Quest® Archive Manager 5.11

Administration Guide

© 2026 Quest Software Inc.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

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

Quest Software Inc.
Attn: LEGAL Dept.
20 Enterprise, Suite 100,
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 Administration Guide
Updated - February 2026
Software Version - 5.11

Contents

Administration menu 9
General 9
Email Archiving 10
Lync Archiving 11
Reports 11

Authentication modes 12

Data loaders 13
About data loaders 13
Data loaders and Outlook message classes 15
Message processing 16
Add, edit or delete a data loader 16
Add a data loader 16
Edit a data loader 16
Delete a data loader 16

Download tools 18
About download tools 18
Search Exporter 18
Prerequisites 19
Installing and running the Search Exporter 19
Additional configuration options 19
Exporting data 20
Open exported search results 21
Outlook Components tool 21
Prerequisites 21
Installing the Outlook Components tool using a group policy 22
Recovery Manager for Exchange 23
Offline Client 24
Prerequisites 24
Downloading the Offline Client 24
Enabling offline access to the archive 24
Adding administrative templates 24
Deploying the Archive Manager Offline Client 26
Deploy using group policy 26
Outlook Web App (OWA) reconstruction tool 27
Limitations 27
Installing OWA reconstruction tool 27
URL Redirect 28
Prerequisites 28
Installation 28
Editing the RedirectConfig.xml file 29
Deploying the URL Redirect link 29

Logging in to the URL Redirect website . . . 29
Changing the Archive Manager server . . . 30
API and SDK . . . 30

Federated Search Instances . . . 31
About Federated Search Instances . . . 31
Adding Federated Search Instances . . . 31
Editing Federated Search Instances . . . 32
Performing searches on Federated Search Instances . . . 32
Troubleshooting . . . 32

Groups . . . 33
About groups . . . 33
Add, edit or delete a group . . . 33
Add a group . . . 33
Edit a group . . . 33
Delete a group . . . 35

Index management . . . 36
Overview . . . 36
Index topology . . . 36
Configuring the Full Text Index . . . 38
Index Dashboard . . . 38
Index Overview tab . . . 38
Message Index tab . . . 39
Attachment Index tab . . . 39
Work-In-Progress Index tab . . . 40
Deleted Index tab . . . 40
Partition set, shard, and details page . . . 40
Index Operation Log . . . 42
Index Rollover Policy . . . 43
Partition Locations . . . 43
Failover Mode . . . 44
Limit Type Settings . . . 44
Primary Indexing Schedule . . . 44
Primary Backup Settings . . . 44
Secondary Refresh Settings . . . 44

Logins . . . 45
About logins . . . 45
Using an Exchange login . . . 45
Using a GroupWise login . . . 46
Add, edit or delete a login . . . 46
Add a login . . . 46
Edit a login . . . 46
Delete a login . . . 48

Security roles . . . 50

About security roles . . . 50
Add, edit or delete a security role . . . 50
Add a security role . . . 50
Edit a security role . . . 51
Delete a security role . . . 51
Security actions . . . 51

Storage location . . . 55
Storage location and migration . . . 55
Prerequisites . . . 55
Storage Location tab . . . 55
Storage Migration tab . . . 57
Migration Status . . . 58
View Storage Migration History . . . 58

Message tags . . . 59
About message tags . . . 59
Add, edit or delete a message tag . . . 59
Add a message tag . . . 59
Edit a message tag . . . 60
Delete a message tag . . . 60

Proxy credentials . . . 61
About proxy credentials . . . 61
Add, edit or delete proxy credentials . . . 61

Alert Service Policies . . . 63
About Alert Service Policies . . . 63
Default Global Settings . . . 63
Adding an Alert Policy . . . 63
Modifying an Alert Policy . . . 64
Sample alert message . . . 64

Exclusion rules . . . 66
About exclusion rules . . . 66
Add, edit or delete an exclusion rule . . . 67
Add an exclusion rule . . . 67
Edit an exclusion rule . . . 67
Delete an exclusion rule . . . 67

Mail servers . . . 68
About mail servers . . . 68
Edit a mail server . . . 68

Mailbox assignment . . . 70
About mailbox assignment . . . 70
Select users . . . 70
Select mailboxes . . . 70

Mailboxes 71
About mailboxes 71
Add, edit or delete a mailbox 71
Add a mailbox 71
Edit a mailbox 72
Delete a mailbox 75

Lync servers 76
About Lync servers 76
Edit a Lync server 76

Lync user assignment 77
About Lync user assignment 77
Select users 77
Select Lync users 77

Lync users 78
About Lync users 78
Edit or delete a Lync user 78
Edit a Lync user 78

Reports 80
About reports 80
Mailbox Scan Status report 80
My Search Log report 81
Questionable Access report 81
Viewing your search results 81
Of All Email (by Specific Person) report 82
Of My Email (by Anyone) report 82
Search Log report 83
Viewing your search results 84
Storage Statistics report 84
Viewed Messages report 84
Delegation Log report 85
Delegation Status report 85
. 86

Message policies 87
About message policies 87
Message policies and deleted items 87
Add, edit, or delete a message policy 88
Add a message policy 89
Edit a message policy 90
Delete a message policy 90
Setting up archiving without journaling 90

Message policy assignments 92
About message policy assignments 92

To view the users associated with a message policy . . . 93
Associate users with a message policy . . . 93
Mailbox Search . . . 93
Group Search . . . 94
Message Policy Search . . . 94
Disassociate users from a message policy . . . 94

Retention policies . . . 95
Retention policy overview . . . 95
Retention policy tabs . . . 96
Policy Editor tab . . . 96
Adding a Keep Policy . . . 96
Adding a Delete Policy . . . 98
Editing Policies . . . 99
Removing Policies . . . 99
Execution Log tab . . . 100
Change Log tab . . . 101
Legal Hold tab . . . 101
Adding a Legal Hold . . . 102
Unlocking a Legal Hold . . . 102
Deleting a Legal Hold . . . 102
Schedule tab . . . 103
Settings tab . . . 103

Tenants . . . 104
About tenants . . . 104
Edit a tenant . . . 104

System maintenance . . . 105
About system maintenance . . . 105
Cleaning up "scratch" tables . . . 105
Cleaning up the AfterMail_Temp database . . . 105

Log Viewer . . . 106
About the Log Viewer . . . 106
Log Viewer menus and toolbar . . . 106
File menu . . . 106
Edit menu . . . 107
View menu . . . 107
Help menu . . . 107
How to 107
Configuring logs . . . 108
EventLogAppender . . . 108
TraceAppender . . . 108
RollingFileAppender . . . 109
ColoredConsoleAppender . . . 109
Additional information . . . 109

Exchange Utility 110
About the Exchange Utility 110
Install and run the Exchange Utility 110
Menu items 110
Get mailboxes 111
Create Outlook Archive Manager folder 111
Install Outlook Form 111
Update Archive Manager URL 112
Reconstruct stubbed messages 112
Update stubbed message checksums 112

Administering in a hosted Exchange environment 114
System requirements for running ESM in a hosted Exchange environment 114
Configuring ownership and access to user mailboxes on hosted Exchange 114
URL parameter 115
Agreement text 115
Auditing 115

Appendix A: Moving database or attachment store 116
Moving the database 116
Moving the attachment store 117

Appendix B: Enabling generating publisher evidence 118

About us 119

1

Administration menu

The Administration home page of the Archive Manager administration website displays the Administration menu. The Administration menu provides access to the following system management functions:

- General
- Email Archiving
- Lync Archiving
- Reports

General

Table 1. General

Icon	Function	Description
	Authentication Mode	Select the mode used for authenticating Archive Manager users.
	Data Loaders	Configure how messages are loaded into Archive Manager and the locations of those messages.
	Documentation	View all current Archive Manager documentation available for download.
	Download Tools	Display all the current Archive Manager tools available for download.
	Federated Search Instances	Create and update remote Archive Manager servers so they can be searched simultaneously.
	Groups	Create, update, and delete groups and memberships.
	Index Dashboard	View and configure Full Text Index partitions.
	Index Operation Log	View and search Full Text Index operation logs.
	Index Rollover Policy	View, create and configure rollover policies for message and attachment indices.
	Logins	Create, update, and delete user accounts.

Table 1. General

Icon	Function	Description
	Message Tags	Create, update, delete and define message or file tags and metadata to assign to email messages or file for easier retrieval of email or file data.
	Proxy Credentials	View and manage your proxy credentials.
	Security Roles	Create, update, and delete security settings for user groups.
	Storage Location	Configure storage locations and migrate attachments from one storage location to another.
	Support	Search all current Archive Manager knowledge base available for support.

Email Archiving

Table 2. Email Archiving

Icon	Function	Description
	Alert Service Policies	Manage alert service policies and configure global alert setting.
	Exclusion Rules	Create, update, and delete rules for managing messages.
	Mail Servers	Connect to and configure mail servers.
	Mailbox Assignment	Manage mailboxes and apply mailboxes to selected login.
	Mailboxes	Create, update, and delete mailboxes.
	Message Policies	Create, update, and delete policies for managing the mail server and the quantity and types of messages contained there.
	Policy Assignment	Manage message policies and apply policies to users and to the folders in their mailboxes.
	Retention Policies	Implement your retention policies.
	Tenants	View and manage the message policies, and enable or disable the Store Manager for your Office 365 tenants.

Lync Archiving

Table 3. Lync Archiving

Icon	Function	Description
	Lync Servers	Connect to and configure Lync servers.
	Lync User Assignment	Manage Lync users and apply Lync users to selected logins.
	Lync Users	Update and delete Lync Users.

Reports

Table 4. Reports

Icon	Function	Description
	Mailbox Scan Status	View the current status of mailbox scans.
	My Search Log	View details of searches performed during a specified date range.
	Questionable Access	View all questionable Archive Manager access during a specified date range.
	Search Log	View searches performed by an Archive Manager user, during a specified date range.
	Storage Statistics	View storage-related information about the Archive Manager system.
	Viewed Messages	View all messages viewed by an Archive Manager user during a specified date range.

2

Authentication modes

Archive Manager supports either Forms Authentication or Windows Authentication to provide secure access to the Archive Manager application:

- **Forms Authentication** uses an HTML-based form to process sign in information and is more suitable for providing access to Archive Manager over the Internet.
- **Windows Authentication** uses any security models established by using Microsoft Active Directory or Windows NT LAN Manager (NTLM). Windows Authentication is required to enable offline access to archived email with Microsoft Outlook. When running Windows Authentication with a Windows environment, multiple failed sign in attempts can lock out an Active Directory account. This specific number is dependent on the Default Domain Policy set on the Domain Controller:

  Computer Configuration | Windows Settings | Security Settings | Account Lockout Policy | Account lockout threshold

You must restart Internet Information Services (IIS) after changing the authentication mode between Forms and Windows.

3

Data loaders

- About data loaders
- Data loaders and Outlook message classes
- Message processing
- Add, edit or delete a data loader

About data loaders

The Data Loaders Administration section controls where the Archive Manager data loading service looks for email messages. There are five types of services:

NOTE: MAPI is the required service for a Microsoft Exchange server. IMAP4 and POP3 are not supported for Exchange. IMAP4 and POP3 Data Loaders will delete the original copy from the server.

Table 5. Data Loading Services

Data Loader Type	Description
File System	Reads messages directly from a file share. Reads files from the Export directory and loads the message data into the Archive Manager Database.
MAPI	Offloads messages from Exchange Journal mailboxes into the export directory and loads the journal envelopes into the Archive Manager database. Because the MAPI data loader does not link the processing messages to any folder or mailbox (JRDL will do that), only the Archive Manager administrators can access and search the messages before the JRDL processes them.
JRDL (Journal Report Data Loader)	Links messages referenced by the journal envelopes to the mailboxes of the sender and recipients. Before the JRDL processes the journal reports, messages can be only searched by the Archive Manager administrators after being processed by the MAPI data loader, because they are not linked to any folder or mailbox yet. JRDL will create a hidden folder named "JournalReports 4242150385DE48B285652A4D918B5C93" for each mailbox, and links each message to the folder, and to the mailboxes that match the email addresses of the sender and recipients in Journal Reports by the email addresses associated to the owner login and mailbox. The default JRDL is inactive when created by the Archive Manager installer, you will need to change it to **Active** when using the Lync Store Manager Service or MAPI Data Loader.
POP3	Offloads messages from POP3 Journal mailboxes into the export directory and loads the journal envelopes into the Archive Manager database. POP3 Data Loaders will delete the original copy from the server.
IMAP4	Offloads messages from IMAP4 Journal mailboxes into the export directory and loads the journal envelopes into the Archive Manager database. IMAP4 Data Loaders will delete the original copy from the server.

When you install Archive Manager, a File System data loader and a Journal Report data loader are installed. The Journal Report data loader is only used if you use one or more MAPI, POP3, or IMAP4 data loaders for journaling. You may need to add additional File System data loaders depending upon your environment.

TIP: Archive Manager supports multiple instances of Data Loader.

A data loader is characterized in Archive Manager by its **Type**, and by a **Start Time** and **End Time** to determine the time frame within which each data loader can start processing email. For example, if you enter a start time of 12:00 a.m. and an end time of 3:00 a.m. for a MAPI mail account, the data loader can start processing the journal mailbox anytime between 12:00 a.m. and 3:00 a.m. If the data loader completes processing the journal mailbox at 2:58 a.m., it will start over and process the entire journal mailbox again because 2:58 a.m. is within its time frame (**Start Time** and **End Time**) to start processing. The data loader will not stop processing at 3:00 a.m.

This can be useful in situations, for example, where email may be processed over a slow network link and you want to designate the time frame within which the data loader can start processing different mail accounts.

A MAPI data loader is used with an Exchange messaging system to offload messages from the Exchange Journal folder(s) into Archive Manager. Exchange's native journaling features consume a great deal of system resources, processing power as well as disk storage capacity, whereas Archive Manager handles data archives much more efficiently. You can dramatically improve overall system performance by using MAPI data loaders to continuously offload data from Exchange to Archive Manager.

NOTE: The Enable Store Management box is checked by default in Archive Manager in the mailbox for the journal user. This box must be **un**checked so that the mailbox is not processed by the Exchange Store Manager (ESM). Journal mailboxes should be processed by the MAPI loader.

The data loaders can be grouped by specifying a **Group** name so that you can select a group of data loaders to run in a server on Configuration Console. The default group name is `default`.

In addition to its **Type**, **Group**, **Start** and **End Time**, a data loader is defined in Archive Manager by several other field values that vary depending on its **Type**:

- File System:
  - **Name:** The friendly name that you want to call the data loader.
  - **Path:** The path from which the data can be loaded; this can be a defined drive letter or a UNC path.
  - **Active** (checkbox): Defines whether the data loader is active or inactive.
- MAPI:
  - **Name:** The friendly name of the mail server.
  - **Server:** The name of the mail server; for example, server.yourdomain.com
  - **User ID:** The login required by the server. For the MAPI data loader only the username (e.g. ArchiveMgr_Journal) is needed. This can be replaced with a Legacy Exchange Distinguished Name if there is a possibility of conflict or ambiguous names. The LEDN should be in the format: /o=Domain/ou=Exchange Admin Group/cn=Recipients/cn=ArchiveMgr_Journal.
  - **Password:** NO password is needed for this type of the data loader.
  - **Active** (checkbox): Defines whether the data loader is active or inactive.

  NOTE: If the MAPI data loader runs before the Active Directory Connector has synchronized the ArchiveMgr_Journal user into the Archive Manager database, the JDL will not find the user in the Archive Manager database and it reports the following error:

  ```
  Unable to obtain server DN for user 'WIN2K3ENT//o=First
  Organization/ou=Exchange Administrative Group
  ```

  NOTE: Once the Active Directory Connector finishes synchronizing, the error message will not display.
- JRDL:
  - No required attributes.
- POP3 or IMAP4:

- **Name:** The friendly name of the mail server.
- **Server:** The name of the mail server; for example, server.yourdomain.com.
- **User ID:** The name used to sign into the POP3/IMAP server. This is usually the username (e.g. JournalUser), but may need to contain the domain or other information, depending on the POP3/IMAP server. Please refer to your POP3/IMAP server documentation for more information.
- **Password:** Enter the password for the journal mailbox user.
- **Active** (checkbox): Defines whether the data loader is active or inactive.

Data loaders and Outlook message classes

GroupWise does not discriminate among message types or "classes" the way Outlook does, so the information in this section applies only to Archive Manager installations configured to work with Exchange/Outlook messaging systems.

In an Exchange system, by default, Archive Manager data loaders will load all standard Outlook item types into the archive except Journal entries (activities), regardless of message class. Archive-able items include the message classes listed in the table below, which also shows what Archive Manager can do with each item type.

Table 6. Message Classes

Message Class	Common Name	Export*?	Stub*?	Age*?
IPM.Appointment	Meeting	yes		
IPM.Contact	Contact (person)	yes		
IPM.DistList	Contact (distrib list)	yes		
IPM.Document.*	Document	yes	OptionalSee note below.	yes
IPM.Note	Mail	yes	yes	yes
IPM.OLE.Class.*	Meeting (exception)	yes		
IPM.Outlook.Recall.*	Recall request	yes		yes
IPM.Post	Mail (posted)	yes	yes	yes
IPM.Recall.*	Recall request	yes		yes
IPM.Report.*	Report (non-deliv, receipt)	yes		yes
IPM.Schedule.*	Meeting invitation/response	yes		yes
IPM.StickyNote	Note	yes		
IPM.Task	Task	yes		
IPM.TaskRequest.*	Task request/response	yes		yes
Report.*	Report (non-deliv, receipt)	yes		yes

- **Export**: Add to archive.
- **Stub**: Stubbing (or leaving a message Stub) in Exchange, to reduce overall storage size on the mail server.
- **Age**: Delete messages or message stubs from Exchange based on age.

NOTE: IPM.Document items can be enabled for stubbing when there is a stubbing policy in place on the folder in which they reside.

Message processing

Once messages have been processed by a data loader, SQL jobs link the messages to virtual mailboxes and assign security to embedded messages. These SQL jobs include:

- **Mailbox Maintenance - Link Embedded Messages - Archive Manager:** This job discovers messages that are attached to other messages and grants users security to the attached messages if they are not already in the user's mailbox. This job is enabled by default.
- **Mailbox Maintenance - Populate Virtual Mailboxes - Archive Manager:** This job links messages to virtual mailboxes based on the configured parameters of the virtual mailbox. This job is enabled by default.

Add, edit or delete a data loader

The following sections discuss managing data loaders.

Add a data loader

1. Click on the **Add a Data Loader** link.
2. Select a **Type** value from the drop-down list: File System, IMAP4, MAPI or POP3, as defined above.
3. Enter a **Group** name. If not specified, the default group name `default` will be applied.
4. Enter or select additional field values as requested by the form.
5. Click **Add**. The **Data Loader Administration** form is displayed with the new data loader and related details.

Edit a data loader

1. In the **Data Loader Administration** form: Locate the data loader in the list. Either:
   - Scroll through the list of data loaders; ***or***
   - Enter a value in the **Name** field and click **Search**.
2. Click **Edit** to the left of the data loader name to display the **Edit Data Loader** form for the selected data loader.
3. Revise the information and then click **Update**. The specified changes to the data loader are saved, and the **Data Loader Administration** form is displayed.

   NOTE: To return to the Data Loader Administration screen without editing, click **Cancel**.

Delete a data loader

1. In the **Data Loader Administration** form: Locate the data loader in the list. Either:
   - Scroll through the list of data loaders; ***or***
   - Enter a value in the **Name** field and click **Search**.
2. Click **Delete** to the left of the data loader name. The **Delete Data Loader** confirmation message is displayed.

3 Click **OK** to confirm the deletion. The selected Data Loader is deleted, and the **Data Loader Administration** form is displayed.

> **NOTE:** Alternatively, a data loader can be deleted by opening the **Edit Data Loader** form, clicking **Delete**, and confirming the deletion.

4

Download tools

- About download tools
- Search Exporter
- Outlook Components tool
- Recovery Manager for Exchange
- Offline Client
- Outlook Web App (OWA) reconstruction tool
- URL Redirect
- API and SDK

About download tools

The **Download Tools** screen displays additional Archive Manager tools that are available for you to download. For each available tool, the screen briefly explains what the tool does, and provides a link to download the tool.

NOTE: These tools are viewable only if you have specific permissions, and are accessible at the discretion of the administrator.

The following download tools are available on the Download Tools page:

- Search Exporter
- Outlook Components Tool
- Offline Client
- Outlook Web App (OWA) Reconstruction Tool
- URL Redirect
- API SDK

To download the additional tools available:

1. Open the Archive Manager Administration page, and click the **Download Tools** link.
2. Locate the tool you wish to download in the list and click the link. The Download dialog is displayed.
3. Follow the instructions in the Download dialog to perform the installation.

Search Exporter

The Archive Manager Search Exporter works in conjunction with Archive Manager to allow for the offline rendering of search results.

The results are stored as HTML, MIME, PST or XML format (together with any attachments). They can be accessed without the need to be online or burned to a CD and distributed to people who are not Archive Manager users. If you export to the HTML format, comments are also exported.

This tool is very useful during a legal discovery, when items must be submitted to the court in a format that can be accessed and preserved by the court (in other words, that can be used as evidence).

Prerequisites

The following requirements apply to the workstation where the Search Exporter will be installed:

- Microsoft Outlook for Office 365 ProPlus, 32-bit, **or**
- Microsoft Outlook 2019, 32-bit only, **or**
- Microsoft Outlook 2024, 64-bit or 32-bit, running on Windows 10, 8.1, 8, or 7, **or**
- Microsoft Outlook 2021, 64-bit or 32-bit, running on Windows 10, 8.1, 8, or 7 SP1
- Windows Installer 3.1 or later (only for installation).
- Microsoft .NET Framework Version 4.8.

Installing and running the Search Exporter

Install the Search Exporter on the PC of the person who will use the tool (normally the system administrator).

NOTE: Remember that Microsoft .NET Framework 4.5.2 and 3.5 (SP1) must be installed on any workstation where the Search Exporter will run.

To install the tool, go to the **Download Tools** page of the Administration Web Site and click the **Search Exporter** link. Or, run the **EmailExport.msi** file located on the Archive Manager Reseller and Customer Portal site. Follow the prompts to install the application on the PC.

Before running the Search Exporter, you need to ensure that the Archive Manager security roles that will use the application have permissions to use it.

Administrators: Perform the following steps to ensure that the appropriate permissions are set to run the Search Exporter.

1. Go to the Archive Manager Website by clicking **Administration** at the top right of the Archive Manager application.
2. Select **Security Roles** to obtain a list of all roles in the system.
3. Click **Edit** for the role that you want to edit.
4. Ensure that the **Export Email** security action has been added to the role.

Depending upon how the Archive Manager Search Exporter application will be used in your organization, an additional security action may need to be selected. Typically, the tool is used only by administrators or other users with special permissions who need to export data from the Archive Manager application. If you need to search email across all mailboxes in the enterprise, you need to make sure that the security role has the following security action selected:

- Search All Emails

Additional configuration options

The following settings can be configured in the **SearchExporter.exe.config** file.

- **AMFolderName**: The name of the folder where exported messages will be placed. The default folder name is **ArchiveManager**.

- **AMFolderComment**: Allows you to define a comment to add to the folder where exported messages will be placed.
- **MaxMsgPerPst:** The maximum number of messages to put into a PST file before creating a new PST file. The default value is 1 million.
- **MaxMsgPerFolder:** The maximum number of messages to put in a folder before creating a new subfolder for the top-level folder. The default value is 10,000. Each new folder will be named by a sequential number.
- **WebServicePageSize**: The number of message IDs to retrieve from the server in a single batch. The default value is 1000 messages.
- **MaxFileSize**: The maximum size in bytes of an Outlook 97-2002 PST File. The default value is 2 GB. When the PST reaches the maximum size, a new PST file will be created.
- **MaxLargeFileSize**: The maximum size in bytes of an Office Outlook PST File. The default value is 20 GB. When the PST reaches the maximum size, a new PST file will be created.

Exporting data

To export email from the Archive Manager system:

1 Enter the search criteria using one or more of the processes described in the User Guide.

> **NOTE:** If you select to export attachments, then the email messages containing those attachments are exported along with the attachments. Exporting attachments only is currently not supported. For example, if you have multiple emails containing the same attachment and you select to export attachments, all email messages containing that attachment are exported.

