

HP Email Archiving software for Microsoft Exchange Version 2.2 Administrator Guide

HP Part Number: PDF
Published: December 2010
Edition: Second



© Copyright 2004, 2005, 2006, 2007, 2008, 2009, 2010 Hewlett-Packard Development Company, L.P.

Hewlett-Packard Company makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of Hewlett-Packard. The information contained in this document is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Microsoft®, Windows®, Windows XP®, and Windows Vista® are U.S. registered trademarks of Microsoft Corporation.

Hewlett-Packard Company shall not be liable for technical or editorial errors or omissions contained herein. The information is provided "as is" without warranty of any kind and is subject to change without notice. The warranties for Hewlett-Packard Company products are set forth in the express limited warranty statements for such products. Nothing herein should be construed as constituting an additional warranty.

Contents

About this guide.....	8
Intended audience.....	8
Related documentation.....	8
Document conventions and symbols.....	8
Support.....	9
Subscription service.....	9
1 HP EAs Exchange Software Overview.....	10
Overview.....	10
Compliance Archiving.....	10
Compliance Archiving using journal mailboxes.....	10
SMTP Premium Journaling.....	11
Selective Archiving.....	11
PST Import Manager.....	12
End user applications.....	12
2 System requirements and prerequisites.....	13
HP EAs Exchange system requirements.....	13
Prerequisites.....	13
Creating the archive service account.....	13
Configuring the Exchange Server for Public Folder archiving.....	15
3 Using HP EAs Exchange software.....	16
Launching EAsE software.....	16
Navigating in the HP EAs Exchange software.....	16
4 Configuring Credentials.....	18
Configuring the IAP credentials.....	18
Configuring the Exchange server credentials.....	18
5 Configuring the Archive Engine defaults.....	20
Essential concepts.....	20
Tombstones and Stealth Archiving.....	20
TNEF message format.....	20
Default Routing Address.....	21
Access Control Lists (ACL).....	21
Navigating to the default settings.....	21
General Defaults.....	21
Compliance Archiving Defaults.....	22
Selective Archiving Defaults.....	22
Delete Synchronization Defaults.....	22
Tombstone Maintenance Defaults.....	22
Maintenance Defaults.....	23
6 Compliance Archiving with journal mailboxes.....	24
Overview of Compliance Archiving.....	24
Configuring the Exchange server for journaling.....	24

Configuration for Exchange 2010.....	24
Creating journal mailboxes.....	24
Enabling Compliance Archiving on mailbox stores.....	25
Exchange 2007.....	25
Pre-2007 Exchange servers.....	25
Configuring Compliance Archiving events.....	26
Creating a Compliance Archiving event.....	26
Editing Compliance Archiving events.....	26
General tab.....	27
Configuration tab.....	27
Schedule tab.....	27
IAP Domain tab.....	28
Advanced tab.....	28
Copying a Compliance Archiving event.....	28
Deleting a Compliance Archiving event.....	28
Running Compliance Archiving events.....	29

7 Compliance Archiving with SMTP Premium Journaling.....30

Overview of SMTP Premium Journaling.....	30
Message flow.....	30
Multiple Archive Gateways.....	30
Archive failures.....	30
Configuring Exchange and the Archive Gateway.....	30
Configuring the Archive Gateway.....	31
Join the Archive Gateway to the Exchange domain.....	31
Configuring the Exchange server for SMTP Premium Journaling.....	32
Create DNS records for the Archive Gateway.....	32
Configure the Hub Transport settings.....	33
Create the Mail Contact record.....	33
Create the ENDR mailbox.....	34
Create a new Hub Transport Journal Rule.....	34
Creating an SMTP Journal event.....	34
Working with SMTP Journaling events.....	36
Enabling and disabling SMTP journaling.....	36
Enabling and disabling SMTP Journaling events.....	37
Specifying ENDR processing.....	37
Working with the Local SMTP configuration.....	37
Examining SMTP Tasks.....	37

8 Configuring Selective Archiving.....39

Overview of Selective Archiving.....	39
Configuring the Policy Engine.....	40
Setting CAS server and Administration Mailbox.....	40
Adding mailboxes.....	42
Adding public folders.....	42
Excluding system mailboxes.....	43
Setting up Auto-Search.....	43
Creating Selective Archiving events.....	44
Configuring Policy Engine rules.....	46
Information Stores tab.....	47
Folders tab.....	48
Selection tab.....	50
Messages tab.....	53

Conditions tab.....	54
Adding conditions to an existing list.....	54
Determining how conditions are applied.....	55
Actions tab.....	55
Schedule tab.....	56
Working with Selective Archiving events.....	57
Editing Selective Archiving events.....	57
General tab.....	57
Configuration tab.....	58
IAP Domain tab.....	58
Advanced tab.....	58
Copying a Selective Archiving event.....	59
Deleting a Selective Archiving event.....	59
Running Selective Archiving events.....	59
Executing a Policy Engine rule manually.....	59
Using Information Store Groups for rule processing.....	60
9 Using tombstone maintenance.....	63
Configuring tombstone maintenance events.....	63
Configuring tombstone maintenance events with folder capture.....	64
10 Configuring end-user delete.....	66
Location of deleted items.....	66
Deleted items tag.....	66
Enabling deletion retention on the Exchange server.....	66
Exchange 2007 and later.....	66
Pre-2007 Exchange servers.....	67
Scheduling deletion from the IAP.....	68
Creating the event.....	68
Creating a Policy Engine rule.....	68
11 Working with folder capture.....	70
Indexing folder information.....	70
Enabling folder capture.....	70
Enabling folder capture on the IAP.....	70
Enabling folder capture in the archiving global configuration file.....	71
Enabling folder capture for a specific event.....	71
Enabling folder capture in PST Import Manager.....	71
How folder capture works with archiving events.....	71
Folder capture and Selective Archiving events.....	72
Folder capture and Tombstone Folder Synchronization events.....	72
Folder capture and Synchronize Deleted Items events.....	72
Folder capture and PST Import Manager.....	72
Folder capture and the merging of duplicate messages.....	72
12 Monitoring performance.....	74
Monitoring alerts.....	74
Monitoring system resources.....	74
Monitoring Archive Engine status.....	75
Monitoring SMTP Premium Journaling status.....	76
SMTP Journaling Stats.....	77
SMTP Journaling Graphs.....	77

13 Archiving with PST Import Manager.....	78
Installing the PST Import Manager.....	78
Installation requirements.....	78
Installation procedure.....	78
Launching the PST Import Manager.....	79
Establishing archive credentials.....	79
Creating and queuing the Import Description.....	80
Creating or editing an Import Description file.....	81
Queuing the Import Description file.....	83
Importing and monitoring.....	83
Importing PST data.....	83
Monitoring progress.....	84
Working with log files.....	84
14 Working with end-user applications.....	86
Overview of the applications.....	86
Using the IAP Web Interface.....	86
Using single sign-on.....	87
Installing and configuring the Outlook extension.....	87
Installing the Outlook extension for users.....	87
The Archive Options tab.....	88
Using the Archive Options tab in Outlook 2003 and 2007.....	88
Using the Archive Options tab in Outlook 2010.....	89
Setting host information.....	89
Displaying the About dialog box.....	90
Configuring Archive Cache.....	91
HP EAsE Archive Cache status icon.....	92
Registry settings.....	93
Default registry settings.....	93
Manually creating other registry settings.....	93
Overriding the language in the Outlook extension user interface.....	93
Changing the language in Archive Options tab, Archive Cache, and PST Export Utility.....	93
Changing the language in Integrated Archive Search.....	94
Localized languages in Outlook extension.....	94
Using the extension with Citrix Presentation Manager.....	95
Exporting messages from the IAP.....	95
Overview of the export process.....	95
Exporting messages.....	96
Problems exporting messages.....	99
15 Working with HP OWA Extension.....	100
System requirements.....	100
Multiple mail stores.....	100
Multiple IAP systems.....	101
Temporary storage in Drafts folder.....	101
Deleting temporary Drafts copies using a rule.....	101
Creating a rule with the EASE_Tombstone_Delete template.....	101
Making tombstoned mail items visible in OWA.....	102
Viewing the Web.config file in Exchange 2007 and later installations.....	102
Working with the asp.config file in Exchange 2003 installations.....	103
IAP appliances.....	103
URL templates.....	103
ASP pages.....	103

Changing the ASP time-out in Exchange 2003 installations.....	103
Browser functionality.....	104
Multi-user support.....	104
Large attachments.....	104
16 Troubleshooting.....	105
OWA 2007 users cannot open folders containing tombstoned messages.....	105
OWA 2007 and later users cannot retrieve tombstoned messages.....	105
Behavior in Microsoft Exchange Server 2007 and later impacts detection of message duplicates.....	105
Overview.....	105
HP RIM 1.x.....	105
HP EAs Exchange 2.x.....	106
Selective archiving does not process all folders in user mailbox.....	106
Changes not captured in email attachments.....	106
Users cannot find messages sent to a distribution list.....	106
DiskSpaceBuffer error.....	107
HP Batch Export error.....	107
Creating a file type association.....	108
Changing the file type association.....	109
A Indexed document and content types.....	110
Indexed document types.....	110
Exchange items.....	110
Indexed file types.....	110
Message MIME types.....	111
Additional indexing detail/limitations for Microsoft Office 2007.....	112
Office 2007 supported features and properties.....	112
Microsoft Office 2007 indexing limitations.....	115
B Character support.....	116
C PST Import Manager: Archive Request file specifications.....	117
Settings description.....	117
Sample Archive Request file.....	119
D Outlook extension registry settings.....	120
Cache related registry settings.....	120
IAP retrieval related registry entries.....	122
Search and export related registry settings.....	122
Administrative registry settings.....	123
Index.....	124

About this guide

HP Email Archiving software for Microsoft Exchange (HP EAs Exchange or EAsE) is mail administration software that archives messages from Exchange mail accounts in the HP Integrated Archive Platform (IAP). This guide explains how to configure and administer HP EAs Exchange.

NOTE: The Integrated Archive Platform was formerly known as the Reference Information Storage System, or RISS. HP Email Archiving software for Microsoft Exchange was formerly known as HP Reference Information Manager for Exchange.

Intended audience

This guide is intended for:

- HP IAP administrators
- HP EAsE administrators

Related documentation

In addition to this guide, HP provides the following IAP and EAsE documentation.

For administrators and installers:

- *HP Email Archiving software for Microsoft Exchange Installation Guide* (available to HP personnel installing IAP and EAsE)
- *HP Email Archiving software for Microsoft Exchange Release Notes*
- *HP Integrated Archive Platform Installation Guide* (available to HP personnel installing IAP and EAsE)
- *HP Integrated Archive Platform Administrator Guide*
- Online help for the Platform Control Center (PCC), also included in the *HP Integrated Archive Platform Administrator Guide*

For users:

- *HP Email Archiving software for Microsoft Exchange User Guide*
- *HP Integrated Archive Platform User Guide*

Document conventions and symbols

Table 1 Document conventions

Convention	Element
Medium blue text: Related documentation	Cross-reference links and email addresses
Medium blue, underlined text (http://www.hp.com)	Web site addresses
Bold font	<ul style="list-style-type: none">• Key names• Text typed into a GUI element, such as into a box• GUI elements that are clicked or selected, such as menu and list items, buttons, and check boxes
<i>Italic font</i>	Text emphasis

Table 1 Document conventions *(continued)*

Convention	Element
Monospace font	<ul style="list-style-type: none">• File and directory names• System output• Code• Text typed at the command line
<i>Monospace, italic font</i>	<ul style="list-style-type: none">• Code variables• Command-line variables
Monospace, bold font	Emphasis of file and directory names, system output, code, and text typed at the command line



IMPORTANT: Provides clarifying information or specific instructions.

NOTE: Provides additional information.



TIP: Provides helpful hints and shortcuts.

Support

You can visit the HP Software Support web site at: <http://www.hp.com/go/hpssoftwaresupport>
HP Software Support Online provides an efficient way to access interactive technical support tools. As a valued support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract.

To find more information about access levels, go to: http://support.openview.hp.com/new_access_levels.jsp

Subscription service

HP strongly recommends that customers register online using the Subscriber's choice Web site: <http://www.hp.com/go/e-updates>.

Subscribing to this service provides you with email updates on the latest product enhancements, newest driver versions, and firmware documentation updates as well as instant access to numerous other product resources.

1 HP EAs Exchange Software Overview

This chapter gives an overview of the HP EAs Exchange software and describes its main modules.

Overview

HP EAs Exchange is a combination of hardware and software that archives mail from your Exchange server to external storage. You can use EAsE for regulatory compliance or for keeping your Exchange users's mailboxes to a manageable size with little or no intervention on their part.

The hardware is the Archive Gateway, a Windows server that sits between your Exchange servers and the HP Integrated Archiving Platform (IAP). Depending on the size of your installation and the number of Exchange servers you run, you may have more than one Archive Gateway.

The Archive Gateway runs HP EAsE (Enterprise Archiving software for Exchange), which is a collection of software modules that perform specific archiving tasks and related maintenance tasks.

In addition to the software that runs on the Archive Gateway itself, there are applications that you can deploy on end user machines that they can use to work with data that has been archived on the IAP.

This chapter describes how the different parts of the EAsE software work to archive mail.

The Archive Engine is the workhorse of the archiving software. With it you create and manage the tasks that archive items from the Exchange server to the IAP. The Archive Engine provides two different archiving systems: Compliance Archiving and Selective Archiving.

Compliance Archiving

HP EAsE software offers two ways to do compliance archiving: compliance archiving using journal mailboxes and SMTP journaling. Both perform the same task but in different ways.

In compliance archiving using journal mailboxes, mail from all users is copied into a specially designated journal mailbox. The EAsE software scans the journal mailbox periodically and archives its contents to the IAP. This method is called “pull processing” because the Archive Engine polls the journal mailbox and pulls mail from it to archive it. In earlier versions of EAsE software, pull processing was the only way to do compliance archiving, and it is the only way to implement compliance archiving on older Exchange installations.

In SMTP journaling, every message going through the Exchange server is sent to the Archive Engine as well as its intended recipients. This method is called “push processing” because the Exchange server pushes the mail to the Archive Engine. SMTP journaling uses fewer resource on the Exchange server, but is only available on Exchange 2007 and later.

Compliance Archiving using journal mailboxes

Compliance Archiving takes every message coming into or going out of an Exchange server and archives it to the IAP. You generally use this feature to meet regulatory compliance requirements.

To use Compliance Archiving, you create one or more journal mailboxes on an Exchange server and configure the information stores on the server to use those mailboxes for journaling. The journal mailbox can be in the same information store that you are archiving, a different information store on the same server, or on a separate server altogether. As messages and other Exchange items come into the server, Exchange copies them into the appropriate journal mailbox.

With the Archive Engine you create a Compliance Archiving event. The event is a task that is associated with a journal mailbox and runs periodically. It checks the journal mailbox for new items, archives them to the IAP, and deletes them from the journal mailbox. The Archive Engine pulls messages from the Exchange server and archives them in the IAP. You need to create at least one Compliance Archiving event for each journal mailbox you wish to archive to the IAP.

Every user has a corresponding repository on the IAP. Each archived item is stored in the user's repository. If a message comes into the Exchange server that cannot be delivered to a specific user, it goes into a catchall repository.

The items on the IAP are kept according to the retention policies specified by your enterprise.

SMTP Premium Journaling

SMTP Premium Journaling is another form of compliance archiving that archives every message coming into or going out of an Exchange server to the IAP but uses a different mechanism, available only on Exchange 2007 servers and later, to do so.

To use SMTP Premium Journaling, you configure an Exchange journal rule to send all messages coming through the server out through an SMTP send connector. Similarly, you configure the Archive Gateway to accept incoming messages from the Exchange server on the SMTP virtual server.

Messages move directly from the Exchange server, to the Archive Gateway, to the IAP without using journal mailboxes. SMTP Premium Journaling can provide higher throughput rates than the journal mailbox approach, but it requires slightly more complicated configuration of the Exchange environment.

Selective Archiving

While Compliance Archiving archives everything that passes through an Exchange journal mailbox, Selective Archiving gives you more fine-grained control over what gets archived. You can archive specific kinds of messages (email, calendar items, tasks, documents, and post items.) and specific sets of mailboxes. Selective Archiving is best for unobtrusive, enterprise-wide mailbox maintenance, although it can be used in some cases for investigations and discovery.

As with Compliance Archiving, you use the Archive Engine to create a Selective Archiving task that specifies the kind of Exchange items you want to archive. Next, you use the Policy Engine to create a rule that specifies the mailboxes that the task applies to. The Policy Engine also lets you refine the archiving rule to apply to messages with specific attributes such as content, age, number of attachments, and so on.

The Selective Archiving task archives items from the selected mailboxes to the IAP. You can choose what happens to the original message on the Exchange server:

- You can leave it as is on the Exchange server.
This is known as “stealth archiving” because there is no indication that the item has been archived.
- You can trim the body from the item. Moving the messages to the IAP reduces the size of the end user's mailbox. The truncated item remains in the user's mailbox along with a marker, called a tombstone, that indicates where on the IAP the archived message can be found.
- You can trim the attachments off an item, leaving the body on the Exchange server. EAsE replaces the attachments with a stub that lists the original attachments, and the message is marked with a tombstone.

An Outlook extension lets users seamlessly access the original message and attachments from tombstoned items. Users can also use IAP's Web interface to access archived items.

In addition to Compliance Archiving and Selective Archiving, the Archive Engine lets you create two maintenance tasks, Deletion Synchronization and Tombstone Maintenance. Deletion Synchronization scans the Exchange server for deleted archived (tombstoned) items and deletes the corresponding item in the IAP repository. Note that if the Deletion Synchronization task runs after a deleted message is no longer in the Exchange server, it will not be deleted from the IAP. In some cases the archived item will remain in the IAP repository if regulatory policies require it. Tombstone Maintenance is a housekeeping task that scans previously archived items on the Exchange and checks that they are properly synchronized with the archived items on the IAP.

PST Import Manager

The PST Import Manager is an application that lets you import the contents of PST files into the IAP. Its main purpose is to archive legacy data that you had stored in PST files into the IAP. The PST Importer does not run on the Archive Gateway. Instead, it runs on an administrator's system set up for that purpose. The PST Importer lets you specify which PST file to import, the IAP repository in which to store the messages, and whether to use stealth archiving or tombstone archiving on the messages.

