7 SP1, **or**
- Microsoft Outlook 2013, 32-bit only, running on Windows 10, 8.1, 8, or 7, **or**
- Microsoft Outlook 2010, 32-bit only, running on Windows 10, 8, 7, or Vista SP1, **and**
- Windows Installer 3.1 or later (only for installation)
- Microsoft .NET Framework Version 4.5.2 and 3.5 SP1.

Web browsers

Any of:

- Microsoft Internet Explorer 11, 10 or 9

  NOTE: When using enhanced security on any server-based operating system, the Archive Manager website must be added to the list of trusted sites to work correctly.

- Microsoft Edge
- Firefox (latest version) running on Windows or Macintosh
- Chrome (latest version) running on Windows or Macintosh
- Safari running on Macintosh or mobile devices
- Android browsers

Archive Manager rights and permissions

- **Administrator Account:** The account you are logged in with when you run the Archive Manager Install program.
    - The user who runs the installer must be an administrator over the local computer, as well as on the SQL Server and the Exchange Server.
    - The account you specify during the installation must have the same permissions.
- **Service Account** (default account name is *ArchiveMgr_Service*): Specified in the configuration Console. Used by the Directory Connector, Alert Service, Full-Text Index, Full-Text Search and Message Retention Services. If no Journal dataloader is created at install time, then this account will be used for the Data Load Service too.
    - Account is granted full access to the Archive Manager and AfterMail_TEMP databases by the installer.
    - Requires read access to AD, and to the Exchange Organization so it can determine Storage Group information.
    - Must be in the Users group on the local machine, and a member of the local IIS_WPG group on the Web Servers. This is typically done by the installer.
    - Is a member of ArchiveManagerServiceUsers group.
    - You may want to add the service account to the Domain Administrators group. This will ensure that the Active Directory Connector has access to deleted user accounts for the purpose of disabling the accounts in Archive Manager. Or, Microsoft provides a program that grants Administrator rights on a per user basis. The utility is available at http://support.microsoft.com/kb/892806.
- **Journal Account** (default account name is *ArchiveMgr_Journal*): Specified after the Database Install/Upgrade in the installer. Used by the Dataloader. This is configured for use by the DataLoader only if a Journal DataLoader is configured. If Journaling is not present, then the ArchiveMgr_Service user is used.
    - Account requires "Receive-As" rights to any account nominated as a Journal Mailbox Account. This user must also be an Exchange View-Only Administrator.
    - Should be a Domain User; does not need to be an Administrator.
    - Is a member of ArchiveManagerServiceUsers group.
- **ESM Account** (default account name is *ArchiveMgr_ESM*): Specified after the Database Install/Upgrade in the installer. Used by the Exchange Store Manager Service.
    - Account needs access to all mailboxes; however this permission is granted to the group Archive Manager Exchange Admins, rather than to the account itself.
    - Should be a domain user; does not need to be an Administrator.
    - Is a member of ArchiveManagerServiceUsers group.
- **ArchiveManagerServiceUsers Group:** A Domain Group containing the Service, Journal and ESM accounts.
    - Group is used by installer to apply permissions to file-system locations used by Archive Manager.
- **Archive Manager Exchange Admins Group:** A Domain Group containing the ESM Account. Note that this group is ***not*** created by the installer, so must be created manually. It is recommended that this account be created *before* Archive Manager is installed.
    - Group must contain the ArchiveMgr_Service and ArchiveMgr_ESM users. If journaling is enabled on the Exchange Server and a MAPI DataLoader is required, then the ArchiveMgr_Journal user must also be added to this group. This group must be granted Exchange "Receive-As" permission on all mailboxes. Should also be a member of the Exchange View-Only Administrators group.

- If a new Exchange mailbox store is added after Archive Manager is installed, the permissions for this group must be set again. Otherwise, an error may occur when the ESM processes mailboxes in the new mailbox store.

3

Hardware recommendations

Archive Manager Services server

The services listed below are installed on the Archive Manager Services server. These services can also be spread among other server hardware:

- **Active Directory Connector (ADC):** The ADC synchronizes Archive Manager with users and security maintained in your existing Active Directory store.
- **Exchange Store Manager (ESM):** The ESM synchronizes Archive Manager with the current state of the enterprise's Exchange mail server.
- **Data Loader:** The Data Loader populates Archive Manager with email messages from the enterprise mail server and/or other data sources.

  TIP: Archive Manager supports multiple instances of Data Loader.

- **Search Service:** The Search Service consists of two separate services: **Full Text Index Service (FTI)** and **Full Text Search Service (FTS)**. The Full Text Index Service indexes the full text of messages within the Archive Manager store, storing security context as well, for high-speed full-text searches. The Full Text Search Service performs full-text searches against the Archive Manager Full Text Index, providing results to the Archive Manager core search engine.
- **Message Retention Policy Service:** The Retention Policy Service deletes email messages from the archive according to the retention rules and policies defined in the Retention Policy Editor.
- **Alert Service:** The Alert Service runs SQL queries on the Archive Manager database, and WMI queries on your server and sends Alert emails.
- **Website:** The Archive Manager website allows you to search your archive and administer various components of Archive Manager. The installer can place the Archive Manager website on a different server than the services server.

Archive Manager SQL database server

The Archive Manager SQL database server performs the following functions:

- The Archive Manager SQL database server hosts your the Archive Manager database, which contains all message and user data, except for attachments.

Archive Manager hardware recommendations

This following sections show the estimated hardware recommendations for Archive Manager Services server and SQL database server. These are minimum recommendations and are subject to change based upon your messaging environment. For operating systems and other software requirements, see the System requirements in this Guide.

SQL database server

SQL Server					~100 Msg/Day Per Mailbox	
Operating System	Microsoft Windows 2008R2 x64					
Light Access	**500 users**	**1000 users**	**2500 users**	**5000 users**	**7500 users**	**10,000+ users**
CPU (Total Cores)	4 x 2.4 GHz	4 x 2.4 GHz	4 x 2.4 GHz	8 x 3.0 GHz	8 x 3.0 GHz	8+ x 3.0 GHz
*Memory**	8 GB	8 GB	16 GB	16 GB	32 GB	64+ GB
Moderate Access	**500 users**	**1000 users**	**2500 users**	**5000 users**	**7500 users**	**10,000+ users**
CPU (Total Cores)	4 x 2.4 GHz	4 x 2.4 GHz	4 x 2.4 GHz	8 x 3.0 GHz	8 x 3.0 GHz	12+ x 3.0 GHz
*Memory**	16 GB	16 GB	32 GB	32 GB	64 GB	64+ GB
Heavy Access	**500 users**	**1000 users**	**2500 users**	**5000 users**	**7500 users**	**10,000+ users**
CPU (Total Cores)	4 x 2.4 GHz	4 x 2.4 GHz	4 x 3.0 GHz	8 x 3.0 GHz	8 x 3.2 GHz	16+ x 3.2 GHz
*Memory**	16 GB	16 GB	32 GB	64 GB	64 GB	64+ GB
Disk Configuration						
OS Disk	15K SCSI, RAID 1 or RAID 5					
SQL Temp DB	Can be placed on OS Disk					
*AM Database Data***	15K SCSI, RAID 0+1					
AM Database Logs	15K SCSI, RAID 1 or RAID 0+1					

- **Memory***: The total amount of required operating memory may be lower during initial archiving. As more data is archived and indexed, the memory footprint will increase.
- **AM Database Data**:** Database read/write speeds are key to Archive Manager performance. The faster the data can be read from the database, the faster a request is returned to the user.

Services server

Archive Manager Server						~100 Msg/Day Per Mailbox
Operating System	Microsoft Windows 2008R2 x64					
Light Access	**500 users**	**1000 users**	**2500 users**	**5000 users**	**7500 users**	**10,000+ users**
*CPU (Total Cores)**	4 x 2.4 GHz	4 x 2.4 GHz	4 x 2.4 GHz	8 x 3.0 GHz	8 x 3.0 GHz	12+ x 3.2 GHz
*Memory***	8 GB	8 GB	16 GB	16 GB	16 GB	32 GB
Moderate Access	**500 users**	**1000 users**	**2500 users**	**5000 users**	**7500 users**	**10,000+ users**
*CPU (Total Cores)**	4 x 2.4 GHz	4 x 2.4 GHz	4 x 2.4 GHz	8 x 3.0 GHz	8 x 3.2 GHz	16+ x 3.2 GHz
*Memory***	8 GB	16 GB	16 GB	16 GB	16 GB	32 GB
Heavy Access	**500 users**	**1000 users**	**2500 users**	**5000 users**	**7500 users**	**10,000+ users**
*CPU (Total Cores)**	4 x 2.4 GHz	4 x 2.4 GHz	4 x 3.0 GHz	8 x 3.2 GHz	8 x 3.2 GHz	16+ x 3.2 GHz
*Memory***	8 GB	16 GB	16 GB	16 GB	32 GB	32+ GB
Disk Configuration						
OS Disk	15K SCSI, RAID 1					
Work Disk	Can be placed on OS Disk					
*Index Disk(s)****	15K SCSI, RAID 0+1, 1+0, or 5					
*Attachment Disk*****	10K - 15K SCSI, RAID 5 or RAID 6					

- **CPU (Total Cores)***: The total amount of required CPU cores increases as the number of active threads increases. The store management service will export a single mailbox in a single thread. More active threads allow a faster ingestion rate. Full Text Index also has the ability to run multiple processing threads. The administrator needs to find the appropriate balance.
- **Memory****: The total amount of required operating memory may be lower during initial archiving. As more data is archived and indexed, the memory footprint will increase.
- **Index Disk(s)*****: The performance of the index disk will greatly impact the general performance of the product. For best results, use dedicated attached storage. New indexing technology allows the ability to span the index across multiple disk for both performance and fault tolerance.
- **Attachment Disk******: The performance of the attachment disk has less impact on the general performance of the product, but for the fastest retrievals, a faster disk is recommended.

NOTE: When running the 64-bit Archive Manager Full Text Search service, a minimum of 8 GB RAM is recommended. The total amount of memory recommended can be calculated by determining the disk space used by the indexes (messages + attachments) in GB, dividing that number by 100, and adding it to the 8 GB RAM minimum. For example, if the total space used for your indexes is 400 GB, then you should have (8 + 400/100) or 12 GB of RAM installed on your Archive Manager system.