2 Click **Export** to initiate the export to display the **File Download** dialog box.

3 Click **Open** to open the export file in the Archive Manager Search Exporter. The Search Exporter Wizard screen appears.

> **NOTE:** Or, the user can click **Save** to save their search for a future export.

4 Enter the requested information into the fields on this screen:

- **Export Directory:** The destination location for the exported data. You may use the Browse feature (the "..." button to the right of the field blank) to locate and specify the location.
- **Format:** The format into which the exported messages will be saved. If you choose the PST or HTML **Format**, then you must also specify:
- **File Name:** Configurable. The default is Default.xxx.
- **Type (for export to PST only):** Office Outlook, or Outlook 97-2002.

  You may use the Browse feature (the "..." button to the right of the field blank) to specify these values.

  > **NOTE:** For messages that contain characters in a codepage that is different from the computer's configured codepage, you must export to Office Outlook (Unicode) PST files. The Office Outlook PST file format is available with Microsoft Outlook 2003 and later versions.

- **Ignore errors for missing attachment:** If this checkbox is selected, messages with missing attachment(s) will be exported without generating any errors.
- **Connect Using:** The authentication method to be used to confirm the authenticity of the person performing the export.

  > **NOTE:** Both the Archive Manager Website and the Archive Manager Web Service must use the same authentication method for the Search Exporter to work.

- **User Name:** The username, as used in Archive Manager. The **User Name** will likely be the same values you use to sign into Archive Manager, as determined by the organization.
- **Password:** The user's password, as used in Archive Manager. The **Password** will likely be the same values you use to sign into Archive Manager, as determined by the organization.

  NOTE: Before beginning the export, you must verify that you have sufficient disk space to save exported data.

5 Click **Export** to begin the export.

The progress bar will track the progress of the export. When the process is complete, a **Finish** button appears at the bottom of the Search Exporter Wizard dialog box.

Open exported search results

To open the exported search results, browse to the folder you selected to export your email to. How you open exported messages depends on the format of the exported messages:

- **HTML format:** These messages are accessed via a main HTML page named Default.html, with each message listed on that page. You can simply click on a link to open an HTML version of that message, and the content of the message, along with all attachments, will be available from within the message.
- **MIME format:** Email messages that have been exported in MIME format can be opened with any standard email application that can read these messages.
- **PST format:** Email messages that have been exported to PST format can be opened with Microsoft Outlook. Go to the **File** menu, and select **Open/Outlook Data File**. Select the folder where your PST file is located and double-click the PST file you want to open.
- **XML format:** Email messages that have been exported to XML can be viewed with a Web browser, though much of the content will be Base64 encoded. Some data, such as the attachment name and mailbox, can be viewed. Email messages that have been exported to XML can also be imported into another Archive Manager instance.

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.

Prerequisites

The Archive Manager Outlook Components tool can only be installed with supported versions of Archive Manager.

- Microsoft .NET Framework version 4.8.
- 64-bit versions of Outlook require the **Archive Manager Outlook Components x64.msi**. All other versions of Outlook require the **Archive Manager Outlook Components X86.msi**.
- Microsoft Outlook for Office 365 ProPlus, **or**
- Microsoft Outlook 2019, **or**
- Microsoft Outlook 2024, 64-bit or 32-bit, running on Windows 10, 8.1, 8, or 7, **or**
- Microsoft Outlook 2021, 64-bit or 32-bit, running on Windows 10, 8.1, 8, or 7 SP1
- Windows Installer 3.1 or later (only for installation).

Installing the Outlook Components tool using a group policy

To install the Outlook Components tool on computers that are running a supported Windows, please refer to the Assign a Package section of the following Microsoft support article:

http://support.microsoft.com/kb/816102

The Outlook Add-in will be installed at the first reboot of the computer after the group policy has been applied. The Outlook Form will be installed automatically the next time a user logs in to Outlook after the Outlook Components tool has been installed. By default, the Outlook Form is installed with standard mail icons. If you wish to install the Outlook Form with Archive Manager icons, see the additional instructions below.

The installation will make changes to the Windows Registry on your computer. For more information, see the following Microsoft support article: https://support.office.com/en-us/article/Custom-form-script-is-now-disabled-by-default-bd8ea308-733f-4728-bfcc-d7cce0120e94

A reboot may be required after to install the Outlook Form after installation of the Archive Manager Outlook Components tool with older versions of Outlook, or if the form has been manually removed from Outlook prior to reinstalling the tool. If you are reinstalling this tool on a client computer that is running Outlook 2003, you must delete the following file in order for the Outlook Form to be installed again: *<archive_manager_home>\Outlook Components\OutlookAddIn.default.config*

Installing the Outlook Components tool to deploy the form with Archive Manager icons using a group policy

1. When installing the Archive Manager Outlook Components tool, on the Deploy Software screen, click **Advanced**, then **OK**.
2. Under the Modifications tab, click **Add**.
3. Select UseAMIcons.mst.

Installing the Outlook Components tool manually

1. Log in to a computer with Administrator credentials.
2. Launch Archive Manager Outlook Components.msi.
3. Follow the prompts in the Windows installer.

The Outlook Form will be installed automatically the next time a user logs in to Outlook after the Outlook Components tool has been installed. By default, the Outlook Form is installed with standard mail icons. If you wish to install the Outlook Form with Archive Manager icons, see the additional instructions below.

Installing the Outlook Components tool manually to deploy the form With Archive Manager icons

1. Log in to a computer with Administrator credentials.
2. From a command prompt, navigate to the directory where you have placed the Archive Manager Outlook Components.msi file.
3. Use the following command to install the package with Archive Manager icons:

   MSIEXEC /I "Archive Manager Outlook Components.msi" FORMAMICONS="1"
4. Follow the prompts in the Windows installer.

Installation options

For manual installation, the Archive Manager Outlook Components.msi package can be run in a "silent" mode. In silent mode, no user interface is displayed. To install with silent mode enabled, run the following command at a command prompt:

```
"Archive Manager Outlook Components.msi" /quiet
```

Recovery Manager for Exchange

Recovery Manager for Exchange replaces the PST Import Wizard tool that was previously included in Download Tools.

Archive Manager includes a free license for Recovery Manager for Exchange (RME). RME is the recommended tool for importing PSTs. RME allows you to find and retrieve message-level data from multiple sources in minutes, from a single console.

You can find exactly what you need with intelligent search based on sender, recipient, date, attachment type, subject, message keyword, attachment keyword, message class, message type, or even advanced pattern searching and other custom queries. You can also compare the contents of an online mailbox with a backup mailbox to identify any differences.

Use the following procedures to obtain an Archive Manager compatible RME license and to install RME.

To obtain a Recovery Manager for Exchange (RME) license for use with Archive Manager

1. Go to https://support.quest.com/productswap.
2. Sign in. If not already registered for the Quest support portal, register and then sign in.
3. Click the **expand** arrow for the Windows Swap Program.
4. Check the **Archive Manager to Archive Manager for Email Discovery/Recovery** check box.
5. Check the Terms and Conditions check boxes and any others you want.
6. Click **Submit**.

   An email will be sent to you and a representative will contact you shortly about the exchange program.

   NOTE: Obtaining the license file for RME may take a few days.

To obtain RME software and documentation

1. Go to https://support.quest.com.
2. Search for “RME” in the search box at the top of the page.
3. Download RME software.
4. Download RME technical documentation. You will need the Release Notes and User Guide to provision a machine and install RME.
5. Provision a machine for RME based on the prerequisites in the RME Release Notes. This cannot be the Archive Manager server.
6. Once you receive your license file for RME, install RME, using the procedure in the RME User Guide.

   NOTE: Your Archive Manager license will remain unchanged. You will receive an additional license for RME with a subset of capabilities appropriate for use with Archive Manager. The RME User Guide explains the differences of the Archive Manager edition.

Offline Client

The Archive Manager Offline Client allows stubbed messages to be reconstructed while offline. It does not provide the ability to search the entire email archive, and does not work in a pure Office 365 environment.

Prerequisites

Archive Manager requires updating all Offline Client versions to the current version.

- Microsoft Outlook for Office 365 ProPlus, **or**
- Microsoft Outlook 2019, **or**
- Microsoft Outlook 2024, 64-bit or 32-bit, running on Windows 10, 8.1, 8, or 7, **or**
- Microsoft Outlook 2021, 64-bit or 32-bit, running on Windows 10, 8.1, 8, or 7 SP1
- Windows Installer 3.1 or later (only for installation)
- Microsoft .NET Framework Version 4.8
- Microsoft SQL Server Compact 4.0
- Visual Studio 2010 Tools for Office Runtime
- MSXML 6.0 SP1

The prerequisites software will be installed automatically if *Setup.exe* is run without them installed on the system.

Downloading the Offline Client

To download the Offline Client, go to the Download Tools page on the Administration Web Site and click the **Offline Client** link.

Enabling offline access to the archive

The Offline Client allows users to reconstruct stubbed messages with Microsoft Outlook while offline, using the Outlook Form. This requires that the Outlook Form is configured on each client. See the *Reconstructing messages using the Archive Manager Outlook Form* section in the Archive Manager *User Guide*.

The Offline Client also requires that you disable anonymous access and select **Windows Authentication** as the authentication mode. To change the authentication mode, see Authentication modes.

Adding administrative templates

In order to allow users reconstruct their stubbed messages offline, you must specify the Archive Manager Web Site address as described in the following section:

> **NOTE:** Keep in mind that all policies are applied only after the time interval specified in the **Group Policy refresh interval for computers** policy. The policy is located in **Computer Configuration | Administrative Templates | System | Group Policy** and **User Configuration | Administrative Templates | System | Group Policy**.

For Windows 2019, 2016, 2012 or 2008 R2

1. From the server desktop, click **Start** and then **Run**.
2. In the Run box, type **mmc**, then click **OK**.

3 If you already have an mmc configuration with the Group Policy Management Editor snap-in, go to step 9. Otherwise, proceed to the next step.

4 From the File menu, click **Add/Remove Snap-in**.

5 Select Group Policy Management Editor and click **Add**.

6 In the Select Group Policy Object box, click **Browse**.

7 Select an existing policy or create a new one, and then click **OK**.

8 Click **Finish/OK**.

9 Expand the policy that you've selected, then expand User Configuration | Policies. Right-click Administrative Templates and select **Add/Remove Templates**.

10 In the Add/Remove Templates dialog, click **Add**.

11 Browse to the **ArchiveManagerOfflineClient.adm** file, which can be found in your Archive Manager Installation directory under **<archive_manager_home>\Website\Tools\OfflineClient.exe**.

12 Select the file and click **Open**. The template will appear in the Add/Remove Templates dialog. Click **Close**.

13 Browse to **POLICY_NAME | User Configuration | Policies | Administrative Templates | Classic Administrative Templates | Quest Archive Manager | Client Adjustments | Cached Mode Settings** and select the Cached Mode Settings node.

14 If the node is missing, select the Administrative Templates node under User Configuration, and uncheck **Filter On** on the View menu.

15 In the right pane, double-click the **Set the Archive Manager URL**.

16 In the policy's Properties dialog, select the **Enabled** option and specify the Web URL in the following format: http://<archivemanager>/, which must be based on your archive manager settings.

17 Click **OK** to apply your changes.

The following policies can be configured in the Group Policy Object Editor:

- **Set the Archive Manager URL:** In order to use the Archive Manager Offline Client, you must set the URL for the Archive Manager Web Site. Users will not be able to override settings specified by the policy.
- **Set automatic synchronization frequency:** Users need to synchronize their cache to keep them up-to-date. This can be done automatically. Using the Set automatic synchronization frequency policy, you can specify how frequently the contents of cache will automatically be synchronized with the archive. Users will not be able to override settings specified by the policy.
- **Set the Offline Content Age:** Local cache lets you set an age limit for messages to be cached so you can avoid caching outdated messages. The age limit can be specified automatically by the policy. Users will not be able to override settings specified by the policy.
- **Set synchronization batch size:** To avoid the client computer overload, the Offline Client will uses batch processing so it does not synchronize too many messages or attachments at a time. Users will not be able to override settings specified by the policy.

To configure a policy:

1 In the Group Policy Object Editor, browse to **User Configuration | Administrative Templates | Quest Archive Manager Settings | Client Adjustments | Cached Mode Settings**.

2 Select the node. The policies are displayed in the right pane.

3 Double-click the policy you wish to configure.

4 In the policy Properties dialog, select the **Enabled** option.

5 Configure the policy in the dialog box.

6 Click **OK** to apply your changes.

Deploying the Archive Manager Offline Client

The Offline Client component must be deployed on each user's workstation to provide offline reconstruction of stubbed messages. You can use the Group Policy Software Installation Extension to deploy the Offline Client on workstations.

> **TIP:** If a large volume of users creates increased load on the Offline Client, you can improve performance by deploying a separate dedicated IIS server for the website and web services. Deploy a second, duplicate IIS Archive Manager server. Then, point users' Offline Clients to the website component of the second server.

Note that software installation requires administrative rights on the workstation. If users are not allowed to install software on their workstations, assign the installation package to users using group policies.

Deploy using group policy

> **NOTE:** You can also use computer policy, but this might require restarting the workstations. For more information, see https://support.microsoft.com/en-us/help/816102/how-to-use-group-policy-to-remotely-install-software-in-windows-server.

- Group Policy deployment does not install prerequisites. Prerequisites must be installed prior to deployment.

For Windows 2019, 2016, 2012 or 2008 R2

1. Copy the **OfflineClientInstaller.msi** file to a file share (a distribution point).

   For example: \\AMServer\Tools\OfflineClient\OfflineClientInstaller.msi
2. From the server desktop, click **Start** and then **Run**.
3. In the Run box, type **mmc**, then click **OK**.
4. If you already have an mmc configuration with the Group Policy Management Editor snap-in, go to step 8. Otherwise, proceed to the next step.
5. From the File menu, click **Add/Remove Snap-in**.
6. Select **Group Policy Management Editor** and click **Add**.
7. In the Select Group Policy Object box, click **Browse**.
8. Select an existing policy or create a new one, and then click **OK**.
9. Click **Finish/OK**.
10. In the Group Policy snap-in, right-click **User Configuration | Software Settings | Software Installation**, and select **New | Package** from the shortcut menu.
11. You will be prompted for the setup file. Browse to the file share and specify the **ArchiveManagerInstaller.msi** package.
12. In the Deploy Software dialog box, select the **Assigned** deployment method.
13. Click **OK**.
14. Right-click the software package you created, and select **Properties** from the shortcut menu.
15. Go to the Deployment tab and select the **Install this application at logon** checkbox.
16. Click **OK**.

Outlook Web App (OWA) reconstruction tool

The Outlook Web App (OWA) reconstruction tool allows you to reconstruct stubbed messages and attachments in the OWA with the following Exchange Server versions:

- Exchange Server 2019
- Exchange Server 2016
- Exchange Server 2013
- Exchange Server 2010 SP3 or SP2

Limitations

The OWA reconstruction tool has the following limitations:

- The reconstruction tool requires Windows Authentication as the authentication mode for the Archive Manager Website.
- For Exchange 2019, 2016, and 2013, the reconstruction tool requires Internet Explorer 10 and later versions, Microsoft Edge, Firefox and Chrome.
- For Exchange 2010, if you are using Internet Explorer 11, the compatibility mode must be enabled when accessing the OWA website.
- The reconstruction tool does not support for Office 365.

Installing OWA reconstruction tool

Prior to installing the OWA reconstruction tool, note the following:

- If you have multiple CAS servers, you must install the reconstruction tool to each OWA virtual directory.
- For Exchange 2019, 2016, and 2013, the PowerShell Remoting should be enabled to run the cmdlets from the installer, otherwise you must run them manually as prompted by the installer to finish the installation.

To install the OWA reconstruction tool:

1. Copy the installer *OWAReconstructInstaller.msi* to your server.
2. Run the Archive Manager OWA Reconstruction Installer on the OWA server.
3. On the Welcome screen, click **Next**.
4. On the Transaction Product Agreement screen, review the license agreement and select the **I accept the terms …** checkbox and click **Next**.
5. On the Exchange Version screen, select an Exchange version and click **Next**.
6. On the OWA Virtual Directory screen, verify that the OWA path is correct. Modify the path if needed and click **Next**.
7. (Only required for Exchange 2013 and later versions) On the OWA URL screen, input the OWA URL and click **Next**.
8. On the Ready to Install the Program screen, click **Install**.
9. On the last screen of the installation wizard, select the **Restart IIS Now** checkbox and click **Finish** to exit the installation wizard.

For instructions on reconstructing messages using the OWA reconstruction tool, see the *Reconstructing messages using the Outlook Web App (OWA)* section of the *Working with Messages* chapter of the *Archive Manager User Guide*.

URL Redirect

When multiple Archive Manager servers are deployed, the Archive Manager URL Redirect website allows users to go to a single URL that redirects them to the Archive Manager server that has their active login. If a user has more than one active login, the user can select the desired Archive Manager server from a list of servers with active logins.

Users with Forms authentication need to enter a user name on the URL Redirect page the first time they log in, and a user name and password to log in to Archive Manager. They will have to do this periodically when they log in after that.

Users with Windows authentication do not need to enter a user name when they go to the URL Redirect page. Depending upon whether user authentication is set to prompt for a user name and password, users may be automatically logged in to Archive Manager, or they may have to enter a user name and password.

Once logged in, the Email Search page of the Archive Manager website is displayed.

Prerequisites

- Microsoft .NET Framework 4.5.2 must be installed on the machine where you extract the files from the UrlRedirect.exe file.

IIS and Web.Config Setup:

- **For Windows Authentication With Archive Manager:** Internet Information Services (IIS) for the URL Redirect website must be configured, making sure to turn off Anonymous and Forms.
- **For Forms Authentication With Archive Manager:** Remove the lines marked for removal in web.config. Internet Information Services (IIS) for the URL Redirect website must be configured, making sure that Anonymous Authentication is set.
- The Application Pool used must have the same credentials as the Archive Manager Website to ensure that security and the connection strings will work properly.

Installation

Advanced knowledge of IIS is required for setup. High-level instructions for setting up IIS are listed below.

1. Download the UrlRedirect.exe from the Download Tools page of the Archive Manager Administration website.
2. Unzip the file to the desired location on the web server.
3. Create a website in IIS that points to the directory where you unzipped the UrlRedirect.exe files.
    - Add a host header value to the website, and make sure that value is in your DNS.
    - Verify that the Application Pool user has correct file system security on the installation directory and files.
    - Toggle your authentication to match either a Windows or Forms authentication configuration.
4. Edit the RedirectConfig.xml file and then test the website.

Editing the RedirectConfig.xml file

- **Expire Days:** For all servers, this setting determines the number of days before a user has to select the server again. The default is 15 days.

This setting is used when using Forms authentication. Windows Authentication users will not need this setting because they are automatically directed to the appropriate server without selecting it.

- **ConnectionTimeout:** This sets the SQL Server connection string timeout. If a timeout occurs users will have to wait this long before receiving an error message.

For each server, you can create the following entries:

- **Name:** Helps identify which server is associated with each connection string. Used to identify servers and connections with errors.
- **Connection:** The encrypted connection string of your AM instance. Users can go to *http://<redirectSite>/Configure.aspx* to configure the connection string.

  Usage:

  If a user has an active login for more than 1 server, the user can select which server to be redirected to.

  Once a server is selected, the user will be redirected to the selected server automatically for "ExpireDays" (default 15).

  Users will not be redirected if they sign out of Archive Manager (when using Forms Authentication) for security reasons, such as sharing computers.

  Uses will not be redirected if another user signs in (when using Windows Authentication) for security reasons, such as sharing computers.

  If the server selection needs to be changed, users can go to *http://<redirectSite>/Reset.aspx* to clear the selection and try again.

  Alternatively, users can remove any cookies they have for the site.

Under certain scenarios, users will not be automatically redirected to the selected Archive Manager server. These scenarios include:

- **Forms Authentication:** If a user with Forms authentication signs out of Archive Manager, the user will not be automatically redirected to the selected Archive Manager server for security reasons. For example, the user may have signed out because the computer is shared.
- **Windows Authentication:** If a user is logged in with Windows authentication and multiple active logins to different Archive Manager servers exist, the user must select an Archive Manager server from a list. For a default time period of 15 days, that user is automatically redirected to the selected Archive Manager server. If another user logs in within the 15 days, the next time the original user logs in the desired Archive Manager server must be selected again. This may happen if a user logs in at a Kiosk or a shared computer.

Deploying the URL Redirect link

Once the administrator has set up the URL Redirect website, the administrator sends an email containing a link to the website to users.

Logging in to the URL Redirect website

To log in to the URL Redirect website:

1. Click on the link to the URL Redirect website that is provided in an email from the administrator.
2. For users with Windows authentication, clicking the URL automatically logs you in to the appropriate Archive Manager server.

If the user account has an active login to multiple Archive Manager servers, select the appropriate server from a list displayed in the dialog box.

3 For users with Forms authentication, type your user name and password and you will be directed to the appropriate Archive Manager server.

If the user account has an active login to multiple Archive Manager servers, select the appropriate server from a list displayed in the dialog box.

Changing the Archive Manager server

If you need to change the Archive Manager server after you have logged in, go to the following website to clear the server selection and then log in again:

```
http://<redirectSite>/Reset.aspx
```

Or, remove any cookies that your browser has set for the site and log in again.

API and SDK

The Archive Manager Software Development Kit allows you to write applications that directly interface with the archive. See the *Archive Manager RESTful Web Service API* and the *Archive Manager SDK* guides for additional information.

5

Federated Search Instances

- About Federated Search Instances
- Troubleshooting
- Editing Federated Search Instances
- Performing searches on Federated Search Instances
- Troubleshooting

About Federated Search Instances

The **Federated Search Instances** menu option allows the administrator to create and update remote Archive Manager instances so they can be searched simultaneously. This option is useful if you have multiple Archive Manager instances located at different sites. In order to search a remote instance, you must set up a Federated Search Instance, and configure all the websites launched by your Archive Manager instances at different sites as the same authentication mode. For more information about how to configure the authentication mode, see Authentication modes.

Note that when searching Federated Search Instances, certain features of Archive Manager cannot be used remotely. However, you can go directly to the remote instance(s) to perform the following actions:

- Use the **Access History** tab to view information about users that have accessed messages that reside on a remote instance.
- Use the **Tags** tab to view or add tags and tag values to messages that reside on a remote instance.
- Use the **Comments** tab to add comments to messages that reside on a remote instance.

Adding Federated Search Instances

To add a Federated Search Instance:

1. Go to the Archive Manager Administration menu page and click **Federated Search Instances**.
2. On the Federated Search Instance Administration page, click **Click here to Add a Federated Search Instance**.
3. Enter the following information:
    - **Name:** The display name of your Federated Search Instance.
    - **Remote Server:** The name of the remote Archive Manager server that you want to add.
    - **Remote URL:** The URL of the remote instance. For example, http://<archivemanager>
    - **Weight:** Enter a numeric value between 0 and 255 to indicate the order of the Federated Search Instances when returning search results. Search results will be displayed in order from the highest numbered Federated Search Instance to the lowest. The local server will always be searched first.

- **Username:** The user account used to sign in to the Federated Search Instance. The user must have the Impersonate security action. For information on security roles and adding actions to security roles, see the Security roles chapter in this guide.

  NOTE: The user conducting the search must sign in to the local server and have an account on the remote instance(s). For Windows Authentication, the user must be a domain user; for Forms Authentication, the user can be a domain user, or an Archive Manager user, such as “Admin”.

- **Password:** The password for the user account used to sign in to the Federated Search Instance.
- **Domain:** The domain where the Federated Search Instance resides.

  NOTE: The domain name must exactly match the one shown in the **Logins** page of the Administration Website for this account.

- **Active:** Check this box to include the Federated Search Instance that you are adding to the search.

4 Click **Add** to add a Federated Search Instance.

Editing Federated Search Instances

To edit a Federated Search Instance that you have added:

1 Click the **Edit** icon located to the left of the name of the server you want to edit.

2 Edit the desired fields and click **Update**.

To add or modify a Federated Search Instance, you first need to add the **Edit Federated Search Instances** action to your security role. This action is added by default to the Administrator role.