End user applications

The end user applications give your Outlook Exchange users access to their archived data in three ways: through an Outlook extension, through an OWA (Outlook Web Access) extension, and through the IAP web interface.

The Outlook extension gives end users nearly seamless access to their archived messages. When a user requests a message that has been archived or an attachment that has been archived, the extension resolves the request and displays the message and its attachments as a regular Outlook message. For mobile users, the extension offers a local cache of the archive so that they can work with archived content even if they are not connected to the network. Finally, the Outlook extension provides an integrated search that lets end users search for particular messages stored in the IAP.

The OWA extension gives users who use Outlook web access the ability to fetch and display archived messages.

IAP Web Access gives users direct access to items stored in their repositories on the IAP. If the Outlook extension is installed, the results of the searches can be exported to a PST file.

2 System requirements and prerequisites

This chapter describes the requirements and prerequisites for running the HP EAsE software. It contains the following topics:

HP EAs Exchange system requirements

See the Support Matrix for the following HP EAs Exchange system requirements:

- Compliance and Selective Archiving
- PST Import Manager
- Outlook extension, including Archive Cache and PST Export
- OWA Extension

HP EAs Exchange is specifically designed as an application connector to the HP Integrated Archive Platform (IAP). IAP is the only compatible archiving platform for HP EAs Exchange 2.2.

Prerequisites

Before the HP EAs Exchange software is installed, ensure that the following conditions are met.

- Your company's Exchange servers and client systems must support the software to be installed. See the HP EAs Exchange Support Matrix for system requirements.
- In order to use SMTP Premium Journaling, you must be running a Microsoft Exchange 2007 (or later) Enterprise Server CAL.
- Create and configure the archive service account. You can also work with the HP service representative to create this account. See "Creating the archive service account" (page 13).

Creating the archive service account

Before the HP service representative installs the HP EAs Exchange software, create a domain user account and mailbox for the archive service in Active Directory.

Make sure the following conditions are met:

1. Name the user. In this document, we use the name HPAEServiceAccount for the service account.
2. Use the same name for the user logon name and mailbox alias: HPAEServiceAccount.
3. Ensure that the user is a member of Administrators, Domain Admins and Enterprise Admins groups.
4. Using the Exchange Management Console, ensure that the user has Exchange Organization Administrator rights on the IAP Service account. Note that these rights are not granted through a script.
5. Enter a password for the account.
6. In Exchange 2003:
 - Add the HPAEServiceAccount to Mailbox Rights with the following permissions:
 - Delete mailbox storage
 - Read permissions
 - Change permissions

- Take ownership
 - Full mailbox access
 - Add Administrator, Domain Admins, Enterprise Admins, and Exchange Domain Servers to Mailbox Rights.
7. In Exchange 2007 and later, add the access rights and permissions for HPAEServiceAccount using the following command in the Exchange Management Shell:

```
get-MailboxDatabase | add-ADPermission -User HPAEServiceAccount
-ExtendedRights Receive-As
```

NOTE: This command modifies the permissions for all mailbox databases. Use the `-Identity` switch to specify particular mailbox databases.

You can remove the permissions from the archive service account by issuing the following command in the Exchange Management Shell. Removing the permissions prevents the archive service account from performing Compliance and Selective Archiving from Exchange 2007 and later servers. Permissions can only be removed if they were granted previously.

```
get-MailboxDatabase | remove-ADPermission -User HPAEServiceAccount
-ExtendedRights Receive-As
```

8. For Exchange 2007 and later, issue the following command in the Exchange Management Shell:

```
get-PublicFolder -Identity \ -Recurse |
add-PublicFolderClientPermission -User HPAEServiceAccount
-AccessRights ReadItems,EditAllItems
```

This command grants the appropriate permissions to the archive service account for selectively archiving **all** public folders on Exchange 2007 and later.

If the archive service account already has one or more of the specified permissions, a warning message is displayed.

NOTE: An error is generated for the root folder, "\", because Exchange does not allow permissions to be changed on this entity. You can ignore this error.

To remove these permissions from the archive service account, issue the following command:

```
get-PublicFolder -Identity \ -Recurse |
remove-PublicFolderClientPermission -User HPAEServiceAccount
-AccessRights ReadItems,EditAllItems
```

This command prevents the archive service account from selectively archiving public folders in the future. Note that permissions can only be removed if they were granted previously.

Note the following about Mailbox rights permissions:

- Including the account as a Domain Admin automatically includes it as member of the local Archive Gateway's Local Administrators group (and no other group).
- View only Administrators group:
View-Only Administrators group for Exchange 2007 or AD interrogation, View-Only Organization Management group for Exchange 2010
Membership in these groups lets the service account access the AD objects and the code interrogates.
- Domain Users provides read-only access to AD user and group information.

Configuring the Exchange Server for Public Folder archiving

If you plan on archiving the contents of Public Folders, you will need to give the archive service account additional permissions.

If you are using Exchange 2003, follow this procedure:

1. Open the Exchange System Manager.
2. Navigate to the Public Folder Store and locate the public folder(s) that the archive service account will access.
3. Select the public folder to modify.
4. In the Actions pane, click the **Permissions** tab, and then click **Client Permissions**.
5. In the Add Users window, click **Add**, and then add the service account, and then click **OK**.
6. In the Client Permissions window:
 - a. Select the archive service account.
 - b. Select **Editor** in the Roles drop-down list.
 - c. Select the **Create Items**, **Read Items**, and **Folder Visible** check boxes.
 - d. Click **OK**.
7. Repeat steps 3–6 for all public folders to be archived.

If you are using Exchange 2007 and later, follow this procedure:

1. Open the Exchange Management Shell.
2. Issue the following command:

```
get-PublicFolder -Identity \ -Recurse |  
add-PublicFolderClientPermission -User HPAEServiceAccount  
-AccessRights ReadItems,EditAllItems
```

This command grants the appropriate permissions to the archive service account for selectively archiving **all** public folders on Exchange 2007 and later.

If the archive service account already has one or more of the specified permissions, a warning message is displayed.

NOTE: An error is generated for the root folder, "\", because Exchange does not allow permissions to be changed on this entity. You can ignore this error.

3. To remove these permissions from the archive service account, issue the following command:

```
get-PublicFolder -Identity \ -Recurse |  
remove-PublicFolderClientPermission -User HPAEServiceAccount  
-AccessRights ReadItems,EditAllItems
```

This command prevents the archive service account from selectively archiving public folders in the future. Note that permissions can only be removed if they were granted previously.

3 Using HP EAs Exchange software

This chapter describes how to launch the HP EAs Exchange software

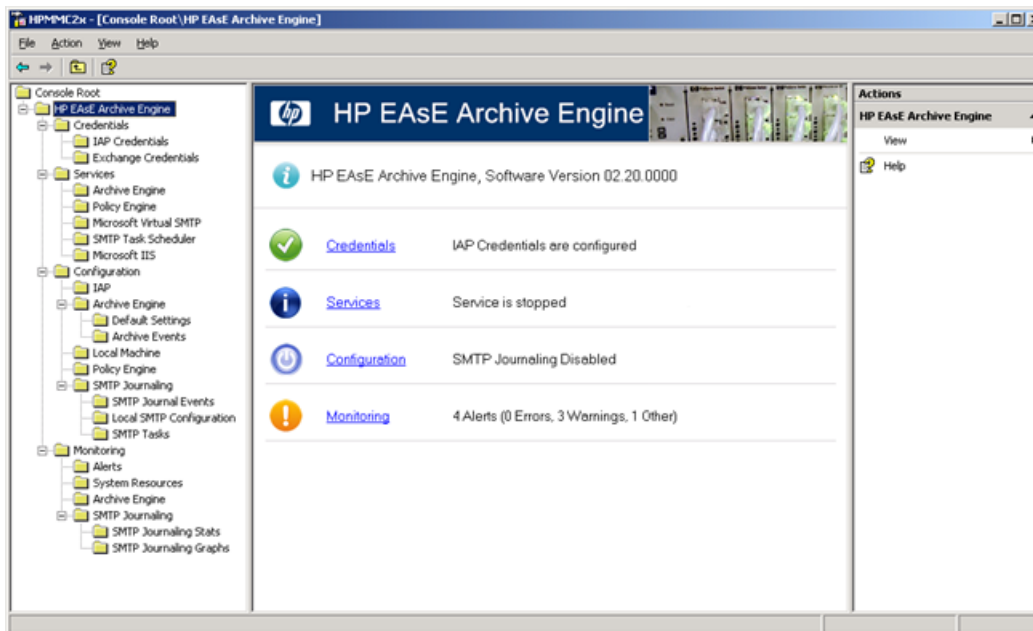
Launching EAsE software

Log on to the Archive Gateway with the archive service account you set up in “Creating the archive service account” (page 13). In this document, this account is named HPAEServiceAccount. Double-click the HP EAsE Archive Engine Administration icon on the desktop to launch the software.



- ❗ **IMPORTANT:** You must log in to the Archive Gateway with the HPAEServiceAccount (or whichever name you chose). If you log in with any other account, you will not be able to configure the EAsE software properly.

The EAsE Archive Engine console appears. You will manage the EAsE software from this console.



The center pane displays the part of the EAsE software that you are working on. You can click the links on this pane to drill down to specific modules.

The left pane has a tree control that lets you navigate to specific modules quickly.

The right pane changes to display actions that you can take depending on the contents of the center pane.

NOTE: Some of the commands in the Actions pane, such as **View** and **Help** do not apply to the EAsE software.

Navigating in the HP EAs Exchange software

Throughout this guide, navigation instructions are given in the form **Configuration**→**Archive Engine**→**Default Settings**. That means that you can either:

1. Click the **Configuration** link in the main pane to open the Configuration pane.
2. Click the **Archive Engine** link in the Configuration pane to open the Archive Engine pane.
3. Click the **Default Settings** link in the Archive Engine pane to open the Default Settings pane.

The left pane displays a tree control that you can use to get to a particular pane quickly.

Or you can:

1. Expand the **Configuration** node in the tree control in the left pane.
2. Expand the **Archive Engine** node.
3. Click the **Default Settings** node to open the Default Settings page in the center pane.

4 Configuring Credentials

When your system is installed, your HP representative configures the credentials on the Archive Gateway that give the service account access to the IAP and to the Exchange mailboxes to be archived.

In most cases, you will only need to perform the procedure in this chapter when:

- You update the HP EAs Exchange software on the Archive Gateway.
- You change the archive service account password periodically.

If you change the password, make the change in Active Directory and the Archive Gateway, then change the password with the HP EAs Exchange software as described in this chapter.

-
- ❗ **IMPORTANT:** The IAP credentials and the Exchange server credentials are two separate credentials. Both must be configured properly for the EAsE software to function.
-

Configuring the IAP credentials

The IAP credentials give the EAsE software access to the IAP.

1. Navigate to **Credentials**→**IAP Credentials**. To learn about navigating see “Navigating in the HP EAs Exchange software” (page 16).

The IAP Credentials pane appears.

2. In the Admin User box, enter the name of the IAP administrator account that is associated with the IAP domain used to archive email.

NOTE: The IAP administrator account is not the same as the Archive Gateway service account you created in “Creating the archive service account” (page 13).

3. In the Password box, enter the password for the IAP administrator account.
4. In the IP Address box, enter the IP for the HTTP portal for the IAP domain you wish to use as the default IAP domain for the EAsE software.
5. Click **Verify** to verify the IAP credentials.

If the account information was verified successfully, you will be asked if you want to apply the credentials. Click **Yes** to apply the credentials, or **No** to apply them later.

Configuring the Exchange server credentials

The Exchange server credentials give the EAsE software access to the Exchange server.

-
- ❗ **IMPORTANT:** Be sure that you have given the HPAEService account the correct access rights as described in “Creating the archive service account” (page 13).
-

1. Navigate to **Credentials**→**Exchange Credentials**. To learn about navigating see “Navigating in the HP EAs Exchange software” (page 16).

The Exchange Credentials pane appears.

2. In the Domain\Username box, enter <Windows domain>\HPAEServiceAccount.
3. In the Password box, enter the password for the archive service account.

4. Click **Verify** to verify the Exchange credentials.

During verification, the EAsE software tries to determine the Exchange server and mailbox associated with archive service account. If it cannot find one, or if you wish to use a different one, enter the address of an Exchange server and a mailbox.

If the account information was verified successfully, you will be asked if you want to apply the credentials. Click **Yes** to apply the credentials, or **No** to apply them later.

When you apply the credentials the EAsE software shuts down any running services and restarts them with the new credentials. Verification will never start a process that was not already running.

5 Configuring the Archive Engine defaults

The Archive Engine is the part of the HP EAsE software that handles Compliance Archiving, Selective Archiving, and the associated maintenance tasks. Your HP representative will set up the appropriate defaults for your installation. This chapter tells you how to examine and change the default settings

Essential concepts

This section describes some concepts that apply throughout the EAsE software.

Tombstones and Stealth Archiving

When Selective Archiving archives items to the IAP, the EAsE software can do several things with the original message on the Exchange server.

Option	Description
Stealth Archiving	The message is left untouched on the Exchange server. There is no indication to the end user that the message has been archived.
Trim Attachments	The attachments are removed from the message. The attachments remain archived on the IAP.
Trim Body	The body is removed from the message. The body remains archived on the IAP.

When a message is archived with Selective Archiving, the EAsE software marks the original message with a “tombstone” visible in the end user's exchange client that indicates that the message has been archived. If you choose to use Stealth Archiving, the EAsE software marks the message as having been archived, but does not make that information available to the end user.

If you trim attachments, the body of the message remains on the Exchange server, but the attachments are replaced with a stub that lists the names of the original attachments.

An Outlook extension transparently retrieves the archived attachments or body from the IAP so that end users can access them without additional steps. See “Working with end-user applications” (page 86) to learn more about the Outlook extension and other tools end users can use to retrieve archived content.

TNEF message format

TNEF (Transport Neutral Encapsulation Format) was created by Microsoft to capture MAPI message properties in a stream. When Outlook clients communicate with an Exchange server using MAPI, properties such as those described in this section are submitted and stored in Exchange. These properties would be lost in standard MIME/SMTP message delivery.

- If custom MAPI properties are delivered with a message, TNEF can capture them while MIME cannot. Since it is possible for sensitive data to be transmitted in custom MAPI properties that are not normally visible in Outlook, the data would be lost without TNEF capture.
- Attachments in Exchange maintain the creation time and last modified time in the attachment's MAPI properties. TNEF captures these properties while MIME does not. These properties might prove to be important during an investigation.
- If TNEF is disabled, message body content is archived either as HTML or as plain text. MIME does not support a Rich Text body format that adheres to Microsoft's Rich Text specification. A translation from Rich Text to HTML can cause some subtle changes in body layout and formatting. With TNEF enabled, body content is preserved as it was originally transmitted.

HP EAs Exchange automatically archives nonstandard messages (meetings, tasks, documents) using TNEF. Standard email messages (IPM.Note) can be archived using TNEF or MIME.

For Compliance Archiving, HP recommends that all messages are archived using TNEF to provide the most complete level of message fidelity.

Default Routing Address

This comma-separated list of addresses is added to the address list of each item to be archived. If none of the addresses correspond to a repository in the IAP, the item is archived in the catchall repository.

Addresses in this list must have IAP Admin privileges.

Access Control Lists (ACL)

In general, only users who are listed in the To, From, Cc, and Bcc fields of a message have access to the message when it is stored in the IAP. However, you can enable the ExpandACL setting for certain Selective Archiving events, the message is archived to the repositories of all users listed in the original mailbox user's Access Control List (ACL).

To avoid archiving message to repositories where they may not belong, you should enable ACL expansion only for two types of Selective Archiving events:

- Public folder events
- Archiving of shared (team) mailboxes

The ACL cannot be updated in messages that have already been archived.

You can give users access to a team's archived messages through ACL expansion or through the IAP software by granting access to a team repository. Messages to a team mailbox are archived to the individual members's IAP repositories as long as they are members of the team. In order to gain access to messages that were archived before or after they were members, they will need access to the team repository.

Navigating to the default settings

To show the Archive Engine defaults, navigate to **Configuration**→**Archive Engine**→**Default Settings**. To learn about navigating see "Navigating in the HP EAs Exchange software" (page 16).

The center pane shows the six sections of default settings. The small arrow to the right of the section name expands or collapses the section.

General Defaults

These defaults apply to many of the modules in the EAsE software.

Field	Description
Default Routing Address(es)	A list of additional addresses (corresponding to IAP repositories) to which every item will also be archived. See "Default Routing Address" (page 21).
Launch Manager Log Verbosity	Select how much detail you would like in the Launch Manager log files.

Compliance Archiving Defaults

These defaults apply to Compliance Archiving. See “Compliance Archiving with journal mailboxes” (page 24) to learn more.

Field	Description
Capture Email in TNEF	If selected, messages are stored using Transport Neutral Encapsulation Format. Otherwise, messages are stored using MIME format. See “TNEF message format” (page 20) to learn more about TNEF.
Log Verbosity	Select how much detail you would like in the Compliance Archiving log files.

Selective Archiving Defaults

These defaults apply to Selective Archiving. See “Configuring Selective Archiving” (page 39) to learn more.

Field	Description
Capture Email in TNEF	If selected, messages are stored using Transport Neutral Encapsulation Format. Otherwise, messages are stored using MIME format. See “TNEF message format” (page 20) to learn more about TNEF.
Trim Attachments	Whether to remove attachments in a user's mailbox when a message is archived. See “TNEF message format” (page 20) at the beginning of this chapter.
Trim Message Body	Whether to remove the body of the message when a message is archived. See “TNEF message format” (page 20) at the beginning of this chapter.
Stealth Archiving	Whether messages are archived without any indication to the end user. See “TNEF message format” (page 20) at the beginning of this chapter.
Log Verbosity	Select how much detail you would like in the Selective Archiving log files.

Delete Synchronization Defaults

These defaults apply to the synchronization of deleted items. See “Configuring end-user delete” (page 66).

Field	Description
Remove Folder References	Whether the item's folder location in the IAP should be removed from the individual's repository reference.
Delete Non-Tombstone Items	Whether items that are not tombstoned should be deleted from the Exchange Dumpster when encountered. This option will reclaim space in the Dumpster before the specified expiration. Check this option only if end users are used to restoring deleted emails back to their mailbox.
Log Verbosity	Select how much detail you would like in the Delete Synchronization log files.