Dedicated IIS server

Dedicated IIS Server*						~100 Msg/Day Per Mailbox
Operating System	Microsoft Windows 2008R2 x64					
Light Access	**500 users**	**1000 users**	**2500 users**	**5000 users**	**7500 users**	**10,000+ users**
*CPU (Total Cores)***	4 x 2.4 GHz	4 x 2.4 GHz	4 x 3.0 GHz	4 x 3.2 GHz	4 x 3.2 GHz	4+ x 3.2 GHz
Memory	4 GB	4 GB	4 GB	8 GB	8 GB	8 GB
Moderate Access	**500 users**	**1000 users**	**2500 users**	**5000 users**	**7500 users**	**10,000+ users**
*CPU (Total Cores)***	4 x 2.4 GHz	4 x 2.4 GHz	4 x 3.0 GHz	4 x 3.2 GHz	8 x 3.2 GHz	8+ x 3.2 GHz
Memory	4 GB	4 GB	4 GB	8 GB	8 GB	8 GB
Heavy Access	**500 users**	**1000 users**	**2500 users**	**5000 users**	**7500 users**	**10,000+ users**
*CPU (Total Cores)***	4 x 2.4 GHz	4 x 2.4 GHz	4 x 3.0 GHz	8 x 3.2 GHz	8 x 3.2 GHz	8+ x 3.2 GHz
Memory	4 GB	4 GB	4 GB	8 GB	8 GB	8+ GB
Disk Configuration						
*OS Disk****	10K - 15K SCSI, RAID 1					

- **Dedicated IIS Server*:** The IIS Server can host multiple instances of the Archive Manager website. The website also supports Network Load Balancing (NLB) with IP-based affinity. Multiple web servers can be configured to host multiple Archive Manager website instances.
- **CPU (Total Cores)**:** Total cores required will vary based on message policies. If stubbing is used, consider your environment moderate access or heavy access and plan accordingly.
- **OS Disk***:** The OS disk will store attachments temporarily while users are downloading them. Disk speeds are typically not a bottleneck.

Sizing the Microsoft SQL database and Archive Manager attachment store

Archive Manager's storage recommendations must be considered when planning storage, whether the data is to be stored on the same hardware as the software or stored on a separate high-speed disk. Specifically, there needs be either capacity for growth of archive data when Archive Manager is installed or the ability to increase capacity as the archive grows, or both.

IMPORTANT: For best performance, it is recommended that the full-text index files **not** reside on the same physical disk as other Archive Manager data repositories—neither the SQL database nor an attachment store.

The Archive Manager database must always be stored on high performance disks, such as a local SCSI RAID 5 disk (with as many physical spindles as possible), or a fast high-speed attached disk.

The Archive Manager attachment store may be stored on a slower disk to reduce cost, as archived attachment retrieval is not as speed-sensitive as a database.

Table 2. Archive Manager storage recommendations

Number of users	Number of messages (millions)	SQL Server database (GB)	Full Text Index	Attachment store (GB)
100	1	4	1.6	40
1,000	10	40	16	400
5,000	50	200	80	2,000
10,000	100	400	160	4,000

4

Pre-installation preparations

- Configuring the Archive Manager Services server
- Configuring the Archive Manager SQL database server
- Creating accounts and granting permissions
- Configuring the Exchange server for journaling
- Configuring and Registering a new Archive Manager application on Azure Portal
- Steps to Enable Secured Auto-logon on QAM Server

Before installing Archive Manager, complete the following pre-installation steps:

- Install the required prerequisites and configure the Archive Manager Services server.
- Set up and configure the Archive Manager database server.
- Create the accounts required for Archive Manager and grant permissions.
- Configure your Exchange server for journaling, if necessary.

NOTE: You can install Archive Manager Services and the Archive Manager SQL database on the same computer.

- Configure and Register a new Archive Manager application on Azure Portal
- Delete the previous instance of ESM-Automation task and the Quest-ESM-Automation folder as well

Each of these steps is explained in detail in the sections below.

Configuring the Archive Manager Services server

TIP: See the System requirements chapter for required versions of the components cited in this section,

To configure the Archive Manager Services server:

1. Update the server.
   Install the latest supported service pack levels for use with Archive Manager.
2. Configure your antivirus software.
   - Disable real-time scanning.
   - Prevent your antivirus software from scanning the Data Load directory and the Microsoft SQL Server database files.
   - Remove Antivirus scanning from the %temp% directory.
3. Configure your firewall.
   - If you are installing Archive Manager from a remote computer, open port 8686 for the Installation Wizard. The port should be opened during the installation session only.

- If you are planning to install web services and the Full-Text search service on separate computers, open port 8687 for the Archive Manager search service.
- Note that this is not the common configuration, but it is available if needed. If an application-level firewall is installed, the Archive Manager Full-Text Search Service must be allowed to listen on port 8687.

4 (Optional) Install IFilters.
Install third-party IFilters to enable searching attachment file formats. Searching and indexing of all attachment file types is enabled by the installation of particular IFilters for particular file types. See the System requirements chapter of this guide for more information about obtaining the IFilters you need.

5 (Optional) Create a DNS Entry.
Create a DNS entry for "ArchiveManager" that points to the Archive Manager web server. If necessary, refer to Microsoft's KnowledgeBase article #814591 (link current as of this document release) for more information.

Configuring the Archive Manager SQL database server

To configure the Archive Manager SQL database server:

1 Install Microsoft SQL Server.
Ensure the folder containing the database files is not compressed.

2 Configure the SQL Agent service.
Make sure the SQL Agent service is started and that its startup method is set to Automatic.

Creating accounts and granting permissions

Archive Manager requires the creation of several accounts and one group in Active Directory Users and Computers:

NOTE: When creating the accounts, remember to clear the **User must change password at next logon** check box and mark **Password never expires**.

Table 3. Account purposes

Account or group	Purpose
Exchange Storage Manager account (**ArchiveMgr_ESM**)	This account will be used to run the Exchange Store Manager Service. If you have a parent/child domain setup and are installing Archive Manager in the child domain, you need to create two accounts. An Exchange Store Manager account must be created in the child domain for the Archive Manager installation, and another Exchange Store Manager account must be created in the parent domain. Remember to make the account mailbox-enabled.
Archive Manager Service account (**ArchiveMgr_Service**)	This account will be used to run other Archive Manager services, the Web site, and any other processes that do not require specific access to Exchange.
Journaling account (**ArchiveMgr_Journal**)	This account will be used to access the journal mailbox. Remember to make the account mailbox-enabled.

Table 3. Account purposes

Account or group	Purpose
Global security group (ArchiveManagerServiceUsers)	This group will include the Exchange Storage Manager account and the Journaling account.
Archive Manager Exchange Admins Group	A Domain Group containing the ESM Account. Note that this group is not created by the installer, so must be created manually. This account should be created before Archive Manager is installed. Group must contain the ArchiveMgr_Service and Archive- Mgr_ESM users. If journaling is enabled on the Exchange Server and a MAPI DataLoader is required, then the ArchiveMgr_Journal user must also be added to this group. This group must be granted Exchange "Receive-As" permission on all mailboxes. Should also be a member of the Exchange View-Only Adminstra- tors group.

Granting permissions to the Exchange Admin group

Microsoft Exchange security needs to be configured in order to run the Archive Manager Exchange Store Manager Service and to export email from the current Exchange store into Archive Manager.

We recommend that you create the **Archive Manager Exchange Admin** group and grant permissions to the group; however, you can instead just grant the permissions to a user. The advantage to adding the permissions to a group is that you don't have to modify Exchange if you want to change the user; you can just add a user to or remove a user from the group.

Permissions can be granted at various levels within Exchange: at a site level, across multiple servers, on an individual server, or for a single mailbox.

To grant permissions in Exchange 2019, 2016, 2013 or 2010:

1. Add <*your Archive Manager user or group*> to the "View-Only Organization Management" role group.
2. Run this PowerShell command:

   ```
   get-mailboxdatabase | add-adpermission -extendedright receive-as -user <your Archive Manager user or group>.
   ```

NOTE: These permission changes may take quite some time to propagate. To speed the process, it may be worth restarting the Exchange Information Store service or rebooting the Exchange server.

NOTE: When Exchange 2019, 2016 or 2013 works with Outlook 2019 or Outlook 2013 SP1 (32-bit, with KB3114941 and KB4022169 installed), and MAPI over HTTP is enabled on both ends,

- The ESM service account must have full access permissions to the exported mailboxes. To grant full access, run the following command at the Exchange PowerShell command prompt:

  ```
  Add-MailboxPermission -Identity <mailboxIdentity> -User <your Archive Manager user or group> -AccessRights FullAccess -InheritanceType All -AutoMapping $false
  ```

To test your changes, go to a PC that has Microsoft Outlook installed and sign in as the user or a user in the group to which you granted permission. Try to add the new mailboxes that have been created to that user's profile. If the user is able to access those mailboxes, the security has been configured successfully.

Granting permissions to Lync Admin group

Microsoft Exchange security needs to be configured in order to run the Archive Manager Exchange Store Manager Service and to export email from the current Exchange store into Archive Manager.

To grant permissions in Skype for Business Server 2019, 2015, 2013 or 2010, add the Service Account to the following groups (default account name is ArchiveMgr_Service):

- CSAdministrator
- RTCHSUniversalServices
- RTCComponentUniversalServices
- RTCUniversalServerAdmins
- RTCUniversalConfigReplicator

Configuring the Exchange server for journaling

Journaling is not required for store management. If you intend to install Archive Manager with journaling, to capture messages to meet a legal standard of compliance, you can enable envelope journaling with Archive Manager. In that case, you must first turn on envelope journaling and then enable journaling for each mailbox store you want to journal.

Configuring Exchange 2019, 2016 or 2013

To configure Exchange 2019, 2016 or 2013:

1. Open the Exchange Management Shell.
2. Add your Archive Manager Service user account (ArchiveMgr_Service) to the "View-Only Organization Management" security role.