Performing searches on Federated Search Instances

To perform searches of Federated Search Instances using the Email Search Web page, you must add the **Search All Instances** action to your security role. This action is added by default to the Administrator role.

Once the **Search All Instances** role has been added, the **All Instances** checkbox displays on the Email Search Web page. Check this box to search all local and Federated Search Instances when performing a search.

For information on security roles and adding actions to security roles, see the Security roles chapter in this guide.

Troubleshooting

The most common problem you may encounter with Federated Search Instances will be incorrect security settings. Here are some actions that you can take to verify the security settings:

- Copy and paste the Remote URL into the browser to verify that it is correct.
- Verify the Username and Password on the remote server is correct in Federated Search Server area.
- Try to sign in to the remote Federated Search Server using specified credentials and check the security.

6

Groups

- About groups
- Add, edit or delete a group

About groups

Groups provide a flexible way to manage multiple individual users or mailboxes.

Archive Manager has two types of groups:

- Directory Groups - These are automatically generated by the directory service to which Archive Manager is connected (e.g. Active Directory Security and Distribution Groups, GroupWise Distribution Lists).
- Archive Manager Groups - These are created within Archive Manager.

NOTE: GroupWise groups are not imported into Archive Manager.

NOTE: An administrator can create an Archive Manager group only from within Archive Manager.

Add, edit or delete a group

The following sections discuss managing groups.

Add a group

In the Add Group form:

1. Enter a **Name** for the group.
2. Click **Add**. The new group is added to the system.

Edit a group

1. Locate the group in the list of groups displayed in the **Group Administration** form. Either:
   - Scroll through the list of groups; ***or***
   - Enter a value in the **Name** field and then click **Search.**
2. Click **Edit** to the left of the group name to display the **Edit Group** form for the selected group.
3. Revise the group information as described in the following steps and then click **Add to group**. The specified changes to the group are saved, and the **Group Administration** form is displayed.

Group name

To change the name of a group, simply enter a new value in the **Name** field.

Default Policy

Set a default policy for the group users' mailboxes. This setting is only available to AD and Azure AD groups.

Inbox Policy

Set a policy for the group users' Inbox folders. This setting is only available to AD and Azure AD groups.

Sent Items Policy

Set a policy for the group users' Sent Items folders. This setting is only available to AD and Azure AD groups.

Deleted Items Policy

Set a policy for the group users' Deleted Items folders. This setting is only available to AD and Azure AD groups.

Add a user to a group

1. On the **Users** tab of the **Edit Group** form: Locate the user login in the list of users. Either:
   - Enter the name of the desired group in the **Find Group** field, and click **Search**; ***or***
   - Use the page browsing controls ("Page x of y") below the groups list to browse for the desired group.
2. Select the checkboxes to the right of the users you want to add to the group.

   NOTE: Although multiple users can be added at once, the selected users must all be displayed on the same page. If you browse to another page, any selections on the current page will be lost.
3. Click **Add to group**. The selected users are added to the list of users in the **Users** tab of the **Edit Group** form.

Delete a user from a group

1. In the **Add a Group** form, in the list of users on the **Users** tab: Click **Delete** to the right of the user you want to delete. The **Delete User** confirmation message is displayed.
2. Click **OK** to confirm the deletion. The selected user is deleted from the list of users, and the **Group Administration** form is displayed.

Add a mailbox to a group

1. Locate the desired mailbox in the list of mailboxes displayed on the **Mailboxes** tab of the **Edit Group** form. Either:
   - Enter the name of the desired mailbox in the **Name** field, and click **Search**; ***or***
   - Use the page browsing controls below the list (Page x of y") to browse for the desired mailbox.
2. Select the checkbox to the right of the mailbox to select mailboxes you want to add to the group.

   NOTE: Although multiple mailboxes can be added at once, the mailboxes must all be displayed on the same page of the list of mailboxes. If you browse to another page, any selections on the current page will be lost.
3. Click **Add to group**. The selected mailboxes are added to the list of mailboxes displayed on the left side of the **Mailboxes** tab of the **Edit Group** form.

Delete a mailbox from a group

1. In the **Mailboxes** tab of the **Edit Group** form: Click **Delete** to the right of the mailbox you want to delete. The **Delete Mailbox** confirmation message is displayed.
2. Click **OK** to confirm the deletion. The selected mailbox is deleted from the list, and the **Group Administration** form is displayed.

Delete a group

1. Locate the group in the list of groups displayed in the **Group Administration** form by doing one of the following:
   - Scroll through the list of groups.
   - Entering a value in the Name field and then clicking **Search.**
2. Click **Delete** to the left of the group name. The Delete Group confirmation message is displayed.
3. Click **OK** to confirm the deletion. The selected group is deleted, and the **Group Administration** form is displayed.

   NOTE: Alternatively, you can delete a group by opening the **Edit Group** form, clicking **Delete**, and confirming the deletion.

7

Index management

- Overview
- Configuring the Full Text Index
- Index Dashboard
- Index Operation Log
- Index Rollover Policy

Overview

The Full Text Index is a collection of message and attachment data to facilitate fast and accurate search results based on queries. The Full Text Index is split into individual partitions, each of which indexes a subset of message or attachment data into a separate index directory. The items contained in each partition are defined by the Index Rollover Policy.

Multiple drives can be used to enhance indexing in the following ways:

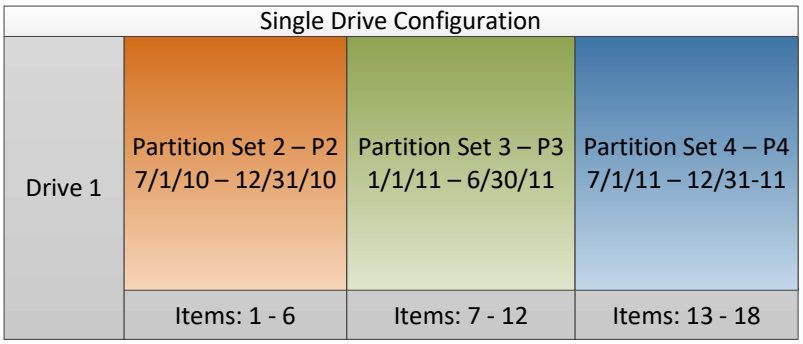
- **Redundancy:** A secondary or failover partition is used as a backup to a primary partition. The secondary partition is used if there is a problem with the primary partition.
- **Performance:** Performance is enhanced by distributing items in a round robin method across multiple partitions on multiple drives. This method allows multiple partitions and drives to share the load of indexing and searching.

The following terms are used throughout this chapter:

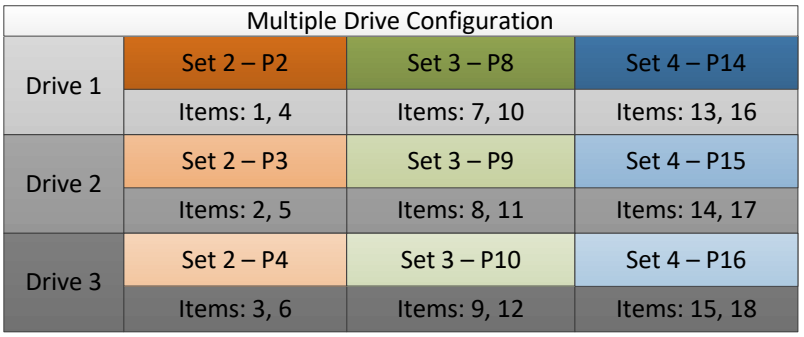
- **Partition set:** A partition set is a group of shards that span a date range. The date range is approximately 180 days per drive. Depending upon how many drives you have configured, your partition set will consist of 1, 2, 3, or 4 shards.
- **Partition:** A group of index files used to facilitate fast and accurate search results based on queries.
- **Shard:** A shard contains a primary partition, and if failover is enabled a shard also contains a secondary (failover) partition. The number of shards is equal to the number of index drives selected, up to 4 drives.
- **Index:** An index is a collection of message or attachment partition sets. The partition set name is based upon the date of the first item indexed in the set. When a new partition set is automatically created, it is defined based upon the Index Rollover Policy.

Index topology

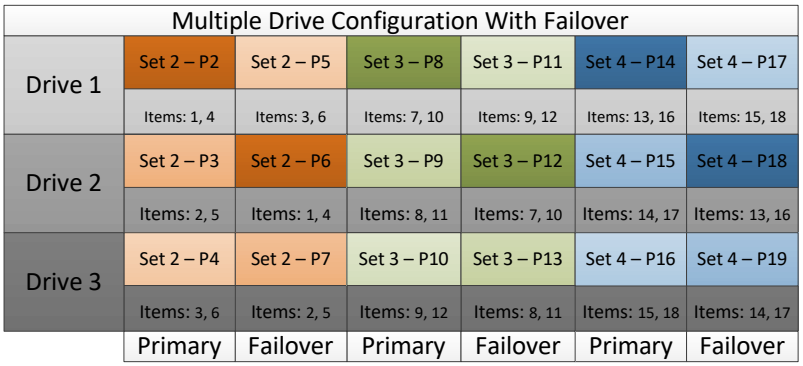
The following graphics show possible index configurations.



The Single Drive Configuration graphic illustrates a possible scenario for configuring an index with a single drive. In this example, an index with one partition has been divided based on date ranges. The default date range for each partition set on a single drive is approximately 6 months (180 days). Each partition set contains a range of items.



The Multiple Drive Configuration graphic illustrates distributing the partition sets from the Single Drive Configuration graphic across three drives. All items are distributed evenly across all partitions in the set to balance the indexing load. In a multiple drive configuration, the number of partition sets is based on a date range. The number of shards in a set is based on the number of drives. In the example above, Set 2 - P2 references partition 2 of set 2, and individual shards are indicated by color. The default date range for this configuration is 540 days, or 180 days for each of the 3 drives.



The Multiple Drive Configuration With Failover graphic illustrates adding failover capabilities which will duplicate index data across multiple drives for fault tolerance. For example, Set 2 - P2 on drive 1 contains items 1 and 4. These items are duplicated in Set 2 - P6 on drive 2. In this example, the shard consists of Set 2 - P2 and Set 2 - P6, where P6 represents the failover partition.

Configuring the Full Text Index

The Full Text Index is installed when you install Archive Manager. During the install, the user is prompted to configure the Full Text Index. The installer prompts the administrator to designate which disks will be used to store partitions. Using multiple hard disks is required for index failover (fault tolerance) and may improve indexing and searching performance. A failover partition that is used as a backup must be located on a different drive than the original data. If one drive fails, the failover partition is used.

It is recommended to select the **Default Configuration** option on the Full Text Index Setup page. Using this option creates a default rollover policy based on time. The amount of time between rollovers depends upon the number of drives configured during the install, or added from the website. More than one drive results in failover becoming enabled. The rollover policy is used to determine when the current newest partition rolls over and a newly-created partition becomes the current partition. It also defines the configuration of the partitions.

The rollover policy created when selecting this option can be viewed and edited on the Index Rollover Policy page. Backup settings can be customized after the installation has completed.

Index Dashboard

The Index Dashboard provides a user interface for performing operations and viewing the status of the Full Text Index. The Index Dashboard contains the following tabs:

- Index Overview tab
- Message Index tab
- Attachment Index tab
- Work-In-Progress Index tab
- Deleted Index tab

Error and warning icons are displayed when needed. These icons appear at the top of the Index Overview tab and on individual partition sets. Clicking on either icon displays a pop-up window that provides warning or error text. If a partition has an error message and a warning message, the error icon is displayed. When you click on the error icon, both error messages and warning messages are displayed.

If there are partitions with errors that are serious enough to affect searching, they are displayed in the Problem Partition Sets section of the Overview tab.

Index Overview tab

The Index Overview tab displays general information about the Message Index and the Attachment Index. The page displays if any portion of either index is not searchable.

This tab also displays the following fields for both active partitions and all partitions:

Active Partitions

- **Total Active Partitions:** The number of partitions used when conducting searches.
- **Most Critical Active Status:** The most critical state of partitions in the set.
- **Least Critical Active Status:** The least critical state of partitions in the set.
- **Total Active Size on Disk:** The combined size of all files belonging to all index partitions.

All Partitions

- **Total Partitions:** The number of partitions used when conducting searches.
- **Most Critical Status:** The most critical state of partitions in the set.
- **Least Critical Status:** The least critical state of partitions in the set.
- **Total Size on Disk:** The combined size of all files belonging to all index partitions.

Links to the following items are also displayed:

- Newest Message Partition Set
- Newest Attachment Partition Set
- Problem Partition Sets

Message Index tab

A message index is a Full Text Index for message data. See the Overview section for a definition of the Full Text Index. The Message Index tab displays a link to the rollover policy for each message index. It also provides a summary of the status of active partitions and all partitions, including:

Active Partitions

- **Total Active Partitions:** The number of partitions used when conducting searches.
- **Most Critical Active Status:** The most critical state of partitions in the set.
- **Least Critical Active Status:** The least critical state of partitions in the set.
- **Total Active Size on Disk:** The combined size of all files belonging to all index partitions.

All Partitions

- **Total Partitions:** The number of partitions used when conducting searches.
- **Most Critical Status:** The most critical state of partitions in the set.
- **Least Critical Status:** The least critical state of partitions in the set.
- **Total Size on Disk:** The combined size of all files belonging to all index partitions.

The Partition Sets box lists all of the partition sets that are part of the index. They are listed in order from oldest to newest.

Attachment Index tab

An attachment index is a Full Text Index for attachment data. See the Overview section for a definition of the Full Text Index. The Attachment Index tab displays a link to the rollover policy for the attachment index. It also provides a summary of the status of active partitions and all partitions, including:

Active Partitions

- **Total Active Partitions:** The number of partitions used when conducting searches.
- **Most Critical Active Status:** The most critical state of partitions in the set.
- **Least Critical Active Status:** The least critical state of partitions in the set.
- **Total Active Size on Disk:** The combined size of all files belonging to all index partitions.

All Partitions

- **Total Partitions:** The number of partitions used when conducting searches.
- **Most Critical Status:** The most critical state of partitions in the set.
- **Least Critical Status:** The least critical state of partitions in the set.
- **Total Size on Disk:** The combined size of all files belonging to all index partitions.

The Partition Sets box shows all of the partition sets that are part of the index. They are listed in order from oldest to newest.

Work-In-Progress Index tab

The Work-In-Progress Index tab displays partitions that are not yet part of the index, but are being prepared by a current operation. The following information

- **Number of Partitions:** The number of partitions that are being prepared by the current operation.
- **Total Size on Disk:** The size of all partitions being prepared by the current operation.
- **Message Partition Sets:** The names of the message partition sets that are being prepared by the current operation.
- **Attachment Partition Sets:** The names of the attachment partition sets that are being prepared by the current operation.

If there are no such partitions, this is indicated on the tab.

NOTE: Partition sets, shards, and individual partitions which are in a state of Work-in-Progress or Deleted do not have tabs for changing settings or requesting new operations. The state of the partition is displayed in the Partition Status field.

Deleted Index tab

Once a partition has been replaced with a new partition, it becomes a legacy partition. The Deleted Index tab displays partition sets that are no longer used in the index. The administrator can choose to delete these index files.

NOTE: Partition sets, shards, and individual partitions which are in a state of Work-in-Progress or Deleted do not have tabs for changing settings or requesting new operations. The state of the partition is displayed in the Partition Status field.

Partition set, shard, and details page

The Partition Set, Shard, and Details pages show varying levels of information regarding groups of partitions or a single partition. These pages are nearly identical in their layout and functionality.

From the Dashboard page, you can view a partition set. From a partition set, you can navigate to shards. From a shard, you can select to view individual partitions. Links at the top of the page provide the ability to navigate backwards up the hierarchy of pages.

Each page provides the following information:

- The title of the current item (partition, shard, or set).
- The status of the current item.
- Links used to navigate pages. For example, you can click on a partition set link to view the shards or individual partitions.

- Links to primary or secondary partitions when viewing a partition (whichever is opposite of the partition you are currently viewing). If no secondary partition is configured, a message is displayed that failover is not enabled.
- A Partition Operations table and Details, Statistics, and Request Operations tabs. See the following sections for additional information.

At the partition set or shard levels, the administrator can choose whether to apply the operation to all partitions or a specific grouping of partitions.

The Partition Details page will have the following additional tabs, with the exception of the Refresh Settings tab for primary partitions:

- **Schedule Settings**: The Schedule Settings tab allows the administrator to change the index schedule settings. The fields are initially set from the rollover policy from which the partition was created. If all partitions do not have the same schedule, the Scheduling fields contain dashes to indicate that multiple [schedule] configurations exist. To update all partitions, change the configuration and apply the settings. To change individual partitions, select a partition and change the configuration. Values can not be changed to an unset state. The defaults are: 180-day rollover, primary indexing delay of 12 hours; and indexing runs 24 hours per day.
- **Backup Settings**: The Backup Settings tab allows the administrator to change the index backup settings. The fields are initially set from the rollover policy from which the partition was created. If all partitions do not have the same schedule, the Backup Settings fields contain dashes to indicate that multiple [backup] configurations exist. To update all partitions, change the configuration and apply the settings. To change individual partitions, select a partition and change the configuration. Values can not be changed to an unset state. Backups are disabled by default.
- **Refresh Settings**: The Refresh Settings tab contains the schedule for when the secondary partition will be refreshed from its primary partition. The fields are initially set from the rollover policy from which the partition was created. If all partitions do not have the same schedule, the Refresh fields contain dashes to indicate that multiple [refresh] configurations exist. To update all partitions, change the configuration and apply the settings. To change individual partitions, select a partition and change the configuration. Values can not be changed to an unset state. The default refresh settings if there is a secondary partition are 24 hours per day, every day.

Common tabs

Each screen for a partition, a partition set, or a shard contains the following tabs:

- **Details**: The **Details** tab displays information about the current item, including:
  - **Role**: Role is displayed only at the partition level. Indicates whether the partition is the primary or the secondary partition.
  - **Item Type**: Indicates whether the partition(s) contains messages or attachments.
  - **Searchable**: Displays the percent of the partition(s) that is searchable.
  - **Common Location**: The location of the partitions. If the partitions are located on different drives, the location is listed as Various Locations.
  - **Indexing**: Indicates whether the partition is being actively indexed.
  - **Location**: Location is displayed only at the partition level. The disk directory where the index is stored.
  - **Minimum Threshold**: The earliest date of items contained in the partition(s).
  - **Maximum Threshold**: The latest date of items contained in the partition(s).
  - **Least Critical Status**: The least critical state of partitions in the set.
  - **Most Critical Status**: The most critical state of partitions in the set.

For partition sets and shards, the information is an aggregate of information from all child items in the set or shard.

- **Statistics**: The Statistics tab displays index statistics. If multiple partitions exist, the user can select the partition for which to view statistics. These statistics include:

Processing Statistics:

- **Target Time**: Any item modified more recently than this time is not yet eligible for processing.
- **Processed Through**: The modified time of the item that the index has most recently processed.
- **Status**: Indicates whether the index is up to date, behind or backfilling.

Index Statistics:

- **Size On Disk**: The size of the index files.
- **Total Segments**: The number of Lucene segments.
- **Total Documents**: The number of Lucene documents.
- **Total Deleted Items**: The total number of Lucene-deleted items.

- **Request Operation**: The **Request Operation** tab gives the administrator the ability to create new ad-hoc operations. These operations include:
  - **Repair**: Fix corruption.
  - **Revert**: Revert primary partition(s) to secondary partition(s).
  - **Refresh**: Update secondary partition(s) from primary partition(s).
  - **Move**: Move partition(s) from current location(s) to specified location(s).
  - **Itemize**: Verify the contents of partition(s) and account for missing items.
  - **Backup**: Back up partition files to disk.
  - **Restore**: Restore partition files from disk.

The Partition Operations table

When you click on a partition, a partition set, or a shard in the dashboard a Partition Operations table is displayed. This table provides details on any current operations which are generated automatically by the system or by the user. The table allows you to navigate through pages of results or sort by columns. At the partition level, you can click View Full Log to go to the main Index Operation Log, which provides filtering options.

The top of the table contains a Show Completed checkbox that allows the administrator to view completed operations in addition to those that have not finished. The table also allows you to click the red X to the right of the action to cancel manual operations. Automatic operations cannot be canceled.

Index Operation Log

The Index Operation Log page allows you to view and search index operation logs. The page provides several filter options which correspond to the columns in the Operation Log table. The page contains the following filters:

- **Requested Time:** The date and time selected to start the operation.
- **Start Time:** The date and time the operation was actually started.
- **End Time:** The date and time the operation ended.
- **Source Partition:** The partition selected for the operation.
- **Other Partition:** A partition that was impacted by the operation performed on the source partition.
- **Action:** The type of operation logged. Actions include:
  - **Index:** Normal Full Text Index operations.
  - **Search:** Normal Full Text Search operations.
  - **Split:** Divide a large legacy partition into multiple partitions.

    - **Backup:** Back up partition files to disk.
    - **Move:** Move partition(s) from current location(s) to specified location(s).
    - **Restore:** Restore partition files from disk.
    - **Revert:** Revert primary partition(s) to secondary partition(s).
    - **Refresh:** Update secondary partition(s) from primary partition(s).
    - **Itemize:** Verify the contents of partition(s) and account for missing items.
    - **Repair:** Fix corruption.
- **State:** One of the following: Pending, Running, Complete, Failed, Canceled, Interrupted
- **Warning Count Min:** Search for logs with the minimum number of warnings specified.
- **Error Count Min:** Search for logs with the minimum number of errors specified.
- **Warning Count Max:** Search for logs with the maximum number of warnings specified.
- **Error Count Max:** Search for logs with the maximum number of errors specified.
- **Source Type:** The type of operation requested: All, Automatic, Manual, or Scheduled.
- **Login Name:** The login name of the user who requested the operation. This applies only to manual operations.

Index Rollover Policy

The Index Rollover Policy page displays current settings about when the current (newest) partition rolls over and a newly-created partition becomes the current partition. It also defines the configuration of the partitions.If you selected **Default Configuration** in the Archive Manager installer, the rollover policy is populated with the default settings.

The Index Rollover Policy page has two tabs: Message and Attachment. Each tab provides the policy for its index.You can edit the rollover policy by the following settings on the Message or Attachment tab:

- Partition Locations
- Failover Mode
- Limit Type Settings
- Primary Indexing Schedule
- Primary Backup Settings
- Secondary Refresh Settings

Click **Update Rollover** to save the form data on this page. If you wish to revert to the last saved version of the form, click **Reset**.

Partition Locations

Specify where new partitions will be located by entering the desired drives and their Failover Mode. At least one drive is required for the policy to be valid, and a policy that does not specify a drive cannot be saved.

To specify a new partition

1 Type the drive name in the text box, for example, "C".

2 Click **Add**.

Failover Mode

This section provides these options for partitions to enable or disable failover mode:

- **None**: No failover enabled
- **Passive**
- **Remove existing secondary partitions** (available when you select **None** for failover mode): The existing secondary partitions will be removed when this option is selected. If not removed, these partitions can still work without failover enabled.

Limit Type Settings

This section allows the administrator to set a threshold for partitions to roll over. The threshold can be set by the following options:

- **Age**: Partitions will roll over after a specified number of days.
- **Count**: Partitions will roll over when the total number of messages or attachments exceeds specified limit.
- **Size**: Partitions will roll over when the total size of messages or attachments exceeds specified limit.

Primary Indexing Schedule

The Primary Indexing Schedule settings specify when new primary partitions will be indexed and at what priority.

- **Index Delay (Minutes):** The amount of time an item has to remain unchanged before it is indexed. The default is 720 minutes (12 hours).
- **Priority:** The level of resources devoted to indexing.
- **Index Between:** Select the hours you would like indexing to run.

Primary Backup Settings

The Primary Backup Settings section allows the administrator to configure whether the primary partition will be backed up to disk, when and to which directory. It can be configured in increments of days or weeks. The time scheduled is displayed to the right of the controls.

- **Enable Backups:** Select this checkbox to enable backup of the primary partition.
- **Parent Directory:** Enter the directory in which to place the backup data.
- **Start Between:** Select the time frame in which to conduct the backup.
- **On every:** Select the number of days or weeks between backups and the day on which to start the backup.

Secondary Refresh Settings

The Secondary Refresh Settings section indicates if and when each new failover partition will be refreshed from its primary partition. It can be configured in increments of days or weeks. This section only displays when there are more than one drive.