Tombstone Maintenance Defaults

These defaults apply to Tombstone Maintenance. See “Using tombstone maintenance” (page 63).

Field	Description
Stealth Archiving	Whether messages are archived without any indication to the end user.
Log Verbosity	Select how much detail you would like in the Tombstone Maintenance log files.

Maintenance Defaults

These defaults apply to periodic maintenance tasks that the EAsE software performs. You should not need to change these values unless instructed to by an HP representative.

Field	Description
Maintenance Task runs every	Specify how often the EAsE maintenance task runs.
Retain Log Files for	Specify how long EAsE log files should be retained.
Retain DB Schedule for	Specify how much historical data should be retained in the EAsE schedule database.
Retain Queue Schedule for	Specify how much historical data should be retained in the Policy Engine queue.

6 Compliance Archiving with journal mailboxes

This chapter describes how to use HP EAs Exchange Compliance Archiving.

Overview of Compliance Archiving

HP EAs Exchange Compliance Archiving takes messages from a journal mailbox on an Exchange server and transfers them to the IAP for long term storage. Use Compliance Archiving when you need to keep a complete record of mail messages in your organization.

HP EAs Exchange Compliance Archiving captures the following Exchange items:

- Standard Email (IPM.Note)
Includes secure and encrypted email
- Non-Delivery Reports (REPORT.IPM)
- Meeting Requests (IPM.Schedule)
- Task Requests (IPM.TaskRequest)

If an item contains an attachment, it is archived as well.

NOTE: Exchange does not place calendar items (IPM.Appointment) or documents (IPM.Document) in the journal mailbox. Compliance Archiving does not archive these items.

Configuring the Exchange server for journaling

To archive data from Exchange to the IAP, you need to create a journal mailbox and configure the Exchange server to place copies of all mail in it.

Configuration for Exchange 2010

If you are using Exchange 2010, follow the instructions in this section. If you are using Exchange 2007 or earlier, go on to “Creating journal mailboxes” (page 24).

To create the journal mailboxes, see the Microsoft TechNet article *Create and Configure a Journaling Mailbox* at <http://technet.microsoft.com/en-us/library/bb124985.aspx>. Be sure that the HPAEServiceAccount is given full access rights.

Next follow the instructions in the article *Enable Per-Mailbox Database Journaling* at <http://technet.microsoft.com/en-us/library/bb123817.aspx> to enable journaling to the mailbox you created.

Because there are serious security and performance considerations when configuring journaling in any Exchange environment, Exchange administrators should thoroughly read and understand these Microsoft TechNet articles.

Creating journal mailboxes

Before you can archive messages, you need to create one or more journal mailboxes.

Since journal mailboxes potentially receive and store copies of every message that passes through an Exchange server, they present special performance and security issues. It is important, then, that you set up journal mailboxes properly. For instance, you probably do not want to put the journal mailbox on the same server that handles a large volume of mail. Please consult your Exchange documentation for best practices on setting up journal mailboxes. A good place to start is Microsoft's Exchange Server library: [http://technet.microsoft.com/en-us/library/aa996058\(EXCHG.80\).aspx](http://technet.microsoft.com/en-us/library/aa996058(EXCHG.80).aspx)

1. Check that you have set up the archive service account properly as described in “Creating the archive service account” (page 13)

2. Create one or more journal mailboxes in Active Directory.
You can choose any name you wish for a journal user account, but a descriptive name such as JournalUser will make it easier to keep track of the purpose of the account.
All journal mailbox accounts must meet the following conditions:
 - The user must be a member of Domain Users.
 - The archive service account (HPAEServiceAccount) must have access to the journal user's mailbox.

NOTE: HP strongly recommends using envelope journaling to capture full blind carbon copy (BCC) information and to expand distribution lists.

Enabling Compliance Archiving on mailbox stores

Once you've created the journal user mailboxes, set the mailbox store properties to enable Compliance Archiving.

Exchange 2007

To enable Compliance Archiving on Exchange 2007:

1. Log on to the Exchange server.
2. Open the Exchange Management Console.
3. Expand **Server Configuration**, and then click **Mailbox**.
At the bottom of the console, the Storage Groups and associated Mailbox Databases appear.
4. Right-click the relevant Mailbox Database, and select **Properties**.
5. Select the **Journal Recipient** check box.
6. Click **Browse**, select the journal user, and click **OK**.
7. Open the **Maintenance schedule** drop-down list and do one of the following:
 - Select a time range
 - Select **Use Custom Schedule** and click **Customize**. Select 1 hour or 15 Minute, select each cell in the schedule, and then click **OK**.
8. Click **OK**.
9. Repeat steps 4–8 for each relevant Storage Group on the server.

Repeat this procedure on other Exchange servers with mailbox stores used for Compliance Archiving.

Pre-2007 Exchange servers

To enable Compliance Archiving on pre-2007 Exchange servers:

1. Log on to the Exchange server.
2. Open the Exchange System Manager.
3. Open the **Servers** folder.
4. For each server listed:
 - a. Expand the server tab.
 - b. Open a Storage Group.
 - c. Right-click **Mailbox Store** and select **Properties**.
 - d. Click **General**.
 - e. Select **Archive all messages sent or received by mailboxes in this store**.
 - f. Click **Browse**.
 - g. In the Select Recipient dialog box, click **Locations**, select the domain, and click **OK** in the popup dialog box.

- h. Enter the journal user account in the **Enter the object name to select** box, and select **Check Names to validate user name**.
 - i. Click **OK** twice.
 - j. Repeat steps b–i for each relevant Storage Group on the server.
5. Repeat this procedure on other Exchange servers with mailbox stores used for Compliance Archiving.

Configuring Compliance Archiving events

Compliance Archiving events are managed completely within the EAsE software and run at a specified time interval.

After messages are archived on the IAP, they are automatically deleted from the journal mailbox.

Creating a Compliance Archiving event

A separate event must be created for each journal mailbox that is archived.

To create a new event follow these steps:

1. Navigate to **Configuration**→**Archive Engine**→**Archive Events**. To learn about navigating see “Navigating in the HP EAs Exchange software” (page 16).
2. Click **New Archive Event** from the Actions pane on the right side of the window.
3. In the dialog box that appears, select **Compliance Archiving** and click **OK** to display the Create Archive Event window.
4. Enter a descriptive name for the event in the Name box and an optional description in the Description box.
5. Click the **Configuration** tab to display the configuration pane.
6. Enter the IP address of the Exchange server in the Exchange Server box and the name of a journal mailbox in the Journal Mailbox box.

You can use the **Find** button to get a list of all the known Exchange servers with journal mailboxes.

The Default Routing Address(es) box lists addresses that are added to the address list of the message. See “Default Routing Address” (page 21).

7. If you know your Exchange server is heavily loaded, you may want to change the number of processes per event. Click the **Schedule** tab and see “Schedule tab” (page 27) for more information.
8. If your installation uses more than one IAP domain, click the **IAP Domain** tab, and select the one you wish to use from the list. To learn more about the **IAP Domain** tab see “IAP Domain tab” (page 28).
9. Click **Create** to close the window and create the event.

The newly created archive event is not enabled by default. See “Running Compliance Archiving events” (page 29) to learn about enabling archive events.

Editing Compliance Archiving events

To edit a Compliance Archiving event:

1. Navigate to **Configuration**→**Archive Engine**→**Archive Events**. To learn about navigating see “Navigating in the HP EAs Exchange software” (page 16).
2. Select the Event from the Archive Engine pane.
3. Click **Edit** from the Actions pane on the right side of the window.

If you do not see an **Edit** item in the Actions pane, make sure that you have selected only one event from the list.

4. Edit the settings you wish to change. The settings on each tab are described in the following sections.
5. Click **Save** to apply the changes.

NOTE: Modifications are not applied to events that are currently running. The changes will be applied when the process completes and is restarted. See “Running Compliance Archiving events” (page 29).

General tab

In the **General** tab, you can only edit the description of the event. You cannot change the name of an event.

Configuration tab

The **Configuration** tab lets you specify the following items:

Field	Description
Exchange Server	The IP address or the name of the Exchange server for which Compliance Archiving is configured. This server name must be resolvable by DNS.
Journal Mailbox	The journal account name specified when the journal mailbox is set up.
Default Routing Address(es)	A list of additional addresses (corresponding to IAP repositories) to which every item will also be archived. See “Default Routing Address” (page 21).
Capture Email in TNEF	If selected, messages are stored using Transport Neutral Encapsulation Format. Otherwise, messages are stored using MIME format. See “TNEF message format” (page 20) to learn more about TNEF.

Schedule tab

The **Schedule** tab lets you specify how often the archiving process runs and how many instance of the process are created when it does.

Field	Description
Frequency	Use these controls to set how often the archive event runs. The default is every two minutes.
Number of Processes	<p>This field defines number of processes for each event.</p> <p>The right number of processes depends on the load on your Exchange server:</p> <ul style="list-style-type: none"> • For lightly loaded servers, use 1 process. • For heavily loaded servers, use 5 processes. • In no case should you specify more than 7 processes. <p>The total number of processes for all archive events (including compliance archiving, selective archiving, delete synchronization, and tombstone maintenance) is limited to 24.</p>

IAP Domain tab

The **IAP Domain** tab contains information about the IAP that collects the archived messages.

Field	Description
IAP Domain Name	The name of the IAP domain to which the email from the journal mailbox should be stored. You can choose one of the known domain names from the menu. If you change this field, the following three values will change as well.
IAP Domain ID	The domain ID that matches the IAP Domain Name. The Domain ID must match exactly the domain ID attribute in <code>Domain.jcml</code> .
IAP Domain VIP (SMTP)	The IAP Virtual IP (VIP) used for SMTP delivery.
IAP HTTP Portal Address	The IAP Virtual IP (VIP) used for HTTP delivery.

CAUTION: In order to change the IAP Domain ID, IAP Domain VIP, or IAP HTTP Portal Address values, you must first select **Override Domain Information**. However, do not do so except under the direction of an HP representative.

Advanced tab

The **Advanced** tab lets you examine the values for all of the event parameters. If directed by HP support, click **Edit** to edit these values.

Copying a Compliance Archiving event

Each journal mailbox that is archived requires a separate archive event. If you are archiving messages from more than one journal mailbox, you can use the first event as the basis for other Compliance Archiving events.

To copy an event follow these steps:

1. Navigate to **Configuration**→**Archive Engine**→**Archive Events**. To learn about navigating see “Navigating in the HP EAs Exchange software” (page 16).
2. Select an event from the Archive Events pane.
and click **Copy**.
3. Click **Copy** from the Actions pane on the right side of the window.
A new window with an event named “Copy of” the original event appears.
4. Give the event a new name and make changes in the **Configuration** tab as needed.

The newly created archive event is not enabled by default. See “Running Compliance Archiving events” (page 29) to learn about enabling archive events.

Deleting a Compliance Archiving event

To delete a scheduled Compliance Archiving event:

1. Navigate to **Configuration**→**Archive Engine**→**Archive Events**. To learn about navigating see “Navigating in the HP EAs Exchange software” (page 16).
2. Select an event from the Archive Events pane and click **Remove**.
A dialog box appears asking you to confirm that you want to remove the event.
3. Click **Yes** to remove the event.
The event is removed.

Note that messages will continue to arrive in mailboxes on an active server. Check the journal inbox to ensure there are no messages waiting to be archived.

Running Compliance Archiving events

Compliance Archiving events start running as scheduled as soon as they are enabled. You can check whether an event is enabled or disabled in the State column of the Archive Events pane.

To enable or disable archiving events, select one from the Archive Events pane and click one of the following from the Actions pane on the right side of the window:

- Enable All
- Disable All
- Enable
- Disable

Enabling an archive event will cause it to start running, usually within one minute.

Disabling an event will prevent it from running at its next scheduled time after it completes. Note that disabling an event does not stop it immediately.

If you are creating or editing several events, it is best to stop the Compliance Archiving service to ensure that any running processes stop. Restart the service after making your changes.

7 Compliance Archiving with SMTP Premium Journaling

This chapter describes SMTP Premium Journaling, a form of compliance archiving that does not use journal mailboxes.

Overview of SMTP Premium Journaling

SMTP Premium Journaling takes advantage of features found in Exchange 2007 and later. Instead of the Archive Gateway pulling messages from an Exchange journaling mailbox, the Exchange server pushes the message to the Archive Gateway for processing.

Message flow

The Hub Transport component of the Exchange server controls the flow of messages in and out of Exchange. A Hub Transport Journal rule determines which of the messages passing through the server are candidates for archiving. When a message matches the rule, the message is sent from the Hub Transport to a mail contact.

The mail contact address routes the message to the Archive Gateway. On the Archive Gateway, the mail contact address is associated with an SMTP Journaling event.

The SMTP Journaling event provides a binding between the Archive Gateway and the IAP.

Multiple Archive Gateways

Before being routed to the Archive Gateway, messages pass through a load balancer. If your installation includes more than one Archive Gateway, the load balancer routes the message to the next available Archive Gateway to ensure that the traffic is distributed efficiently.

The EAsE software uses a federated configuration to keep the settings of all the Archive Gateways that are participating in SMTP journaling synchronized. When you make a change to the configuration of one Archive Gateway, the change is propagated to all the other Archive Gateways.

Archive failures

The EAsE software has several strategies for dealing with messages that cannot be archived.

For transient failures, such as a busy IAP or an IAP rebooting, EAsE retries archiving the message. In most cases, the condition that caused the failure will resolve itself. Messages that are not archived because of transient failures remain in the Exchange queue.

Non-transient failures occur rarely. They're usually due to serious hardware failures, malformed messages, or a problem with the software itself. In this case, EAsE creates an ENDR (EAsE Non Delivery Report) message that contains the original message and the conditions that caused it to fail to be processed or archived. The ENDR message is routed to the special ENDR mailbox (see "Create the ENDR mailbox" (page 34)) where it is stored until it can be resolved. Periodically, an automatic ENDR task runs to mine the ENDR mailbox to try to rearchive the failed messages to the IAP.

If the EAsE software detects many archive failures in a short time, or if the multiple messages fail consecutively, EAsE will stop processing messages from Exchange for a period time; the default is five minutes. This prevents the ENDR mailbox from becoming overrun. During this time, EAsE relies on the Exchange and Hub Transport queues to handle the break in service.

Configuring Exchange and the Archive Gateway

In order for SMTP journaling to work correctly, the Exchange server must be set up to send its traffic to an SMTP address represented by the mail contact, and the Archive Gateway must be configured to accept SMTP traffic from the Exchange server through an SMTP Journaling event.

NOTE: Your HP representative will configure both the Exchange server and the Archive Gateway when your system is installed. Unless there are changes to your system, you should not need to follow any of the steps outlined in this section.

Configuring Exchange and Archive Gateway consists of the following tasks:

- Joining the Archive Gateway to the Exchange domain and verifying its SMTP settings
This places the Archive Gateway and the Exchange server on the same network so that the Archive Gateway can receive SMTP traffic from the Exchange server.
- Creating DNS records for the Archive Gateway and verifying the Hub Transport settings
This creates DNS address and mail records so that the Hub Transport server can send SMTP mail to the Archive Gateway
- Creating the Mail Contact record
This is the journal address that receives copies of all the messages passing through the Exchange server.
- Creating the ENDR mailbox
This is the mailbox on the Exchange server that holds messages that could not be archived.
- Creating a Hub Transport Journal rule
This is the rule on the Exchange server that sets up the actual journaling.

Configuring the Archive Gateway

In order for SMTP Premium Journaling to work correctly, you need to join the Archive Gateway to the Exchange Hub Transport's domain.

Join the Archive Gateway to the Exchange domain

First specify the DNS server in the Archive Gateway's TCP/IP settings.

1. Open the Network Connections control panel.
2. Right-click the active network connection and choose **Properties**.
3. Select **Internet Protocol (TCP/IP)** from the list and click **Properties**.
4. Select **Use the following DNS server addresses** and enter the IP address of the Active Directory DNS in your Exchange environment.

Next follow this procedure to join the Archive Gateway to the Active Directory domain.

1. Open the System control panel.
2. Click the **Computer Name** tab.
3. Click **Change**.
4. In the Member of section, click **Domain** and enter the domain name of the Exchange environment.
5. Click **OK** to close the dialog.
6. You will be prompted to enter the name and password of an Administrator in the Exchange domain.
7. You will need to restart the Archive Gateway.

Configuring the Exchange server for SMTP Premium Journaling

Setting up the Exchange server for SMTP Premium Journaling requires that you:

- Create DNS records for the Archive Gateway.
- Configure the hub transport to create a remote domain entry and a send connector on the Exchange server.
- Create the mail contact record on the Exchange server.
- Create the ENDR mailbox.
- Create a hub transport journal rule.

ⓘ **IMPORTANT:** You must have one MX record, one remote domain, one send connector, and one mail contact for *each* SMTP Journal event on the Archive Gateway.

Create DNS records for the Archive Gateway

The Hub Transport Server needs appropriate DNS and MX records to be able to send SMTP mail to the Archive Gateway via the load balancer.

Create a DNS record for the Archive Gateway's EAsE VIP. The EAsE VIP is the virtual IP address on the IAP's network interface that receives SMTP traffic.

1. Choose **New Host (A)...** from the **Action** menu to create an address record for the Archive Gateway.
2. In the **Name** field give the Archive Gateway VIP a name such as **easevip**.
3. In the **IP Address** field, enter the Archive Gateway's EAsE VIP address.

You can find the EAsE VIP address by navigating to **Configuration**→**IAP** page of the HP EAsE Console.



4. Click **Add Host** to create the A record.

Next, create an MX record that points to the Archive Gateway's EAsE VIP.

1. Choose **New Mail Exchanger (MX)...** from the **Action** menu to create an MX record for the EAsE VIP.
2. In the **Host or child domain** field give the MX record a name such as **smtpjournal**.
3. In the **Fully qualified domain name (FQDN) of mail server** field, enter the name of the Archive Gateway's EAsE VIP you selected when you created the A record above.

For example, if you named the EAsE VIP **easevip** and your company's domain is **example.com**, you would enter **easevip.example.com**.

4. Click **OK** to create the MX record.

At this point you have two DNS records:

- An A record for the EAsE VIP (easevip.example.com)
- An MX record for the mail host (smtpjournal.example.com)

Configure the Hub Transport settings

Configure the Exchange Hub Transport remote domain settings. First, create a new remote domain entry.