   Sample syntax:

```
>Add-RoleGroupMember "View-Only Organization Management" -Member <youruseraccount>
```

To create a Journal Mailbox in Exchange 2019, 2016 or 2013:

1. Create a new mailbox for Archive Manager on the Exchange Server. For example, name the mailbox **ArchiveMgr_Journal**.
2. Create a user mailbox object in the Microsoft Exchange Admin Center recipients page.

To implement Journaling Rules for Exchange 2019, 2016 or 2013:

1. Open the Exchange Admin Center to begin setting up journaling rules.
2. In the compliance management page, select the **Journal Rules** tab.
3. In the Actions pane, select **New.**
4. In the **Send Journal reports to email address** box, enter the name of the mailbox you created for journaling on the Exchange Server for Archive Manager. This refers to the ArchiveMgr_Journal mailbox created in the Create a Journal Mailbox section.
5. In the **Rule name** box, enter a name for the journal rule you are about to create.
6. In ***If the message is sent to or received from**, select **[Apply to all messages]**
7. In ***Journal the following messages …**, select **All Messages**.
8. Click **Save.**
9. In the warning “Do you want this rule to apply to all future messages? “, click **Yes**.

To configure the Hub Transport for Exchange 2019, 2016 or 2013:

To allow the Archive Manager Website to send email using SMTP through Exchange 2019, 2016 or 2013, you must configure the Hub Transport Receive Connector to accept anonymous connections.

Use the Exchange Admin Center Console (ECP) to perform this procedure:

1. In the **Mail Flow Configuration** page, select the **Receive Connectors** tab.
2. Double-click the default connector for the Exchange server, for which the role must be HubTransport.
3. Click the **Security** tab, and locate the **Permission Groups** area.
4. Check the **Anonymous users** check box.
5. Click **Save**.

Configuring Exchange 2010

To configure Exchange 2010:

1. Open the Exchange Management Shell.
2. Add your Archive Manager Service user account (ArchiveMgr_Service) to the "View-Only Organization Management" security role.

Sample syntax:

```
>Add-RoleGroupMember "View-Only Organization Management" -Member <youruseraccount>
```

To create a Journal Mailbox in Exchange 2010:

1. Create a new mailbox for Archive Manager on the Exchange Server. For example, name the mailbox ArchiveMgr_Journal.
2. Create a recipient object in the Microsoft Exchange Management Console. The recipient should be an Exchange 2010 mailbox set up specifically for journaling.

To implement Journaling Rules for Exchange 2010:

1. Open the Exchange Management Console to begin setting up journaling rules.
2. Under the Organization Configuration node, select **Hub Transport**.
3. In the **Hub Transport** page, select the **Journal Rules** tab.
4. In the **Actions** pane, select **New Journal Rule**.
5. In the **Rule name** box, enter a name for the journal rule you are about to create.
6. In the **Send Journal reports to email address** box, enter the name of the mailbox you created for journaling on the Exchange Server for Archive Manager.

   This refers to the ArchiveMgr Journal mailbox created in the Create a Journal Mailbox section.
7. In the **Scope** field, select **Global – all messages**.
8. Leave the **Journal messages for recipient** check box unchecked.
9. Check the **Enable Rule** check box to activate this journaling rule for the Exchange Server.
10. Click **New** to save your changes.
11. Click **Finish** to exit the New Journal Rule wizard.

To configure the Hub Transport for Exchange 2010:

To allow the Archive Manager Website to send email using SMTP through Exchange 2010, you must configure the Hub Transport Receive Connector to accept anonymous connections.

Use the Exchange Management Console (EMC) to perform this procedure:

1. Select the **Server Configuration | Hub Transport** node.
2. Double-click the default connector for the Exchange server that you will use as your SMTP server for the Archive Manager Website.
3. Click on the **Permission Groups** tab.
4. Check the **Anonymous users** check box.
5. Click **Apply**.

Configuring and Registering a new Archive Manager application on Azure Portal

To use OAuth (Modern Authentication):

To use OAuth (Modern Authentication), an application must have an application ID issued by Azure Active Directory. Since QAM is a console application, so the user needs to register the application as a public client with Azure Active Directory. The user can register an application in the Azure Active Directory admin center.

1. Open a browser and navigate to the Azure Active Directory admin center and login using the Global Admin Account for O365 tenant.
2. Select **Azure Active Directory** in the left navigation pane, then select **App registrations** under **Manage**.
3. Select **New registration**. On the Register an application page, set the values as follows:
   - Set Name to **Archive Manager**.
   - For **Redirect URI**, change the dropdown to **Public client (mobile & desktop)** and set the value to https://login.microsoftonline.com/common/oauth2/nativeclient
4. Choose **Register**. On the next page, copy the values of the **Application (client) ID** and **Directory (tenant) ID** and save them as the user will need them later.

Configure for delegated authentication

Use the following steps to pre-configure EWS permissions.

1. Select **Manifest** in the left-hand navigation under **Manage**.
2. Locate the requiredResourceAccess property in the manifest, and add the following inside the square brackets ([]):

```
{
   "resourceAppId": "00000002-0000-0ff1-ce00-000000000000",
   "resourceAccess":
[
   {
       "id": "3b5f3d61-589b-4a3c-a359-5dd4b5ee5bd5",
       "type": "Scope"
   }
]
}
```

3. Select **Save**.
4. Select **API permissions** under **Manage**. Confirm that the **EWS.AccessAsUser.All** permission is listed and grant Admin Consent for the same.

Steps to Enable Secured Auto-logon on QAM Server

TIP: See the System requirements chapter for required versions of the components cited in this section,

To enable the user to logon to the AM server automatically on start-up for Archiving to run in the background:

1. Navigate to the Archive Manager Installation Directory and locate Autologon.exe (Autologon64.exe is only for 64-bit OS).
2. Launch the Autologon.exe and enter the user credentials for the ESM Automation task and click **Enable**.

To lock the screen after logging in on server start-up for security purposes:

1. Navigate to the Archive Manager Installation Directory and locate **Secure.bat** file.
2. Copy **Secure.bat** file, go to **Run** and open **shell:startup**.
3. Paste the **Secure.bat** file to enable screen lock.

5

Installing and configuring Archive Manager

Installing Archive Manager

To access the installer for Archive Manager:

1. From the Archive Manager installation CD, run the **ArchiveManagerInstaller.msi** program.
2. Click the **Install** tab.
3. Under Product, click the **Archive Manager** link to run the installer.

NOTE: Please refer to the System requirements chapter of this guide prior to installing Archive Manager.

To install Archive Manager:

1. On the **Welcome to the Quest® Archive Manager Setup Wizard** screen, click **Next**.
2. On the **License** screen, scroll through the license agreement and then select the **I accept the terms of the license agreement** check box and click **Next** to continue.
3. On the **SQL Server settings** screen, enter the following information:
   a. **Server name:** The name of the SQL Server you plan to use.

      To specify a SQL Server availability group, enter the availability group listener name.

   b. In the **Log on to the server** section, select either **Use Windows Authentication** or **Use SQL Server Authentication** and specify credentials, if required. The authentication mode you specify will be used to install the Archive Manager database.

   c. **Database name:** Enter a name for the Archive Manager database.
4. Click **Next**. If no database exists, the following message is displayed:

   The specified database does not exist. Create it now?

   If a database does exist, you will be asked if you want to upgrade.
5. Click **Yes** to create a new database.
6. On the **Log folder** screen, click **Next** to install to the default log folder or click **Change...** to select another folder.

CAUTION: The Log folder should not be installed in the Archive Manager installation path.

7 On the **Destination Folder** screen, click **Next** to install to the default destination folder or click **Change...** to select another folder.

8 On the **Custom Setup** screen, select your environment and the product features to be installed. Each feature can be installed independently.

Product features include:

- Exchange Environment
  - Active Directory Connector
  - Exchange Store Manager
  - Lync Store Manager
- GroupWise Environment
  - GroupWise Directory Connector Service
  - GroupWise Store Manager Service
- Data Load Service
- Full Text Index and Search Service
- Message Retention Policy Service
- Alert Service
- Website

9 The **Features to Install** screen displays the features that you have selected for installation, and the prerequisite software that will also be installed. If the list is correct, click **Next**.

10 On the **Ready to install Quest® Archive Manager** screen, click **Install** to begin the installation. If you want to review or change any of your installation options prior to starting the installer, click **Back** to go to the previous screens.

11 The **Installing Quest® Archive Manager** screen provides installation status messages as the installation progresses.

12 The **Completed the Quest® Archive Manager Setup Wizard** screen is displayed when the installation has completed. The **Launch the Configuration Console when setup exits** check box is checked by default. If you do not want to go straight to the Configuration Console, deselect the check box.

If there were any problems installing the prerequisites, a **View Installation Warnings** check box is displayed. Select this check box to get detailed list of the installation warnings.

13 Click **Finish** to exit the setup wizard and launch the Configuration Console if you have selected to do so.

NOTE: If a SQL Server availability group has been specified when you install Archive Manager, you must add the databases `Archivemanager` (the one you specified in Step 3) and `Aftermail_TEMP` to the **Availability Databases** of the owner node after the installation. To check which is the owner node with **Failover Cluster Manager,** expand the cluster name, and click **Roles**.

Configuring Archive Manager

The Archive Manager Configuration Console allows you to configure the settings needed to begin using Archive Manager. The first time you configure Archive Manager, you must walk through the screens in order by clicking **Next** after each screen.

After completing the initial configuration, the Configuration Console will switch to an edit mode where any screen can be configured in any order. In edit mode, click **Apply** to save your settings.

Configuration pages are displayed only for the features that you selected during installation.

If you are upgrading from a previous version of Archive Manager, the settings are populated with your previous selections.

CAUTION: Configurable paths, such as Base Data Directory, Attachment Store, Index, or Export, should not be installed in the Archive Manager installation path.

1. The **Welcome** screen provides a list of information that you need to gather to configure Archive Manager. Review this list and click **Next** to begin configuring Archive Manager.
2. On the **License** screen, click **Browse...** to locate your license andclick **Install** to install it. You can overwrite an existing license by entering a new license and installing it. Once a valid license is installed, the following information is displayed:
   - **Type:** The type of license purchased.
   - **Expires:** The expiration date of the license.
   - **Seats Licensed:** The number of seats available from the license.
   - **Seats Used:** The number of seats currently used.