- **Start Between:** Select the time frame in which to conduct the backup.
- **On every:** Select the number of days or weeks between backups and the day on which to start the backup.

8

Logins

- About logins
- Using an Exchange login
- Using a GroupWise login
- Add, edit or delete a login

About logins

Archive Manager supports two types of logins:

- The login that is generated from the directory service in the organization (for example, Active Directory)
- The Archive Manager internal login, which uses information from Archive Manager's SQL database to sign in and is maintained from the Archive Manager user interface

NOTE: GroupWise logins are limited to 79 characters. The limit applies to the number of characters in the common name and its context.

The Archive Manager Directory Connector will generally keep your Directory Service logins in sync with their status in the directory (for example, Deleted or Disabled).

Mailboxes are automatically generated and associated with a login; however, Archive Manager also lets you add virtual mailboxes and associate them with logins.

Like mailboxes, some groups are automatically generated, and you can also create Archive Manager-specific groups that comprise specific logins or mailboxes.

Under normal conditions, logins are managed automatically through the Archive Manager Directory Connectors. However, Archive Manager provides the Login Administration page for manual management of user accounts, including the display name, email address, password, security role, and account activation.

Archive Manager uses 'mixed mode' security, which allows authentication of logins against either the Archive Manager database or, where applicable, a directory service such as Microsoft Active Directory.

Using an Exchange login

The following Archive Manager items are displayed on the Archive Manager login screen:

- **User Name:** Enter the user name for the account you wish to use to sign in to Archive Manager.
- **Password:** Enter the password for the account that you entered to sign in to Archive Manager.
- **Remember Me:** Check this box if you want Archive Manager to remember the user name and domain the next time you sign in to Archive Manager from the machine you are currently using to sign in.
- **Login:** Click this button to sign in to Archive Manager after entering your credentials.

Using a GroupWise login

To sign in to Archive Manager for GroupWise environments, enter your login credentials. The following items are displayed on the Archive Manager login screen:

- **User Name:** Enter the user name for the account you wish to use to sign in to Archive Manager.
- **Password:** Enter the password for the account that you entered to sign in to Archive Manager.
- **Remember Me:** Check this box if you want Archive Manager to remember the user name and domain the next time you sign in to Archive Manager from the machine you are currently using to sign in.
- **Login:** Click this button to sign in to Archive Manager after entering your credentials.

If the user name for the account that you use enter to sign in to Archive Manager is unique to one tree and one context, the login screen does not display the Tree and Context fields. If the user name for the account that you enter to sign in to Archive Manager is not unique because it appears in multiple trees and/or contexts, the Tree and Context fields are displayed when you tab to or click in the Password box.

- **Tree:** In Novell Directory Services (NDS), the container objects and all the leaf objects that make up the hierarchical structure of the NDS database.
- **Context:** Specify the complete path name for that NDS tree in the Context field.

Add, edit or delete a login

The following sections provide information on adding, editing, or deleting a login.

Add a login

1. Select the **Add a Login** link to display the **Add Login** form.
2. Enter or select values for the following:
   - **Login Name** - The email address or user name that the user will use to sign into Archive Manager.
   - **Display Name** - The “friendly” name used to identify the user in Archive Manager.
   - **Email address** - The email address associated with this login if this user sends or replies to email messages from within Archive Manager.
   - **Password** - The password that the user will use to sign into Archive Manager.
   - **Security Role** - The security settings associated with the login (see the Security roles chapter for more information).
   - **Active** (checkbox) - Sets the login to 'Active' status.
3. Click **Add** to add the new login to the system.

   NOTE: This will only create an Archive Manager managed login. This will NOT create an account in your directory service.

Edit a login

To modify a login:

1. Locate the login in the list of logins displayed in the Login Administration form. Logins can be located by:
   - Scrolling through the list of logins.

- Entering a value in the Login Name or Display Name field.
- Choosing a security role from the drop-down list.
- Choosing a login domain from the drop-down list.
- Choosing whether the login is active or inactive.

2 Click **Search**.

3 Click the **Edit** icon to the left of the login name to display the **Edit Login** form for the selected login.

All fields are editable for a login created in Archive Manager (not by the directory connector). Editable fields include:

- Login Name
- Display Name
- Email Address
- Password
- Security Role
- Active

NOTE: For logins created by GroupWise Directory Connector (GDC) or the Active Directory Connector (ADC), some login fields are editable. However, it is not recommended that you edit any fields except the Security Role because they will be overwritten the next time the directory connector runs.

While editing a login, you can:

- Change the general information associated with a login.
- Add Login to a Group.
- Delete a Group from a Login.
- Add a Mailbox to a Login.
- Delete a Mailbox from a Login.

General information

To change the general information associated with a login:

1 Enter or select new values for the displayed fields.

2 Click **Update**. Your changes to the login are saved, and the **Login Administration** form is displayed.

Add a login to a group

Two types of groups are used to manage multiple users or mailboxes as a single entity:

- Directory Groups - These are automatically generated by the directory service to which Archive Manager is connected.
- Archive Manager Groups - These are created within Archive Manager.

Archive Manager administrators are only able to add and modify Archive Manager groups from within the application.

To add a Login to a Group:

1 Locate the desired group in the list of groups displayed on the right side of the Groups tab of the Edit Login form by doing one of the following:

- Enter the name of the desired group in the Find Group field, and click **Search**.

- Use the page browsing controls below the list of groups to browse for the desired group.

2 Select the checkboxes to the right of the groups to which you want to assign the user.

> **NOTE:** Although multiple groups can be added at once, the selected groups must all be displayed on the same page. If you browse to another page, any selections on the current page will be lost.

3 Click **Add Selection**. The selected groups are added to the list of groups displayed on the left side of the Groups tab of the Edit Login form.

Delete a group from a login

1 Click **Delete** to the right of the group in the list of groups displayed on the left side of the **Groups** tab of the **Edit Login** form. The **Delete Group** confirmation message is displayed.

2 Click **OK** to confirm the deletion. The selected group is deleted from the list of groups, and the **Edit Login** form is displayed.

Add a mailbox to a login

1 Locate the desired mailbox in the list of mailboxes displayed on the right side of the **Mailboxes** tab of the **Edit Login** form by doing either of the following:

- Entering the name of the desired mailbox in the **Find Mailbox** field, and then clicking **Search**.
- Using the page browsing controls below the list of mailboxes to browse for the desired mailbox.

2 Select the checkboxes to the right of the mailboxes that you want to assign the user to.

> **NOTE:** Although multiple mailboxes can be added at once, the selected mailboxes must all be displayed on the same page. If you browse to another page, any selections on the current page will be lost.

3 Click **Add to Mailbox**. The selected mailboxes are added to the list of mailboxes displayed on the left side of the **Mailboxes** tab of the **Edit Login** form.

Delete a mailbox from a login

1 Locate the mailbox you want to delete from the list of mailboxes displayed on the left side of the **Mailboxes** tab of the **Edit Login** form.

2 Click **Delete** to the right of the mailbox to display the **Delete Mailbox** confirmation message.

3 Click **OK** to confirm the deletion. The selected mailbox is deleted from the list of mailboxes, and the **Edit Login** form is displayed.

Delete a login

1 Locate the login in the list of logins displayed in the **Login Administration** form. Logins can be located by doing any of the following:

- Scrolling through the list of logins
- Entering a value in the **Login Name** or **Display Name** field
- Choosing a security role from the drop-down list
- Choosing a login domain from the drop-down list
- Choosing whether the login is active or inactive

2 Click **Search**.

3 Click **Delete.**

4 Click to the left of the login name to display the **Delete Login** confirmation message.

5 Click **OK** to confirm the deletion. The selected login is deleted, and the **Login Administration** form is displayed.

NOTE: Alternatively, a login can be deleted by opening the Edit Login form, clicking **Delete**, and confirming the deletion.

NOTE: Logins originating from the mail server will be added back the next time the directory connector runs. Only Archive Manager logins will remain permanently deleted.

9

Security roles

- About security roles
- Add, edit or delete a security role
- Security actions

About security roles

A security role defines a set of program activities and functions that can be made available to a particular category or class of Archive Manager users. A security role is assigned to every Archive Manager user, and that assignment determines what the user can and cannot do within Archive Manager. The definition of a security role is essentially a checklist of program activities, called *security actions*, showing which ones a user of that class is authorized to perform.

NOTE: Security roles can be assigned only to users.

Archive Manager installs with four pre-defined security roles, for *Administrator*, *Manager*, *Resource* and *User*—simply because these are common role designations at many Archive Manager sites. But you are free to change (add or subtract) the authorized security actions for any of these default security roles, or add new security roles of your own design, or delete security roles for which your organization has no use, except for the Administrator security role.

The Security actions section at the end of this chapter provides a complete list of all security actions that may be assigned to a security role. The four default Archive Manager security roles, as installed, permit these security actions:

Table 7. Security roles

Administrator	Manager	Resource	User
All except: • View BCC • View Report- My Search Logs • Impersonate	• Add/Edit Custom Mailboxes • Reply and Forward • Search All Emails	• Add/Edit Customer Mailboxes	• Add/Edit Custom Mailboxes • Reply and Forward

Add, edit or delete a security role

The following sections provide information on adding, editing, or deleting a Security Role.

Add a security role

1. Select the **Add a Security Role** link to display the **Add Security Role** form.
2. Enter a name for the security group in the **Security Role** field.

3 Click **Add** to add the new security role to the system.

Edit a security role

1 In the list of security roles, locate the one you want to edit. Either:

- Scroll through the list of security roles; ***or***
- Enter a value in the **Security Role** field and click **Search**.

2 Click **Edit** to the left of the security role name to display the **Edit Security Role** form for the selected role.

Revise the security role information as described in the following steps.

To add a security action:

1 Locate the security action in the list of available security actions.

2 Select the checkbox to the right of each security action you want to associate with this security role, and click **Add Selection** (at the bottom of the column).

The specified security action is moved from the list of actions available to add to the list of actions currently loaded and associated with the security role.

To delete a security action:

1 Locate the security action in the list of currently selected security actions displayed in the **Edit Security Role** form.

2 Click **Delete** to the right of the security action. The **Delete Security Action** confirmation message is displayed.

3 Click **OK** to confirm the deletion. The selected security action is removed from the list of currently-loaded security actions associated with the security role and re-displayed in the list of security actions available to add.

Delete a security role

1 Locate the security role in the list of security roles by doing one of the following:

- Scrolling through the list of security roles.
- Entering a value in the **Security Role** field and clicking **Search**.

2 Click **Delete** to the left of the group name. The **Delete Group** confirmation message is displayed.

3 Click **OK** to confirm the deletion. The selected security role is deleted, and the **Security Role Administration** form is displayed.

NOTE: Alternatively, you can delete a security role by opening the **Edit Security Role** form (as described in the section **Edit Security Role**), clicking **Delete**, and confirming the deletion.

Security actions

Security actions grant permissions for specific actions. Each security role has actions assigned to it that define permissions for users assigned to that role. The following is a list of security actions in Archive Manager:

- **Add/Edit Custom Mailboxes:** Removes the ability to see or access Custom Mailboxes, but the pane always remains in view.
- **Add Messages:** Lets a user add new messages to Archive Manager by API.

- **Assign PST Migration Policy:** A legacy action from a previous version of Archive Manager (for backward compatibility only).
- **Change Authentication Mode:** Lets a user access the Administration section of Archive Manager and change whether users will sign in with Windows authentication or Forms authentication. It is recommended that this action be restricted to administrators only. Changing authentication modes requires some manual configuration of the Website through the IIS Manager. Please see the see the Authentication modes chapter.
- **Delegate Mailboxes:** Allows users to delegate permissions to the mailboxes that they own. It is assigned to the **Administrator** security role by default.
- **Download Tools:** Lets a user access the Administration section of Archive Manager and download any of the available tools. Many of these tools augment administrative functions of Archive Manager, and it is recommended that this action be restricted to administrators only.
- **Edit Alert Service Policies:** Lets a user create, edit and delete alert service policies.
- **Edit Config Settings:** Lets a user to create, edit and delete configuration settings.
- **Edit Data Loaders:** Lets a user access the Administration section of Archive Manager with rights to add, edit, and delete the Data Loader configuration. It is recommended that this action be restricted to only administrators who understand the impacts of the Data Loader configuration.
- **Edit Exclusion Rules:** Lets a user access the Administration section of Archive Manager, with rights to add, edit, and delete Exclusion Rules. Exclusion Rules are processed by the Data Loader and can be used to prevent certain types of content from entering the archive.
- **Edit Federated Search Instances:** Lets a user access the Administration section or Archive Manager, with rights to add, edit, and delete the Federated Search Instance configuration. This configuration also lets Archive Manager search other instances. (This action does not let a user search other instances, which is controlled by the *Search All Instances* security action.)
- **Edit Groups:** Lets a user access the Administration section of Archive Manager, with rights to review groups that have been populated by the Active Directory Connector. The user can also create, edit, and delete Groups for the DEFAULT domain, which is the Archive Manager Security domain.
- **Edit Legal Hold:** Lets a user set and remove Legal Hold. To do this, the user must have the Archive Manager Retention Editor installed. The *Legal Hold* tab is used to put an immediate stop on the Retention engine while urgent policy change is evaluated.
- **Edit Logins:** Lets a user access the Administration section of Archive manager, and review the Logins that have been populated by the Active Directory Connector. The user can also create, edit, and delete Logins for the DEFAULT domain, which is the Archive Manager Security Domain. In addition, the user can edit security roles, and access mailboxes for users populated by the Directory Connector. Users cannot change their own security roles, but if they have access to the *Edit Security Roles* action, they will be able to add or remove actions from their security roles.
- **Edit Lync Archiving:** Lets a user access the Administration section of Archive Manager to edit, enable, or disable a Lync server, and edit and delete security roles. Users cannot delete security roles that are in use; a security role must be removed from all logins before it can be deleted.
- **Edit Mailboxes:** Lets a user access the Administration section of the Archive Manager website, and review mailboxes that have been populated by the Active Directory Connector. The user can also create, edit and delete Custom Mailboxes, and can edit which logins can access mailboxes populated by the AD Connector.
- **Edit Message Policies:** Lets a user access the Administration section of Archive Manager, and create, edit and delete message policies. Use caution in assigning this privilege, since editing existing message policies can change the operational parameters for the archive and may cause unwanted behavior such as the deletion of messages from the Exchange Mailbox Store. Users cannot delete message policies that are currently in use.
- **Edit Message Tags:** Lets a user access the Administration section of Archive Manager, and create, edit and delete message tags. Users cannot delete tags that are in use.
- **Edit Proxy Credentials:** Lets a user manage the proxy credentials for Office 365 or hosted Exchange mailboxes.

- **Edit PST Migration Policies:** A legacy action from a previous version of Archive Manager (for backward compatibility only).
- **Edit Retention Policies:** Lets a user create, edit and delete retention policies.
- **Edit Security Roles:** Lets a user access the Administration section of Archive Manager, and create, edit and delete security roles. Users cannot delete security roles that are in use; a security role must be removed from all logins before it can be deleted. Use caution in assigning this privilege, since it controls your permissions within Archive Manager.
- **Export Email:** Makes the *Export* button accessible on the right-hand side of the search interface. Since this export feature applies only to search results, the button is available only when a search has been completed. The Search Exporter must be installed on the workstation for this button to export the result.
- **Impersonate:** This security action is used for performing a Federated Search. It assigns credentials for a user on the remote instance you wish to search. When configuring Federated Instances, the Impersonate security action must be applied to the Security Role containing the configured federated user.
- **Person Search:** Allows access to the Person Search dialog box from the *To/From* Search tab and the Send Message window in the Website.
- **Reply and Forward:** Makes the *Reply*, *Forward,* and *Send To Me* buttons available when viewing a message. These buttons appear only when enabled if the user has an SMTP email address listed in the login record.
- **Search All Emails:** Makes the *Search All Emails* check box available in the Search section of the Archive Manager User Website. Since this privilege lets a user search all email in the Archive Manager store, it should be extended only to end users who need this level of control. By default, this action is assigned to the Administrator security role, but you should consider removing it from that role once the system is in production.
- **Search All Instances:** Makes the *Search All Instances* check box available in the Search section of the Archive Manager User Website, which lets a user search all email in the Archive Manager store on federated instances. The federated instances are controlled by the administrator from the Administration Website. There is no option to restrict the user to a specific instance; this action allows a user to search all configured instances.
- **Set Message Tags:** Lets a user see the *Tags* tab when viewing a message, and set any of the available tags on the message. It does not let the user create tags. Creating tags is handled by the *Edit Message Tags* action described above.
- **Storage Location:** Lets a user to create, edit and delete storage location.
- **View Additional Documentation:** Lets a user access the Documentation section of the Administration Website.
- **View BCC:** Lets a user see the BCC information for a message when it is viewed through the Archive Manager Website.
- **View Config Settings:** Lets a user view all configuration settings.
- **View Delegation:** Produces a report that lets a user view the history of the hosted mailbox delegation.
- **View Message Access History:** Displays an *Access* tab when viewing a message in the Archive Manager Website. The *Access* tab lists all users that have opened and viewed the message from the Archive Manager Website. This action is not assigned to users by default.
- **View Message Comments:** Displays a *Comments* tab when viewing a message, which lets a user view and add comments to the message. Comments can be marked public or private. Public comments are visible to all users who have the *View Message Comments* action; private comments are visible only to the user who created them.
- **View Message Headers:** Displays a *Header* tab when viewing a message, which lets a user see the MIME header of the message.
- **View Message Journal Report:** When using Journaling, displays extended information such as Distribution List expansion and BCC recipient in addition to the Journal Report.

- **View Message Tags:** Displays the *Tags* tab when viewing a message, which lets the user view tags that have been applied to the message. If users need to add or delete tags, they must also have the *Set Message Tags* security action.
- **View Report - Event Log:** This report is no longer available. Use the Windows Event Viewer application to view the Archive Manager Event Log.
- **View Report - Mailbox Scan Status:** Produces a report that lets a user view the latest status of the mailbox scanning.
- **View Report - My Search Log:** Produces a report that lets a user view a history of his/her searches within Archive Manager. This action is disabled by default. It is specifically excluded from the Administrator Security Role since that security role has access to the *View Report - Search Log* security action, which provides the same level of access.
- **View Report - Search Log:** Produces a report that lets a user view a history of either a specific user over a given time period, or all users over a given time period.
- **View Report - Security Breach:** This report is no longer available. Assign access the *Unauthorized Access* report instead.
- **View Report - Viewed Messages:** This report shows all messages opened by the user.

10

Storage location

- Storage location and migration
- Prerequisites
- Storage Location tab
- Storage Migration tab
- View Storage Migration History

Storage location and migration

The storage location and migration pages allow you to configure the storage location and migrate attachments from the current storage location to another storage location.

Prerequisites

- Storage Location Security Action

  To add this security action, see the Security roles chapter in this guide.

Storage Location tab

The Storage Location link is located on the navigation bar of the Archive Manager Administration website. Click this link to access the Storage Location page. All existing storage locations are displayed here.

To add a storage location:

1. Click the **Click here to create a new Storage Location** link to view the Storage Location page.
2. In the Type drop-down list, select one of the following storage location types:
   - File System
   - EMC Centera
   - NetApp SnapLock
   - Caringo DX

If **File System** is selected as the storage location, enter the following information:

- **Server and Share Name:** The Path of attachment store share.
- **Store message data for compliance:** Select this check box if you want to keep a copy of your message archive outside of the message database.
- **Compliance Directory Path:** The location of the compliance archive.

- **Default Storage Location:** Select this to check box to remove the existing default storage location and set the current storage location as the default. Only one default storage location is allowed.

If **EMC Centera** is selected as the storage location, enter the following information:

- **EMC Centera Connection String:** The location of the .pea file.
- **Store message data for compliance:** Select this check box if you want to keep a copy of your message archive outside of the message database.
- **Default Storage Location:** Select this to check box to remove the existing default storage location and set the current storage location as the default. Only one default storage location is allowed.

If **NetApp SnapLock** is selected as the storage location, enter the following information:

- **Share name:** The path to the volume. The format is *computer name* or *IP address**volume* name.
- **Retention Mode:** Select one of the following three options:

  If you select **SnapLock Default**, Archive Manager uses SnapLock's default time to store messages.

  If you select **Archive Manager Default**, enter the following Retention Time settings:

  - Days
  - Months
  - Years

  If you select **SnapLock Compliance**, there is a minimum of 0 days and a maximum of 30 years. The default is the maximum of 30 years. If you are running SnapLock Enterprise, the default is the minimum of 0 days.
- **Store message data for compliance:** Select this check box if you want to keep a copy of your message archive outside of the message database.
- **Default Storage Location:** Select this to check box to remove the existing default storage location and set the current storage location as the default. Only one default storage location is allowed.
- **Login:** The account name used to connect to the SnapLock volume.
- **Password:** The password for the account used to connect to the SnapLock volume.
- **Hostname:** The name of the SnapLock volume.
- **Test:** Click this button to test that the user input is valid.

If **Caringo DX** is selected as the storage location, enter the following information:

- **Hosts**: The hosts to connect to. Multiple hosts are 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.

The following additional information may be defined for a Caringo DX storage location.

- **Cluster Name**: The name of the cluster for the Caringo DX storage location.
- **Proxy Address**: The cluster reverse proxy IP address.
- **Proxy Port**: The cluster reverse proxy access port.
- **Max Retries**: The 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.
- **Connection Timeout**: The time in seconds that a request will wait for a connection and for activity on a request.
- **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.

- **Realm**: The Caringo security domain/realm.
- **Bucket**: The name of the container within the device.
- **Hash Type**: The hash algorithm to use to verify content integrity.
- **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.
- **Store message Data for Compliance**: Like other storage types, users can choose to save copies of all of the email to be stored in external storage. This check box controls the behavior.
- **Default Storage Location**: Select this to check box to remove the existing default storage location and set the current storage location as the default. Only one default storage location is allowed.
- **Test**: Click this button to test that the user input is valid, and the Caringo DX storage can be reached.

To edit or delete the storage location:

- To edit a storage location, click the **Edit** button to the left of the Type column.
- To delete a storage location, click the **Delete** button located to the left of the Type column.

Storage Migration tab

The Storage Migration tab allow you to migrate attachments files from the storage location to another storage location.

To migrate attachment files:

1. Enter the following information on the screen:
    - **Name:** The migration task name.
    - **Source storage location:** The storage location to copy. After a storage location is selected, the file count and file size will be shown below.
    - **Target storage location:** The destination storage location.
    - **Delete source files after migrated:** Delete the attachment files in the source storage location after the migration task is committed.
    - **Auto commit if there is no error in the migration process:** The migration task will be auto committed if there is no error, such as cannot read source file, cannot write to target storage location, cannot update database, etc.
    - **Batch size:** The number of attachment files to migrate in a single batch. The default value is 1000.
    - **Batch Delay:** The time in milliseconds to wait before start next batch.
    - **Maximum number of retries:** The number of times to retry if the migration tool cannot migrate a single attachment file. For example, if it cannot read source file, the migration tool tries to migrate the attachment file. This setting defines how many retries.
    - **Number of processes:** As Archive Manager uses the remote host to process to read/write attachment files, this setting declares that how many remote host processes are created.
2. When all of the information has been entered, click **Save**.

    After clicking **Save**, three new buttons are displayed:
    - **Start:** Click this button to start the migration task.
    - **Edit:** Click this button to edit the migration task.

- **Delete:** Click this button to delete the migration task.

Migration Status

The migration status is displayed in the top right-hand corner of the Storage Migration page.

- **New:** The status when a user creates and saves a migration task.

  In this state, a task can be deleted by clicking the **Delete** button.

- **In Progress:** The status after clicking the **Start** button to start the migration task.

  In this state, the migration task cannot be edited or deleted.

- **Executed:** The status after all the attachment files are moved to the target storage location. When the status is Executed, the following buttons are displayed on the bottom right-hand side of the screen:
  - **Retry:** If there are attachment files that have failed to migration due to an error (cannot read, cannot write, etc.), the user can click **Retry** to attempt the migration again.

    After the **Retry** button is clicked, the status becomes **In Progress** again.

    After retrying to migrate all failed attachment files, the migration status becomes **Executed** again.
  - **Cancel:** Deletes all of the attachments that have been copied to the target storage location and updates the data table "AttachmentFile." Attachments files from the existing source will be used.