1. Open the Exchange Management Console.
2. Navigate to **Organization Configuration**→**Hub Transport**.
3. Click the **Remote Domains** tab.
4. Select **New Remote Domain** from the Actions pane to open the New Remote Domain wizard.
5. Give the new remote domain entry a name so you can identify it later.
6. In the Domain Name box, enter the domain name you set up for the MX record in the previous section. For example smtpjournal.example.com.
7. Click **Next**, then **Finish**.
8. Double-click the newly created remote domain entry.
9. Click the **Format of original message sent as attachment to journal report** tab on Exchange 2007 or **Message Format** tab on Exchange 2010.
10. Ensure that the following items are set:
 - **Display sender's name on messages** is checked.
 - **Exchange rich-text format** is set to **Always use** if you plan on archiving messages in TNEF format. Otherwise choose **Never**.
11. Click **OK** to close the window, but do not close the Exchange Management Console.

Next, create a Send Connector.

1. Click the **Send Connectors** tab.
2. Select **New Send Connector** from the Actions pane to open the New Send Connector wizard.
3. For Exchange Server 2010, you can optionally enter a name for the send connector and specify **Custom** as the intended use.

NOTE: Back Connection host names are only required if “Unauthorized errors” occur while opening tomb stoned messages through OWA.

4. Click **Next**.
5. Click **Add** to open the SMTP Address Space window.
6. In the Address box, enter the domain name you set up for the MX record in the previous section. For example smtpjournal.example.com.
7. Click **Next**.
8. Select **Use Domain Name System (DNS) “MX” records to route mail automatically**.
9. Click **Next**.
10. For Source Server, select the appropriate Hub Transport servers that should deliver messages to be archived.
11. Click **Next**.
12. Confirm your settings by clicking **New**, then click **Finish**.

Create the Mail Contact record

Create a new Mail Contact record. This contact maps a journal transport rule on the Exchange server to an SMTP Journal event on the Archive Gateway. You must have one mail contact assigned to the domain name for the MX record you created earlier, for example user@smtpjournal.example.com. This mail contact directs messages sent from an Exchange Hub Transport to a specific SMTP journal event configured on the Archive Gateway.

To create a new Mail Contact record, follow these steps:

1. Open the Exchange Management Console.
2. Navigate to **Recipient Configuration**→**Mail Contact**.

3. Click **New Mail Contact...** in the Actions pane of the Exchange Management Console.
4. Enter a name and an alias for the mail contact.
5. Enter an SMTP address on the mail host associated with the EAsE VIP.

For the name portion, use the same name as the alias you entered in the previous step. The domain should be the full domain name of the MX record you created earlier.

For example, if the MX record you created was named `smtpjournal` and your domain is `example.com`, you would enter `name@smtpjournal.example.com`.

Create the ENDR mailbox

Create the ENDR (EAsE Non-Delivery Report) mailbox on the Exchange server. Messages that cannot be archived are placed in this mailbox.

1. Open the Exchange Management Console.
2. Navigate to **Recipient Configuration**→**Mailbox**.
3. Click **New Mailbox...** in the Actions pane of the Exchange Management Console.
4. When the New Mailbox wizard opens, choose **User Mailbox** and click **Next**.
5. Select **User mailbox** and click **Next**.
6. Select **New user** and click **Next**.
7. In the User Information pane, enter at least a last name, a password, and a unique alias, then click **Next**.

You will use this alias to the ENDR mailbox when you configure the SMTP Journal event.

8. In the Mailbox Settings pane, select the information store and server where the mailbox will reside.
9. Click **OK** then **Next** to review the settings.
10. Click **New** to create the ENDR mailbox.

Create a new Hub Transport Journal Rule

Create a new Hub Transport Journal rule.

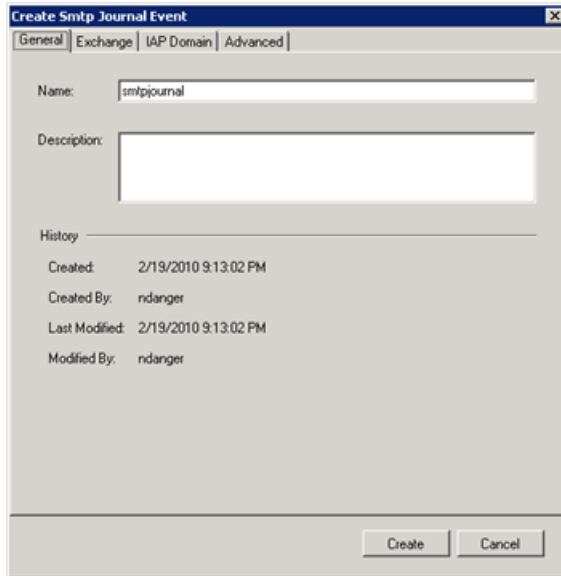
1. Open the Exchange Management Console.
2. Navigate to **Organization Configuration**→**Hub Transport**.
3. Click **New Journal Rule...** in the Actions pane of the Exchange Management Console.
4. Give the rule a descriptive name.
5. Use the **Browse** button in the **Send Journal reports to e-mail address** to select the mail contact you created earlier.
6. In the **Scope** section, select **Global — all messages** to archive all messages. If you need to do more refined filtering, you can adjust it here.
7. Click **OK** to create the rule.

Creating an SMTP Journal event

To create an SMTP Journaling event, follow these steps:

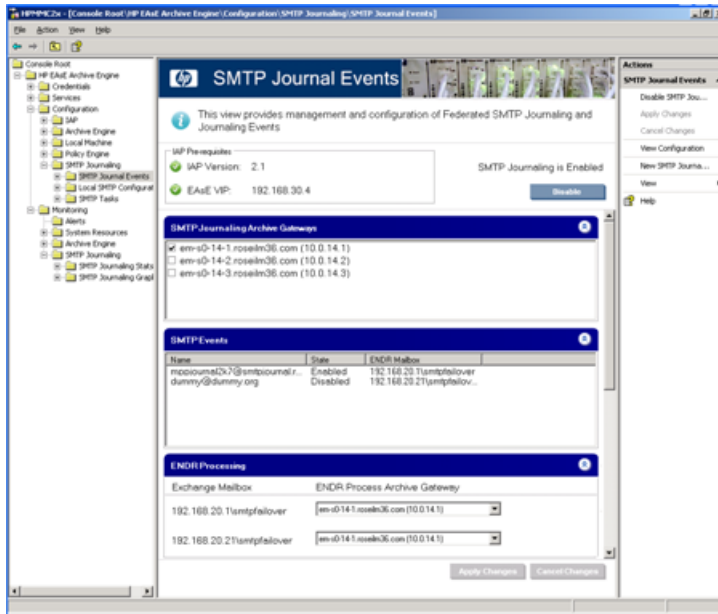
1. Log on to the Archive Gateway using the archive service account and launch the HP EAsE software (see “Launching EAsE software” (page 16)).
2. Navigate to **Configuration**→**SMTP Journaling**→**SMTP Journal Events**. To learn about navigating see “Navigating in the HP EAs Exchange software” (page 16).

3. Click **New SMTP Journaling Event** from the Actions pane on the right side of the window. An SMTP Journal Event window appears.



4. In the **General** tab, give the rule a name.
The mail contact is a good choice because it indicates the link between the hub transport rule and the journal event.
5. In the **Exchange** tab, click **Select Rule** and find the Hub Transport Rule you created earlier.
6. Click **New ENDR Mailbox**.
7. In the Specify ENDR Mailbox window that opens:
 - a. In the Exchange Server box, enter the IP address or the name of the Exchange server where the ENDR mailbox is located.
 - b. In the Mailbox box, enter the alias of the ENDR mailbox.
 - c. Click **Verify**.
 - d. Click **OK** to close the Specify ENDR Mailbox window.
8. The Default Recipients box should already have the address that you specified in "General Defaults" (page 21). You can enter a different address.
9. The **IAP** tab should be filled with appropriate values. Do not change them or the **Advanced** tab unless directed by an HP representative.
10. Click **Create** to create the event.

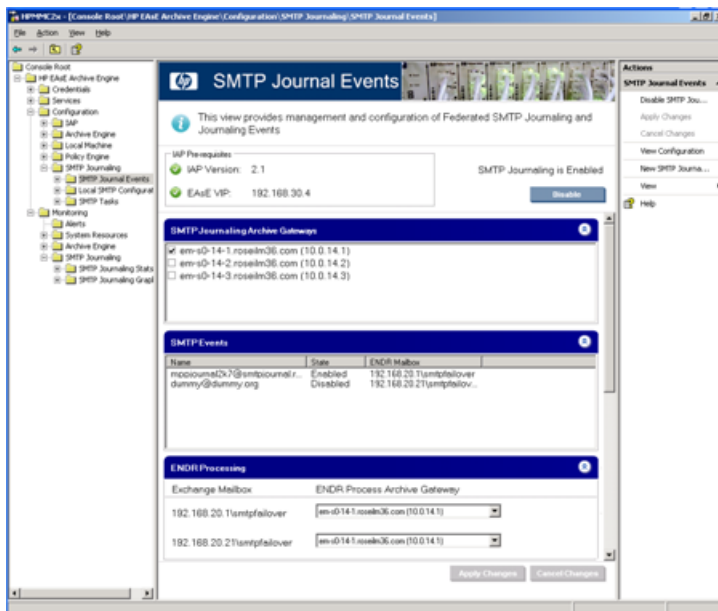
The new event appears in the SMTP Events box. Click **Apply Changes**. The changes will be propagated to all of the other Archive Gateways in your system within a short time.



Make sure that SMTP Journaling is enabled. You will see “SMTP Journaling is Enabled” if SMTP Journaling is running. If it is not, click **Enable**. At this point, SMTP Premium Journaling is running and ready to process message. You can monitor SMTP Premium Journaling by expanding **Monitoring** in the tree control on the left side of the Archive Engine console and clicking **SMTP Journaling**.

Working with SMTP Journaling events

Use the SMTP Journal Events pane to manage SMTP Journaling. To display the SMTP Journal Events pan, navigate to **Configuration**→**SMTP Journaling**→**SMTP Journal Events**.



Enabling and disabling SMTP journaling

You can enable or disable SMTP journaling altogether by clicking the **Enable/Disable** at the top of the pane.

The SMTP Journaling Gateways section shows all the Archive Gateways that can accept SMTP journal messages from the Exchange server. You can enable or disable SMTP journaling for an individual Archive Gateway by checking or unchecking the next to its name.

Enabling and disabling SMTP Journaling events

The SMTP Journaling events you create appear in the SMTP Events section. When you select an event, new commands appear in the Action pane that let you enable, disable, edit or delete SMTP Events.

NOTE: If you disable or delete an SMTP Journaling event, any corresponding Hub Transport journal rule will continue to run. The Exchange server will continue to send journaling requests to the Archive Gateway, but they will not be handled.

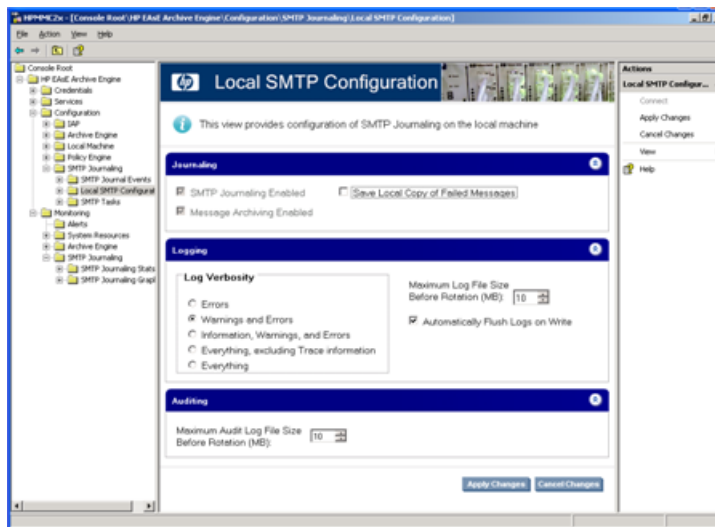
Specifying ENDR processing

As described in “Archive failures” (page 30), messages that cannot be archived are moved to an ENDR mailbox on the Exchange server. A periodic task on the Archive Gateway mines this ENDR mailbox to try to rearchive any messages that might be there.

The ENDR Processing section lets you choose which Archive Gateway runs the periodic task for each of the ENDR mailboxes you specified when you create the SMTP Journaling events.

Working with the Local SMTP configuration

As described in “Multiple Archive Gateways” (page 30), most of the SMTP Journaling settings are propagated to other Archive Gateways. The Local SMTP Configuration pane lets you work with settings for the Archive Gateway that you are logged in to. To display the Local SMTP Configuration pane, navigate to **Configuration**→**SMTP Journaling**→**Local SMTP Configuration**.

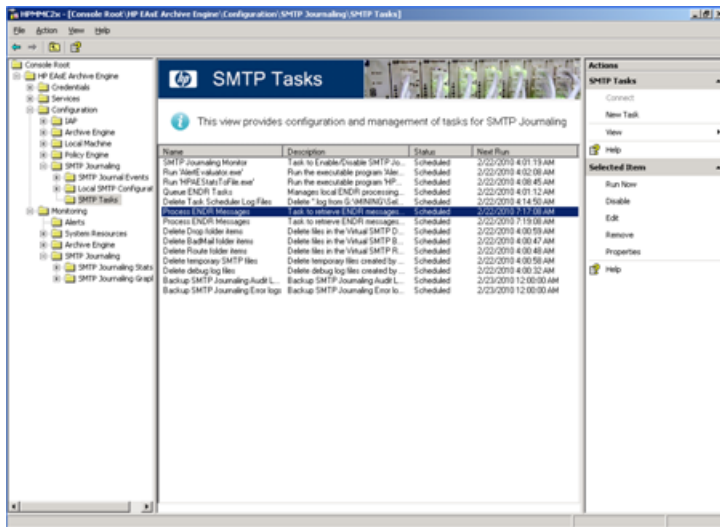


This pane shows whether SMTP journaling is enabled and whether this Archive Gateway is participating in SMTP journaling. You can also change the log file preference in this pane.

The **Save Local Copy of Failed Messages** option is sometimes useful when trying to resolve problems with SMTP journaling. Do not check this option except under the direction of an HP representative.

Examining SMTP Tasks

SMTP Journaling employs several tasks to do its job. For example, the process that periodically mines the ENDR mailbox is one of these tasks. To see these tasks, navigate to **Configuration**→**SMTP Journaling**→**SMTP Tasks**.



These tasks are added automatically by the EAsE software. You should not need to make any changes to items in this pane except under the direction of an HP representative.

8 Configuring Selective Archiving

Selective Archiving lets you specify which messages are archived to the IAP. You can select messages from specific mailboxes, messages of a particular type, or messages that meet specific criteria. When a message is archived, Selective Archiving can replace either the entire message or any attachments with a tombstone. A tombstone is a link from the item in the user's mailbox to the archived item stored in the IAP. Tombstones help reduce the amount of disk space that a user's mailbox takes up on the Exchange server.

Overview of Selective Archiving

While Compliance Archiving archives everything that passes through an Exchange journal mailbox, Selective Archiving gives you more fine-grained control over what gets archived. You can archive specific kinds of messages and specific sets of mailboxes.

As with Compliance Archiving, you use the Archive Engine to create a Selective Archiving task that specifies the kind of Exchange items you want to archive. Next, you use the Policy Engine to create a rule that specifies the mailboxes that the task applies to. The Policy Engine also lets you refine the archiving rule to apply to messages with specific attributes such as content, age, number of attachments, and so on.

The Selective Archiving task archives items from the selected mailboxes to the IAP. You can choose what happens to the original message on the Exchange server:

- You can leave it as is on the Exchange server. This is known as “stealth archiving” because there is no indication that the item has been archived.
- You can trim the attachments off an item, leaving the body on the Exchange server. EAsE replaces the attachments with a stub that lists the original attachments.
- You can trim the body from the item.

Whenever EAsE trims either the body or the attachments from a message, it leaves behind a mark, called a “tombstone,” that indicates where the trimmed portions are located on the IAP.

An Outlook extension lets users seamlessly access the original message and attachments from tombstoned items. Users can also use IAP's Web interface to access archived items.

In addition to Compliance Archiving and Selective Archiving, the Archive Engine lets you create two maintenance tasks, Deletion Synchronization and Tombstone Maintenance. Deletion Synchronization scans the Exchange server for deleted archived (tombstoned) items and deletes the corresponding item in the IAP repository. Note that if the Deletion Synchronization task runs after a deleted message is no longer in the Exchange server, it will not be deleted from the IAP. In some cases the archived item will remain in the IAP repository if regulatory policies require it. Tombstone Maintenance is a housekeeping task that scans previously archived items on the Exchange and checks that they are properly synchronized with the archived items on the IAP.

Selective Archiving captures the following Exchange items and attachments to the items:

- Standard Email (IPM.Note)
Includes secure and encrypted email
- Calendar items (IPM.Appointment)
- Tasks (IPM.Task)
- Documents (IPM.Document)
- Public Folder Items (IPM.Post)

There are some limitations:

- Only calendar items that occurred in the past and have no future occurrences can be archived.
- Only completed tasks can be archived.

Configuring the Policy Engine

When the EAs Exchange environment is configured, your HP service representative sets up the Policy Engine so that it can access all of the mailboxes and public folders that can be selectively archived. At the same time, your service representative sets up Auto Search to keep the list current. When the Selective Archiving rules are created, the mailboxes or folders that are covered by a particular rule are selected from this list.