   License information can also be viewed at any time by clicking the Help icon and selecting the **Licenses** tab.
3. On the **Service User Credentials** screen, enter credentials for the following Archive Manager service users:
   - General Service User
   - Exchange Store Manager Service User
   - Journaling Service User
   - Archive Manager Administrative Group

   Use the default credentials or enter new credentials. If the service accounts exist you will need to confirm the password. If it does not exist, enter the password twice and the account will be created.
4. On the **General Settings** screen, enter the directory path for the base data directory and the log path.
   - **Base Data Directory: Directory Path:** The Base Data Directory path contains storage for errors, exclusions, exporting, and temporary storage for searching. Make sure to select a directory with adequate free space. Enter a directory for the Archive Manager base data directory. The default path is the following: C:\Quest\ArchiveManager
   - **Log Path: Directory Path:** Enter the path to the Archive Manager log folder. The default path is the following: C:\Quest\ArchiveManager\Logs\
5. On the **AD Connector** screen, configure the directory services. Click **None** to not enable archiving within any on-premises domains, and you will need to configure the Azure AD Connector on the next screen. Click **Simple** to enable archiving within the currently joined domain. Click **Advanced** to add multiple domains or specify a domain configuration. Click **Add** to access the **Directory Connector Setup** screen and configure the following screens. Click **Edit** to edit an existing directory connector, or **Remove** to remove an existing directory connector.
   Select the checkbox **Skip all domains above for ADC service** to NOT synchronize AD objects from the domains in the list above.

   When upgrading, the adc.config file will be discovered and imported into the settings.

   New Domain:
   - **NetBIOS Name:** The NetBIOS name of the target domain.
   - **Domain Topology:** Select one of the following options from the drop-down list. See Appendix C, *Active Directory Connector*, for a description of domain topologies.
     - Active Directory Single
     - Active Directory User/Resource Forest
     - Active Directory Lightweight Directory Services (AD LDS)

If you select **Active Directory Single**, enter the following information**:**

- **Server Address:** Specify either a domain (corp.company.com), or a host name (dc1.corp.company.com).
    - Use SSL: Select this check box to connect to the AD using LDAP over SSL.

You can also specify a protocol and port. For example, LDAP:\\corp.company.com:636.

- **Address Type:** Select one of the following:
    - Domain
    - Host
- **Require Additional Credentials:** If the domain that you are connecting to requires additional credentials, select this check box to provide an authentication method, username and password.
- **Authentication Method:** Select one of the following:
    - NTLM
    - Basic
- **Username (DOMAIN\Administrator):** The username used to connect to the domain.
- **Password:** The password for the user account used to connect to the domain.
- **Do Not Sync:**
    - **All AD objects from this domain:** Select this check box to NOT synchronize AD objects from the domain.

Advanced Configuration (Optional):

- **Search Base:** The root container for object discovery. For example: OU=America,DC=corp,DC=company,DC=com
- **Containers:** Restricts searches to the specified containers. For example, OU=Sales would search within the OU=Sales,OU=America,DC=corp,DC=company,DC=com search base.
- **Filters:** Provide LDAP filters for various object types. For example a User filter of (!cn=User1) would filter out anyone with a commonName of User1.
- **Import:** Select the **Users Without Mailboxes** check box to allow users without mailboxes to log in to Archive Manager.

Summary:

The **Summary** screen displays a list of the settings that you have selected. Review the settings and click **Finish** to set up the directory connector.

If you select **Active Directory User/Resource Forest**, enter configure the following pages.

Active Directory User Forest

- **Server Address:** Specify either a domain (corp.company.com), or a host name (dc1.corp.company.com).
    - Use SSL: Select this check box to connect to the AD using LDAP over SSL.

You can also specify a protocol and port. For example, LDAP:\\corp.company.com:636.

- **Address Type:** Select one of the following:
    - Domain
    - Host
- **Require Additional Credentials:** If the domain that you are connecting to requires additional credentials, select this check box to provide an authentication method, username and password.
- **Authentication Method:** Select one of the following:
    - NTLM

    - Basic
- **Username (DOMAIN\Administrator):** The username used to connect to the domain.
- **Password:** The password for the user account used to connect to the domain.

User Advanced:

- **Search Base:** The root container for object discovery. For example: OU=America,DC=corp,DC=company,DC=com
- **Containers:** Restricts searches to the specified containers. For example, OU=Sales would search within the organizational unit, Sales, relative to the search base. To add a container, type in the container name and click **Add**. To remove a container, select a container and click **Remove**.
- **Filters:** Provide LDAP filters for various object types. For example a User filter of **(!cn=User1)** would filter out anyone with a commonName of User1. To add a filter, select the type of filter from the drop-down list, enter a name for the filter, and click **Add**. To remove a filter, select the filter and click **Remove**.

Resource Forest:

- **Server Address:** Specify either a domain (corp.company.com), or a host name (dc1.corp.company.com).
    - Use SSL: Select this check box to connect to the AD using LDAP over SSL.

You can also specify a protocol and port. For example, LDAP:\\corp.company.com:636.

- **Address Type:** Select one of the following:
    - Domain
    - Host
- **Require Additional Credentials:** If the domain that you are connecting to requires additional credentials, select this check box to provide an authentication method, username and password.
- **Authentication Method:** Select one of the following:
    - NTLM
    - Basic
- **Username (DOMAIN\Administrator):** The username used to connect to the domain.
- **Password:** The password for the user account used to connect to the domain.

Resource Advanced:

- **Search Base:** The root container for object discovery. For example: OU=America,DC=corp,DC=company,DC=com
- **Containers:** Restricts searches to the specified containers. For example, **OU=Sales** would search within the organizational unit, Sales, relative to the search base. To add a container, type in the container name and click **Add**. To remove a container, select a container and click **Remove**.
- **Filters:** Provide LDAP filters for various object types. For example a User filter of **(!cn=User1)** would filter out anyone with a commonName of User1. To add a filter, select the type of filter from the drop-down list, enter a name for the filter, and click **Add**. To remove a filter, select the filter and click **Remove**.

Summary:

The **Summary** screen displays a list of the settings that you have selected. Review the settings and click **Finish** to set up the directory connector.

If you select **Active Directory Lightweight Directory Services (AD LDS)**, enter the following information**:**

Active Directory (AD LDS):

- **Server Address:** Specify either a domain (corp.company.com), or a host name (dc1.corp.company.com).

- Use SSL: Select this check box to connect to the AD using LDAP over SSL.

You can also specify a protocol and port. For example, LDAP:\\corp.company.com:636.

- **Address Type:** Select one of the following:
  - Domain
  - Host
- **Search Base:** The root container for object discovery. For example: OU=America,DC=corp,DC=company,DC=com
- **Import Users: AD LDS/ADAM Users:** Select the **AD LDS/ADAM Users** check box to import user accounts from the AD LDS directory.
- **Username (DOMAIN\Administrator):** The username used to connect to the domain.
- **Password:** The password for the user account used to connect to the domain.
- **Mail Server Display Name:** Enter a name to use for display on the Archive Manager website.

Advanced Configuration:

- **Containers:** Restricts searches to the specified containers. For example, **OU=Sales** would search within the organizational unit, Sales, relative to the search base. To add a container, type in the container name and click **Add**. To remove a container, select a container and click **Remove**.
- **Filters:** Provide LDAP filters for various object types. For example a User filter of **(!cn=User1)** would filter out anyone with a commonName of User1. To add a filter, select the type of filter from the drop-down list, enter a name for the filter, and click **Add**. To remove a filter, select the filter and click **Remove**.

Summary:

The **Summary** screen displays a list of the settings that you have selected. Review the settings and click **Finish** to set up the directory connector.

6 On the **Azure AD Connector** screen,

- **Archive from on-premises when object properties conflict with Office 365**: Select this checkbox to archive from on-premises for those users and groups migrated to Office 365.
- **Skip all tenants above for ADC service**: Select this checkbox to NOT synchronize Azure AD objects from the tenants in the list above.

Enter the following tenant information when you add or edit a tenant:

- **New Tenant**
  - **Tenant Name:** Enter the tenant name.
  - **Do Not Sync**
    - **All Azure AD objects from this tenant:** Select this checkbox to NOT synchronize Azure AD objects from the tenant.
- **Azure Active Directory:** Provide credentials to access your tenant.
  - **Authentication Method**: Select an authentication method. The default value is **Modern**.
  - **User Name/Password**: The credentials must have Recipient Management permissions, and have MFA (Multi-Factor Authentication) not enabled on Office 365 unless you have added the Archive Manager servers to Trusted IPs.
- **Advanced Configuration:** Configure the discovery options for the tenant.
  - **Service Provider:** Select your Office 365 service provider.
  - **Overridden URI:** If your Office 365 provider is "Office 365 US Government", please enter your own Exchange Online PowerShell URI. Otherwise, leave it empty.

- **Organization Unit**: This organization unit name is used to filter the Exchange Online mailboxes. To find all of the organization units, execute the following cmdlet from the Exchange Online PowerShell:

  ```
  Get-OrganizationalUnit -ResultSize unlimited
  ```

- **Filters:** Archive Manager uses PowerShell cmdlets to fetch users (`Get-AzureADUser`), groups (`Get-AzureADGroup`), and mailboxes (`Get-Mailbox`). Refer to the `Filter` parameter for each cmdlet.
- **Import Users without mailboxes**: Select this check box to allow users without mailboxes to log in to Archive Manager.
- **Import Migrated Office 365 objects not found on-premises**: Select this check box to allow Archive Manager to synchronize migrated users and groups that are not found in on-premises domain by SID (Security Identifier).

- **Hybrid Configuration:** Configure your on-premises Active Directory for a hybrid environment. See Step 5 for more information about the fields.
- **Summary:** This screen displays a list of the settings that you have selected. Review the settings and click **Finish** to set up the Azure AD Connector.

7 On the **Exchange Store Manager** screen, enter the directory path for the Exchange Store Manager Export folder, and select the Store Manager Group which you want the Exchange Store Manager to process on the local machine.