    The user can click **Cancel** at any time. After the **Cancel** button is clicked, the status becomes **In Progress**. After all the attachment files are canceled, the task status becomes **Canceled**.
  - **Commit:** Ignore the failed attachment files and commit the task.
- **Done:** The status when the task is committed. In this state, the task cannot be canceled or deleted.

When the status is changed from **New** to **In Progress** by clicking the **Start** button, a grid is displayed at the bottom of the page that includes the following information:

- **Pending:** The number of attachment files waiting to migrate.
- **Moved:** The number of attachment files that migrated.
- **Canceling:** The number of attachment files that waiting to be canceled.
- **Canceled:** The number of attachment files that have been canceled.
- **Failed:** The number of attachment files that cannot be migrated. (Cannot read, cannot write, etc.)

View Storage Migration History

To view a history of migration storage locations, click the **View Storage Migration History** link.

The storage history table contains the following columns:

- Task Name
- Source
- Target
- Created Time
- Status

If you do not see the task name that you are looking for in the table, enter the task name in the **Name** field to conduct a search.

11

Message tags

- About message tags
- Add, edit or delete a message tag

About message tags

Additional properties can be assigned to messages in Archive Manager. For example, you can tag messages with information relating to an investigation or a particular customer. This makes it easy to group messages together to identify them for particular purposes.

Users can then search for messages with these user-defined properties, in addition to any other search criteria.

A message tag is characterized by the values of these four fields:

- **Tag Name:** The name for the tag that is being created.
- **Tag Type:** Five different types are available:
  - **Boolean:** True or False.
  - **DateTime:** Date, Time.
  - **Flag:** User-defined (Personal, Important, Follow-up, etc.).
  - **Number:** Numerical.
  - **String** (default): Any text, including letters, numbers.
- **Default Tag Value:** The default value of the tag. The values available depend on the tag type selected.
- **System Property** (checkbox): Whether this is an Archive Manager-managed tag or a user-managed tag.

CAUTION: Tags are set globally. When a retention delete policy is defined by a tag, the policy will delete all tagged messages in the database, in all mailbox locations—not just in the mailbox where the tag was added. That is, if a message is tagged in a particular mailbox, and then the same tag is used in a delete policy applied to a higher-level container (e.g., OU), the message will be deleted from the archive at the higher container level, in all mailboxes.

Add, edit or delete a message tag

The following sections discuss managing message tags.

Add a message tag

1. Click the **Add a Tag** link.
2. Enter or select values for the fields, as defined above.
3. Click **Add**. The tag will be created and the **Message Tag Administration** screen will be displayed.

Edit a message tag

1. Locate the message tag in the list of tags displayed in the **Message Tag Administration** form.
2. Click **Edit** to the left of the tag name to display the **Edit Message Tag** form for the selected Tag.
3. Revise the information and then click **Update**. Your changes to the tag are saved, and the **Message Tag Administration** form is displayed.

NOTE: To return to the Message Tag Administration screen without editing the tag, click **Cancel**.

Delete a message tag

1. Locate the message tag in the list of tags displayed in the **Message Tag Administration** form.
2. Click **Delete** to the left of the tag name. The **Delete Tag** confirmation message is displayed.
3. Click **OK** to confirm the deletion. The selected tag is deleted, and the **Message Tag Administration** form is displayed.

NOTE: A message tag can only be deleted if it is not applied to any messages. If you try to delete a message tag that is in use, you will see an error message.

NOTE: Alternatively, a tag can be deleted by opening the **Edit Message Tags** form, clicking **Delete**, and confirming the deletion.

12

Proxy credentials

- About proxy credentials
- Add, edit or delete proxy credentials

About proxy credentials

Proxy credentials are used by Archive Manager to access your Office 365 or hosted Exchange mailboxes. The **Proxy Credentials** page in the Archive Manager Website allows you to view and manage your proxy credentials.

This page is only visible when you have the **Edit Proxy Credentials** permission, and one of the following conditions is met:

- You have added an Office 365 tenant in Configuration Console.
- You have set the parameter **EnableRemoteMailBoxDelegation** to **True** in Configuration Console.

Add, edit or delete proxy credentials

The following section discusses managing proxy credentials.

To add proxy credentials:

1. On the **Proxy Credentials** page, click **Click here to Add Credentials**.
2. Enter or select values for the fields.

   NOTE: The login domains in the drop down list are in the format `<domain_name>(<LDAP_type>)`, for example, a domain in Office 365 will be `<domain_name>(Azure AD)`.

3. Click **Add**.

NOTE: For Office 365, you must assign an Exchange Online license to the proxy credentials you want to add, and make sure that one of the following conditions is met:

- MFA (Multi-Factor Authentication) is not enabled on Office 365.
- You have added the Archive Manager servers to Trusted IPs.

NOTE: For hosted Exchange mailboxes, users must re-enable access to their remote mailboxes on the **Configure Archive Access** page to delegate access to newly-added proxy credentials.

To edit proxy credentials:

1. On the **Proxy Credentials** page, click the **Edit** icon to the left of the login name for the selected credentials in the list.
2. Revise the information and then click **Update**.
3. In the **Mail Servers** tab, manage the mail servers that the proxy credentials are assigned to.

To grant permissions to a new mail server, search it by the mail server name, select the check box and click **Add Selection**. To remove permissions from a mail server, click the delete icon .

NOTE: You may see the status showing as **Granting** or **Removing** for a while because the operation is performed by the Active Directory Connector service which runs periodically. The status will change to **Granted**, or the mail servers will be removed after the service runs again.
To grant or remove permissions immediately, open Command Prompt and switch to the Archive Manager root folder, and execute the following command:

```
ActiveDirectoryConnectorService.exe -console -mspermission
```

OR

```
ActiveDirectoryConnectorService.exe -console -mspermission -remove
```

The commands are as follows for an hosted environment:

```
ActiveDirectoryConnectorService.exe -console -mspermission -hosted
```

OR

```
ActiveDirectoryConnectorService.exe -console -mspermission -hosted -removed
```

To delete proxy credentials:

1. On the **Proxy Credentials** page, click the delete icon to the left of the login name for the selected credentials in the list.
2. Confirm the deletion.

NOTE: Proxy credentials that have been assigned to a mail server cannot be deleted.

13

Alert Service Policies

- About Alert Service Policies
- Default Global Settings
- Adding an Alert Policy
- Modifying an Alert Policy

About Alert Service Policies

The Archive Manager Alert Service allows you to run SQL queries on the Archive Manager database and WMI queries on your server. The administrator can configure the Alert Service Policies to instruct the Alert Service to send out email alerts, based on the results of a query. For example, if an administrator wants be alerted when the attachments to index queue becomes too large, an Alert Service Policy can be configured to have the Alert Service send out an email when the number of messages to index exceeds a specified threshold.

Default Global Settings

The first time you open the Alert Service Policies page, you are asked to set the Default Global Settings. All other controls on this page are grayed out until Default Global Settings are defined. These defaults can be changed later by clicking **Default Global Settings** on the Alert Service Policies screen.

On the **Default Global Settings** screen, enter the following information:

- **When: Count Threshold**: A numeric value for the number of messages. Select **Greater Than** or **Less Than.** When this threshold is exceeded, the Alert Service sends an alert message for your query.
- **From**: The email address from which the alert message is sent.
- **To**: The email address of the user(s) to which the email alert is sent.
- **Subject**: The subject of the alert email message.
- **Message Body**: The message body. You may want to include key words that could be used by a message filter.
- **Check Interval**: A number of minutes, hours, or days. This is the time interval between checks of query results by the Alert Service.

Adding an Alert Policy

To add an alert policy:

1 On the Archive Manager **Alert Service Policies** page, click **+Alert**.

NOTE: If the **Use Defaults** check box is selected, only the **Name** field is editable and values for the remaining fields are taken from the Default Global Settings.

2 In the **New Alert Policy** screen, select a query **Name** from the drop-down list. The following query names are available:

- Archive Manager Full Text Index Service
- Archive Manager Active Directory Connector Service
- Archive Manager Data Load Service
- Archive Manager Exchange Store Manager Service
- Archive Manager Full Text Search Service
- Archive Manager Message Retention Policy Service
- Archive Manager Error Folder
- Archive Manager Export Folder
- Archive Manager Messages to Index
- Archive Manager Attachments to Index
- Archive Manager Unprocessed Mailboxes
- Archive Manager Pending Messages
- Archive Manager Database Size (query results returned in MBs)
- Archive Manager Min Proxy Credentials on Hosted Mail Servers: Traverses all hosted mail servers to find out which one has been assigned the minimum number of proxy credentials, and retrieves that number.
- Archive Manager Min Days Left to Expire for Proxy Credentials: Traverses all proxy credentials to find out which one is closest to expiration, and retrieves the number of days left.
- Archive Manager Number of Expired Proxy Credentials: Retrieves the number of proxy credentials that have expired.

3 To change any other field, deselect the **Use Defaults** check box. See Default Global Settings for field definitions.

4 Click **Save** to save the alert policy and return to the **Alert Service Policies** screen.

Modifying an Alert Policy

You can modify or delete an alert policy by clicking the Edit or Delete icon in the Alert Service Policies screen.

Sample alert message

The following is an example of how an alert message may be set up.

An administrator wants to be alerted when the attachments to index queue becomes greater than 100,000 messages. The alert is to be sent from Alerts@company.com to Administrator@company.com with the subject of “Attachments to Index Queue is Too Large”. The alert service is to check the status attachments to index every 15 minutes.

The alert policy would be defined as follows:

- **Name**: Archive Manager Attachments to Index
- **When: Count Threshold**: Greater Than or Equal To 100000
- **From**: Alerts@company.com
- **To**: Administrator@company.com
- **Subject**: Attachments to Index Queue is Too Large

- **Message Body**: Administrative action is required within 24 hours to resolve this situation.
- **Check Interval**: 12 hours

The alert message would contain the following information:

```
Name: Archive Manager Attachments to Index
Date: 9/7/2008 2:23:31 PM
Query: Select Count (*) From AttachmentToIndex
Returned: 150000
Threshold: GreaterThanOrEqualTo 100000
```

14

Exclusion rules

- About exclusion rules
- Add, edit or delete an exclusion rule

About exclusion rules

Exclusion rules allow Archive Manager to ignore an email message based on specified attributes. This can be useful for ensuring that system-generated or administration messages are not included in the Archive Manager store. Archive Manager stores an MD5 value of excluded messages, which can be purged if required.

Archive Manager includes four Exclusion Rules by default. Exchange 2013 sends automatically generated email to monitor the health of the system. It is not necessary to archive these emails. These Exclusion Rules can be deleted if needed.

- **BUILTIN: E2013 Health Monitor: From HealthMailbox:** From: HealthMailbox*
- **BUILTIN: E2013 Health Monitor: To HealthMailbox:** To HealthMailbox*
- **BUILTIN: E2013 Health Monitor: From inboundproxy:** From inboundproxy@inboundproxy.com
- **BUILTIN: E2013 Health Monitor: To inboundproxy:** To inboundproxy@inboundproxy.com

An exclusion rule cannot be deleted after an email has been excluded by that rule. Exclusion rules have the following characteristics:

- Exclusion rules are case insensitive.
- Wildcards are supported anywhere in the rule.

The Exclusion Rule criteria may include one or more of the following parameters:

NOTE: Email addresses in the To/From fields are case insensitive.

- **Name:** The name by which you want the exclusion rule to be identified (for example, "System files").
- **From:** The email address where the message(s) originated (example: *administrator@mydomain.com*).
- **To:** The email address to which the excluded email message(s) are sent. **Important:** The rule will work only where there is a single recipient in the **To** field of the message.
- **Subject:** The **Subject** of email(s) you want to exclude. The exclusion will apply only to email(s) whose **Subject**s match exactly the string entered here. You may use a wildcard asterisk in this string to represent one or more characters at the beginning or end of the string, or somewhere within the string.
- **Header:** Header information included in the email messages to be excluded (example: Content-Transfer-Encoding). The **Header Value** field (below) must contain a corresponding value for this **Header** setting to take effect.
- **Header Value:** Header value information contained in excluded email messages (example: binary).

These field notes apply to both the **Add** and **Edit** features for exclusion rules.

Add, edit or delete an exclusion rule

The following sections discuss managing exclusion rules.

Add an exclusion rule

1. Click the **Add an Exclusion Rule** link.
2. In the **Exclusion Rule** form: Enter or select values for some or all of the fields.
3. Click **Add**. The new exclusion rule is added to the system and the **Exclusion Rule Administration** screen is displayed.

NOTE: To return to the **Exclusion Rule Administration** screen without creating a rule, click **Cancel**.

Edit an exclusion rule

1. Locate the exclusion rule in the list of rules displayed in the **Exclusion Rule Administration** form.
2. Click **Edit** to the left of the exclusion rule name to display the **Edit Exclusion Rule** form for the selected Rule.
3. Revise the information and then click **Update**. Your changes to the rule are saved, and the **Exclusion Rule Administration** form is displayed.

NOTE: To return to the **Exclusion Rule Administration** screen without editing the rule, click **Cancel**.

Delete an exclusion rule

1. Locate the exclusion rule in the list of rules displayed in the **Exclusion Rule Administration** form
2. Click **Delete** to the left of the rule name. The **Delete Rule** confirmation message is displayed.
3. Click **OK** to confirm the deletion. The selected rule is deleted, and the **Exclusion Rule Administration** form is displayed.

NOTE: Alternatively, a rule can be deleted by opening the **Edit Exclusion Rule** form, clicking **Delete**, and confirming the deletion.

15

Mail servers

- About mail servers
- Edit a mail server

About mail servers

Archive Manager lets you manage each mail server. You can specify which message policies apply to each server, and to folders on that server.

Archive Manager uses mail servers to group Office 365 mailboxes and balance the workload for each Exchange Store Manager instance. Mailboxes in an Office 365 tenant are evenly divided by the value of the Active Directory Connector setting **Max Enable Store Manager MailBox Count Per O365 MailServer**, and managed by the mail servers as required. These mail servers show in the list with a name prefix `[Tenant_Name]_O365`.

Edit a mail server

1. In the **Mail Server Administration** form: Locate the mail server in the list of mail servers displayed.
2. Click **Edit** to the left of the mail server name. The **Edit Mail Server** form for the selected mail server is displayed.
3. Revise the mail server information as described below, and then click **Update**. The specified changes to the mail server are saved, and the **Mail Server Administration** form is displayed.

General Information

To change the general information associated with a mail server, enter or select new values for some or all of these fields:

- **Start Time:** Defines when the store management service (Exchange Store Manager or GroupWise Store Manager) will start exporting data for the mailboxes contained by that mail server.
- **End Time:** Defines the end of the time frame when the store management service (Exchange Store Manager or GroupWise Store Manager) can start exporting data for the mailboxes contained by that mail server.

  For example, if you enter a start time of 1:00 a.m. and an end time of 3:00 a.m., the store manager can start exporting data any time between 1:00 a.m. and 3:00 a.m. If the store manager completes exporting data at 2:50 a.m., it will initiate another data export pass for all users enabled for store management because 2:50 a.m. is within its time frame (**Start Time** and **End Time**) to start exporting data. The store manager will continue until it has finished exporting data for the entire list of users. It will not stop exporting data at 3:00 a.m.
- **Enable Store Manager:** A check box that enables or disables the Store Manager for the selected mail server.
- **Store Manager Group**: Specifies a group name for Store Manager. The default value is `default`.
- **Default Policy:** The Default policy for the selected mail server.

- **Inbox Policy** (applies to Exchange and Office 365 only): The policy for the Inbox for the selected mail server.
- **Sent Items Policy** (applies to Exchange and Office 365 only): The policy for Sent Items for the selected mail server.
- **Deleted Items Policy** (applies to Exchange and Office 365 only): The policy for Deleted Items for the selected mail server.
- **Public Folder Policy** (applies to Exchange and Office 365 only): The policy for the Public Folder for the selected mail server.

NOTE: Public folders are not processed (and do not appear in Archive Manager) unless a Public Folder Policy is set. Once a Public Folder Policy is set, it applies to all Public Folders on the mail server.

- **Use Proxy** (applies to hosted Exchange only): Use proxy credentials to log in to mailboxes on the server.

In the **Proxy Credentials** tab,

- **Proxy Credentials** (applies to mail servers using proxy credentials): Allows to grant or remove permissions to access Office 365 or hosted Exchange mail servers by adding or removing proxy credentials.

NOTE: You may see the status showing as **Granting** or **Removing** for a while because the operation is performed by the Active Directory Connector service which runs periodically. The status will change to **Granted**, or the proxy credentials will be removed after the service runs again.
To grant or remove permissions immediately, open Command Prompt and switch to the Archive Manager root folder, and execute the following command:

```
ActiveDirectoryConnectorService.exe -console -mspermission
```

OR

```
ActiveDirectoryConnectorService.exe -console -mspermission -remove
```

The commands are as follows for an hosted environment:

```
ActiveDirectoryConnectorService.exe -console -mspermission -hosted
```

OR

```
ActiveDirectoryConnectorService.exe -console -mspermission -hosted -removed
```

16

Mailbox assignment

- About mailbox assignment
- Select users
- Select mailboxes

About mailbox assignment

The Mailbox Assignment Administration screen lets you define which users can access which mailboxes.

Select users

1 Click **Browse** to select a User to add to the **Mailbox** field.

2 Click the user you want to select. Or, search for users by typing your criteria in the **Login Name** field or **Display Name** field, and then click **Search** to view a list of users that match your search criteria.

This takes you back to the Mailbox Assignment Administration screen. The display name for the selected user is displayed in the Name box.

3 On the Mailbox Assignment Administration screen, click **Search** to view the list of mailboxes assigned to the user you selected.

The list is displayed in the left-hand User column.

Select mailboxes

To grant the selected user access to mailboxes:

1 Click **Browse** next to the right-hand Name box to view a Mailbox Name list, or the Group Box to view a Group Name list.

2 Click the Mailbox Name or Group Name you want to add to the Name box or Group box.

3 Click Search to view the list of mailboxes that meet your search criteria.

4 Click the checkbox to the right of the mailboxes you want to assign access to the currently selected user.

5 Or, click **Select All** to select all mailboxes shown on the current page.

6 Click **Assign** to assign the selected mailbox(s) to the currently selected user.

17

Mailboxes

- About mailboxes
- Add, edit or delete a mailbox

About mailboxes

Archive Manager mailboxes work in a way similar to mailboxes in Microsoft Exchange, Novell GroupWise, or other similar email systems. Archive Manager provides two main types of mailboxes:

- **User:** A standard mailbox, which typically corresponds to an individual user's email address. User mailboxes are created by the Archive Manager Directory Connector.
- **Virtual:** A more flexible mailbox created to provide access using specific criteria, including external email addresses. The email addresses that comprise a virtual mailbox are a combination of specific individual email addresses or a wildcard email address.

Virtual mailboxes collect all addresses from the email address list, expand any wildcards out, and find all matching addresses. This creates a list of all possible addresses the virtual mailbox can hold. It then removes any “excluded” email addresses from the list. Archive Manager then finds all email messages with addresses that are contained in the list that was created and displays them in the virtual mailbox.

An administrator can create a wildcard email address so that all email sent to or from addresses that match the pattern defined by the administrator is included in the virtual mailbox.

NOTE: Custom mailboxes are virtual mailboxes created by users in the Archive Manager user interface. These mailboxes are managed by the administrator in the same manner as other virtual mailboxes. For more information on how users manage their custom mailboxes, see the User Guide.

Security can be assigned to both users and groups.

Add, edit or delete a mailbox

The following sections discuss managing mailboxes.

Add a mailbox

1. To add a new mailbox, click the **Add a Mailbox** link to display the **Add Mailbox** form.
2. Enter a **Name** for the mailbox.

   The **Type** field is set to Virtual—the only type that users are permitted to add.
3. Click **Add**. The new mailbox is added to the system.

   NOTE: The directory connector will automatically assign users and groups to mailboxes to match what was found in source system's directory. The Active Directory group "Domain Users" does not get assigned to any mailboxes by the directory connector.

Edit a mailbox

1. Locate the mailbox in the list of mailboxes displayed in the **Mailbox Administration** form by doing any of the following:
   - Scrolling through the list of mailboxes
   - Entering a value in the **Name** or Display **Owner** field
   - Choosing a server from the drop-down list
   - Choosing a mailbox type from the drop-down list
   - Choosing whether the mailbox has been deleted
2. Click **Search**.
3. Click **Edit** to the left of the mailbox name to display the **Edit Mailbox** form for the selected mailbox.

Mailbox name

To change the **Name** of a mailbox, simply enter a new value in the **Name** field.

You can add or update mailbox policy information for the following mailboxes:

- Mailbox Default
- Inbox
- Sent Items
- Deleted Items

The same or different policies can be assigned to each mailbox. (See the Message policies chapter for more information.)

NOTE: If the Archive Manager Store Manager is being used to synchronize users' folders, then this screen also enables the administrator to set whether users' folders are synchronized.

Add users to a mailbox

Logins are used to manage who has access to Archive Manager and which functions each user may perform.

1. Locate the desired user in the list of users displayed on the right side of the **Users** tab of the **Edit Mailbox** form. Either:
   - Enter the name of the desired user in the **Find User** field and then click **Search**; ***or***
   - Use the page browsing controls below the list of users to browse for the desired user.
2. Select the checkbox to the right of the user.

   NOTE: Although multiple users can be added at once, the selected users must all be displayed on the same page. If you browse to another page, any selections on the current page will be lost.
3. Click **Add to Mailbox**. The selected users are added to the list of users displayed on the left side of the **Users** tab of the **Edit Mailbox** form.

Delete users from a mailbox

- In the **Edit Mailbox** form for the **Users** tab, select the checkbox to the right of the user you want to delete, and click **Remove Access**.

The selected user is deleted from the list of users, and the **Edit Mailbox Administration** form is displayed.

Add groups to a mailbox

Groups provide a flexible way to manage multiple individual users or mailboxes.

1. Locate the desired group by doing one of the following:
   - Enter the name of the desired group in the **Find Group** field, and then click **Search**
   - Use the page browsing controls ("Page x of y") below the groups list to browse for the desired group.
   - Mark the checkbox to the right of each group you want to add to the mailbox.

     NOTE: Although multiple groups can be added at once, the selected groups must all be displayed on the same page. If you browse to another page, any selections on the current page will be lost.
2. Click **Add to Mailbox**.

   The selected groups are added to the list of groups displayed on the left side of the **Groups** tab of the **Edit Mailbox** form.

Delete groups from a mailbox

1. In the **Groups** tab of the **Edit Mailbox** form, click **Delete** to the right of the group you want to delete.

   The **Delete Group** confirmation message is displayed.
2. Click **OK** to confirm the deletion.

   The selected group is deleted from the list of groups, and the **Edit Mailbox Administration** form is displayed.

Add associated email addresses

An associated email address can be added to a mailbox by the administrator so that all messages sent to and from that email address are included in the mailbox. When processing mailboxes, the Active Directory Connector adds the values found in the following properties of the objects:

- Mail
- otherMailbox
- proxyAddresses

The connector enters any addresses found in these properties. In the case of otherMailbox and proxyAddresses properties, the address must be prefixed smtp: for it to be included. X400 and other types are ignored.

The GroupWise Directory Connector does not add any associated email addresses.

1. In the **Email Addresses** tab of the **Edit Mailbox** form: Locate the desired email address by entering all or part of the address in the **Email Address** field, and click **Search**.
2. Mark the checkbox to the right of each email address you want to add to the mailbox.

   NOTE: Although multiple email addresses can be added at once, the email addresses must all be displayed on the same page. If you browse to another page, any selections on the current page will be lost.
3. Click **Add to Mailbox**. The selected email addresses are added to the list of email addresses displayed on the left side of the **Email Addresses** tab of the **Edit Mailbox** form.

Delete associated email addresses

1. On the left side of the **Email Addresses** tab of the **Edit Mailbox** form: Click **Delete** to the right of the email address you want to delete. The **Delete Email Address** confirmation message is displayed.
2. Click **OK** to confirm the deletion.
3. The selected email address is deleted from the list of email addresses, and the **Edit Mailbox Administration** form is displayed.

Add excluded email addresses

Administrators can exclude an email address from a mailbox so that all email sent to or from the email address is not included in the mailbox. This feature is visible only for virtual mailboxes.