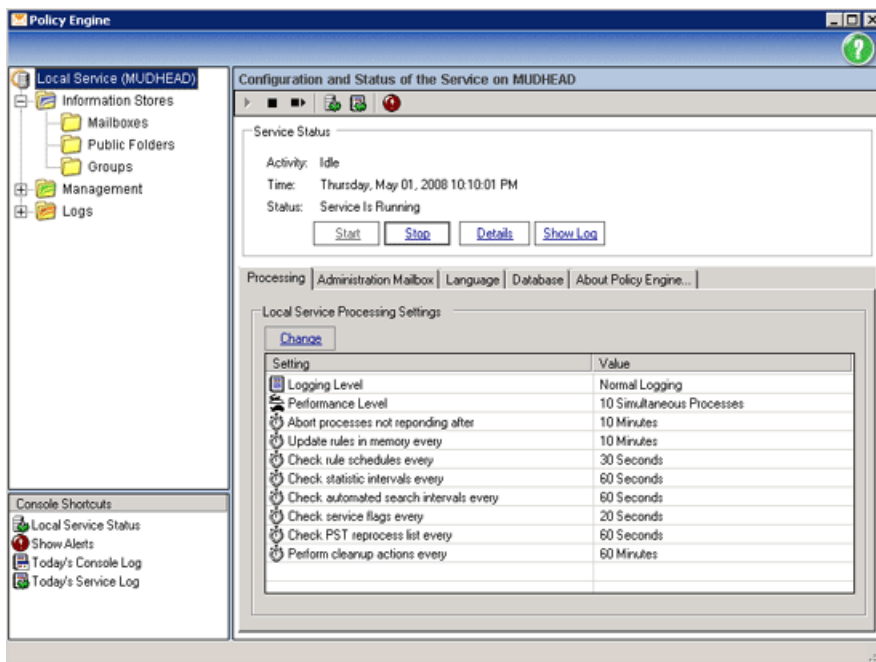
After the initial setup, you can add a mailbox immediately (and not wait for the Auto Search update) by following the steps in “Adding mailboxes” (page 42). You can also make changes to the Auto Search configuration.

- ❗ **IMPORTANT:** All journal mailboxes and SMTP and System Attendant information stores must be excluded from Selective Archiving processing.

Setting CAS server and Administration Mailbox

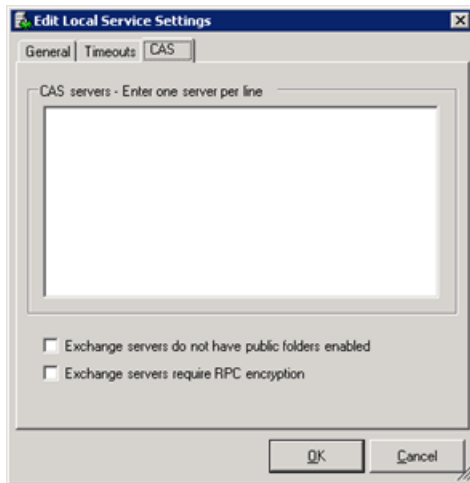
Follow these steps to set the CAS servers and to see the local service settings of the Policy Engine, click the Local Service item in the left pane.

1. Log on to the Archive Gateway using the HPAEServiceAccount and launch the HP EAsE software (see “Launching EAsE software” (page 16).
2. Navigate to **Configuration**→**Policy Engine**.
3. Click **Launch** to launch the Policy Engine administration application.
4. In the left pane, click the Local Service item.



5. Click the **Processing** tab.
6. Click **Change**.

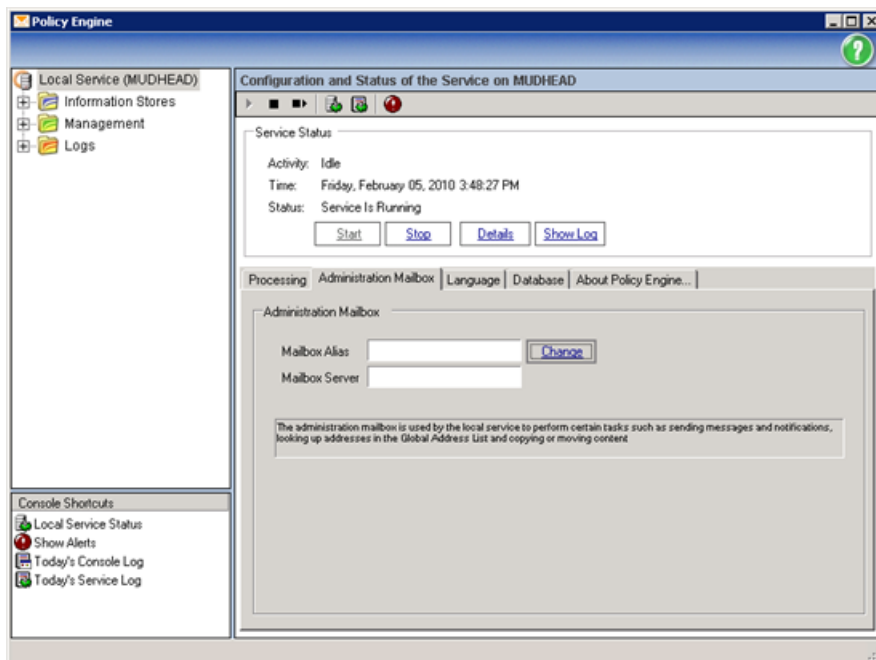
7. If you are running Exchange 2010 or later, you must specify the CAS server. If you do not, you will not be able to specify the mailboxes. Click the **CAS** tab, and enter the addresses of your CAS servers.



8. You can change the logging level and service time-out settings by clicking **Timeouts** and **General** tabs. Click **OK** to close the Local Service Settings window.

CAUTION: Consult HP technical support before changing the number of simultaneous processes.

9. Click **OK** to close the Edit Local Service Settings window.
10. Click the **Administration Mailbox** tab to create an Outlook profile. The administration mailbox is used by the local Policy Engine service to perform tasks such as sending messages and notifications, looking up addresses in the GAL, and copying or moving content.

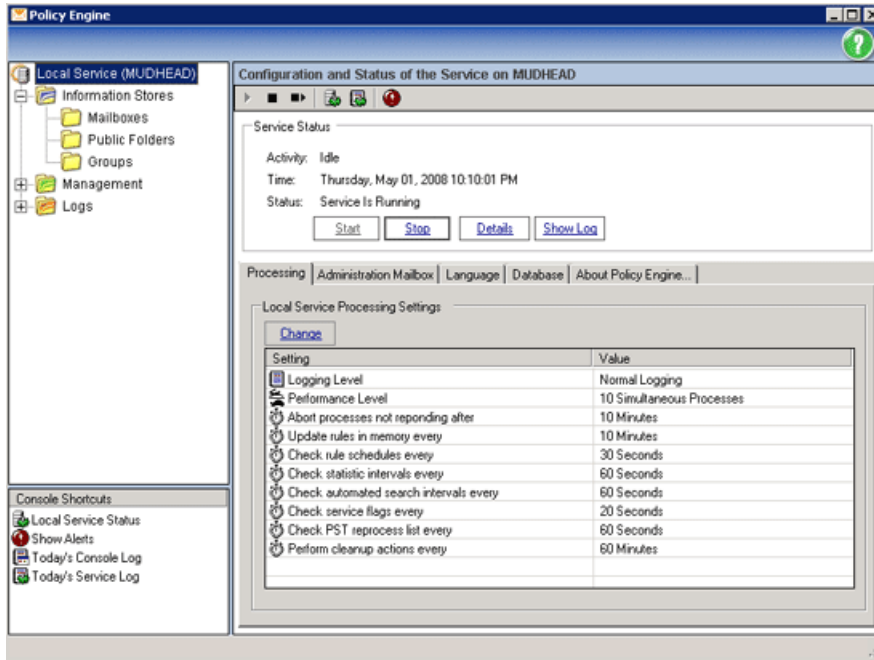


11. Click **Change** and enter a mailbox and an Exchange server.
12. Click **OK** to close the Choose a Mailbox window.
13. Leave the Policy Engine open, and continue to the next section.

Adding mailboxes

The mailboxes containing the messages to be archived are added using HP EAs Exchange Policy Engine.

1. In the left pane, expand the Information Stores folder.



2. In the left pane, select **Mailboxes**.
3. Right-click in the right pane and select **Add Mailboxes > From an Exchange Server > Browse Network**.
4. From the window that appears, select the appropriate Exchange Server, and click **OK** to continue.
5. Choose an Outlook profile that can access the Global Address List (GAL), and click **OK**.
Based on the previous selections, known mailboxes populate the right pane.

NOTE: If you are adding many mailboxes (several thousand), you may see an error that indicates that too many items were selected. In this case, select a smaller number of mailboxes, and add them several passes.

Adding public folders

If you plan to archive public folders, be sure that you have configured the Exchange server to do so as described in “Configuring the Exchange Server for Public Folder archiving” (page 15).

1. In the left pane, expand the Information Stores folder if it is not expanded already.
2. In the left pane, select **Public Folders**.
3. Right-click in the right pane and select **Add Public Folders > From the Global Address List**.
4. Select an Outlook profile that can access the Global Address List (GAL), and click **OK**.
5. In the window that appears, select the service account mailbox (HPAEServiceAccount) as the mailbox to access the public folders, and then click **OK**.

Known public folders populate the right pane of the Policy Engine window.

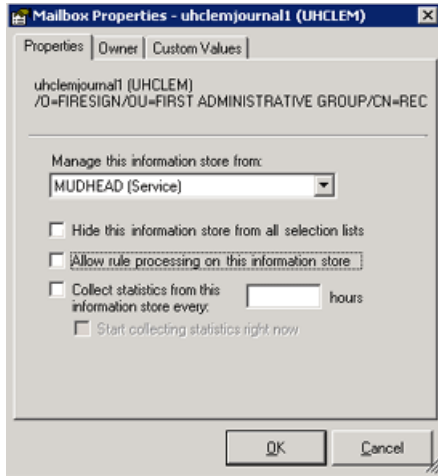
Excluding system mailboxes

Certain mailboxes should not be archived. In particular journal mailboxes and the System Attendant and SMTP information stores should be excluded from the list of mailboxes that can be selectively archived.

1. Verify that **Mailboxes** is selected in the left pane.
2. Click the settings view button to change to the Settings View.



3. Locate and double-click the journal mailbox to display the Properties window.
4. In the Properties window, verify that all check boxes are unselected.



NOTE: If you select the **Hide this information from all selection lists** option, this mailbox will never appear in any selection lists.

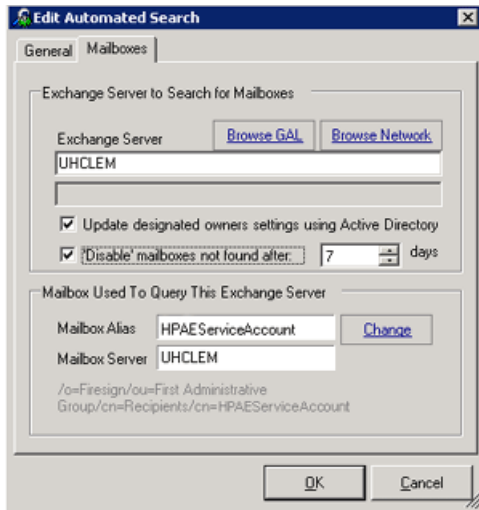
5. Click **OK** when finished.
6. Repeat these steps for any other journal mailboxes and for the SMTP and System Attendant information stores.

Setting up Auto-Search

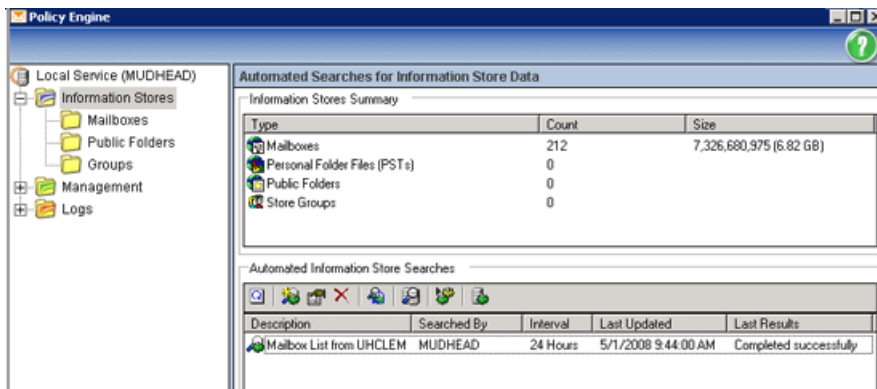
Auto-Search sets up a process that scans the Information Stores for new mailboxes and adds them automatically.

1. In the left pane of the Policy Engine, select the **Information Stores** folder.
2. The bottom of the right pane displays the Automated Information Store Searches window. Right-click in this pane and select **New Auto-Search**.
The Edit Automated Search window appears.
3. In the Automated Search Type box:
 - Ensure **Search Exchange for Mailboxes** is selected.
 - The **Search should be performed by** field is populated automatically with the name of the local machine.
 - Select the time interval for performing the search.
The default interval is 24 hours. HP recommends that this interval is never less than 24 hours.
4. Click the **Mailboxes** tab, click **Browse Network**, and then select the Exchange Server.

5. Select HPAEServiceAccount as the mailbox used to query the Exchange server. See “Creating the archive service account” (page 13) for information on this account.
6. Click **Change**, complete the Mailbox Alias and Mailbox Exchange Server boxes, then click **OK**.



7. Click **OK** to complete the setup process and add the search. The search now appears in the Automated Information Store Searches window.
8. Repeat steps 2–6 for all servers that contain mailboxes to be archived. To view the status of the automated search, select **Information Stores**. The information appears in the right pane of the window.



Creating Selective Archiving events

This section describes how to create Selective Archiving events. To learn how to edit, copy, and delete Selective Archiving events, see “Working with Selective Archiving events” (page 57).

In general, you should create archiving events for specific classes of mailboxes. For example, you may have a Selective Archiving event for archiving individual mailboxes, another one for a set of public folders, and yet another for archiving team (shared) mailboxes.

To create a new Selective Archiving event follow these steps:

1. Navigate to **Configuration**→**Archive Engine**→**Archive Events**. To learn about navigating see “Navigating in the HP EAs Exchange software” (page 16).
2. Click **New Archive Event** from the Actions pane on the right side of the window.
3. In the dialog box that appears, select **Selective Archiving** and click **OK** to display the Create Archive Event window.

4. Enter a descriptive name for the event in the Name box and an optional description in the Description box.

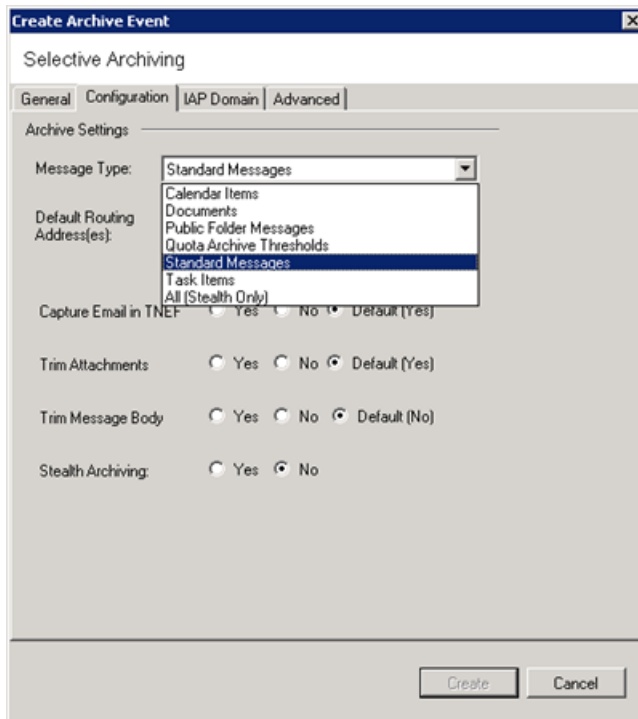
The name should not contain any special characters.

5. Click the **Configuration** tab to display the configuration pane.
6. Select the type of message from the **Message Type** drop-down list:

- Calendar items
- Documents
- Public Folder messages
- Quota archive thresholds.

The quota event and its corresponding Policy Engine rule mine information stores to ensure that their size stays under a particular threshold.

- Standard messages
Includes secure and encrypted email.
- Task Items
- All Items (available only with stealth archiving)



7. Select how you want the selective archiving event to handle the archived messages. In most cases, the default is the best choice.

To learn more about Selective Archiving defaults see “Selective Archiving Defaults” (page 22)

Field	Description
Capture Email with TNEF	If selected, messages are stored using Transport Neutral Encapsulation Format. Otherwise, messages are stored using MIME format. See “TNEF message format” (page 20) to learn more about TNEF.
Trim Attachments	Selecting Yes removes attachments when messages are archived, replaces the attachments with a proxy file, and marks the message with a tombstone. See “Tombstones and Stealth Archiving” (page 20) to learn more about tombstones In Outlook the proxy appears under its filename, <code>ArchiveInfo.htm</code> . In OWA the proxy appears under its display name, <code>Attachment Info.htm</code> .
Trim Message Body	Selecting Yes removes the message body and marks the message with a tombstone. See “Tombstones and Stealth Archiving” (page 20) to learn more about tombstones.
Stealth Archiving	Selecting Yes leaves the message on the server with no indication that it was archived. If you select Stealth Archiving, Trim Attachments and Trim Message Body are disabled.

8. If the Message Type you chose is Public Folder messages, or if the event archives team mailboxes, you must enable ACL expansion. To learn more about Access Control Lists, see “Access Control Lists (ACL)” (page 21). Follow these steps to enable ACL expansion for a Public Folders event:

- a. Click the **Advanced** tab to display the advanced settings for the event.
- b. Click **Edit** to enable editing of the settings.
- c. Add the following statements:


```
[ExchSelectiveArchiving]
ExpandACL=True
```
- d. Click **Update**.

9. Click **Create** to close the window and create the event.

A window appears that announces that a Policy Engine rule with the same name as the Selective Archiving event has been created.

10. Click **Launch Policy Engine Admin** to launch the policy engine and continue with step 3 of the next section, “Configuring Policy Engine rules” (page 46) to configure the archiving rule.

Configuring Policy Engine rules

When you create a Selective Archiving event, the software creates a corresponding rule with the same name in the Policy Engine. You can use the Policy Engine to refine a rule.

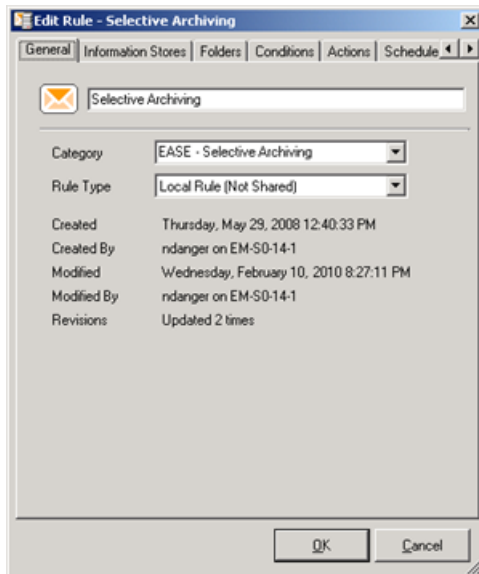
- ⓘ **IMPORTANT:** You can make changes to a rule, but do not delete any items that were configured when the rule was created. Doing so will cause the Selective Archiving event to perform unpredictably.