- **Export folder: Directory Path**: You can select a local path or a network share path to store the XML files that are exported by the Export Store Manager.

  This data can become quite large, depending on your settings. Select a directory with an adequate amount of space. The default path is the following: C:\Quest\ArchiveManager\Export.
- **Store Manager: Store Manager Group**: Select the Store Manager Group which you want the Exchange Store Manager to process. The selected group name can be configured on the Archive Manager website, in the Mail Servers page.

8 On the **Lync Store Manager** screen, enter the directory path for the Lync Store Manager Export folder, and select the Store Manager Group which you want the Lync Store Manager to process on the local machine.

- **Export folder: Directory Path**: You can select a local path or a network share path to store the XML files that export by the Lync Store Manager.

  This data can become quite large, depending on your settings. Select a directory with an adequate amount of space. The default path is the following: C:\Quest\ArchiveManager\Export.
- **Store Manager: Store Manager Group**: Select the Store manager group which you want the Lync Store Manager to process. The selected group name can be configured on the Archive Manager website, in the Lync Servers page.

9 On the **Data Loader** screen, select a data loader group from the drop down list to run in the server.

10 On the **SMTP Mail Server** screen, enter the information for the outgoing SMTP mail server:

- **Mail Server Name:** Enter the host name of the SMTP mail server. If your mail server requires SMTP authentication, enter the login details below. Leaving these fields blank forces Archive Manager not to authenticate.
- **Mail Server Port**: Enter the port number of the SMTP mail server. The default value is 25.
- **SMTP Login:** The login name for the mail server.
- **SMTP Password:** The password for the mail server.

If your mail server requires SSL to encrypt the connection, check the checkbox **Enable SSL for SMTP**; When it is checked, you have the option to **Trust All Certificates for SMTP**.

To send messages from a proxy server, check the checkbox **Send Messages from Proxy**.

11 On the **Website** screen, enter the settings for the Archive Manager website:

- **Website Name:** Name for the Archive Manager site.

- **Host Header:** Name of the server without the protocol prefix (without "http://" or "https://").
- **IP Address:** IP address of the web server.
- **Port:** Port number (default=80) for the Archive Manager web server.
- **Reset Password:** When upgrading from a previous version of Archive Manager, to reset the Admin account password, select the Reset Password check box and enter a new password.
- **Admin Password:** Password for the Archive Manager administrator. You cannot leave the password blank. Note that the Archive Administrator's login name is *Admin*, and this cannot be changed at the time of installation.
- **Confirm Password:** Re-enter the administrator password.

Secondary Websites: To add secondary websites, click **Add** under the Secondary Websites section. This opens the Secondary Website Setup screen. Enter the following information:

- **Website Name:** Name for the Archive Manager site.
- **Host Header:** Name of the server without the protocol prefix (without "http://" or "https://").
- **IP Address** IP address of the web server.
- **Port:** Port number for the Archive Manager web server.
- **Share main website files:** Archive Manager will use the same files on disk. Use this option if both instances of Archive Manager use the same authentication type (e.g., Windows or Forms).
- **Create separate files for this website:** Archive Manager will create a copy of the website files for the new website. Use this option if you need different authentication schemes for each of your website instances.

To edit a website, click **Edit...**. To remove a website, click **Remove**.

12 On the **Storage Location** screen, set up the location for the attachment store. Click **Add...** to access the Storage Location Type screen, then select an attachment store type and configure it.

File System or other storages deployed as a file system

a Select **File System** from the drop-down list and click **Next** to access the **File System Store Setup** screen and enter the following information.

- **Path:** Click **Browse** to select a path for the attachment store.
- **Network Share:** Enter the name of the share for the storage location.
- **Store message data for compliance:** Select this check box to save copies of all of the emails to be stored in external storage. This setting will apply to all storage locations.
- **Compliance Directory Path:** Enter a storage location path in this box. This can be an absolute path or a shared path with Full Control permissions to the Archive Manager Administrative Group.
- **Default Storage Location:** Select this check box to make the current storage location the default storage location.

b Click **Next** to access the **Summary** screen. This screen displays a list of the selected options.

EMC Centera

a Select **EMC Centera** from the drop-down list and click Next to access the EMC Centera Store Setup screen and enter the following information.

- **Connection String**: The connection string specifies the Centera device.
- **Store message data for compliance:** Select this check box to save copies of all of the emails to be stored in external storage. This setting will apply to all storage locations.
- **Default Storage Location:** Select this check box to make the current storage location the default storage location.

b Click **Next** to access the **Summary** screen. This screen displays a list of the selected options.

NetApp SnapLock

a Select **NetApp SnapLock** from the drop-down list and click Next to access the NetApp SnapLock Store Setup screen and enter the following information.

- **Share Name:** Enter the share name for the storage location.
- **Retention Mode:** Select **SnapLock Default** or **Archive Manager Default**.
- **Retention Time:** Enter the number of days, months, and years for retention. These settings are enabled only if you have selected **Archive Manager Default**.
- **Store message data for compliance:** Select this check box to save copies of all of the emails to be stored in external storage. This setting will apply to all storage locations.
- **Default Storage Location:** Select this check box to make the current storage location the default storage location.

b Click **Next** to access the **Summary** screen. This screen displays a list of the selected options.

Caringo DX

a Select **Caringo DX** from the drop-down list and click Next to access the Caringo DX Store Setup screen and enter the following information.

- **Hosts**: Enter the hosts to connect to. If there are multiple hosts, they should be entered in a comma-separated list.
- **Port**: The port to connect to.
- **Username**: The User Name to connect to the Caringo service.
- **Password**: The password for the account used to connect to the Caringo service.
- **Store message data for compliance:** Select this check box to save copies of all of the emails to be stored in external storage. This setting will apply to all storage locations.
- **Default Storage Location:** Select this check box to make the current storage location the default storage location.

b Click Next to access the **Caringo DX Advanced** configuration screen.

Caringo DX Advanced (Optional)

- **Cluster Name:** The name of the cluster for the Caringo DX storage location.
- **Proxy Address:** The cluster reverse proxy IP address.
- **Port:** The cluster reverse proxy access port.
- **Realm:** The Caringo security domain/realm.
- **Bucket:** The name of the container within the device.
- **Max Retries:** Maximum number of times to retry a command on a communication or server failure.
- **Max Stored Connections:** The maximum number of connections stored in the connection pool.
- **Pool Timeout:** The time in seconds that the connection pool will store an open connection.
- **Locator Retry Timeout:** The amount of time the locator should wait before retrying a previously discarded host address.
- **Hash Type:** The hash algorithm to use to verify content integrity.
- **Connection Timeout:** Time in seconds that a request will wait for a connection and for activity on a request.
- **Named:** Check to enable the use of Named objects. Uncheck to use automatically generated UUIDs (Unique User IDs).
- **Validate:** Check to enable content integrity verification.

        - **Replicate:** Check to enable immediate replication of objects as they are stored.

    c Click **Next** to access the **Summary** screen. This screen displays a list of the selected options.

13 On the **Full Text Index Setup** screen, the **Default Configuration** check box is selected by default. The Full Text Index will be sectioned into partitions based upon the default rollover policy. Using multiple (physical) hard disks may improve indexing and searching performance and is required for automatic index failover (recovery).

- **Index drives:** Select the drive(s) to use for indexing. Automatic index failover requires 2 or more drives to be selected.

14 On the **Outlook Form** screen, enter the following information.

The Outlook Form can be installed automatically if public folders are enabled and you have selected the **Install/Reinstall Outlook Form into Exchange Server** check box. If public folders are not enabled, the Outlook Form can be installed via the Archive Manager Outlook Components tool. See the Deploying the Outlook Form using the Archive Manager Outlook Components tool section. If the form is not installed, a user can easily access an archived message via a shortcut displayed in the body text of the stub.You can only install the Outlook Form for your on-premises Exchange servers, it will not apply to your Office 365 mailboxes.

- **Install/Reinstall Outlook Form into Exchange Server:** Select this check box to install or reinstall an Outlook Form and then select an Outlook Form from the drop-down list. If you have already installed the Outlook Form, you do not need to install it again. If you have upgraded to a new version of the product, select this check box to install a new version of the Outlook Form.
- **Mail Server:** Select the mail server you want to install the Outlook Form into and enter a delegate email address.
- **Same address for all mail servers:** Click this button to automatically populate all selected mail servers with the delegate address you entered.

15 The **Default Policy** screen displays tenants or mail servers that have been found with the directory connector settings entered previously. Enter the following information.

- **Create a default policy on tenants/servers defined below:** Select this check box to add a default message policy to the tenants or servers listed. Selecting this check box selects the entire server or tenant list. You may deselect individual tenants or servers.

16 On the **Advanced Settings** screen, configure the additional optional settings if needed. Click **Add** to add a configuration setting. Click **Remove** to remove a configuration setting. Click **Revert All** to go back to the original settings.

If you are doing an upgrade, your settings will be populated from the previous version of Archive Manager.

17 The **Summary** screen lists all of the settings you have entered. Click **Finish** to apply these settings in the Configuration Console.

18 Restart the Archive Manager servers.

Useful configuration settings

The following configuration settings can be added/edited in the Advanced Settings screen in the Configuration Console, if needed.

- General
- Archive Manager Database
- Autodiscover
- Active Directory Connector (ADC)
- Exchange Store Manager (ESM)
- Lync Store Manager (LSM)

- Data Loader
- Full Text Index (FTI)
- Full Text Search (FTS)
- Website
- ClientID
- TenantID
- Exchange Utility (EU)

General

- **AfterMail URL**: Sets Archive Manager website URL. This field should be auto filled by Configuration Console. If you have changed the website URL by IIS, change this setting accordingly.
- **CACHE TIME**: The time in minutes to keep the message and attachment search result in cache. The default value is 30 (minutes).
- **CommandTimeout**: The maximum time in seconds to execute a command. The default value is 600 (seconds).
- **Hosted Server Proxy Credentials Password Validity Days**: The default password validity period of proxy credentials for hosted mail servers. This setting applies to the proxy credentials without an expiration date specified when added. The default value is 80 (days).
- **Enable Delegate View Message**: This setting enables users to view messages in Archive Manager without permission check. When it is set to True, for example, a message that was originally forwarded as an attachment to a user will be visible in Archive Manager and can be opened by the user. The default value is False.