1. On the right side of the **Exclude Email Addresses** tab of the **Edit Mailbox** form: Enter any part of the address in the **Email Address** field to locate it in the list, and then click **Search**.
2. Mark the checkbox to the right of each email address you want to add to the group.

   NOTE: Although multiple email addresses can be added at once, the email addresses must all be displayed on the same page. If you browse to another page, any selections on the current page will be lost.

3. Click **Add to Exclusion**. The selected addresses are added to the list of excluded addresses displayed on the left side of the **Exclude Email Addresses** tab.

Delete excluded email addresses

1. On the left side of the **Email Addresses** tab of the **Edit Mailbox** form, in the list of excluded addresses:

   Click **Delete** to the right of the address you want to delete. The **Delete Email Address** confirmation message is displayed.
2. Click **OK** to confirm the deletion. The selected email address is deleted from the list of excluded email addresses, and the **Edit Mailbox Administration** form is displayed.

Add wildcard email addresses

An administrator can create a wildcard email address so that all email sent to or from addresses that match the pattern defined by the administrator is included in the virtual mailbox. This functionality is only available for virtual mailboxes.

A wildcard email address could be specified in the following formats:

- *@somecompany.com.
- name@*
- name@*company.com

NOTE: Specifying a wildcard in an email address may produce a large list of email addresses. Please be aware of performance issues.

1. Enter a wildcard address (e.g., *@example.com) in the **Email Address** field.
2. Click **Add**. The Wildcard Email Address is added to the list of **Email Addresses** displayed on the left side of the **Wildcard Email Addresses** tab of the **Edit Mailbox** form.

Delete wildcard email addresses

1. Click **Delete** to the right of the email address in the list of wildcard email addresses displayed on the left side of the **Email Addresses** tab of the **Edit Mailbox** form.

   The **Delete Email Address** confirmation message is displayed.
2. Click **OK** to confirm the deletion.

   The selected email address is deleted from the list of wildcard email addresses, and the **Edit Mailbox Administration** form is displayed.

Delete a mailbox

1. Locate the mailbox in the list of mailboxes displayed in the **Mailbox Administration** form by doing any of the following:
   - Scrolling through the list of mailboxes
   - Entering a value in the **Name** or **Display Owner** field
   - Choosing a server from the drop-down list
   - Choosing a mailbox type from the drop-down list
   - Choosing whether the mailbox has been deleted
2. Click **Search**.
3. Click **Delete** to the left of the mailbox name. The **Delete Mailbox** confirmation message is displayed.
4. Click **OK** to confirm the deletion. The selected mailbox is deleted, and the **Mailbox Administration** form is displayed.

Alternatively, you can delete a mailbox by opening the **Edit Mailbox** form, selecting the **Edit** icon, clicking **Delete**, and confirming the deletion.

18

Lync servers

- About Lync servers
- Edit a Lync server

About Lync servers

Archive Manager lets you manage each Lync server. You can specify which Lync server to enable Lync message archiving, and when to start and end archiving.

NOTE: This page will be invisible if you have not installed the **Lync Store Manager** service (even though you may have the **Edit Lync Archiving** permission).

Edit a Lync server

1. In the **Lync Server Administration** form: Locate the Lync server in the list of Lync servers displayed.
2. Click **Edit** to the left of the Lync server name.

   The **Edit Lync Server** form for the selected Lync server is displayed.
3. Revise the Lync server information as described below, and then click **Update**.

   The specified changes to the Lync server are saved, and the **Lync Server Administration** form is displayed.

General Information:

To change the general information associated with a Lync server, enter or select new values for some or all of these fields:

- **Start Time**: Defines when the Lync Store Manager Service will start exporting conversation data for the Lync users contained by that Lync server.
- **End Time**: Defines the end of the time frame when the Lync Store Manager Service can start exporting conversation data for the Lync users contained by that Lync server. For example, if you enter a start time of 1:00 a.m. and an end time of 3:00 a.m., the Lync Store Manager can start exporting data any time between 1:00 a.m. and 3:00 a.m. If the Lync Store Manager completes exporting data at 2:50 a.m., it will initiate another data export pass for all users enabled for store management because 2:50 a.m. is within its time frame (Start Time and End Time) to start exporting data. The store manager will continue until it has finished exporting data for the entire list of users. It will not stop exporting data at 3:00 a.m.
- **Enable Store Manager**: A check box that enables or disables the Lync Store Manager for the selected Lync server.
- **Store Manager Group:** If all Lync servers are of the same version, this field can be left as default. However, if different versions of Lync servers exist, you must specify a unique store manager group name for each version. This permits each Lync Store Manager to archive Lync server data for a single Lync server version.

19

Lync user assignment

- About Lync user assignment
- Select users
- Select Lync users

About Lync user assignment

Archive Manager Lync users are synchronized from Lync servers and created by the Archive Manager Directory Connector. The Lync User Assignment Administration form lets you define which users can access which Lync user.

NOTE: This page will be invisible if you have not installed the **Lync Store Manager** service (even though you may have the **Edit Lync Archiving** permission).

Select users

To select a User to add to the Users field:

1. In the **Lync User Assignment Administration** form, click the **Browse** button.
2. Click on the user to select it. You can search for users by typing criteria in the **Login Name** field or **Display Name** field, and then clicking **Search** to view a list of users that match your search criteria.
3. In the **Lync User Assignment Administration** form, click **Search** to view the list of Lync users assigned to the user you selected.

   The list is displayed in the left-hand User column.

Select Lync users

To grant the selected user access to Lync users:

1. Click the **Browse** button next to the right-hand Name box to view a Lync user Name list, or the Group Box to view a Group Name list.
2. Click the Lync user Name or Group Name you want to add to the Name box or Group box.
3. Click Search to view the list of Lync users that meet your search criteria.
4. Click the checkbox to the right of the mailboxes you want to assign access to the currently selected user.
5. Or, click **Select All** to select all Lync users shown on the current page.
6. Click **Assign** to assign the selected Lync user(s) to the currently selected user.

20

Lync users

- About Lync users
- Edit or delete a Lync user

About Lync users

Archive Manager Lync users work in a way similar to Lync users in Microsoft Lync Server. However, Lync mailboxes are separate and treated like journal messages because Microsoft does not treat conversation boundaries well when users are added or removed from a conversation. Lync mailboxes and conversations are available to the Admin user by default. The Admin user can assign the Lync Mailbox to any login.

NOTE: This page will be invisible if you have not installed the **Lync Store Manager** service (even though you may have the **Edit Lync Archiving** permission).

Edit or delete a Lync user

The following sections discuss Lync user management.

Edit a Lync user

1. Locate the Lync user in the list of Lync users displayed in the **Lync Users Administration** form by doing any of the following:
   - Scrolling through the list of Lync users
   - Entering a value in the **Name** or **Display Owner** field
   - Choosing a server from the drop-down list
   - Choosing whether the Lync user has been deleted
2. Click **Search**.
3. Click **Edit** to the left of the Lync user name to display the **Edit Lync user** form for the selected Lync user.

Change Lync user name

To change the **Name** of a Lync user, simply enter a new value in the **Name** field.

Add users to a Lync user

Logins are used to manage who has access to Archive Manager and which functions each user may perform.

1. Locate the desired user in the list of users displayed on the right side of the **Users** tab of the **Edit Lync** user form. Do one of the following:
   - Enter the name of the desired user in the **Find User** field and then click **Search**.

- Use the page browsing controls below the list of users to browse for the desired user.

2 Select the checkbox to the right of the user.

3 Click **Add to Selection**. The selected users are added to the list of users displayed on the left side of the **Users** tab of the **Edit Lync User** form.

Delete users from a mailbox

- In the **Edit Mailbox** form for the **Users** tab, select the check box to the right of the user you want to delete, and click **Remove Access**.

The selected user is deleted from the list of users, and the **Edit Lync user Administration** form is displayed.

Add groups to a mailbox

Groups provide a flexible way to manage multiple individual users or Lync users.

NOTE: Although multiple users can be added at once, the selected users must all be displayed on the same page. If you browse to another page, any selections on the current page will be lost.

1 Locate the desired group by doing one of the following:

- Enter the name of the desired group in the **Find Group** field, and then click **Search**
- Use the page browsing controls ("Page x of y") below the groups list to browse for the desired group.
- Mark the checkbox to the right of each group you want to add to the mailbox.

2 Click **Add Selection**.

The selected groups are added to the list of groups displayed on the left side of the Groups tab of the Edit Lync user form.

Delete groups from a Lync user

1 In the **Groups** tab of the **Edit Lync User** form, click **Delete** to the right of the group you want to delete.

The Delete Group confirmation message is displayed.

2 Click **OK** to confirm the deletion.

The selected group is deleted from the list of groups, and the Edit Lync user Administration form is displayed.

Delete a Lync user

1 Locate the Lync user in the list of Lync users displayed in the **Lync Users Administration** form by doing any of the following:

- Scrolling through the list of mailboxes
- Entering a value in the **Name** or **Display Owner** field
- Choosing a server from the drop-down list
- Choosing a mailbox type from the drop-down list
- Choosing whether the mailbox has been deleted

2 Click **Search**.

3 Click **Delete** to the left of the mailbox name. The Delete Lync User confirmation message is displayed.

4 Click **OK** to confirm the deletion.

The selected mailbox is deleted, and the Lync User Administration form is displayed. Alternatively, you can delete a mailbox by opening the Edit Mailbox form, selecting the Edit icon, clicking Delete, and confirming the deletion.

21

Reports

- About reports
- Mailbox Scan Status report
- My Search Log report
- Questionable Access report
- Search Log report
- Storage Statistics report
- Viewed Messages report
- Delegation Log report
- Delegation Status report

About reports

Archive Manager provides a set of reports which can be accessed from within the Archive Manager application. These reports include:

- **Storage Statistics** - Storage-related information on the Archive Manager system.
- **Search Log** - Displays searches performed by Archive Manager users within a specified date range.
- **Questionable Access** - Displays searches conducted by other users on your mail and on others' mail.
- **Viewed Messages** - Displays all messages viewed by a user within a specified date range.
- **My Search Log** - Displays all the searches you have conducted within a specified date range.

NOTE: Only those reports that you have access permissions for will be visible.

Mailbox Scan Status report

The Mailbox Scan Status report contains information about mailbox processing by the Exchange Store Manager (ESM). Available information includes the following:

- **Mailbox Name**: The name of the mailbox being processed by the ESM.
- **Status Start Date**: The start date and time of the last scan.
- **Last Scan Status**: Displays whether the scan was successful or failed.
- **Runs at Current Status**: The number of times the scan was run at the current scan status.
- **Error Text**: If an error exists, an error message is displayed.

For hosted Exchange, 2 additional fields are displayed in this report:

- **Mailbox Type**: Select All, Local, or Hosted.

- **Delegated Access**: The status of the user's remote mailbox access. The status is Default if the user has not set the status, Enabled if the user has delegated remote access, and Disabled if the user does not delegate remote access.

My Search Log report

This report provides you with a report of all the searches you have conducted within a specified date range. By default, it displays all searches conducted on the current day.

To view this report for a different time period:

1. Choose one of the following options to specify the date range:
   - **All** (Default) - All viewed messages regardless of date received.This option must be used in conjunction with other criteria, such as search text or recipient information. Attempting to search using only the **All** option will generate an error.
   - **Today** - Messages viewed on the current date
   - **Yesterday** - Messages viewed on the previous day
   - **This Week** - Messages viewed within seven days of the current date
   - **Last Week** - Messages viewed within fourteen days of the current date
   - **This Month** - Messages viewed on any day of the current month
   - **Last Month** - Messages viewed on any day of the previous month
   - **Between** (and related fields) - Messages viewed within a specified period. Use the **Date From** and **Date To** fields to specify the date range to search. Enter each date by selecting it from the pop-up calendar that appears when you click on the drop-down arrow next to the date entry field.
2. Click **Search**.

Questionable Access report

The Questionable Access report provides information about possible unauthorized access by Archive Manager users.

This feature tracks users given "Search All Emails" privilege but not the "Edit Logins/Mailbox" privilege and who are reading emails from mailboxes which they are not specifically given access to.

These reports do not necessarily indicate unauthorized access to emails, since the access may have been authorized. Rather, the instances of access in the reports are "questionable"- items that can (should) be investigated if desired.

Viewing your search results

When viewing search results, be aware of the following:

- Message results will be displayed based on the specified date criteria
- Column widths can be resized by dragging the boundary on the right side of the column heading until the column is the width that you want
- Messages can be sorted by clicking once on the title of the column you wish to sort by

- To preview a message, click the **Preview** tab on the right side of the screen. With the preview screen open, the only columns visible are Importance, Icons, Attachments, and Subject. Click the **Preview** tab again to close the preview pane.

NOTE: **Subscribe to RSS** - Receive updates in your RSS reader for new messages that meet the report criteria displayed. The first 100 results are displayed, sorted by date.

Of All Email (by Specific Person) report

Who is Reading Others' Email?

This report provides information to administrators with regard to unauthorized access performed by a specific Archive Manager user, within a specified date range.

To view this report:

1. Click **Browse** [...] to the right of the **Login Name** field to display the **Login Search** dialog box.
   - Enter a value in the **Login Name** or **Display Name** field. If values are entered in both fields, only contacts that match both criteria will be displayed.
   - Click **Search**.
   - Locate the person in the search results and click their name to add them to the **Login Name** field and close the Archive Manager **Login Search** dialog box.
2. Choose one of the following options to specify the date range:
   - **All** (Default) - All viewed messages regardless of date received.This option must be used in conjunction with other criteria, such as search text or recipient information. Attempting to search using only the **All** option will generate an error.
   - **Today** - Messages viewed on the current date
   - **Yesterday** - Messages viewed on the previous day
   - **This Week** - Messages viewed within seven days of the current date
   - **Last Week** - Messages viewed within fourteen days of the current date
   - **This Month** - Messages viewed on any day of the current month
   - **Last Month** - Messages viewed on any day of the previous month
   - **Between** (and related fields) - Messages viewed within a specified period. Use the **Date From** and **Date To** fields to specify the date range to search. Enter each date by selecting it from the pop-up calendar that appears when you click on the drop-down arrow next to the date entry field.
3. Click **Search**.

Of My Email (by Anyone) report

Who Else is Reading My Email?

This report lists all the messages that have been viewed by anyone other than yourself within a specified date range.

To view this access report:

1. Choose one of the following options to specify the date range:

- **All** (Default) - All viewed messages regardless of date received.This option must be used in conjunction with other criteria, such as search text or recipient information. Attempting to search using only the **All** option will generate an error.
- **Today** - Messages viewed on the current date
- **Yesterday** - Messages viewed on the previous day
- **This Week** - Messages viewed within seven days of the current date
- **Last Week** - Messages viewed within fourteen days of the current date
- **This Month** - Messages viewed on any day of the current month
- **Last Month** - Messages viewed on any day of the previous month
- **Between** (and related fields) - Messages viewed within a specified period. Use the **Date From** and **Date To** fields to specify the date range to search. Enter each date by selecting it from the pop-up calendar that appears when you click on the drop-down arrow next to the date entry field.

2 Click **Search**.

Search Log report

This report provides you with the details of all searches performed using Archive Manager, including the keywords that were searched, the person performing the search, and the date and time of the search.

The search log enables administrators to view searches performed by Archive Manager users within a specified date range.

To run a Search Log report:

1 Click **Browse** [...] to the right of the **User** field to display the **Login Search** dialog box.
   - Enter a value in the **Login Name** and/or **Display Name** field (If values are entered in both fields, only contacts that match both criteria will be displayed).
   - Click **Search**.
   - Locate the person in the search results and click the name to add it to the **Login Name** field and close the **Login Search** dialog box.

2 Choose one of the following options to specify the date range:
   - **All** (Default) - All viewed messages regardless of date received.This option must be used in conjunction with other criteria, such as search text or recipient information. Attempting to search using only the **All** option will generate an error.
   - **Today** - Messages viewed on the current date
   - **Yesterday** - Messages viewed on the previous day
   - **This Week** - Messages viewed within seven days of the current date
   - **Last Week** - Messages viewed within fourteen days of the current date
   - **This Month** - Messages viewed on any day of the current month
   - **Last Month** - Messages viewed on any day of the previous month
   - **Between** (and related fields) - Messages viewed within a specified period. Use the **Date From** and **Date To** fields to specify the date range to search. Enter each date by selecting it from the pop-up calendar that appears when you click on the drop-down arrow next to the date entry field.

3 Choose one option to specify which searches to include:
   - **All** - View all searches
   - **No** - View only the searches in which the **Search All Users** checkbox was not selected

- **Yes** - Only searches in which the **Search All Users** checkbox was selected

4 Once you have specified the report criteria, click **Search** once to execute the search.

Viewing your search results

The search log results are returned in a table, with information in these columns:

- **User**: The name of the user that performed the search.
- **Date**: The date and time that the search was run.
- **Search All**: Whether the search was across all users in the system, or just the standard user(s) to whom the person executing the search had access.
- **IP Address**: The IP address from which the search was executed.
- **Search Criteria**: The search criteria used to perform the search.

NOTE: The search can be re-run to display the results by clicking the magnifying glass icon to the left of the user name.

NOTE: **Subscribe to RSS** - Receive updates in your RSS reader for new messages that meet the report criteria displayed. The first 100 results are displayed, sorted by date.

Storage Statistics report

The Archive Manager Storage Statistics report provides storage-related information on the Archive Manager system, including the following statistics:

Table 8. Storage Statistics

Total Storage Size	The total size of the Archive Manager database and attachment and message stores.
Database Size	The size of the Archive Manager database.
Database Log Size	The size of the Archive Manager database log.
Attachment Index Size	The size of the Full Text Index information for attachments.
Message Index Size	The size of the Full Text Index information for messages.
Single Instance Size	The total size of the attachments for which there is only a single instance.
Storage Reduction	The overall percentage reduction in storage size as a result of the single-instance storage.
Number of Attachments	The total number of attachments in the Archive Manager system.
Single Instance Attachments	The number of attachments that are unique (i.e. only a single instance of those attachments has been stored).
Duplicate Attachments	The number of attachments in the system that are duplicates.
Total Messages	The total number of messages in the Archive Manager system.
Attachment Size	The size of the overall attachment store, without taking into consideration the single-instance storage of attachments.

Viewed Messages report

The details of the messages that are viewed in Archive Manager are logged, so that in addition to determining who has searched for a message, it is possible to track who has opened any of the messages that were found. This ensures the Archive Manager system is being used appropriately and that the privacy of the organization and its staff is maintained.

To view this report:

1. Click **Browse** [...] to the right of the **User** field to display the **Login Search** dialog box.
2. Enter a value in the **Login Name** and/or **Display Name** field (If values are entered in both fields, only contacts that match both criteria will be displayed).
3. Click **Search**.
4. Locate the person in the search results and click the name to add it to the **Login Name** field and close the **Login Search** dialog box.
5. Choose one of the following options to specify the date range:
   - **All** (Default) - All viewed messages regardless of date received.This option must be used in conjunction with other criteria, such as search text or recipient information. Attempting to search using only the **All** option will generate an error.
   - **Today** - Messages viewed on the current date
   - **Yesterday** - Messages viewed on the previous day
   - **This Week** - Messages viewed within seven days of the current date
   - **Last Week** - Messages viewed within fourteen days of the current date
   - **This Month** - Messages viewed on any day of the current month
   - **Last Month** - Messages viewed on any day of the previous month
   - **Between** (and related fields) - Messages viewed within a specified period. Use the **Date From** and **Date To** fields to specify the date range to search. Enter each date by selecting it from the pop-up calendar that appears when you click on the drop-down arrow next to the date entry field.
6. Click **Search**.

Delegation Log report

The Delegation Log report shows all attempts by users to change delegation settings. This includes both successful and failed attempts and any associated error messages.

NOTE: The Delegation Log report is available only in a hosted Exchange environment.

Delegation Status report

The Delegation Status report shows the current status of all user delegations. This report allows you to sort and filter by status so it is easy to find users who have not delegated access to their hosted mailbox. For users who have delegated access, a View Agreement link to the agreement and configuration information entered by the user is provided in the report. This includes a green checkmark if the report is valid, or a red x if the report may have been tampered with.

NOTE: The Delegation Status report is available only in a hosted Exchange environment.

22

Message policies

- About message policies
- Message policies and deleted items
- Add, edit, or delete a message policy
- Setting up archiving without journaling

About message policies

Store management message policies are used to manage the mail server store and determine how long messages remain on the mail server. These policies can be used to reduce the size of the mail server store, to maximize the benefits of the storage efficiencies enabled by Archive Manager. Policies can be set either across the organization or on a user-by-user basis.

NOTE: These policies are used in conjunction with the mail server administration to determine which policies apply to which mail servers.

Store management message policies can be applied to different mail folders at different levels, as explained at the beginning of the chapter Message policy assignments.

In an Exchange system, Archive Manager can archive all Outlook item types except journal entries (activities). By default, store management message policies are applied to all Outlook item types. Archived items include the message classes listed in the table below, which also shows what Archive Manager can do with each item type.

NOTE: IPM.Document items can be enabled for stubbing when there is a stubbing policy in place on the folder in which they reside.

Message policies and deleted items

On a Microsoft Exchange server, there are two types of deleted messages: soft-deleted messages and hard-deleted messages. Soft-deleted messages are messages that have been moved to the Deleted Items folder by pressing the DELETE key. Hard-deleted messages are messages that have been removed from any folder by pressing SHIFT+DELETE, or were emptied from the Deleted Items folder. When a message is deleted from a Deleted Items folder, a backup copy or tombstone of the message is kept for a specified period of time. Outlook allows you to get a list of the tombstones in a folder and to either restore the messages back to the original folders or permanently remove the messages from the system.

In versions of Exchange prior to 2010, tombstones contained information about the folder from which they were deleted. The ESM is able to link a deleted message to its last known folder.

In Exchange 2010, tombstones no longer contain information about the folder from which they were deleted. Therefore, the ESM can not determine the folder from which a message was deleted. In Exchange 2010, if the item is already linked to a folder in the mailbox, the ESM no longer changes the folder to which the item is linked. If the item is not currently linked to any folder in the mailbox, the ESM links it to the Deleted Items folder.

Add, edit, or delete a message policy

A message policy is some action or function applied to messages in Exchange that meet certain selection criteria, as defined by these field values:

- **Message Policy Name:** The name for the policy—usually related to what the policy does. This name is how the policy is identified in other parts of Archive Manager.
- **Policy Action** (Export/Delete/Stub/Stub Attachments): What Archive Manager will do with the messages that meet this policy's selection criteria.

NOTE: The **Delete**, **Stub,** and **Stub Attachments** policies apply to Exchange systems only.

NOTE: Remember that Archive Manager can delete (in Outlook) only standard email messages, posts, meeting invitations, and task requests. Similarly, the program can stub only plain email messages and posts in Exchange.

The fields below the **Policy Action** field vary depending on the selected **Policy Action**, and are applied only to messages that meet the days-old and file-size criteria (defined below):

- **Export** copies the message data from your mail system to Archive Manager.
- **Delete** removes any messages in Exchange that match the criteria, and can optionally add them into Archive Manager before deletion.
- **Stub** replaces a message in Exchange with a stubbed-down message that looks like a message to the user, and moves the message data into Archive Manager. When a user views a stubbed message in Outlook, the full message is recreated from data in Archive Manager. You may also, in combination with a Stub policy, delete from Exchange all messages and stubs of a certain age (entered separately from the days-old value for the Stub policy). Stubbed messages can be reconstructed on the Exchange server using the Archive Manager Outlook Form, or viewed using the Offline Client.
- **Stub Attachments** removes attachments from messages in Exchange. When a user views a message with a stubbed attachment, the attachment is recreated from data in Archive Manager. You may also, in combination with a Stub Attachments policy, delete from Exchange all messages and stubs of a certain age (entered separately from the days-old value for the Stub policy). Stubbed attachments can be reconstructed on the Exchange server using the Archive Manager Outlook Form, or viewed using the Offline Client.

Note, for both the **Stub** and **Stub Attachments** policy actions:

NOTE: When applying a Stub Policy with the "Delete Message Shells" option, this actually applies a delete policy. It applies to all messages of the specified age, whether or not they are stubbed.