To edit the Policy Engine rule associated with a Selective Archiving Event:

1. Navigate to **Configuration**→**Policy Engine**. To learn about navigating see `s_Navigating_in_the_HP_EAs_Exchange_software_200912021603`.
2. Click **Launch** to launch the Policy Engine administration application.

3. In the left pane of the Policy Engine Window, expand the Management folder, and then select **Rules**.
4. In the right pane, double-click the rule that corresponds to the Selective Archiving event to be modified.

The Edit Rule window appears with the **General** tab selected. Do not change any of the items in this tab.



5. Modify the settings in the other tabs as necessary:
 - Information Stores tab
 - Folders tab
 - “Conditions tab” (page 54)
 - “Actions tab” (page 55)
 - “Schedule tab” (page 56)
6. Click **OK** to save the modifications to the Policy Engine rule.

Information Stores tab

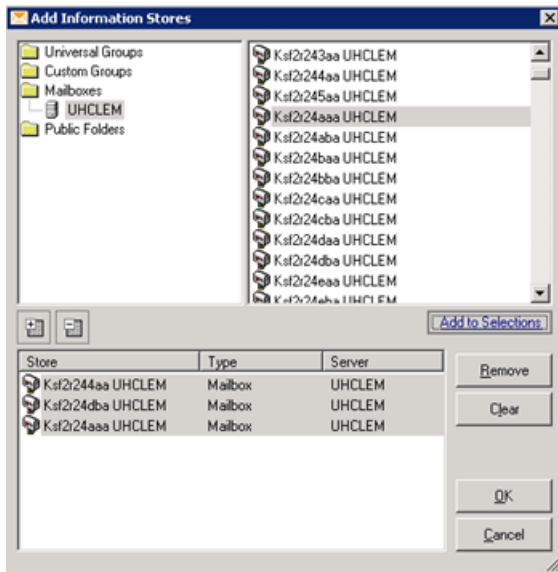
At least one information store must be associated with a rule.

To add information stores:

1. In the Information Stores tab, click **Add** to add the information stores to be processed by the rule.
The Add Information Stores window appears.
2. If the event archives messages, click **Mailboxes** to process either specific mailboxes or all mailboxes or on the Exchange server. The list of mailboxes that appears here is the same one that you specified when you configured the Policy Engine. See “Adding mailboxes” (page 42).

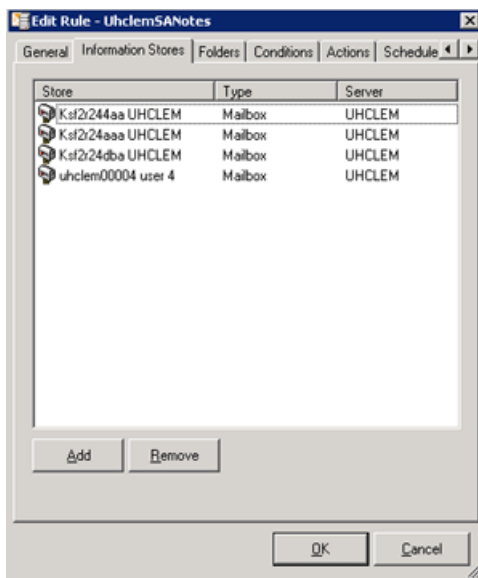
If the event archives public folders, click **Public Folders** to process particular public folders. The list that appears here is the same one that you specified when you configured the public folders in “Adding public folders” (page 42)

3. After making a selection, click **Add to Selections**.



① **IMPORTANT:** All journal mailboxes and SMTP and System Attendant information stores must be excluded from Selective Archiving processing. See “Adding mailboxes” (page 42) to learn more about adding mailboxes.

4. Click **OK** when you have finished adding mailboxes or public folders. The mailboxes are added to the Information Stores tab.



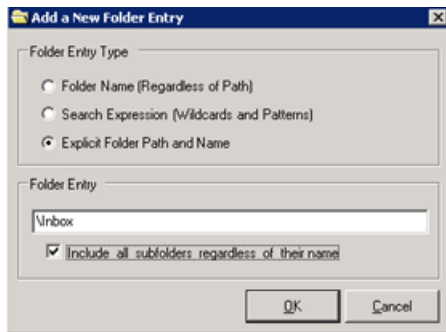
Folders tab

Use the Folders tab to select the Outlook folders to which a rule applies. You can choose to archive:

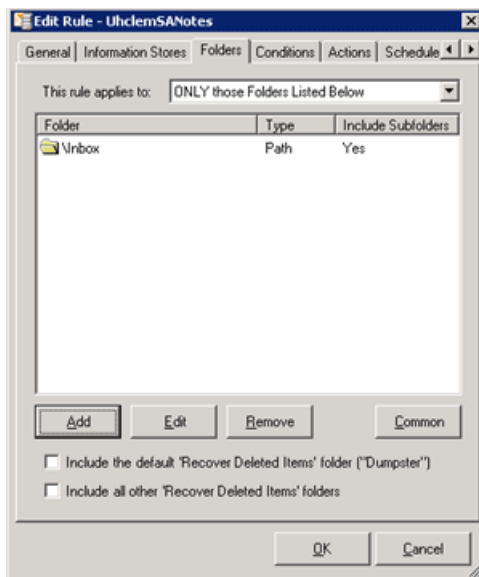
- Items in all folders
- Items in specifically listed folders
- Items in all folders except those specifically listed

For example, to archive only items in users' Inbox folders:

1. Select **ONLY those Folders Listed Below** in the **This rule applies to** drop-down list.
2. Click **Add** to open the New Folder Entry window.
3. Select **Explicit Folder Path and Name**, and then enter `\Inbox` in the Folder Entry box.



4. Select the **Include all subfolders...** check box.
 5. Click **OK**.
- The `\Inbox` folder is now listed on the Folders tab.



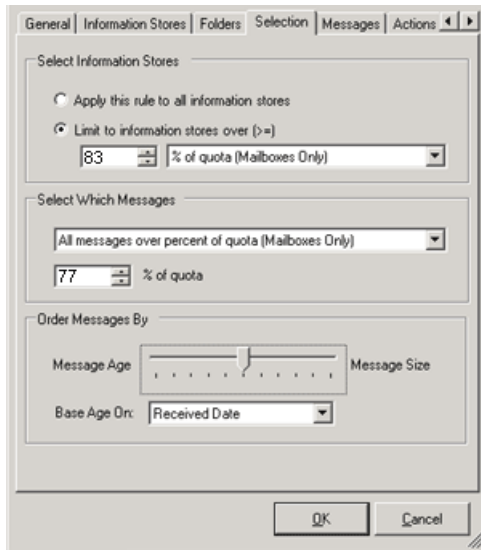
ⓘ **IMPORTANT:** Do not check the boxes giving you the option to include folders containing deleted messages.

For a Policy Engine rule that corresponds to a Public Folder archiving event, select **All Folders**.

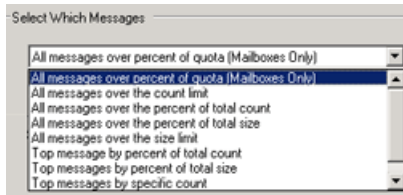
Selection tab

NOTE: The Selection tab is only available for Quota Archive Threshold events.

Use this tab to define the quota threshold and to determine how messages are processed to reduce mailbox size.



1. Determine which information stores are considered for processing.
 - All information stores (mailboxes and public folders).
 - Information stores at or above a certain size limit:
 - Static size: Process mailboxes and public folders that equal or exceed a certain size. If you choose this option, set the size in megabytes.
 - Percentage of quota: Process mailboxes that equal or exceed a certain percentage, or threshold, of the storage limit set in Active Directory. If you choose this option, define the threshold percentage, up to 99%.
If more than one quota setting is defined for a mailbox in Active Directory, the following order is used to determine the threshold: Issue Warning, Prohibit Send, Prohibit Send and Receive.
2. Determine how the messages in the information stores are selected for processing.
Step 1 established the size of the mailboxes that are considered for processing. This step defines the way the data is selected and the amount of data that is processed.



Item	Description
All messages over percent of quota (Mailboxes Only)	<p>Select this option if you chose Limit to information stores over x% of quota (Mailboxes Only) in step 1. Then enter the percentage to which a mailbox should be archived.</p> <p>This is the most typical choice when applying the quota threshold rule.</p> <p>The upper limit (the threshold) is defined in step 1, and the lower limit is defined in this step. The rule identifies the top candidates for archiving between the two percentages. The mailbox messages are weighted and ordered in step 3, then processed until the size of the mailbox is reduced to approximately the limit specified in this field.</p> <p>Tip: Set the high and low quota percentages within an acceptable range of where you want your ideal quota limit to be. The amount of data that is removed from the mailbox in each pass will vary, but will stay within the range you define.</p> <p>For example, if you want the archived mailbox size to be around 80% of the quota, set the threshold at 83% and this lower limit to 77%. Over time, the limit might be as high as 82% but will probably not drop under 77%. On average it should hover in the 80% range.</p>
All messages over the count limit	<p>Determine the maximum number of messages to remain in a mailbox, then enter the number of message items.</p> <p>For example, if you select 100 messages, the messages in a mailbox are ordered in step 3, then processed until the number of messages in the mailbox is reduced to 100.</p>
All messages over the percent of total count	<p>Determine the percentage of messages to remain in the mailbox, then enter the percentage. Base the percentage on the total number of items in the mailbox.</p> <p>For example, if there are 200 messages in a mailbox and you select 70%, the messages are ordered in step 3, then processed until the number of messages in the mailbox is reduced to 70% of the former count, or 140 items.</p>
All messages over the percent of total size	<p>Determine the percentage of messages to remain in the mailbox, then enter the percentage. Base the percentage on the total size of the mailbox.</p> <p>For example, if the mailbox is 100 MB and you select 60%, the messages are ordered in step 3, then processed until the mailbox is reduced to approximately 60% of its former size, or 60 MB.</p>
All messages over the size limit	<p>Process messages when the mailbox exceeds a certain size. Enter the size in megabytes.</p> <p>For example, if the mailbox limit is 60 MB, the messages are ordered in step 3, then processed until the mailbox size is reduced to approximately 60 MB.</p>
Top messages by percent of total count	<p>Determine the percentage of messages to be removed from the mailbox, then enter the percentage. Base the percentage on the total number of items in the mailbox.</p> <p>For example, if there are 200 messages in a mailbox and you select 30%, the messages are ordered in step 3, then processed until the number of messages in the mailbox is reduced by approximately 30%, or 60 items.</p>

Item	Description
Top messages by percent of total size	Determine the percentage of messages to be removed from the mailbox, then enter the percentage. Base the percentage on the total size of the mailbox. For example, if the mailbox is 100 MB and you select 40%, the messages are ordered in step 3, then processed until the mailbox is reduced by approximately 40%, or 40 MB.
Top messages by specific count	Remove a specific number of messages from the mailbox. For example, if you select 50 items, the messages are ordered in step 3, then processed until 50 items are selected and removed from the mailbox.
Top messages by specific size	Remove x MB of messages from the mailbox. For example, if you select 20 MB, the messages are ordered in step 3, then processed until approximately 20 MB of messages are selected and removed from the mailbox.

3. Weight messages according to age or size to establish the order for processing.

The items that can be weighted and processed in a mailbox are defined in the Messages tab and the Folders tab.

Use the scale to calculate the weight given to message age and size.

- For message age to be the only factor in setting the weight, move the slider control all the way to the left. (100% message age.)



- For message size to be the only factor, move the slider all the way to the right. (100% message size.)



- Set the slider in the middle to give equal importance to both age and size. (50% age/50% size.)



- Use the points between Message Age and Message Size to alter the importance of age or size by 10%. For example:

80% age/20% size



60% size/40% age



- Determine how to calculate the age of the message age: by the date it was received by Exchange or by the date it was last modified.

If you set the scale to a 100% message size in step 3, you do not need to configure this option.

After the message weights are calculated, the processing list is sorted and the mailbox is mined according to the criteria in steps 1 and 2.

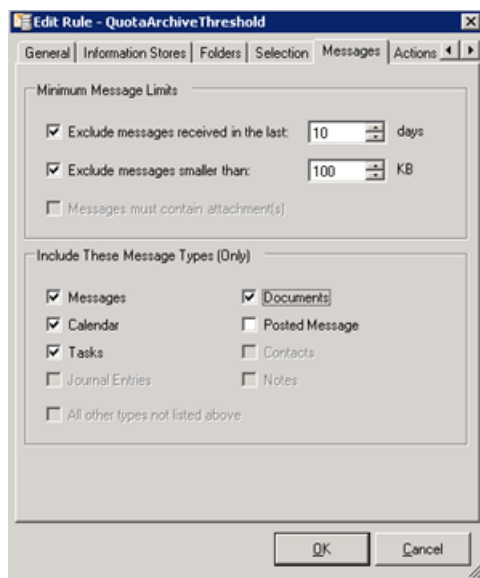
- ❗ **IMPORTANT:** Mailboxes might not be archived to quota if the criteria in the Messages and Folders tabs excludes too many items from processing.

In fact, it is possible to exclude so many items that mining will not take place at all. For example, if you are archiving to a percentage of the quota, it is possible that the upper limit might not be reached and mining will not occur.

Messages tab

NOTE: This tab is only available for Quota Archive Threshold events.

The Messages tab determines which messages are included or excluded from processing in the Selection tab. These messages must reside in the folders defined in the Folders tab.



- Set any minimum message limits.

You can exclude messages that meet one or both of these qualifications:

- Messages received in the last X number of days.
Select or enter a value from 0–365.
If you enter 0 or do not select this option every message is processed, regardless of when it was received.
- Messages smaller than X KB.
Select or enter a value from 0–9999.
If you enter 0 or do not select this option every message is processed, regardless of its size.

2. Select the check box for each message type to be included in the processing.

You must select at least one of the following message types:

- Messages
- Calendar entries
- Tasks
- Documents
- Posted message (in public folder)

Conditions tab

NOTE: This tab is not available for Quota Archive Threshold events.

When a rule is created, the applicable message class is automatically added to the Conditions tab. For example, if an event is created with a message class of IPM.Note (standard messages), that message class is added to the Conditions tab in the corresponding rule.

Adding conditions to an existing list

NOTE: You can add new conditions, but do not delete the conditions that have been preset for a rule.

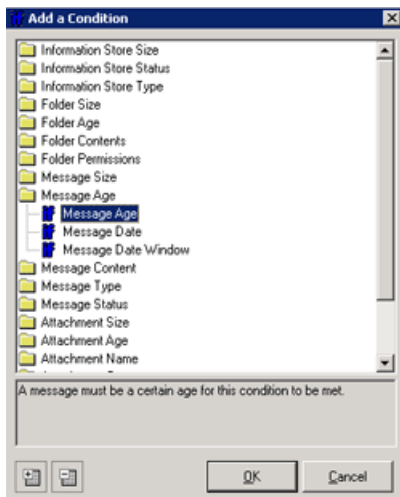
Add new conditions to a Condition List by following these steps:

1. Click **Add**.

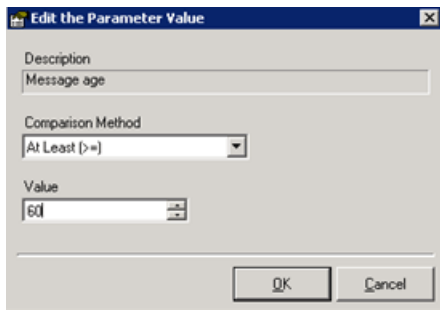
A window containing a list of all the possible conditions appears.

2. Select the condition, and then click **OK**.

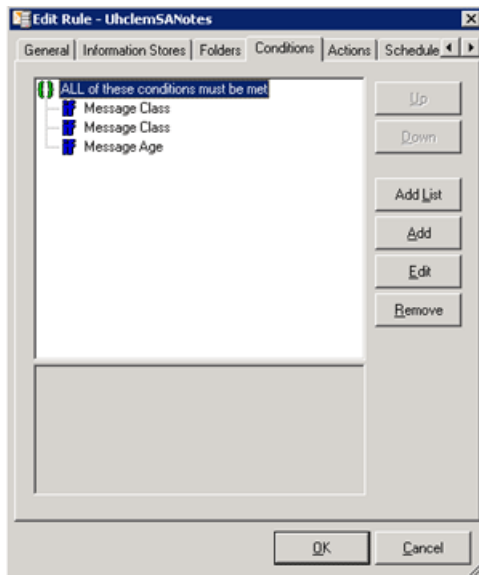
For example, to add the condition to archive messages more than 60 days old, select **Message Age** in the Message Age folder.



3. In the Edit the Condition window that appears, edit any values that you want to change:
 - a. Select the relevant parameter and click **Edit Value**.
For example, to change the Message Age from the default of 90 days to a value of 60 days, select the **Message age** parameter.
 - b. Change the value In the Edit the Parameter window, and then click **OK**.



4. In the Edit the Condition window, click **OK** to add the condition.
The condition now appears in the Condition List.



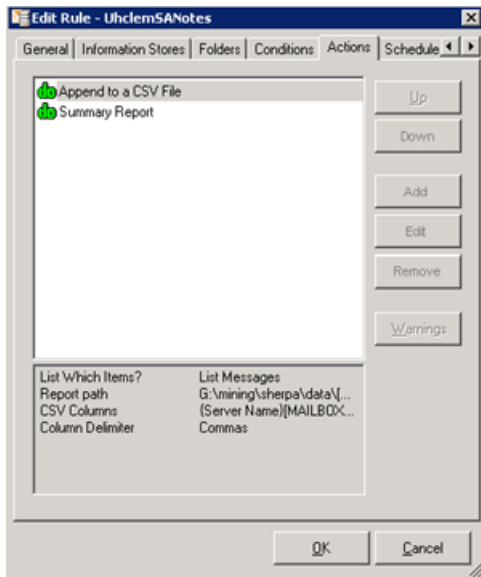
For a Policy Engine rule that corresponds to a Public Folder archiving event, set the **Message age** to 1 minute.