Archive Manager Database

- **CleanUpTime:** Deletes all of the old temporary "scratch" tables that the program generates for searches and other functions. The script defaults to running at 12:01:01 a.m. every day. This time is configurable. Since the Retention Engine also uses temporary tables, the CleanUp script should not be run at the same time as the Retention Engine. Most administrators choose to run the CleanUp script before the Retention Engine, which may occasionally run for prolonged time periods.

Autodiscover

Autodiscover is used to automatically configure a MAPI profile to connect to Exchange 2013 or later versions. By default, Archive Manager uses the internal client configuration for connections to Exchange 2013 or later versions.

- **Autodiscover Use External Mailbox Server:** To use Autodiscover's external client configuration, set this setting to **True**.
- **Autodiscover Override Settings:** Use this configuration setting if you want to override the Autodiscover response with user-defined values. This is useful for customers Basic Authentication. For example: AuthPackage=NTLM;ProxyServer=a.different.proxy.server.address.com;ProxyAuthScheme=NTLM
- **Autodiscover Prefer Mapi over Http**: Checks if MAPI over HTTP is enabled, and if enabled, tries to connect using MAPI over HTTP. The default value is `False`. When Exchange 2013 SP1 or later versions works with Outlook 2019 or Outlook 2013 SP1 (32-bit, with KB3114941 and KB4022169 installed), and MAPI over HTTP is enabled on both ends, this setting must be set to `True`.

  NOTE: This setting does not take effect for Exchange Online.

Active Directory Connector (ADC)

- **Directory Connector Timer Interval**: Sets the number of seconds that the Archive Manager ADC Service will stop before running again.The default value is 7200 (seconds).
- **Directory Connector Add Email Address To MailBox**: Links the email addresses from Active Directory to the mailbox accounts in Archive Manager. The default value is False.
- **Directory Connector Import Mailbox Permissions**: Imports customer-defined groups and user permissions to Archive Manager. The default value is False.
- **Directory Connector Disable Enable Store Manager Update**: Disables or enables mailbox Store Manager when ADC is synchronizing. The default value is False (disabled).
- **Directory Connector Disable Update Names**: Disables updating mailbox names when ADC is synchronizing. The default value is False (enabled).
- **Directory Connector Deactivate Legacy Logins**: Disables legacy logins if they have the same domain, account or email address with the ones of new logins.The default value is True.
- **Directory Connector Cleanup Resource Logins**: Cleans up logins for the linked mailboxes in resource forest. The default value is False.
- **Max Enable Store Manager MailBox Count Per O365 MailServer**: The maximum number of the mailboxes that have enabled Store Manager for each Office 365 mail server. The default value is 1000. For more information about the Office 365 mail server. see the Mail servers section in the Administration Guide.
- **Directory Connector UnSync Azure AD User LoginName Prefixes**: Filters out the users that will not be synchronized to the Archive Manager database by their name's prefix. The default value is "`DiscoverySearchMailbox;SystemMailbox_;Sync_;Exchange_Online;FederatedEmail.;Migration.;HealthMailbox`".
- **Directory Connector with GroupWise Mailbox**: When set to True, it tells ADC to fetch all the logins with an email address. Set this to True when you have GroupWise associated with Active Directory. The default value is False.
- **Directory Connector Identify Hosted Mailbox By Email Address**: This setting works in a hosted Exchange environment. When set to True, it tells ADC to identify mailboxes by email address. This will not create mailbox records for duplicated email addresses even if their object UIDs are different. Please make sure that no duplicated email address exists in your organization. The default value is True.
- **Directory Connector Sync EmailAddress From**: This setting works for on-premises AD only. It specifies the AD property where ADC synchronizes email address from. The property you specify must be of string type. The default value is `proxyAddresses`.
- **Max days to Cache MailBox Password**: The maximum days to cache hosted Exchange mailbox's password. The default value is 5 (days).

Additional Configuration of Active Directory Connector Service

The migration of ADC Service from Azure AD commands to Microsoft Graph PowerShell involves some steps to be configured as following:

1. **Uploading User Certificate**: User Certificate is being created by the QAM installer while upgrading/installing to 5.9.5 under ArchiveMgr_Service User. Login to the ArchiveMgr_Service User, locate the Certificate named "Archive Manager" at the Desktop Location. Login into the Azure Portal with the Admin Credentials, Locate the Archive Manager Application and under "Certificates & Secrets" section upload the certificate. Copy the Certificate Thumbprint generated.
2. **Updating API Permissions**: API Permissions needs to be updated with certain Microsoft Graph Permissions under API Permission tab in Archive Manager Application on Azure Portal. The permission

includes “User.Read.All”, “AccessReview.Read.All”, “Application.Read.All”, “Directory.Read.All”, “Group.Read.All”. Make sure to Grant Admin Consent for the Tenant.

3 **Add Configuration Key**: Enter the Configuration key, CertificateThumbprint with the thumbprint value.

Exchange Store Manager (ESM)

NOTE: ESM will be kept disabled 5.9.3 onwards. ESM through Windows Service will not result in Successful scanning of Mailboxes.

- **Exchange Store Manager Timer Interval:** Sets the number of seconds that the Archive Manager ESM Service will stop before running again.The default value is 90 (seconds)**.**
- **Exchange Store Manager Log Level:**
  - 0 - Error
  - 1 - Warn
  - 2 - Info (default)
  - 3 - Debug
- **Stub Display Message:** The notification that Archive Manager adds to a stubbed message in Outlook (notifying that the message has been stubbed). This notification can be customized with this configuration setting. Use [square brackets] to enclose the string that functions as a link to the message.
- **Exchange Store Manager Force Delete:** When set to True or 1, this setting forces the ESM to delete messages from Exchange even if the message can not be found in the Archive. This happens if a retention Delete policy has been run and the message is still in Exchange. This could also happen if the message has been excluded from the archive through exclusion rules. To be deleted, the message must meet the criteria of a delete policy. The default is False or 0.
- **Exchange Store Manager Max Thread Count:** Determines the number of Exchange mailboxes to which the Archive Manager ESM Service will connect simultaneously. If this value is not specified, it defaults to 1. The maximum allowed value is 13.

  We recommend that you experiment before implementing other settings in a production environment. Start by specifying a value of 2, and then increment the value one at a time until you achieve the desired result. Each thread consumes a significant portion of CPU processing capacity, so settings approaching 10 are almost always counterproductive.
- **Exchange Store Manager Max Thread Count Per Proxy Credentials**: The maximum number of mailboxes that Exchange Store Manager can process at the same time for each pair of proxy credentials. The default value is 3.

  This setting works with the setting **Exchange Store Manager Max Thread Count** to determine the maximum number of mailboxes that Exchange Store Manager can process at the same time. We recommend that the **Exchange Store Manager Max Thread Count** is lower than the **Exchange Store Manager Max Thread Count Per Proxy Credentials.**
- **Exchange Store Manager Only Stamp During Stripping:** Enables the ESM to only stamp attributes used by the ESM when they are needed, such as during stubbing. The default is 1 or True. True or False values can also be used for this setting.
- **Exchange Store Manager Strip IPM.Document:** When set to True or 1, this setting enables stubbing of IPM.Document items when they meet the criteria of a stubbing policy on the folder in which they reside. The default is False or 0.
- **ESMWorker Exclusion Paths**: A list of paths wherein any messages will not be archived by ESM or the Journal Data Loader. The default value is: “Contacts\Recipient Cache”. Additional paths must be separated by “; ”. Specify full paths from root folders (such as Inbox, Contacts, etc.). All sub-folders in a specified path are excluded.

  Note that ESMWorker uses ‘\’ to link the path names, but ‘\’ is a valid character in an outlook folder. If a specified exclusion path ends with a ‘\’, ESM Worker ignores it. (For example, ESMWorker treats “Inbox\ignorefolder\” as “Inbox\ignorefolder”.)

- **Exchange Ignore Message Classes:** This setting applies to all message policy actions. Message classes listed here are not eligible for any policy actions. Use "|" to separate multiple values. For example: "ipm.note.smime|ipm.note.secure.*".
- **Exchange Store Manager Worker Log Retention Days**: How many days the ESM worker logs will be kept in log folder. The default value is 7 (days).
- **Show Soft Delete Messages**: This setting determines whether ESM will scan the Recover Deleted Items (Tombstone) for the messages that have been Shift+Deleted from the mailbox or deleted from “Deleted Items” folder.
    - True (default): ESM will scan the Tombstone. If a message has been Shift+Deleted from the mailbox before ESM can scan it. ESM will scan it from Tombstone in next scan and link it to the “Deleted Items” folder.
    - False: ESM will not scan the Tombstone. If a message has been Shift+Deleted from the mailbox before ESM can scan it, ESM will never scan it.
- **Exchange Store Manager Use AutoDiscover**: This setting can be added and set to True to tell ESM to use Autodiscover for all mailboxes, including non-hosted mailboxes. The default is False.
- **Force Terminate MAPI Worker When Stopped**: Determines whether or not to Force Terminate hanging ESM Worker threads. Default value is False.

Lync Store Manager (LSM)

- **Lync Store Manager Timer Interval**: The time, in seconds, between LSM scans. The default value is 3600 (seconds).
- **LSM Export Delay Hours**: A time delay, in hours, after a conversation starts, before LSM processes the conversation. This delay is necessary because a conversation can only be exported after it is closed and saved (a Microsoft limitation). If LSM runs too soon, active conversations are missed. The default value is 12 (hours). This is the recommended minimum value.
- **LSM Failed Folder**: The location to put conversation files that the Data Loader failed to load. The default value is “<Base Data Directory>\LSMFailed”.