NOTE: When applying a Stub Policy, you should not use a third party document handling system in conjunction with Outlook. Stubbed messages may not be reconstructed.

- The Archive Manager Outlook Form automatically reconstructs the message and/or attachment when Windows Authentication is used. To reconstruct the messages with Forms authentication, sign in to your Archive Manager web site, checking the **Remember Login** box. For more information, see the Authentication modes chapter of this guide.
- When viewing a reconstructed message or attachment with Outlook, users may see this message:

  This item contains active content that cannot be displayed in the Reading Pane. Open the item to read its contents.

  Follow the instructions to see the message. To enable the reading (preview) pane:
- To turn the reading pane back on for newly stubbed or re-stubbed messages:

1. Use the Archive Manager Configuration Console to set the Configuration setting **Disable Preview Pane** to False.
2. Restart the ESM.

3 For any message that is already stubbed, first open the message in Outlook to reconstruct it, and then re-stub it. The ESM then adds a necessary property to the message that lets Outlook display it in the reading pane.

- **Days old:** Age of the messages to which this policy will be applied. Leave the field blank to apply the policy to all messages. Enter 0 to never delete message stubs. This is the only field where 0 indicates "never" instead of the numeric value.
- **KB in size:** Size of the messages to which this policy will be applied. Leave the field blank to apply this to all messages.

  NOTE: The policy will be applied only to messages that meet ***both*** the **Days old** and **KB in size** criteria.

- **Read messages:** Lets you include or exclude unread messages from the policy.
- **Flagged messages:** Lets you include or exclude flagged messages that have not been completed from the policy.
- **Not found:** Lets you include or exclude messages not found in Archive Manager from the policy.

Add a message policy

To define a new message policy:

1 Click the link to **Add a Message Policy**.

2 Enter and select the field values that define the policy—as explained above.

3 Click **Add**. The new message policy is then added to the system. After a policy is defined, it can be applied to a mailbox or mail server.

NOTE: We recommend you use a conservative policy initially. Try to minimize the scope of your policies' effects until you become familiar with how different elements of a policy behave, both independently and in combination with other elements.

A few practical examples of store management message policies that many admins find useful:

Table 9. Store management message policies

Policy Name	Mode	Days/ Size	Unread/ Flagged	Archive if not found	Delete STUBs
Conservative Stubbing	Stub	90 / 10K	NO	YES	NO (blank)
Useful for initial stub testing. It targets mail over 3 months old only.					
Attachment Stubbing	Stub Attachments	30 / 10K	NO	YES	90
Will remove attachments from messages to reduce the Exchange store size. It leaves the body of the message intact so that Outlook Web Access users can view the body of the message and have one-click access to their stubbed attachments.					
Back loading	Export	N/A	N/A	N/A	N/A
Useful for back-loading. It does not remove anything from Exchange, but does place all mail in Archive Manager.					
Exchange Maintenance	Stub	30 / blank	YES	YES	90

Table 9. Store management message policies

Policy Name	Mode	Days/ Size	Unread/ Flagged	Archive if not found	Delete STUBs
Only 30 days of “real” mail is left in Exchange, but all stubs (stubbed messages) are removed after 90 days (a 90-day deletion policy is common in some organizations). All email can still be found in Archive Manager, since it is archived before deletion or stubbing.					
Deletion Management	Delete	90 / 50K	NO	YES	N/A
NOTE: This policy deletes all emails that are 90 days old or older and over 50K; that is, it removes all old, large email. This could be used as an alternative to a System Attendant deletion policy.					

Edit a message policy

1. Locate the policy in the list of policies displayed in the **Message Policy Administration** form by doing one of the following:
   - Scrolling through the list of policies
   - Entering a value in the **Name** field
   - Selecting a policy action from the drop-down list and clicking **Search**.
2. Click **Edit** to the left of the message policy name to display the **Edit Message Policy** form for the selected policy.
3. Revise the policy definition by changing the values of the pertinent fields, as explained above, and then click **Update**.

Delete a message policy

1. Locate the policy in the list of policies displayed in the **Message Policy Administration** form by doing one of the following:
   - Scroll through the list of policies.
   - Enter a value in the **Name** field.
   - Select a policy action from the drop-down list and click **Search**.
2. Click **Delete** to the left of the policy name. The **Delete Policy** confirmation message is displayed.
3. Click **OK** to confirm the deletion.

NOTE: Alternatively, a policy can be deleted by opening the **Edit Message Policy** form, clicking **Delete**, and confirming the deletion.

Setting up archiving without journaling

To enable archiving without using journaling, use Export policies. Export policies let you copy email data from user mailboxes directly into Archive Manager.

To enable this type of archiving, first create an export policy, as follows:

1. Go to the Archive Manager site and sign in using the Administrator account.
2. Click **Administration**.
3. On the Archive Manager Administration page, click **Message Policies**.

4 Click the **Add a Message Policy** link.

5 Specify a name for the policy.

6 Select the Export **Policy Action** from the list.

7 Specify an **Export** option: **Immediately**, or **After ___ days**.

8 Click **Add.**

Then you should assign the export policy to the users you want to be affected by the policy, as follows:

1 Click **Message Policy Assignment** in the left pane.

2 Select the policy tab you want to process (for example, **Default Message Policy**).

3 Select the message policy you created.

4 Locate the desired users in the list of users displayed on the right side of the **Default Message Policy** tab of the **Message Policy Assignment** form by doing one of the following:

- Selecting the name of the desired user in the **Name** field, and then clicking **Search**.
- Using the Mailbox, Group, or Message Policy search, as detailed in the Message policy assignments chapter of this guide.
- Using the page browsing controls below the list of users to browse for the desired user.

5 Select the checkboxes to the right of the users to whom you want to assign the policy.

> **NOTE:** Although multiple users can be added at once, the users must all be displayed on the same page. If you browse to another page, any selections on the current page will be lost.

6 Click **Add to Default Policy**. The selected users will be added to the list of users displayed on the left side of the **Default Message Policy** tab of the **Message Policy Assignment** form.

According to your new configuration, email data from user mailboxes will be copied directly into Archive Manager.

23

Message policy assignments

- About message policy assignments
- Associate users with a message policy
- Mailbox Search
- Disassociate users from a message policy

About message policy assignments

The Message Policy Assignment screen lets you manage message policies, and apply policies to user mailboxes and (with Exchange only) to mailbox folders.

The Message Policy Assignment screen contains four tabs:

- Default Message Policy
- Inbox Message Policy
- Sent Item Message Policy
- Deleted Item Message Policy

NOTE: GroupWise does not support different message policies for different folders. In a GroupWise environment, therefore, any entries in the Inbox, Sent Item and Deleted Item tabs are ignored as irrelevant.

Message policies can be applied to mail folders at two different levels:

- **Server level:** The default policy for all users on the mail server, unless superseded by a user-level policy. Server-level policies can be set through the Archive Manager Administration Web site through the Mail Servers screen. See Edit a mail server.
- **User level:** Can be defined to override the mail server policy for a particular user or group of users. For example, a user-level policy might be configured to keep messages longer in the mailboxes of senior management and the legal department, or to stop message stubbing for a CEO who doesn't want his or her messages stubbed. User-level policies can be set through the Archive Manager Administration Web site Message Policy Assignment screen, or the Archive Manager Administration Web site Mailboxes screen. For information on setting user-level policies through the Mailboxes screen, see the Mailboxes chapter.

In other words, a user-level policy outranks a server-level policy for the users to whom the user-level policy is applied.

Message policies are applied to folders within a user mailbox differently depending on whether Archive Manager is running in an Exchange or GroupWise environment, as described below.

For an Exchange messaging system:

- At either the server or user level, a Default policy applies to all mail folders in a user mailbox, except where it may be superseded by one or more separate policies for the Inbox, Sent Items and/or Deleted Items. That is, policies defined for the Inbox, Sent Items and/or Deleted Items will supersede a Default mailbox or server policy.
- Other than a Default policy, a policy defined for any folder, at any level, is ***not*** automatically applied to its subfolders. But if a policy is applied at any sublevel, it supersedes any policy applied at a higher level.

- Message policies are applied to all archived Outlook item types. Archive Manager archives all Outlook item types except journal entries (activities). In addition to email messages, archived items include: calendar appointments, meeting invitations, tasks, task requests, sticky notes, contacts, and personal distribution lists. However, remember that Archive Manager can delete (in Outlook) only plain email messages, posts, meeting invitations, and task requests. Similarly, the program can stub only plain email messages and posts in Outlook.

For a GroupWise messaging system:

- The Default message policy will be applied to all folders within a given user's mailbox. The GSM does not support different message policies for subfolders below a user's primary mailbox level.
- Any entries in the Inbox, Sent Item and Deleted Item tabs are ignored as irrelevant, although the tabs do still appear in the screen.

To view the users associated with a message policy

1. From the drop-down list, select the message policy: Default, Inbox, Sent Message, or Deleted.
2. The users associated with the message policy will appear on the left side of the **Message Policy Assignment** form.

Associate users with a message policy

1. Select a tab on the Message Policy Assignment screen.
2. Select a policy from the drop-down list. The screen refreshes and displays a list of the users currently associated with the policy.
3. Locate the desired user in the list of users displayed on the right side of the policy tab of the **Message Policy Assignment** form by doing one of the following:
   - Selecting the name of the desired user in the Name field, and then clicking **Search**.
   - Using the Mailbox, Group, or Message Policy search.
   - Using the page browsing controls below the list of users to browse for the desired user.
4. Select the checkboxes to the right of the users to whom you want to assign the policy.

   NOTE: Although multiple users can be added at once, the users must all be displayed on the same page. If you browse to another page, any selections on the current page will be lost.

5. Click **Add to <Policy Name> Policy**. The selected users are added to the list of users displayed on the left side of the **Policy** tab of the **Message Policy Assignment** form.

Mailbox Search

Search for a user—Mailbox selector.

1. Click the **Browse** button to the right of the **Name** field to open the **Mailbox Search** dialog box.
2. Enter a value in the **Mailbox Name** field, and click **Search** to execute the search.
3. Locate the mailbox name in the search results and click the name to add it to the **Name** field and close the **Mailbox Search** dialog box.

Group Search

Search for a group—group selector.

1. Click **Groups** to open the **Group Administration** dialog box.
2. Enter a value in the **Name** field, and click **Search** to execute the search.
3. Locate the group name in the search results, and click a group name to add to the **Group** field and close the dialog box.

Message Policy Search

To search for all users with a specific message policy, select the policy from the drop-down box.

Disassociate users from a message policy

1. From the policy tab that you have selected, select a policy from the drop-down list. The screen refreshes and displays a list of the users currently associated with the selected policy on the left-hand side of the form.
2. Locate the desired user in the list of users displayed on the left side of the **Message Policy** tab of the **Message Policy Assignment** form and click **Delete** . The **Delete User** confirmation message is displayed.
3. Click **OK** to confirm the deletion. The selected user is deleted, and the message policy form for the active tab is displayed.

24

Retention policies

- Retention policy overview
- Retention policy tabs
- Policy Editor tab
- Execution Log tab
- Change Log tab
- Legal Hold tab
- Schedule tab
- Settings tab

Retention policy overview

The Retention Policies screen in the Archive Manager Website allows you to implement your retention policies. To add or edit retention policies, the **Edit Retention Policies** permission is required.

NOTE: Retention policy search criteria must follow the search syntax rules detailed in the *Searching Email* chapter of the *Archive Manager User Guide*.

A retention policy is made up of the following policy items, including:

- The action: Keep/Delete
- The time-frame for performing the action
- Criteria specifying which messages the policy pertains to

These policy items are listed in a hierarchical order that indicates the order of execution (top-to-bottom). The order of execution allows you to specify which policies take precedence.

Sometimes several Policy items might reference some of the same messages. For example, you may have one policy that refers to all messages in mailbox "Bob Smith" and another Policy that refers to all messages in Mailstore "Store One", where the "Bob Smith" mailbox resides.

The Retention service only executes a single policy item for each message, which is the first Policy it encounters, Policy 1 displayed at the top of the list. If the same message appears in another Policy item being executed further down the list, it is ignored.

The Retention Policies screen allows you to set up this execution order by dragging your Policy items around. Hold your cursor over the left corner of the Policy item "Grip" and drag and drop to move the Policy.

NOTE: Messages removed by retention for one user will no longer be loaded by the Exchange Store Manager for another user. For example, if a message is sent to User A and User B and a retention policy deletes the message for User A before it is loaded into Archive Manager for User B, then the message is gone and the ESM cannot load the message for User B.

NOTE: Backloading message data into Archive Manager should be completed for all users for a single Archive Manager instance before retention is configured and implemented to ensure that message data for all users is archived.

Retention policy tabs

The Retention Policies screen contains tabs used to set retention policies, including the following:

- **Policy Editor:** Select to **Add Keep Policy** or **Add Delete Policy**.
- **Execution Log:** View the activity of the Retention service.
- **Change Log:** Displays an audit history of changes made to the retention policies.
- **Legal Hold:** Lets you temporarily suspend all retention policies to prevent the destruction of any email message.
- **Schedule:** Lets you select the days and times that the Retention service will run.
- **Settings:** Lets you select the Operation Mode for retention policies; either Safe mode or Production mode.

The number and order of the tabs displayed vary depending on your permissions.

- If a user has Edit Retention Policies rights, the tabs displayed are Policy Editor, Execution Log, Change Log, Schedule, and Settings.
- If a user has Edit Legal Hold rights, the only tabs displayed are Legal Hold, Execution Log, and Change Log.
- If a user has both Edit Retention Policies and Edit Legal Hold rights, the tabs displayed are Policy Editor, Execution Log, Change Log, Legal Hold, Schedule and Settings.

Policy Editor tab

The Policy Editor tab lets you add **Keep** and **Delete** policies**.**

Adding a Keep Policy

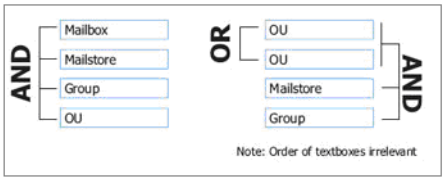
When you add a Keep Policy, you can either keep the messages forever or specify the period of time you want to keep them, after which they are no longer protected by the Keep policy and remain in the Archive Manager database as potential candidates for any other policies to act upon. A Keep Policy is represented as a green policy item.

To add the Keep Policy:

1. From the Policy Editor tab, click **Add Keep Policy**.
2. Enter a policy name in the box next to the policy item number.
3. Select **Keep Forever** to keep messages forever**.** Or, select **Keep For:** and select a number and then **Days**, **Weeks**, **Months**, or **Years** to specify the time frame to keep messages.
4. Select one or more **Message Types**. Message types include **Message**, **Calendar, Delivery Status Notification**, and **Contact**.
5. Message criteria settings are defined in the **Policy Acts Upon** fields. To the right of **Only items within**, select one or more of the following message containers: **Folder**, **Mailstore**, **Mailbox**, **Group** or **OU**. Or, select **Everything (All Messages in Archive)** checkbox to apply the policy to all messages in the archive.
    - **Folder:** Enter the folder path (example: Inbox\Retention Folder). The maximum length of the path is 2,000 characters.
        - **Include Sub Folders**: Select this checkbox to select the folder's sub folders.
    - **Mailstore:** Select a mailstore from the drop-down list.
    - **Mailbox:** Enter at least 3 characters in the Mailbox box to activate the drop-down list and select a mailbox.

- **Group:** Enter at least 3 characters in the Group box to activate the drop-down list and select a group.
    - **Include Former Members:** Select this checkbox to select former members of the selected group. Former members of a group are users that have previously been a part of the selected group in Active Directory.
- **OU:** Select an organizational unit from the drop-down list.

Regardless of the order of the containers in the list, the OR relationship exists between the containers of the same type, and the AND relationship between the containers of different types.



For example, if you specify two different mailboxes, a Mailstore and a Group, the Retention service will keep the messages in either of these mailboxes located in the selected mail store of the users belonging to the group. If these users have mailboxes in other mail stores, or they are members of other groups, the messages in those mailboxes remain untouched.

The list of the Mailstore and Group containers is populated from the entire set existing within the Archive Manager.

For an OU to show in the list, users must be included in it. Empty OUs are not displayed. (OU container is Exchange specific).

6 The collection of messages to be retained can further/also be narrowed by the set of tags in the **Items tagged with** field. This field is visible only if the tags are defined within Archive Manager. Note that the flag tag is not listed in the Retention Editor. String and Number tag policies with no value will function as a wild card.

   a To add a tag, click the **+Tag** button.

   b Select the tag from the drop-down list populated from the entire set of tags defined within Archive Manager.

   c Specify the tag value in the box to the right of the tag.

   Specifying an invalid value generates an Invalid Value warning.

   - Multiple items can be added to the set using the **+Tag** button.
   - To remove a tag from the set, click the **Trash Can** icon.

7 In the **Items that contain the words** box, enter the key words that the messages to be retained should contain.

   In the **Look in:** field, select one or more checkboxes to specify where to look for the words you entered: **Subject**, **Body**, or **Attachment**.

   NOTE: Retention policy search criteria must follow the search syntax rules detailed in the *Searching Email* chapter of the *Archive Manager User Guide*.

8 To implement policies, click **Save** at the top of the Policy Editor screen.

9 Additional Keep Policies can be added by repeating the steps listed above.

Click the **Check Mark** icon at the top of the screen to use the collapsed state of the policy. Click the **Gear** icon to view the policy. If the check mark is gray, the policy is not valid. A red exclamation point will be displayed next to the invalid property.

When the time specified for the **Keep Policy** is over, the messages remain in the Archive Manager database, as potential candidates for any other policies to act upon.

Adding a Delete Policy

The **Delete** policy specifies the criteria for the messages to be deleted. A Delete policy is represented in red.

NOTE: When a single archived message is associated with multiple mailboxes (e.g., one message sent to six recipients), and a Delete policy applies to one or more but not all of the mailboxes, the message is simply unlinked from the mailboxes where it has been deleted, but is ***not*** deleted from the archive altogether. When a message is unlinked from a mailbox in this way, it is reported in the Retention Editor log file in this form: 12:47:21 PM (3) DeleteAfter3Years_Spam : 0 Items Unlinked

NOTE: Tags are set globally. When a delete policy is defined by a tag, the policy will delete all tagged messages in the database, in all mailbox locations— not just in the mailbox where the tag was added. That is, if a message is tagged in a particular mailbox, and then the same tag is used in a delete policy applied to a higher-level container (e.g., OU), the message will be deleted from the archive at the higher container level, in all mailboxes.

To add a Delete Policy:

1. From the Policy Editor tab, click **Add Delete Policy**.
2. Enter a policy name in the box next to the policy item number.
3. Select **Delete After** to define the time frame to delete messages**.** Select a number and **Days**, **Weeks**, **Months**, or **Years** to specify the time after which to delete messages.
4. Select one or more **Message Types**. Message types include **Message**, **Calendar, DSN**, and **Contact**.
5. Select the **Delete Meetings With Future Dates** checkbox to ignore meetings with end times in the future in order to delete the specified items.
6. Select one or more **Message Types**. These include **Message**, **Calendar, DSN**, and **Contact**.
7. Message criteria settings are defined in the **Policy Acts Upon** fields. Next to **Only items within**, select one or more of the following message containers: **Folder**, **Mailstore**, **Mailbox**, **Group** or **OU**. Or, select **Everything (All Messages in Archive)** checkbox to apply the policy to all messages in the archive.
    - **Folder:** Enter the folder path (example: Inbox\Retention Folder). The maximum length of the path is 2,000 characters.
        - **Include Sub Folders:** Select this checkbox to select the folder's sub folders.
    - **Mailstore:** Select a mailstore from the drop-down list.
    - **Mailbox:** Enter at least 3 characters in the Mailbox box to activate the drop-down list and select a mailbox.
    - **Group:** Enter at least 3 characters in the Group box to activate the drop-down list and select a group.
        - **Include Former Members:** Select this checkbox to select former members of the selected group.
    - **OU:** Select an organizational unit from the drop-down list.

    Regardless of the order of the containers in the list, the OR relationship exists between the containers of the same type, and the AND relationship exists between containers of different types.

    For example, if you specify two different mailboxes, a Mailstore and a Group, the Retention service will delete the messages in either of these mailboxes located in the selected mail store of the users belonging to the group. If these users have mailboxes in other mail stores, or they are members of other groups, the messages in those mailboxes remain untouched.

    - The list of the Mailstore and Group containers is populated from the entire set existing within the Archive Manager.
    - For an OU to show in the list, users must be included in it. Empty OUs are not displayed. (OU container is Exchange specific).
    - The format of GroupWise mailboxes/groups in the Retention Policy is "Tree\User" for Mailboxes and "Tree\DistributionList" for Groups. Specifying GroupWise post-offices is not supported.

8 The collection of messages to be retained can further/also be narrowed by the set of tags in the **Items tagged with** field. This field is visible only if the tags are defined within Archive Manager. String and Number tag policies with no value will function as a wildcard.

   a To add a tag, click the **+Tag** button.

   b Select the tag from the drop-down list populated from the entire set of tags defined within Archive Manager.

   c Specify the tag value in the box to the right of the tag.

   Specifying an invalid value generates turns the input box red.

   - Multiple items can be added to the set using the **+Tag** button.
   - To remove a tag from the set, click the **Trash Can** icon.

9 In the **Items that contain the words** box, enter the keywords that the messages to be retained should contain.

   In the **Look in:** field, select one or more checkboxes to specify where to look for the words you entered: **Subject**, **Body**, or **Attachment**.

   NOTE: Retention policy search criteria must follow the search syntax rules detailed in the *Searching Email* chapter of the *Archive Manager User Guide*.

10 To implement policies, click **Save** at the top of the Policy Editor screen.

11 Additional Delete Policies can be added by repeating the steps listed above.

Click the **Check Mark** icon at the top of the screen to use the collapsed state of the policy. Click the **Gear** icon to view the policy. If the check mark is gray, the policy is not valid. A red exclamation point will be displayed next to the invalid property.

When the time specified for the **Delete Policy** is over, the messages are deleted from the indicated containers, and are completely removed from the Archive Manager database if they are no longer in any mailboxes.

Editing Policies

To edit a Keep Policy or a Delete Policy:

1 To edit a policy, expand the view of the policy item by clicking the **Gear** icon in the policy. The collapsed state of the item changes to the expanded state where you can edit the policy settings.

2 Modify the fields in the policy as needed.

3 Click **Save**.

Policies are executed in the hierarchical top-to-bottom order. You can reorder the process hierarchy by using drag-and-drop to move the policy items. Click and drag the grip at the left corner of a policy item. Messages pertaining to policies higher in the list are executed first and then subsequently ignored by policies lower down in the list. This provides a conflict resolution strategy allowing items to be kept safe by capturing them within a Keep policy and placing it at or near the top of the list.

Removing Policies

To remove a Keep Policy or a Delete Policy:

1 Click the **Trash Can** icon at the top right of the policy.

Execution Log tab

All retention activity is logged so that the administrator can review the process history of the Retention Policy service.

The **Execution Log** provides the following information:

- **Start:** The date and time when the Retention service began executing the policy set.
- **Finish:** The date and time when the Retention service completed executing the policy set.
- **State:** The current state of the retention run.
- **Mode:** The mode of retention policy execution: Safe (used for testing purposes), or Production.
- **Committed:** Whether the retention run applied any changes: either true or false.
- **Details:** Details for each execution can be displayed by clicking on the View link.

When you select a row in the execution log, an Execution Run Summary is displayed in the lower half of the screen, and contains the following information:

- **Policy Name:** The name given to the message policy.
- **Start:** The time that the retention policy was started.
- **Finish:** The time that the retention policy finished.
- **Matched Messages:** The number of messages to which the message policy applies.
- **Occluded Messages:** The number of messages that could not be handled by a policy because they were already handled by another policy.
- **Matched Links:** The number of matched messages in user mailboxes.
- **Occluded Links:** The number of links that could not be handled by a policy because they were already handled by another policy.

The details for the execution can be grouped by the following:

- Policy
- Mailbox
- Message

Grouping by **Policy** displays the following information:

- ID
- Retention Policy Name
- Message Count
- Mailbox Count

Click on a row to view additional information about a **Policy**. At this level, you can group by **Mailbox** to view the mailboxes affected the currently-selected policy, including the **Message Count** for each policy. Or, group by **Message** to view the messages affected by the currently-selected policy, including the **Mailbox Count** for each message.