Determining how conditions are applied

By default, all of the conditions must be met for the rule to match. If you want to change how the conditions are applied, refer to the Policy Engine's Help. You can find this information under **Mail Attender**→**Mail Attender Rule Property Pages**→**Conditions**

Actions tab

When a rule is created, the appropriate actions for the rule category and message type are added to the Actions tab. The actions on this tab cannot be edited.



Schedule tab

When you have configured the rule, set the schedule for processing the rule.

NOTE: In order for a Selective Archiving event to work properly, the event must be enabled and its corresponding rule in the Policy Engine must be scheduled.

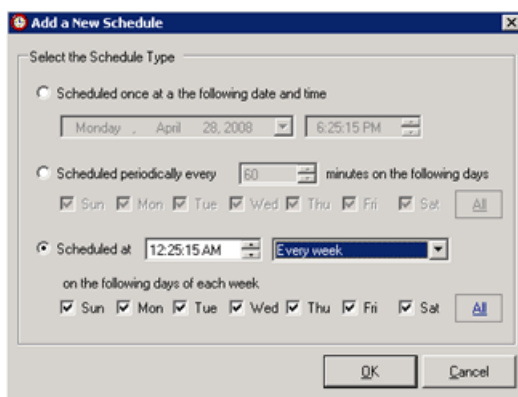
1. Click **Add**.
2. Select the Schedule Type, set the schedule, and then click **OK**.

You can choose to schedule the rule so that

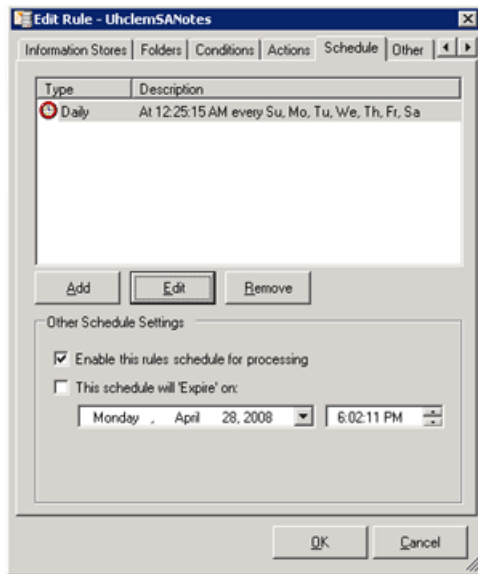
- It only occurs once.
- It occurs periodically throughout the day on specified days.
- It occurs at specified times on specified days and weeks.

NOTE: Rules should be scheduled so that processing does not adversely impact system resources on the Exchange server or the Archive Gateway. Talk to your HP service representative about the rules schedule.

The following example shows a rule set to occur every day of every week at 12:25 a.m.



3. On the Schedule tab, select the check box to enable the rule for processing.



4. (Optional) Set a date and time for the schedule to expire.

Working with Selective Archiving events

This section describes how to edit, copy, and delete Selective Archiving events.

Editing Selective Archiving events

To edit a Selective Archiving event:

1. Navigate to **Configuration**→**Archive Engine**→**Archive Events**. To learn about navigating see “Navigating in the HP EAs Exchange software” (page 16).
2. Select the Event from the Archive Engine pane.
3. Click **Edit** from the Actions pane on the right side of the window.

If you do not see an **Edit** item in the Actions pane, make sure that you have selected only one event from the list.

4. Edit the settings you wish to change. The settings on each tab are described in the following sections.
5. Click **Save** to apply the changes.

NOTE: Modifications are not applied to events that are currently being processed.

General tab

In the **General** tab, you can only edit the description of the event. You cannot change the name of an event.

Configuration tab

The **Configuration** tab lets you specify the following items:

Field	Description
Message Type	Specifies the kind of item the Selective Archiving event archives to the IAP. <ul style="list-style-type: none">• Calendar items (IPM.Appointment)• Documents (IPM.Document)• Standard email messages (IPM.Note) Includes secure and encrypted email.• Task Items (IPM.Task)• All items (applies to stealth archiving only)• Public Folder Messages• Quota Archive Thresholds
Default Routing Address(es)	A list of additional addresses (corresponding to IAP repositories) to which every item will also be archived. See "Default Routing Address" (page 21).
Capture Email with TNEF	If selected, messages are stored using Transport Neutral Encapsulation Format. Otherwise, messages are stored using MIME format. See "TNEF message format" (page 20) to learn more about TNEF.
Trim Attachments	Selecting Yes removes attachments when messages are archived and replaces the attachments with a proxy file in the tombstoned messages. In Outlook the proxy appears under its filename, <code>ArchiveInfo.htm</code> . In OWA the proxy appears under its display name, <code>Attachment Info.htm</code> .
Trim Message Body	Selecting Yes removes the message body from tombstones.
Stealth Archiving	Selecting Yes does not replace the message body with a tombstone. If you select Stealth Archiving, Trim Attachments and Trim Message Body are disabled.

IAP Domain tab

The **IAP Domain** tab contains information about the IAP that collects the archived messages.

Field	Description
IAP Domain Name	The name of the IAP domain to which the email from the journal mailbox should be stored. You can choose one of the known domain names from the menu. If you change this field, the following three values will change as well.
IAP Domain ID	The domain ID that matches the IAP Domain Name. The Domain ID must match exactly the domain ID attribute in <code>Domain.jcml</code> .
IAP Domain VIP (SMTP)	The IAP Virtual IP (VIP) used for SMTP delivery.
IAP HTTP Portal Address	The IAP Virtual IP (VIP) used for HTTP delivery.

CAUTION: In order to change the IAP Domain ID, IAP Domain VIP, or IAP HTTP Portal Address values, you must first select **Override Domain Information**. However, do not do so except under the direction of an HP representative.

Advanced tab

The **Advanced** tab lets you examine the values for all of the event parameters. If directed by HP support, click **Edit** to edit these values.

Copying a Selective Archiving event

To copy an event follow these steps:

1. Navigate to **Configuration**→**Archive Engine**→**Archive Events**. To learn about navigating see “Navigating in the HP EAs Exchange software” (page 16).
2. Select an event from the Archive Events pane and click **Copy**.
3. Click **Copy** from the Actions pane on the right side of the window. A new window with an event named “Copy of” the original event appears.
4. Give the event a new name and make changes in the **Configuration** tab as needed.

Deleting a Selective Archiving event

To delete a scheduled Selective Archiving event:

1. Navigate to **Configuration**→**Archive Engine**→**Archive Events**. To learn about navigating see “Navigating in the HP EAs Exchange software” (page 16).
2. Select an event from the Archive Events pane and click **Remove**. A dialog box appears asking you to confirm that you want to remove the event.
3. Click **Yes** to remove the event. The corresponding Policy Engine rule is also deleted.

Running Selective Archiving events

In order for Selective Archiving events to run, the event must be enabled and the corresponding Policy Engine rule must be scheduled. You can check whether an event is enabled or disabled in the State column of the Archive Events pane. You can check whether the corresponding rule is scheduled in the Policy Engine column.

To enable or disable archiving events, select one from the Archive Events pane and click one of the following from the Actions pane on the right side of the window:

- Enable All
- Disable All
- Enable
- Disable

If you need to schedule a Selective Archiving event's corresponding Policy Engine rule, see “Configuring Policy Engine rules” (page 46)

Once the Selective Archiving event is enabled and its corresponding Policy Engine rule is scheduled, it runs automatically at the scheduled time.

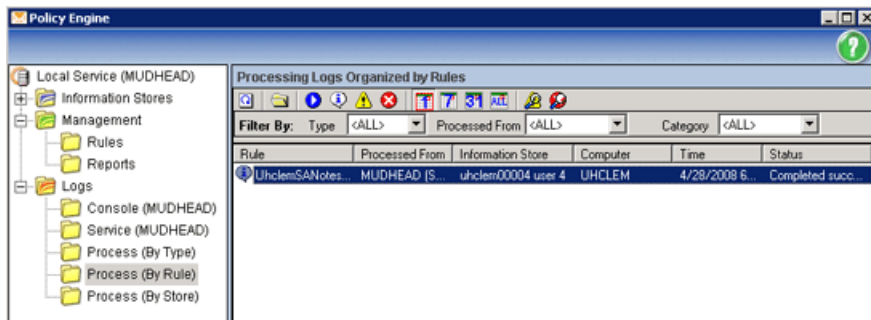
If you disable a Selective Archiving event, be sure to disable the corresponding rule in the Policy Engine.

Executing a Policy Engine rule manually

You can execute a Policy Engine rule manually, without scheduling. The corresponding Selective Archiving event must be enabled for the rule to work properly.

1. Log on to the Archive Gateway using the archive service account and launch the HP EAsE software (see “Launching EAsE software” (page 16).
2. Navigate to **Configuration**→**Policy Engine**.
3. Click **Launch** to launch the Policy Engine administration application.

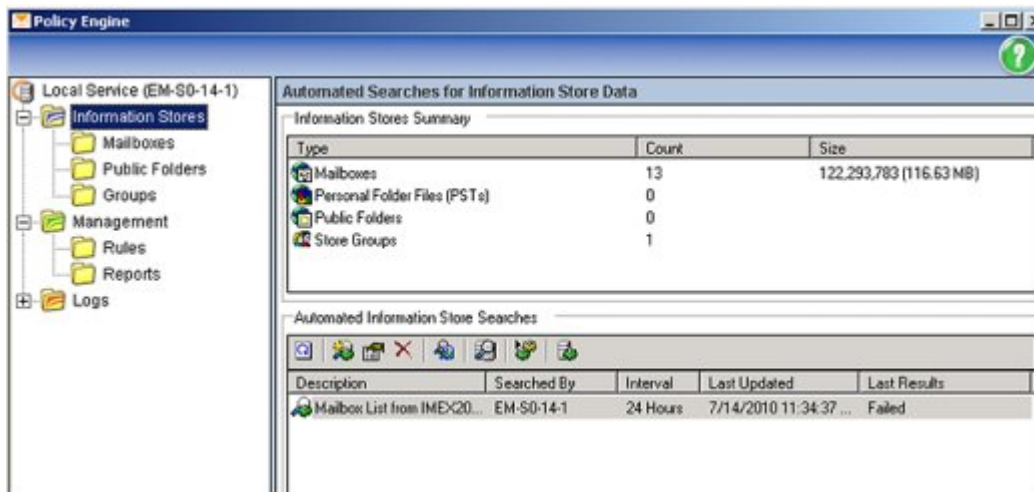
4. In the left pane of the Policy Engine Window, expand the Management folder, and then select **Rules**.
 5. In the Policy Engine window, right-click the rule and select **Process Now**.
- To track the processing of a rule:
1. Expand **Logs** in the left pane of the Policy Engine window.
 2. Select **Process (By Rule)**.
- The log entry appears in the right pane.



3. Double-click the entry to display the log information.

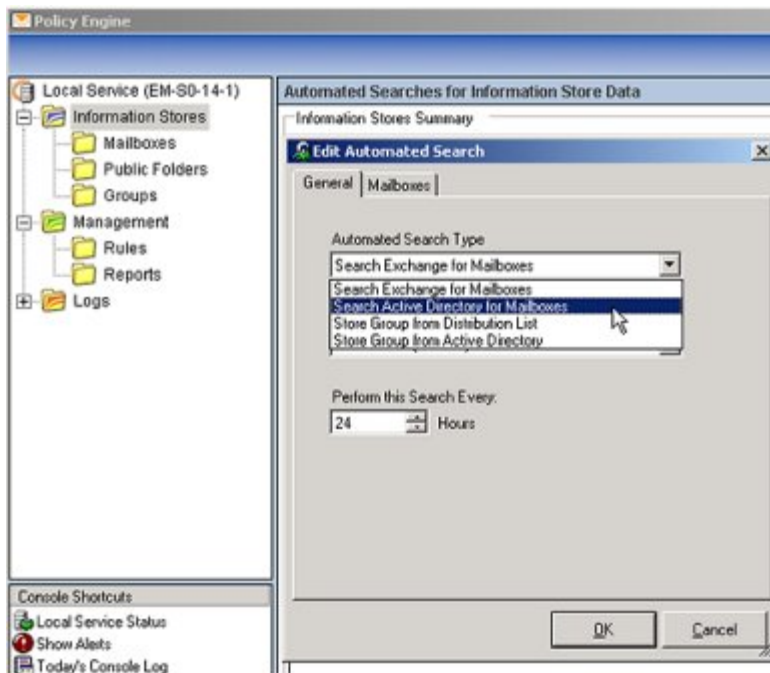
Using Information Store Groups for rule processing

HP EAsE supports a custom grouping mechanism that lets you group mailboxes (and `pst` files) for inclusion in rule processing. This grouping mechanism is called Information Store Groups (as shown in the following example) and can be performed manually, it can be automated, or you can use a combination of both methods.

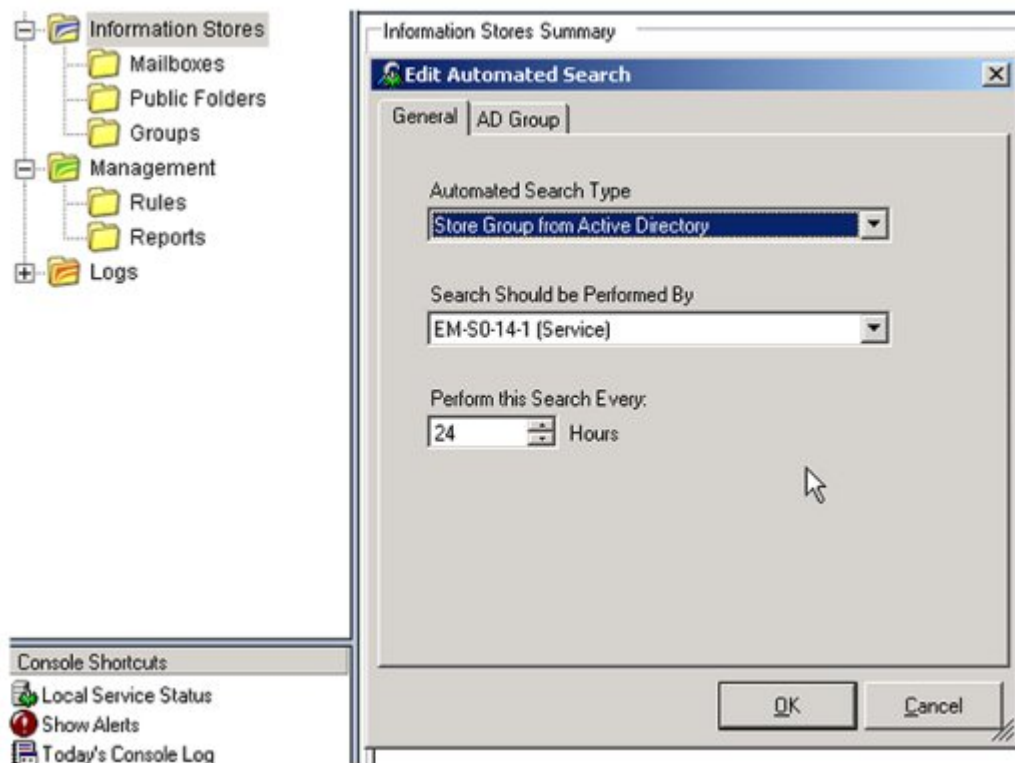


To limit rules to the users of a specific AD:

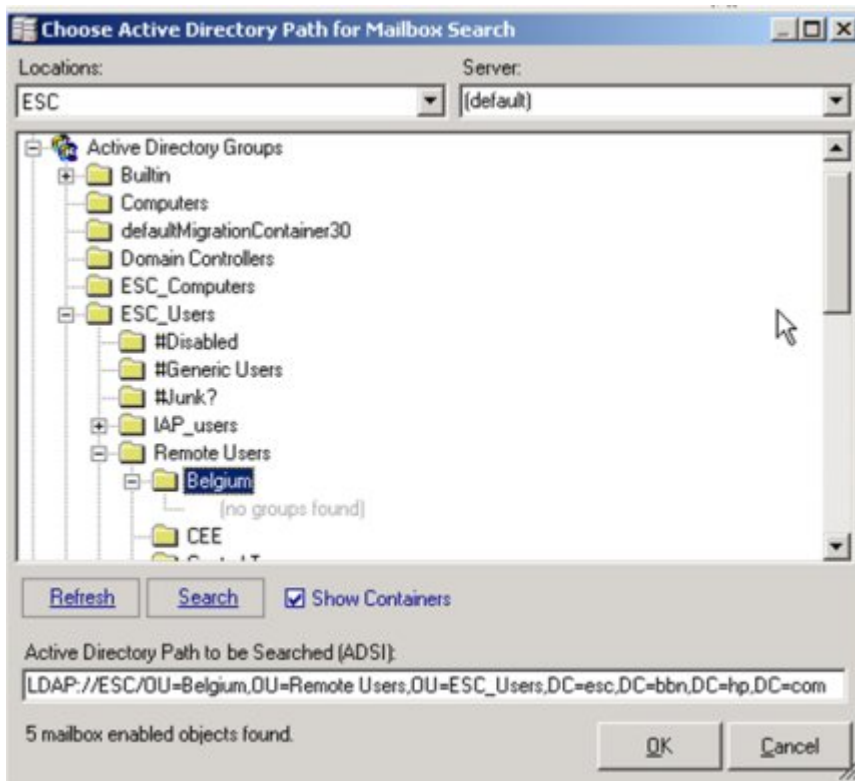
1. Setup an automated query to keep the list of all mailboxes up to date. Doing so ensures that your mailbox is available to EASE to be included in a store group.
Use the automated search feature to perform this at the Information Stores root folder level. You can add a query to the list that periodically scans your AD environment for mailboxes, and add them to the list of known mailboxes in the EASE database



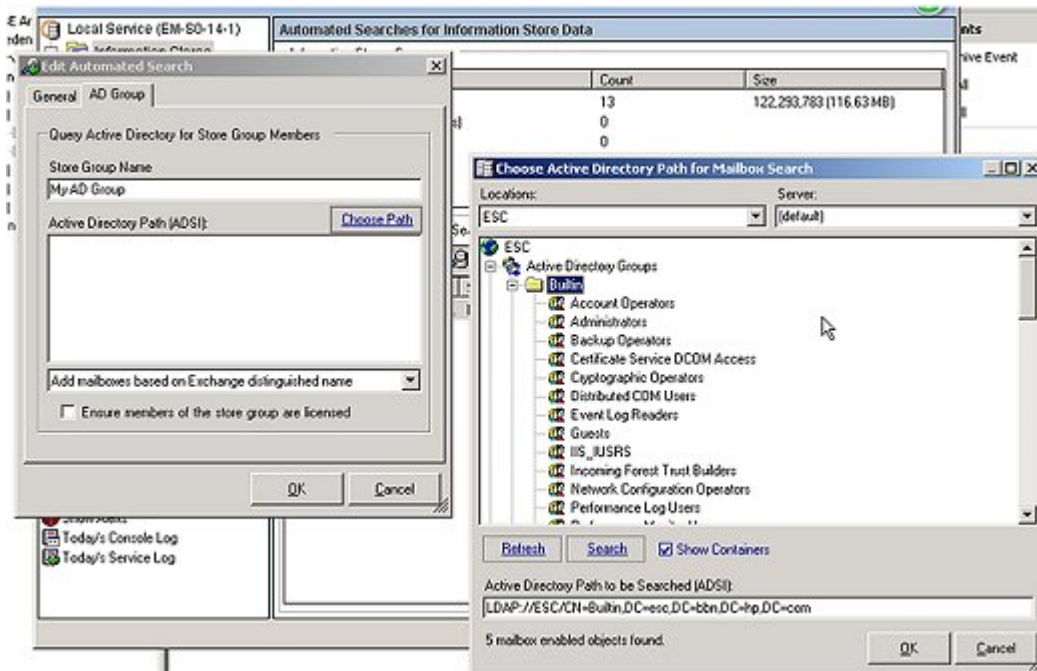
2. Add another automated search that creates an information store group based on an AD group.