Data Loader

- **Dataload Timer Interval:** Sets the number of seconds that the data loader will stop before running through the enabled "Dataloaders" (within the Archive manager user interface), for example, MAPI, Filesystem etc. The default value is 60 (seconds), since the MAPI32 process must have time to unload before the Dataloader processes the Mailbox on its next run. A lower value may work better in some circumstances, but in most cases 60 seconds is the optimum interval.
- **DataLoad Service Max POP Message Size**: The maximum size in MB of message processed by the POP3 data loader. The default value is 50 (MB).
- **Dataload Process Rows**: The number of database records that the data loader will process in a batch. The default value is 2500.
- **Save Excluded Emails**: Save Excluded Emails is a Boolean (true or false) parameter that determines whether File System Data Loader will save all messages that match an exclusion rule to the Exclusion directory as XML. If this feature is enabled, it also will write some metadata to the Exclusion table in Archive Manager. The default value is True.
- **ExclusionDirectory**: Specifies the location to store the excluded XML files. The default value is *C:\Quest\ArchiveManager\Exclusion*.
- **ErrorPath**: Specifies the location to store the XML files that the File System Data Loader fails to load. The default value is *C:\Quest\ArchiveManager\Error.*
- **Data Loader Worker Log Retention Days**: How many days the logs of the MAPI data loader will be kept in the log folder. The default value is 7 (days).

- **Journal Data Loader Log Level**: The log level for the MAPI data loader.
  - 0 - Error
  - 1 - Warn
  - 2 - Info (default)
  - 3 - Debug
- **POP3 Timeout Seconds**: The maximum number of seconds for the POP3 data loader to process a single message. The default value is 3000 (seconds).
- **MAPI Data Loader Timeout Seconds**: Sets the number of seconds that data loader will stop when the ESMWorker hangs.The default value is 1800 (seconds).

Full Text Index (FTI)

- **Full Text Index Include Recipients:** Controls whether or not recipients are added to the Lucene index. The default is False. This setting has historically defaulted to false as the recipients are not searchable in Lucene, but are instead pulled from the Archive Manager database. This setting should remain false.
- **Full Text Index Max Field Length:** This setting can be used to increase or decrease the field length from the default of 100,000 for indexed terms in a single document.
- **Full Text Index Max Merge Docs:** This setting can be used to merge indexes into larger files, increasing search performance. The default is 1000000 documents per file.
- **Full Text Index Merge Factor:** This setting can be used to merge same-sized index files, increasing search performance. The default is 10 files.
- **FTI Max Buffered Docs:** Specifies how many documents Lucene can buffer in RAM before flushing them to an on-disk segment. If set to zero, flushing is triggered by size only, according to "Full Text Index Ram Buffer Size MB". The default is 0.
- **FTI Max Worker Count:** The max number of indexing workers the FTI can devote to a single partition. The default is 10.
- **FTI Max Total Indexer Threads:** Aggregate maximum total number of indexer threads the FTI is allowed to use. If "FTI Max Worker Count" times the number of active partitions exceeds this total, the FTI will scale back each partition's use of threads to try not to exceed this limit. No partition, no matter how low its IndexingPriority, will use less than 1 thread. The default value is 40.
- **FTI Commit Point Keep Count:** The number of Lucene index commit points to retain. This should only be increased above 1 if attempting to gather data on index corruption. The default is 1.
- **FTI Auto Failover:** Controls whether the FTI will initiate failover automatically. The default is True.
- **FTI Auto Repair:** Controls whether the FTI will initiate repair of corruption automatically. The default is True.
- **FTI Repair Auto Fix:** Controls whether the FTI will actually repair the corruption it identifies during a Repair operation. The default is True.
- **FTI Auto Itemize:** Controls whether the FTI will initiate itemize automatically after repair. The default is True.
- **FTI Itemize Auto Fix:** Controls whether the FTI will actually add FailedToIndex records for the items it identifies as missing during an Itemize operation. The default is True.
- **Full Text Index Ram Buffer Size MB:** Determines the amount of RAM that may be used when buffering added documents and deletions before they are flushed to the Directory. This setting corresponds directly to Lucene's SetRAMBufferSizeMB method. The default is disabled. Using the default setting is recommended.

Full Text Search (FTS)

- **Full Text Search Cache Time**: Determines the length of time, in minutes, that a Full Text Index search on the body of a message or attachment will be cached after it runs. The default value is 60 (minutes). The cache lets a user re-run the same search within the Cache Time limit, obtaining the same results, but much faster than if the search were re-run from scratch.
- **Full Text Max Results**: The maximum number of results that the FTS service retrieves. The default value is 5000.

Website

NOTE: You need to restart IIS after changing the value of these Website settings.

- **WWW Page Size**: Determines the number of search results displayed on a single page. The default is 20. This setting affects the entire instance and is not customizable per user.
- **WWW Show Source Properties**: Enables or disables the website to show the source properties of a message. The default value is False.
- **Include Sub Folders By Default**: Determines whether to include the sub folders by default when searching messages or attachments. The default value is False.
- **WWW Show SendToMe Button Only**: If it's set to True, the toolbar buttons **Reply**, **Reply to All** and **Forward** will be hidden when you view a message on the website. The default value is False.
- **EnableRemoteMailBoxDelegation**: Enables or disables the website page where users can configure delegation of hosted mailboxes. The default value is False.

ClientID

- **ClientID**: For manually registered application, you can enter this from the Azure portal shown also as Application ID or it will get populated automatically from the existing application or new application registered during ESM scan.

TenantID

- **TenantID**: For manually registered application, you can enter this from the Azure portal or it will get populated automatically from the existing application or new application registered during ESM scan.

Automation of Exchange Store Manager (ESM)

Exchange Store Manager will now be running through Task Scheduler. For the installation of the task Scheduler, follow below steps:

1. Go the Quest Archive Manager Installation Folder.
2. Locate the Application **TaskSchedulerCreation.exe**.
3. Double click on the .exe for the Task Scheduler to be created.
4. Open the **Task Scheduler** application. On the left panel, click on the Folder **Quest-ESM-Automation**. The Task named "**ESM-Automation**" will appear on the Right.

5 Right click on the "**ESM-Automation**", and click **Run** to initiate the scanning.

NOTE:
Admin rights are required to start the task in the Task Scheduler and modify the default time set.
The default configuration for the Task "ESM-Automation" is set to 1 Day indicating daily task trigger at the mentioned time. For Automated Manual Scan to run properly, ESM service needs to be disabled manually in the Services.

NOTE:
Force Terminate MAPI Worker When Stopped: Determines whether or not to Force Terminate hanging ESM Worker threads. Default value is False.

Exchange Utility (EU)

Exchange Utility Max Thread Count: Determines the number of Exchange mailboxes to which the Archive Manager Exchange Utility will connect simultaneously. If this value is not specified, it defaults to 10. The maximum you can set according to the number of mailboxes to increase the reconstruction and repairing speeds.

6

Upgrading/Uninstalling Archive Manager

CAUTION: Before upgrading or uninstalling Archive Manager, backup your databases, attachment files, export files, index files, log files and any non-program files located in the Archive Manager installation directory. Use the configuration console to obtain the location of these files.

Upgrading Archive Manager

When upgrading Archive Manager, please refer to the release notes for information on supported upgrade versions.

NOTE: When upgrading from version 4.8 to 5.0 or later, uninstall version 4.8 before performing the upgrade.

To upgrade Archive Manager:

1. Stop all Archive Manager services.
2. Run the Archive Manager Installer: **ArchiveManagerInstaller.msi**.
3. Perform an installation as described in the Installing Archive Manager section.
4. Run the Archive Manager Configuration Console to configure your Archive Manager settings. Some settings will be populated with information from your previous installation. These settings can be changed if needed. You will be prompted to enter any required information.
5. Restart the Archive Manager servers.

TIP: After upgrading to Archive Manager 5.1 or later, any mail items that are not associated with a folder will be will be placed in an _Orphans mailbox the first time the Retention service runs. If you wish to delete these items, set a Delete policy in the Retention Policies section of the Administration website.

Uninstalling Archive Manager

To uninstall Archive Manager:

1. Launch the Installer used to install the current version of Archive Manager.
2. Click **Next**.
3. Click **Remove**.

7

Post-installation tasks

Configuring and deploying the Offline Client (optional)

If you are using the Offline Client, the Administrator configures offline access and typically deploys the client through group policies. For information on configuring an deploying the offline client, see the *Download Tools* chapter of the Administration Guide.

TIP: If the volume of users will make the Offline Client load heavy, you can improve performance by deploying a separate dedicated IIS server for web services. That is, deploy a second, duplicate IIS Archive Manager server, then point users' Offline Clients to the web services component of the second, but leave the primary website URL set to the first, original server.

Deploying the Outlook Form (optional)

There are several methods for deploying the Outook Form:

- Deploy the Outook Form to public folders using Configuration Console.
- Deploy the Outlook Form to public folders manually.
- Deploy the Outlook Form by installing the Outlook Components tool via group policy.
- Deploy the Outlook Form by installing the Outlook Components tool manually.

Deploying the Outlook Form to public folders using Configuration Console

The Outlook Form is automatically deployed by the Archive Manager installer when public folders are enabled on the specified on-premises Exchange server, and the **Install Outlook form into Exchange** check box was selected when configuring Configuration Console. See the next section to deploy the Outlook Form when public folders are not enabled. The credentials used to install Outlook Form must be already added to the **Public Folder Management** group.

NOTE: Installing Outlook Form for Office 365 is not supported yet.

Deploying the Outlook Form to public folders manually

The Outlook Form can be deployed to public folders manually using the Archive Manager Exchange Utility. Please see the Exchange Utility chapter in the Archive Manager Administration Guide for instructions. The credentials used to install Outlook Form must be already added to the **Public Folder Management** group.

NOTE: Installing Outlook Form for Office 365 is not supported yet.

Deploying the Outlook Form using the Archive Manager Outlook Components tool

The Archive Manager Outlook Components tool is an add-in that installs the Outlook Form on users' computers when public folders are not enabled on the specified Exchange server. It will automatically install a copy of the form when a user launches Outlook. Therefore, it is only necessary to run this tool once per computer. It can be managed by Group Policy. For instructions on downloading and using the Outlook Components Too, see the *Outlook Components Tool* section of the *Download Tools* chapter of the Archive Manager Administration guide.

Adding MAPI data loaders for Exchange Journal mailboxes

Microsoft Exchange includes optional journaling features that can help an organization meet compliance standards, but that are not installed by default. Archive Manager lets you configure MAPI data loaders to offload messages from Exchange Journal mailbox(es) into Archive Manager.