Grouping by **Mailbox** displays the following information:

- ID
- Mailbox Name
- Retention Policy Count
- Message Count

Click on a row to view additional information about a **Mailbox**. At this level, you can group by **Policy** to view the policies that affected the currently-selected mailbox, including the **Message Count** for each policy. Or, group by

Message to view the messages affected by the policy in the currently-selected mailbox, including the **Retention Policy Count** for each message.

Grouping by **Message** displays the following information:

- ID
- Message Subject
- Message Date Sent
- Retention Policy Count
- Mailbox Count

Click on a row to view additional information about a **Message**. At this level, you can group by **Policy** to view the policies that affected the currently-selected message, including the **Mailbox Count** for each message. Or, group by **Mailbox** to view the mailboxes associated with the currently-selected message, including the **Policy Count** for each mailbox.

Change Log tab

The administrator can review the changes made to the retention policy. The Change Log tab provides the following filters:

- **Login Name:** Filter change logs on the user you specify.
- **Change Type:** Select one of more of the following:
  - **Commit Mode:** View commit mode changes.
  - **Legal Hold:** View Legal Hold changes.
  - **Notifies:** View notification email address changes.
  - **Policies:** View retention policy changes.
  - **Schedule:** View retention schedule changes.

The **Change Log** provides the following information:

- **Change Date:** The date and time the changes were introduced.
- **User:** The name of the user who introduced the change.
- **Change Type:** The category for the change.
- **Summary:** The summary of changes applied to the policy set.

Legal Hold tab

Legal Hold suspends all retention policies to prevent the deletion of email messages that are the subject of pending, or potential, litigation or investigation. Users with the Edit Legal Hold permissions can invoke a Legal Hold, also referred to as a lock. Legal Hold has the following features:

- Legal holds can be placed on an entire archive or on a mailstore, mailbox, group or OU.
- A single user or multiple users can place a Legal Hold on an item.
- A single user can place more than one Legal Hold on an item.
- A single user can place Legal Holds on multiple items.
- Any reason can be entered for the Legal Hold.

- All users who place a Legal Hold on an item are required to remove the Legal Hold before the Retention service resumes operation.

NOTE: There can be various reasons for applying a Legal Hold, such as the nature of the customers' business requiring accurate record keeping, litigation, etc.
In the event of litigation, it is recommended that the customer apply a Legal Hold unless/until it is determined that their legal obligations can be met with their retention policies.

Adding a Legal Hold

To add a Legal Hold:

1. From the Legal Hold tab, enter a reason for placing the legal hold in the **Reason** box.
2. In the Targets field, select one or more message containers on which to place the legal hold: **Mailstore**, **Mailbox**, **Group** or **OU**. Or, select **Everything (All Messages in Archive)** checkbox to place the legal hold on all messages in the archive.
3. Click the **+New Legal Hold** button at the bottom of the box.
4. Add additional Legal Holds by repeating steps 1-3.

The Legal Hold is applied, meaning the Retention service will not process. If other users who did not lock the item sign in with appropriate rights, they can see by whom, when and why the Legal Hold was invoked but they cannot deactivate it.

The Retention service activity related to Legal Hold is as follows:

- If the Retention service is running at the moment when the Legal Hold is activated, the service finishes processing the current policy item and the execution of the policy set is terminated.
- If the Legal Hold is enabled before the Retention service is scheduled to start, the service will ignore the schedule.

Unlocking a Legal Hold

The **Unlock** icon is visible only to the user(s) who invoked the Legal Hold.

To unlock a Legal Hold:

1. Click the **Unlock** icon in the Legal Hold box.
2. Repeat this process for each user who placed a Legal Hold on an item, until you are down to the last user.

Deleting a Legal Hold

The **Delete** icon is visible only to the user(s) who invoked the Legal Hold. When a Legal Hold is deleted, the Retention service will start executing the policy set in accordance with the schedule. The policy set will be processed starting from the first item in the list (not where the execution was terminated).

To delete a Legal Hold:

- Click the **Delete** icon in the Legal Hold box.

Schedule tab

The Schedule tab lets you select the days and times that the Retention service runs, continues an active run, or does not run. Days of the week are displayed on the left side of the grid. Times are displayed along the bottom of the grid.

- **Scheduled:** The Retention service should start a new retention run if none is currently active, or continue an active run.
  - To schedule days and times for the Retention service to start a new retention run, click **Scheduled** and then click in the grid to select days and times.
  - To schedule an entire day of the week that the Retention service can start a new retention run, click **Scheduled** and then click on the day of the week.
  - To schedule a time of day that the Retention service can start a retention run every day of the week, click **Scheduled** and then click on the time.
- **Continue**: The Retention service may continue an active retention run, but may not start a new run.
  - To select days and times to continue an active retention run, click **Continue** and then click in the grid to select days and times.
  - To schedule an entire day of the week that the Retention service can continue an active retention run, click **Continue** and then click on the day of the week.
  - To schedule a time of day that the Retention service can continue an active retention run every day of the week, click **Continue** and then click on the time.
- **None:** The Retention service does not run on that day/time.
  - To deselect items from the grid, select **None** and then click on the items in the grid.
  - To deselect an entire day of the week so that the Retention service does not run during that day, click **None** and then click on the day of the week.
  - To deselect a time of day so that the Retention service does not run during that time, click **None** and then click on the time.

Settings tab

The **Operation Mode** box allows you to change the mode of Retention service activity. **Safe Mode** is used for testing retention policies before they are applied to the actual archive.

NOTE: Safe Mode allows a set of retention policies to be designed without any changes being made to the system. The Retention service will run based on your policy-set design, and the results of what would have happened to the archive can be viewed in the output log.

Production Mode executes the retention policies against the live production system.

NOTE: Retention policies are designed to keep and delete email messages after specified period of time. The incorrect use of these policies may result in data loss. Please ensure you have tested your policies in Safe mode before turning on Production Mode.

25

Tenants

- About tenants
- Edit a tenant

About tenants

The **Tenants** page in the Archive Manager Website allows you to view and manage the message policies, and enable or disable the Store Manager for your Office 365 tenants.

NOTE: This page is visible only if you have the **Edit Message Policies** permission and you have added a tenant by the Configuration Console.

Edit a tenant

To edit a tenant:

1. On the **Tenants** page, click the **Edit** icon to the left of the tenant name for the selected tenant in the list.
2. Revise the information and then click **Update**. For more information about enabling Store Manager and the message policies, see Edit a mail server.

26

System maintenance

- About system maintenance
- Cleaning up "scratch" tables
- Cleaning up the AfterMail_Temp database

About system maintenance

Some Archive Manager features and components require occasional maintenance to function efficiently. For example, some components generate data that eventually becomes obsolete and should be deleted from the disk so it does not burden disk-access functions. This chapter explains how to maintain your Archive Manager system for optimal performance.

Cleaning up "scratch" tables

Archive Manager includes a script that, when invoked, will delete all of the old temporary "scratch" tables that the program generates for searches and other functions. This CleanUp script is configured in the Archive Manager Configuration Console.

You can schedule the script to run at the same time every day (for example, 2:30am local time), by entering the run time as the CleanUpTime setting in the Configuration Console. Since the Retention Engine also uses temporary tables, the CleanUp script should not be run at the same time as the Retention Engine. Most admins choose to run the CleanUp script before the Retention Engine, which may occasionally run for prolonged time periods.

The CleanUp script is a SQL server job that stores its scheduled execution time in its own SQL Job Properties, and the script will delete old tables only if the SQL job time matches the CleanUpTime setting in the Configuration Console. If, for example, someone changes the CleanUpTime setting, then it will be different from the last-saved SQL job time, and the script will not delete old tables at the next CleanUpTime occurrence. Instead, when the script finds such a discrepancy, it will simply reset the SQL job time to match the CleanUpTime, and the script will then delete the old tables at the next occurrence of the CleanUpTime.

Cleaning up the AfterMail_Temp database

The ClearSearchCache SQL job, which is used to clean up the AfterMail_Temp database, may inadvertently delete the tables that are created for retention, rendering the Retention Engine inoperable until scripts are re-run to recreate the tables. The ClearSearchCache SQL Job may also mistakenly leave behind some temporary search tables that should be deleted: files with names prepended with *DOMAIN\SERVICE_NAME* and then the table names.

If you run the ClearSearchCache program subroutine, you may need to run the CleanTempTable script to clean up the AfterMail_Temp database.

27

Log Viewer

- About the Log Viewer
- Log Viewer menus and toolbar
- How to ...
- Configuring logs
- EventLogAppender
- TraceAppender
- RollingFileAppender
- ColoredConsoleAppender
- Additional information

About the Log Viewer

The Log Viewer simplifies the viewing and interpretation of program log files, which document alerts and warnings in Quest programs.

Log Viewer menus and toolbar

Most Log Viewer features are accessible by the program's menus and/or the program tool bar, which share a horizontal band across the top of the screen:

Several features are also available directly from the keyboard, and those keyboard shortcuts are displayed in the menus and noted here.

File menu

- **Open Log File...** (or Ctrl+O): Opens a standard Windows *Open* dialog box, from which you can specify the file you want to open into the Log Viewer. The Log Viewer can open and display *WLog* (optionally compressed) files, and plain text files.

  Drag-and-Drop Option: You can also open a wlog file in the Log Viewer by dragging and dropping a filename from Windows Explorer into the Log Viewer window.
- **Save Copy Of Log File As...** (appears only when a file is open): Opens a standard Windows *Save As* dialog box, from which you can specify the filename and location where you want the open file to be saved. The Log Viewer lets you edit the contents of an open file, but will not replace the original on disk with the edited version (you cannot save it under the same name in the same location).
- **Recent Files:** Shows a list of recently opened files, from which you can select a file to re-open (to quickly re-open a file you have recently viewed and closed).

- **Exit:** Closes the Log Viewer window.

Edit menu

- **Copy (or Ctrl+C):** Copies the selected line to the Windows clipboard.
- **Find... (or Ctrl+F):** Opens a **Find** dialog box that lets you specify a text string to search for within the open file:

  The dialog box lets you search for the next or preceding occurrence, or for the first or last occurrence in the file. The **Find** feature highlights the entire line that contains the target string.
- **Go To Line Number:** Open a dialog box that lets you jump to a particular line number of the file. (Enter the line number and click **OK**.)

View menu

- **Show Line Numbers** (or Ctrl+L): Toggles the display of line numbers (within the open file) on and off.
- **Show Complete Log Entry** (or F5): Opens a *Log Detail* window that shows the entire string for the selected item—useful when the item text overruns the Log Viewer's maximum line length (maximum 259 characters), or if the line extends beyond the right edge of the viewer window without wrapping.
- **Enable Internet Access:** Toggles the Internet connection on and off.
- **Goto Line Number:** Prompts for a line number in the file to display.

Help menu

- **Online Help... (or F1):** Opens Quest's online Help file for the Log Viewer, which documents its features.
- **About...:** Opens a window of information about the Log Viewer—identifying the current release, and asserting Quest's intellectual property rights to the software.

How to ...

This section describes how to complete various tasks in the Log Viewer.

To Open a Specific Log:

- Drag and drop a wlog file name from Windows Explorer into the Log Viewer window.

  – OR –
- Click the **Open Log File** button (in the Toolbar) to view a list of log files that can be opened. In the *File* section of the screen, select a log file and click **OK** to open the log in the Quest Log File Viewer.

To Find a Particular Text String Within an Open File:

- **Edit** menu **| Find...** (or Ctrl+F): Opens a **Find** dialog box that lets you specify a text string to search for within the open file. The **Find** feature highlights the entire line that contains the target string.

To Re-Open a Recently Viewed File:

- **File** menu **| Recent Files:** Shows a list of recently opened files, from which you can select a file to re-open (to quickly re-open a file you have recently viewed and closed).

To Save a Copy of a File:

- **File** menu **| Save Copy Of Log File As...** (appears only when a file is open): Opens a standard Windows *Save As* dialog box, from which you can specify the filename and location where you want the open file to be saved. (This feature does not permit any revisions to the open file. It simply lets you save the file *in its original form* to a new filename and/or a new location.)

To Show or Hide Line Numbers:

- **View** menu **| Show Line Numbers (or Ctrl+L):** Toggles the display of line numbers (within the open file) on and off.

To Jump to a Particular Line Number in the File:

- **Edit** menu **| Go To Line Number:** Opens a dialog box that lets you specify the destination line number. (Enter the number and click **OK**.)

To View an Entire Untruncated Log Entry:

- **View** menu | **Show Complete Log Entry (or F5):** Opens a Log Detail window that shows the entire string for the selected item—useful when the item text overruns the Log Viewer's maximum line length (maximum 259 characters), or if the line extends beyond the right edge of the viewer window without wrapping.

To Turn Internet Access On or Off:

- **View** menu **| Enable Internet Access:** Toggles the Internet connection on and off.

To Copy a Selected Line to the Clipboard:

- **Edit** menu **| Copy** (or Ctrl+C): Copies the selected line to the Windows clipboard.

To Close the Log Viewer:

- **File** menu **| Exit:** Closes the Log Viewer window, or click the Log Viewer **Close** box (**[X]**) to dismiss the window and return to the previous display.

Configuring logs

The logging system is built on the Apache log4net project (http://logging.apache.org/log4net). The following sections describe the log4net appenders used by Archive Manager in more detail.

Logging configuration files for each service can be found within the installation directory in the following locations. To change the logging levels, change the level listed on the root node. The default level is INFO.

- Quest.AM.logging.config

EventLogAppender

The EventLogAppender logs any ERROR level messages to the Windows event log. To log warnings to the event log, change the threshold value for this appender.

TraceAppender

The TraceAppender logs calls made to the .NET Trace system. By default this appender is inactive. To enable tracing, edit the log4net.config for that agent and add a reference to the appender to the root configuration node:

RollingFileAppender

Writes to log files in the Log directory. It will write 10 10MB log files and then begin deleting the oldest log file for each file added after 10.

ColoredConsoleAppender

Writes logging information to a Windows console. If color enabled, it will write in different colors for each logging level.

Additional information

See the following links for additional information about configuring log4net:

- http://logging.apache.org/log4net/release/manual/configuration.html#syntax
- http://logging.apache.org/log4net/release/config-examples.html

28

Exchange Utility

- About the Exchange Utility
- Install and run the Exchange Utility
- Menu items
- Get mailboxes
- Create Outlook Archive Manager folder
- Install Outlook Form
- Update Archive Manager URL
- Reconstruct stubbed messages
- Update stubbed message checksums

About the Exchange Utility

The Exchange Utility performs the following functions:

- Creates an Archive Manager folder in users' Outlook mailboxes that contains a URL to the Archive Manager User Web Site. Users can access the Archive Manager User Web from their Outlook mailboxes by clicking on the Archive Manager folder. They can then use the User Web Site to conduct email searches from their desktops.
- Installs the Outlook Form.
- Updates the Archive Manager URL by redirecting stubbed messages to a new URL if the location of the Archive Manager Web Site has changed.
- Performs bulk reconstruction of stubbed messages.
- Repair stubbed message checksums.

Install and run the Exchange Utility

The Exchange Utility is installed when you install Archive Manager.

To run the Exchange Utility, go to the Archive Manager root folder and locate the **Exchange Utility.exe** file. For customers running an upgraded version of Archive Manager, the path may vary**.**

It is recommended that you run the Exchange Utility as the ESM user.

Menu items

The Exchange Utility contains the following menu items:

- Get Mailboxes
- Create Outlook Archive Manager Folder
- Install Outlook Form
- Update Archive Manager URL
- Reconstruct Stubbed Messages
- Repair Stubbed Message Checksums

Get mailboxes

To select Exchange Outlook mailboxes in which to perform the operations listed above:

1 In the **File** menu, click **Get Mailboxes**.

  This opens the Mailbox Selector screen.

This screen allows you to select mailboxes by any of the following criteria:

- Login
- Group
- MailServer
- MailStore
- Domain
- OU

Items can be added and removed from the list, or toggled on and off. To toggle on and off, click the Green button on the right side. Use the drop down list to make a selection. A preview list is generated in the far right column.

Create Outlook Archive Manager folder

To create a folder that can be used to access the Archive Manager User Website in users' Outlook mailboxes:

1 Go to the **File** menu and click **Create Outlook Archive Manager Folder**, to display the Archive Manager URL screen.

2 In the **Archive Manager URL** box, type in the URL to the Archive Manager Web Site and click **OK**.

3 Verify that the URL is correct in the **Is this the correct URL?** box. When you click **Yes**, the Exchange Utility begins creating the folders.

Install Outlook Form

Select the **File/Install Outlook Form** menu option to install the Outlook Form. 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.

Update Archive Manager URL

To redirect Stubbed messages to a new URL if the location of the Archive Manager Website has changed:

1. If you have not already done so, in the **File** menu, click **Get Mailboxes**, to open the Mailbox Selector screen.
2. Select the mailboxes for which you want to update the Archive Manager URL. All mailboxes are selected by default.
3. Go to the **File** menu, and click **Update Archive Manager URL**.

   This displays the Archive Manager URL screen.
4. In the **Type URL** box, enter the new URL to the Archive Manager Web Site and click **OK**.

   The stubbed messages are now directed to the new URL.

If you have changed the location of the Archive Manager Website and redirected your stubbed messages to a new URL, you also need to update the **AfterMail URL** setting in the Configuration Console. Stubbed messages will not be reconstructed unless you change the AfterMail URL.

Reconstruct stubbed messages

NOTE: Prior to reconstructing stubbed messages, make sure that you have turned off stub policies in Archive Manager. If you do not, Archive Manager may stub the messages again, depending on how your policies are set.

To reconstruct stubbed messages:

1. If you have not already done so, in the **File** menu, click **Get Mailboxes**.

   This opens the Mailbox Selector screen.
2. Select the mailboxes you want to reconstruct. All mailboxes are selected by default.
3. Go to the **File** menu and select **Reconstruct Stubbed Messages**.

   This displays the Web Service Login screen.
4. Enter the following sign-in credentials and click **Login**:
   - **Server URL:** The URL to Archive Manager
   - **User:** The Archive Manager administrator
   - **Password:** The password for the Archive Manager administrator
   - **Domain:** The Administrator's sign-in domain

The status bar displays the status of the message reconstruction. Each mailbox is unchecked after it has been processed.

Update stubbed message checksums

You may need to update stubbed message checksums with the Exchange Utility under the following conditions:

- You had Archive Manager version 4.0.5 installed and applied a stub policy.
- When you click on a message in Outlook in Archive Manager 4.0.5 or later, the message fails to reconstruct but CAN be viewed by clicking on the link within the message.

Under these conditions, the stubbed message needs to be repaired because the checksum doesn't match the checksum of the message in the Archive Manager database. If you are running a version of Archive Manager more recent than version 4.0.5, run the **Update Stubbed Message Checksums** option located in the File menu of the Exchange Utility to reprocess the affected messages. If you are running version 4.0.5, upgrade to the current version of Archive Manager to update the checksums.

29

Administering in a hosted Exchange environment

- System requirements for running ESM in a hosted Exchange environment
- Configuring ownership and access to user mailboxes on hosted Exchange
- URL parameter
- Agreement text
- Auditing

System requirements for running ESM in a hosted Exchange environment

ESM requires one of the following to run in a hosted Exchange environment:

- Outlook 2024 (32-bit)
- Outlook 2021 (32-bit)
- Outlook 2019 (32-bit)

Configuring ownership and access to user mailboxes on hosted Exchange

Each mailbox discovered on the hosted server is considered private. This means that only the owner of the mailbox can execute the following actions:

- View the mailbox
- Search messages in the mailbox
- Change delegation settings for the mailbox

Users cannot access a private mailbox unless the owner grants access to the mailbox. Public mailboxes, as defined in this document, are mailboxes that are not private, and can be searched by all users who have appropriate credentials.

The administration of private mailboxes is also limited. Administrators cannot assign logins or groups to private mailboxes, nor can they perform searches against them. However, administrators can still assign message policies and enable store management for private mailboxes.

For how to configure ownership and access to a mailbox on hosted Exchange, see the section *Working with hosted Exchange mailboxes* in *Archive Manager User Guide*.

If a situation arises where an administrator needs to remove current ownership of a mailbox so that a different user can claim ownership, the administrator can do so through the Mailbox page in the Archive Manager Administration Website. Editing a private mailbox that is currently owned displays a **Remove Owner** button. Clicking this button removes current ownership of the mailbox so that another user can designate ownership.

URL parameter

You can append an email address to the URL of the Manage Archive Access page to manage the user's hosted account. For example, if you want to manage John Smith's hosted account, enter the following URL:

http://<archivemanager>/app.html#/home/manage-remote-access/john.smith@hostingplace.com

The URL listed above populates the Remote Email Address text box with the following:

john.smith@hostingplace.com

This makes it easy to provide a link for users to enable or disable access mailboxes on hosted Exchange. They just need to provide their local and remote passwords.

Agreement text

The agreement text displayed in the Configure Remote Access page is configurable by editing the RemoteAccessAgreement.html document. This document can be found in the Archive Manager Website directory on the Archive Manager web server at:

```
<ArchiveManager>\website\RemoteAccessAgreement.html
```

NOTE: The content of RemoteAccessAgreement.html must be in a standard HTML format.

Auditing

All attempts to change mailbox delegation settings (successful or not) are recorded in the database for audit purposes. The audit record includes the time and date of the action, user information, status of the request (successful or failed), the actual delegation agreement text presented to the user, and other information. See Delegation Log report for detailed descriptions of the reports.

Appendix A: Moving database or attachment store

- Moving the database
- Moving the attachment store

Moving the database

If you are moving from one database server to another database server, such as SQL 2000 to SQL 2005, the AfterMail_Temp table and the Archive Manager database must use the same collation setting. The collation setting must contain Case Insensitive (CI) and Accent Sensitive (AS). Set the value to:

```
SQL_Latin1_General_CP1_CI_AS
```

To move the Archive Manager database:

1. Stop the Archive Manager Web site.
2. Stop all Archive Manager services.
3. Run the Archive Manager installer to create a new, empty database on the new SQL server.

   You can exit the installer after the database is installed.
4. Detach the Archive Manager SQL database and move it to the desired location.
5. Attach the database from the new location.
6. Start the Web site and make sure you can sign in to Archive Manager.
7. Restart all Archive Manager services.

Instead of moving database by running the installer to create a new database, you can also use Configuration Console to configure connection strings to a new database:

1. Stop the Archive Manager Web site.
2. Stop all Archive Manager services.
3. Detach the Archive Manager SQL database and move it to the desired location.
4. Attach the database from the new location.
5. Open the Configuration Console, and click the cog button in the top right corner.
   The Connection String Window opens.
6. Type the new server, and select the database from the drop-down list.
7. Click **OK**.
8. Start the Web site and make sure you can sign in to Archive Manager.
9. Restart all Archive Manager services.

Moving the attachment store

You may need to move your store to a new location, for example, when your SAN fills up or you need to move the store to a new SAN or machine. This usually is preferable to having two filesystem stores, although either option is valid.

1. Stop all Archive Manager services on the Archive Manager server.
2. Move the attachment store to the desired location.
3. Set compression as needed, and set permissions to match the old location.
4. Launch SQL Server Management Studio.
5. Browse to your Archive Manager database.
6. Open the **StorageLocations** table located under the **Tables** node.
7. Specify the new location of the store in the connection string.
8. Restart the previously stopped services on the Archive Manager server.

Appendix B: Enabling generating publisher evidence

The common language runtime (CLR) tries to verify the Authenticode signature at load time to create publisher evidence for the assembly. To reduce startup time of the Archive Manager applications and services, Archive Manager disables creating publisher evidence by default. However, you can enable it for individual application or service when necessary.

To enable creating publisher evidence for an Archive Manager application or a service:

1. Stop the application or service.
2. Locate and open the application config file named as `<ApplicationName>.exe.config`. For example, the file for the ADC service is `ActiveDirectoryService.exe.config`.
3. In the config file, set the following element to `true`:
   ```
   <generatePublisherEvidence enabled="true"/>
   ```
4. Save and close the config file.
5. Start the application or service.

For more information about the <generatePublisherEvidence> element, see https://docs.microsoft.com/en-us/dotnet/framework/configure-apps/file-schema/runtime/generatepublisherevidence-element

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.