The Pre-installation preparations chapter in this Guide suggests that you enable Exchange Journaling, and the installation procedures include steps to configure MAPI data loaders to offload messages from Exchange Journal mailbox(es) into Archive Manager.

If you did not enable Exchange Journaling during installation, you can refer to your Microsoft documentation to install and configure it now. If you did not configure MAPI data loaders in the original installation, you can refer to the *Data Loaders* chapter of the Archive Manager *Administration Guide* for the procedure.

Localizing Archive Manager website (optional)

Both the Archive Manager websites for end users and Administration can be localized using JSON files stored in the Archive Manager installation directory.

To localize the website for end users into your language:

1. In the directory *<ArchiveManager_Home>\WebSite\assets\language*, copy the file *en-US.JSON*, and paste it to the same folder.
2. Rename the copy file with your language code. For example, for French (France), rename it to *fr-fr.JSON*.

3 Translate your language file (For each line in the file, only edit the text between the quotation marks after the colon).

4 Restart IIS.

> **NOTE:** The display language of the website for end users is determined by the user's browser language, and English will be used if no resource file for the desired language can be found in the directory *<ArchiveManager_Home>\WebSite\assets\language*.

To localize the Administration website into your language:

1 Open the language file *<ArchiveManager_Home>\WebSite\Resource\Languages.xml*.

2 For each value code, add a new line with your language code as the culture name, and the translated text in your language.

3 Restart IIS.

> **NOTE:** The display language of Administration website is determined by the Archive Manager server language, and English will be used if no resource for the desired language can be found in the file *Languages.xml*.

Appendix A: Attachment store types

Attachment store types overview

Archive Manager supports different storage types for storing attachments and compliance messages. Details on using each of the storage types are provided below. The storage types supported by Archive Manager include:

- **NTFS / Windows File System:** This is the default option, and stores files on standard disk.
- **NetApp SnapLock:** SnapLock provides fast WORM (Write Once Read Many) storage on magnetic disk. It uses non-rewritable, non-erasable disk storage protects data until a specified retention date.
- **EMC Centera:** This option uses an external EMC Centera server or cluster to store the attachments.
- **Caringo CAStor/Dell DX:** This option uses a Caringo CAStor storage cluster or Dell DX Object Storage Platform to store attachments.
- **Hedvig Distributed Storage Platform:** Works with Archive Manager as the NTFS/Windows file system.

Archive Manager allows more than one type of storage to be used on a running system. However, only one storage location can be considered the default storage location at a time.

When installing Archive Manager, you set the attachment store type on the Attachment Store Type screen. Once the product is installed, additional attachment stores can be added. This process is described in the section Common scenarios for editing the configuration.

In all cases, Archive Manager stores each unique attachment as a single file or the equivalent unit. Archive Manager performs no compression or encryption. This is left to the underlying storage system.

Table 4. Attachment store types

External Storage Type	Archive Manager Version for Deprecation
File System	Supported.
NetApp SnapLock 7.2.4	Supported.
EMC Centera 4.2.1, 4.2, 4.1, 4.0, 3.1.4, or EMC Atmos 2.0	Supported.
Caringo Castor/Dell DX	Supported.
Hedvig Distributed Storage Platform Version 3.7.1	Supported.

NTFS/Windows file system

The file system is the default storage mechanism for Archive Manager. This is a directory structure, usually in *C:\ArchiveManager\Data*, with each file stored represented by its database id and file type. For example: 34.gif

These files are stored in blocks of 1000 files per directory. Each database ID has up to twelve 0's added to the front. For example, 34 becomes 000 000 000 034, and this is converted in a directory name:

```
c:\archivemanager\data\000\000\000\000\34.gif
```

By default, the entire tree, from c:\archivemanager\data down, is set to be compressed using NTFS compression. These files will not be rewritten, so any backup scheme can be used. It is recommended that you do an incremental backup.

NetApp SnapLock

The NetApp SnapLock Setup Wizard allows you to create volumes or WORMS on which Archive Manager can put attachment stores. The volumes containing attachment stores are an effective tool for compliance.

The NetApp SnapLock Wizard is run from the Archive Manager Installer. Run the installer during the installation process, unless you already have all the necessary volumes created.

NOTE: If a CIFS share is already in place, you can upgrade from a Windows file system attachment store to NetApp SnapLock by these two steps:

1. Copy the filesystem data folder (containing the archived attachments) to the NetApp CIFS share.
2. In the Archive Manager SQL database, StorageLocation Table: Change the connection string (originally in the form "DATA=\\archivemanagerserver\filesystemlocation") to point to the new CIFS share location (for example, "DATA=\\NetApp\data").

Prerequisites

- Install all of the necessary licenses for the NetApp Data ONTAP operating system.
- In DataONTAP, run the CIFS (Common Internet File System) setup. The CIFS shows the volume to the Windows system as a drive.

Running the NetApp SnapLock Setup wizard

The NetApp SnapLock Setup Wizard is run from the Archive Manager Installer. The NetApp SnapLock Configuration screen contains a Launch SnapLock Setup Wizard button. When you launch the wizard, fill in the information on the following screens:

Login Page

- **Create New SnapLock Volume:** Select this option to create a new volume.
- **Change Retention Times:** Select this option to change the default retention times. The settings here apply only if you select **SnapLock Default** as the retention mode in the Archive Manager Installer.
- **Filer Address:** IP name or address of the machine running Data ONTAP.
- **User Name:** Account name you want to use to access the machine running Data ONTAP. This account must be an Administrator account, preferably root.
- **Password:** Password for the account used to access the machine running Data ONTAP.

- **Volume Name:** Name of the volume you want to create on the machine running Data ONTAP. Or the name of the volume for which you want to change retention times. This name is case sensitive.

Volume Properties

- **New Volume Name:** Enter the name of the volume you wish to create.
- **Number of Disks to Use:** Enter the number of disks to use on the volume. Because it is a RAID configuration, this must be an even number.
- **Create Data Loader User:** Select this box if you are not using Active Directory and need to set up a Journal User for the data loader.
- **Data Loader Log-In User Name:** Enter the name for the Journal User that you are creating.
- **Data Loader Log-In User Password:** Enter the password you want to create for the Journal User.
- **Verify Password:** Retype the password.

Click **Next** to create the volume If this is a new setup, the volume will be created instantly. If this is an existing setup, the wizard will take some time to prepare the volume for use.

Retention Time

- **Current Retention Times:** Shows the current settings for the minimum time, default time, and maximum time.
- **Set Retention Time:** Enter a number for the minimum time, default time, and maximum time. Select days, months, or years from the drop-down list.

EMC Centera

The EMC Centera is supported for the storage of attachments and compliance messages. The native Centera API is used to store attachments in the Centera cluster. Archive Manager considers the Centera to be an "always-online blind storage system." Archive Manager presents an attachment, and then receives a “ticket”. To get the attachment back, Archive Manager presents the ticket and gets the attachment.

Archive Manager does not set any retention policies on the Centera. This is left to the Centera administrator.

Archive Manager supports any centera settings which can be set on the Centera connection string or in a PEA file.

Using a PEA File

When utilizing a PEA file with a Centera Configuration, it is important that the PEA file is accessible by each component that requires access to it. The Archive Manager components that will access the Centera, and therefore require access to the PEA file, are:

- Archive Data Load Service
- Archive Full-Text Index Service
- Website

As a result, the group *ArchiveManagerServiceUsers* should have permissions to access the PEA file location. The PEA file should also be present on all servers with the above Archive Manager components. (This is important if you have NLB WebServers, and/or a clustered Archive Manager installation).

If the machines are separate, then the PEA file must be either configured with a UNC path, or placed in the same local path as all machines that use the PEA file.

Caringo CAStor/Dell DX

The Caringo CAStor/Dell DX storage cluster is supported for the storage of attachments and compliance messages. The Caringo HTTP interface is used to store and retrieve items. Archive Manager considers the storage cluster to be an online blind storage system; we present an item, and receive a "ticket". To get the item back, we present the ticket and get the item. Note that performing a full text index reindex can overload the storage cluster with restore requests. Please consult Quest before doing this.

Hedvig Distributed Storage Platform

The Hedvig Distributed Storage Platform serves as a local file system when working with Archive Manager. For more information, see NTFS/Windows file system on page 50.

Common scenarios for editing the configuration

The following sections describe different scenarios for editing the configuration.

Using a NAS box

Archive Manager's installer does not support storing attachments on a NAS box, as software is installed on the box, which is most likely not running windows.

If you want to store attachments on a NAS box, use the following workaround:

1. When installing Archive Manager, set the services to NOT start after installation. Install using a normal filesystem storage location.
2. Once Archive Manager is installed, edit the StorageLocation table and change the default storage location to point to the UNC of the NAS box. For example: DATA=\\nasbox\archivemanagerstore
3. You must ensure that all Archive Manager users, *ArchiveMgr_Service, ArchiveMgr_ESM, ArchiveMgr_Journal*, have full access to that folder.
4. Start the services. They will now load and retrieve attachments from the NAS box.

Deleting attachments from a SnapLock volume

The Archive Manager Retention Engine cannot delete attachments from a Data ONTAP device unless the retention settings in SnapLock contain a retention time that precedes or is the same as the one set in the Retention Engine. The Retention Engine generates errors when the retention settings in SnapLock for attachments on a Data ONTAP device are set at a later time than the Archive Manager retention delete policy.

About us

Quest provides software solutions for the rapidly-changing world of enterprise IT. We help simplify the challenges caused by data explosion, cloud expansion, hybrid datacenters, security threats, and regulatory requirements. We are a global provider to 130,000 companies across 100 countries, including 95% of the Fortune 500 and 90% of the Global 1000. Since 1987, we have built a portfolio of solutions that now includes database management, data protection, identity and access management, Microsoft platform management, and unified endpoint management. With Quest, organizations spend less time on IT administration and more time on business innovation. For more information, visit www.quest.com.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request.
- View Knowledge Base articles.
- Sign up for product notifications.
- Download software and technical documentation.
- View how-to-videos.
- Engage in community discussions.
- Chat with support engineers online.
- View services to assist you with your product.