3. After adding the two queries, the service should add all their mailboxes.



In addition, a new group appears in the list of email store groups. If necessary, you can force an immediate update.



9 Using tombstone maintenance

When a message is selectively archived, or is imported into the IAP using the PST Import Manager, a tombstone can be created in the user's mailbox or in the PST file. Tombstoning removes content from the message and substitutes a link to the archived message that is stored on the IAP. Depending on the settings for the Selective Archiving event or PST import:

- Tombstoning is not enabled.
- Only message attachments are tombstoned.
- Both attachments and the message body are tombstoned, leaving only the message header.

When tombstoning is enabled, use the tombstone maintenance events to update legacy mail items, make tombstoned messages visible in Outlook Web Access, and synchronize the location of tombstoned items.

Configuration of tombstone maintenance events and their corresponding rules is explained in the following topics:

- “Configuring tombstone maintenance events” (page 63)
- “Configuring tombstone maintenance events with folder capture” (page 64)

Configuring tombstone maintenance events

A Tombstone Maintenance event and its corresponding rule update legacy mail items and make archived messages visible in Outlook Web Access.

NOTE: Because a tombstone maintenance event looks at every tombstoned message, it is an intensive process and should be used sparingly. HP recommends that you run the event once after a software upgrade, so that the tombstoned items are compliant with the newly installed version of the software. After that, HP recommends you run the event every few months as the needs of your enterprise require.

To create the event and corresponding rule:

1. Click **New Archive Event** from the Actions pane on the right side of the window.
2. In the dialog box that appears, select **Tombstone Archiving** and click **OK** to display the Create Archive Event window.
3. Enter a descriptive name for the event in the Name box and an optional description in the Description box.

The name should not contain any special characters.

If you would like to tombstone maintenance event to not remove messages from the mailbox store, follow these steps:

- a. Click the **Configuration** tab to display the configuration pane.
 - b. Select **Stealth Archiving**.
4. Click **Create** to close the window and create the event.
A window appears that announces that a Policy Engine rule with the same name as the Selective Archiving event has been created.
 5. Click **Launch Policy Engine Admin** to launch the policy engine.
 6. In the left pane of the Policy Engine window, expand the Management folder, and then select **Rules**.
 7. Double-click the tombstone rule in the right pane.

It will have the same name as the event you created in the EAsE Archive Engine.

8. Configure the rule:

Tab	Configuration
Information Stores	Select the mailboxes to be archived. See Information Stores tab.
Folders	Select the Outlook folders containing the messages to be archived. See Folders tab.
Conditions	Do not edit the Message Class. You may specify additional conditions.
Actions	Do not edit.
Schedule	Schedule the rule. See "Schedule tab" (page 56).

9. Click **OK**.

Configuring tombstone maintenance events with folder capture

When folder capture is enabled in the IAP and EAsE, you can create a Tombstone Maintenance event to synchronize the folder location of tombstoned items in Exchange with the folder information that is stored in the IAP. To learn more about folder capture see "Working with folder capture" (page 70).

This event determines if folder information for an archived message has been submitted previously to the IAP. If not, the event submits the folder information to the mailbox owner's repository. If folder information was previously submitted for the message, the current folder path is examined to determine if it has changed. If the path has changed, the folder information is updated in the mailbox owner's repository.

This event does not need to be run frequently and processing is less intensive than for regular tombstone maintenance.

To configure the event and corresponding rule:

1. Click **New Archive Event** from the Actions pane on the right side of the window.
2. In the dialog box that appears, select **Tombstone Archiving** and click **OK** to display the Create Archive Event window.
3. Enter a descriptive name for the event in the Name box and an optional description in the Description box.

The name should not contain any special characters.

4. Click the **Configuration** tab to display the configuration pane.
5. Select **Folder Synchronization**.

If you would like to tombstone maintenance event to not remove messages from the mailbox store, select **Stealth Archiving**.

6. Click **Create** to close the window and create the event.

A window appears that announces that a Policy Engine rule with the same name as the Selective Archiving event has been created.

7. Click **OK**.

A dialog box appears stating that a corresponding rule for the event has been created in the Policy Engine database.

8. Click **Launch Policy Engine Admin** to launch the policy engine.
9. In the left pane of the Policy Engine window, expand the Management folder, and then select **Rules**.
10. Double-click the tombstone rule in the right pane.

It will have the same name as the event you created in the EAsE Archive Engine.

11. Double-click the tombstone rule in the right pane.
It will have the same name as the event you created in the EAsE Archive Engine.
12. Configure the rule:

Tab	Configuration
Information Stores	Select the mailboxes to be archived. See Information Stores tab.
Folders	Select the Outlook folders containing the messages to be archived. See Folders tab.
Conditions	Do not edit the Message Class.
Actions	Do not edit.
Schedule	Schedule the rule. See "Schedule tab" (page 56).

13. Click **OK** to save the rule.

10 Configuring end-user delete

Exchange supports a configurable retention interval on items deleted by end users in Outlook. When the interval lapses, deleted messages are permanently removed (hard deleted) from the Exchange mailbox store.

If end users delete a tombstoned item, the deletion must be coordinated with deletion of the tombstone reference in the IAP. IAP 2.x removes the user's repository reference from the archived item. If folder capture is enabled, folder references are removed from the archived item.

To coordinate the deleted items, create a Synchronize Deleted Items event and rule that execute within the retention interval set in Exchange.

NOTE: These retention settings must be coordinated with two attributes in the `Domain.jcm1` file on the IAP: `MinRegulatedRetentionPeriodDays` and `MinUnRegulatedRetentionPeriodDays`, which define the minimum data retention period for a user repository.

- “Location of deleted items” (page 66)
- Enabling deletion retention on the Exchange server
- “Scheduling deletion from the IAP” (page 68)

Location of deleted items

When users delete a mail item or tombstone from Outlook, the item is moved to the Deleted Items folder. It remains there until user action is taken, such as **Empty “Deleted Items” Folder**. When a user empties the Deleted Items folder, the deleted items move into intermediate Dumpster storage on the Exchange server. They remain there until the Exchange retention interval lapses or the Synchronize Deleted Items rule is executed.

EAs Exchange supports the deletion of items from both the Deleted Items folder and the Dumpster. The Dumpster is considered a required location. The Deleted Items folder is optional and depends on the policy within your organization. The location selection is made in the Synchronize Deleted Items rule.

When a user deletes a tombstoned item from Outlook, the Synchronize Deleted Items event and rule remove references to the tombstone from the message that is archived in the IAP. The rule can also clean up non-tombstoned items in the Exchange Dumpster if configured to do so, which helps you to purge deleted items more quickly from the Exchange server.

Deleted items tag

To provide flexibility in processing mail item deletion, a tag is added to items that fail to delete due to targeted tombstoning or other conditions. The tag is added as a custom MAPI property, `PTDelStatus`.

When the `PTDelStatus` tag exists on a mail item, it indicates that attempts have been made to delete the item and they have failed. This can be due to issues related to IAP retention, a disabled IAP, or other coordination issues. For this reason, the tag is used in the Policy Engine rule to periodically search for such items.

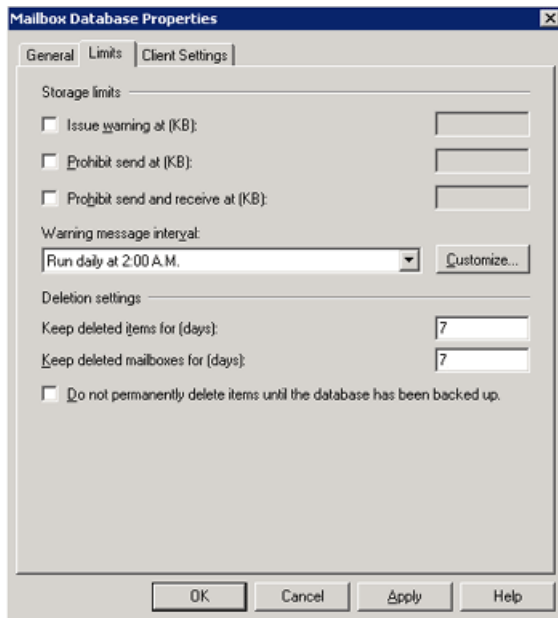
In a well coordinated system, there are no items remaining with the `PTDelStatus` tag.

Enabling deletion retention on the Exchange server

Exchange 2007 and later

To enable deletion retention on the Exchange server, configure the following settings for each mailbox store.

1. Log on to the Exchange server.
2. Open the Exchange Management Console.
3. Expand **Server Configuration**, and then click **Mailbox**.
At the bottom of the console, the Storage Groups and associated Mailbox Databases appear.
4. Right-click the Mailbox Database, and select **Properties**.
5. Click the **Limits** tab and assign the values to Deletion settings.
HP recommends that the **Keep deleted items for (days)** and the **Keep deleted mailboxes for (days)** parameters be set to **7**.



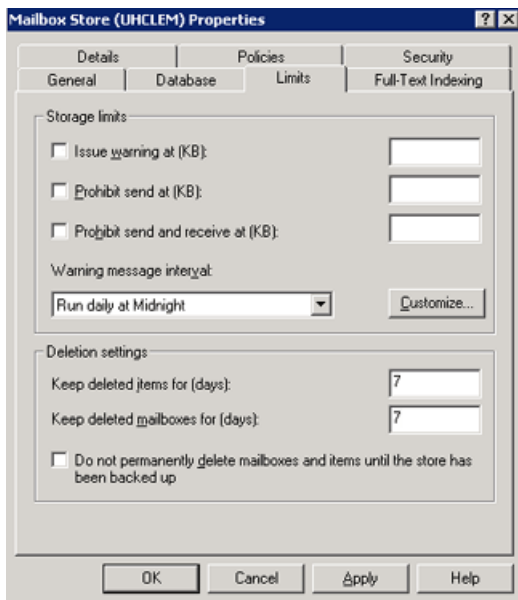
6. Click **Apply**, and then click **OK**.
7. Repeat steps 4–6 for each relevant Storage Group and Mailbox Database.

Pre-2007 Exchange servers

To enable deletion retention on the Exchange server, assign the following settings to each mailbox store.

1. Log on to the Exchange server.
2. Open System Manager and navigate to the Storage Group and Mailbox Store.
3. Right click the Mailbox Store and select **Properties** to display the Properties dialog box.
4. Click the **Limits** tab and assign the values to Deletion Settings.

HP recommends that the **Keep deleted items for (days)** and the **Keep deleted mailboxes for (days)** parameters be set to **7**.



5. Click **Apply**, and click **OK**.
6. Repeat steps 3–5 for each relevant Storage Group and Mailbox Store.

Scheduling deletion from the IAP

To schedule message or tombstone reference deletions, create and enable a Synchronize Deleted Items event and establish a corresponding rule in Policy Engine.

Creating the event

1. Navigate to **Configuration**→**Archive Engine**→**Archive Events**. To learn about navigating see “Navigating in the HP EAs Exchange software” (page 16).
2. Click **New Archive Event** from the Actions pane on the right side of the window.
3. In the dialog box that appears, select **Synchronize Deleted Items** and click **OK** to display the Create Archive Event window.
4. Enter a descriptive name for the event in the Name box and an optional description in the Description box.
The name should not contain any special characters.
5. Click the **Configuration** tab to display the configuration pane.
In most cases, the default values are appropriate, but you can change them to suit your particular situation.
6. Click **Create** to close the window and create the event.
A window appears that announces that a Policy Engine rule with the same name as the Selective Archiving event has been created.
7. Click **Launch Policy Engine Admin** to launch the policy engine.
Continue configuring the corresponding Policy Engine rule in the next section.

Creating a Policy Engine rule

To create the Policy Engine rule:

1. In the left pane of the Policy Engine window, expand the Management folder, and then select **Rules**.
2. Double-click the Synchronize Deleted Items rule in the right pane. The rule has the same name as the event you created.

3. In the Information Stores tab, select the mailboxes to be archived. See Information Stores tab.
4. In the Folders tab:
 - a. Select the folders to be archived.
 - b. Make sure the **Include the default Recover Deleted Items folder (Dumpster)** check box is selected.

ⓘ **IMPORTANT:** Do **not** select the **Include all other Recover Deleted Items folders** check box. Doing so may cause items to be deleted from the IAP unintentionally.

5. In the **Conditions** tab, decide which items are eligible to be deleted.

The rule can select items in the Dumpster only or items in the Dumpster and the Deleted Items folder. If both conditions are set, the rule scans the Deleted Items folder and the Dumpster for eligible items.

- The default condition is to delete items in the Dumpster. This condition is required. If you choose to delete only items in the Dumpster, do not make any changes in the Conditions tab.
- If you want the rule to delete items in the Deleted Items folder as well as the Dumpster, select **Add > Test Keyword Conditions > Test Message Keywords**, and then click **OK**.

In the Edit the Condition window, click **Edit Value**, edit the three fields as shown in the following example, and then click **OK**.

[FOLDER_NAME]	Equals	Deleted Items
---------------	--------	---------------

6. Do not edit the Actions tab.
7. In the Schedule tab, set the schedule so that items are deleted within the retention interval. See "Schedule tab" (page 56) for more information.

11 Working with folder capture

Folder Capture captures the Outlook folder location of a message and updates the corresponding archived documents in the IAP. The folder location (for example, /Inbox/project) is stored as metadata in the archived email.

This chapter explains how folder capture works with the HP EAs Exchange software and how it affects:

- Three types of events:
 - Selective Archiving
 - Tombstone Maintenance (Tombstone Folder Synchronization)
 - Synchronize Deleted Items
- PST Import Manager

Folder capture cannot be used with Compliance Archiving.

Indexing folder information

When folder information is indexed, end users and compliance officers can use the folder name to search for and retrieve messages stored on the IAP. Adding this information to the content indexes takes up additional disk space in the IAP's Smartcells and can impact system performance, especially if the IAP contains a great many archived messages.

To limit the number of archived messages that are re-indexed when folder information is added, your HP service representative specifies a cut off date on the IAP. Messages stored before the cut off date have only their metadata updated, while messages stored after the cut off date have both the metadata and indexes updated with folder information. See “Enabling folder capture on the IAP” (page 70).

NOTE: If your IAP system contains a number of closed Smartcells, available disk space can be quickly depleted when indexed folder information is added—especially if the cut off date is set too far in the past. This situation results in the error described in “DiskSpaceBuffer error” (page 107). To prevent this error, HP recommends setting the cut off date to the date the system is upgraded so that only new emails are indexed.

Enabling folder capture

For folder capture to occur, it must be enabled in both the IAP and HP EAs Exchange.

In HP EAs Exchange, folder capture is enabled by default. On the IAP, it is disabled by default.

In HP EAs Exchange, folder capture can be enabled (or disabled) in the global configuration file, or enabled (or disabled) for a specific archiving event.

Enabling folder capture on the IAP

Folder capture for an IAP domain is set in the `Domain.jcml` file on the kickstart server at `/install/configs/primary/`. If folder capture is enabled, your HP service representative sets the `FolderSupportEnabled` parameter to `true` for the IAP domain.

Indexing of folder information, along with the cut off date, is enabled in the `FolderSupportAutoReindexCutoffDate` parameter in `Domain.jcml`.

Enabling folder capture in the archiving global configuration file

In HP EAs Exchange, folder capture is enabled by default in the global configuration file on the Archive Gateway (G:\Mining>Selective Archiving\HPAE.ini). The UseFolderCapture parameter is located in several places in the file:

- For Selective Archiving:
[ExchSelectiveArchiving]
UseFolderCapture=True
- For Tombstone Maintenance (Tombstone Folder Synchronization):
[ExchStubMaintenance]
UseFolderCapture=True
- For Synchronize Deleted Items:
[ExchDeleteSynch]
UseFolderCapture=True (must be manually added if this type of event is enabled)

To disable folder capture globally, set the value to `False`.

Enabling folder capture for a specific event

For the event types in which folder capture can be used, you can enable (or disable) the setting for a specific event. Doing this overrides the settings assigned in the HPAE.ini file.

Event overrides are placed in separate .ini files in G:\Mining>Selective Archiving\Events.

1. In the EAsE software, locate the event for which you want folder capture enabled and click **Edit**.
2. Click the **Advanced** tab to display the advanced settings for the event.
3. Click **Edit** to enable editing of the settings.
4. Depending on the event type, in the [ExchSelectiveArchiving], [ExchStubMaintenance], or [ExchDeleteSynch] area, manually enter `UseFolderCapture=True` or `UseFolderCapture=False` to override the global value and enable or disable folder capture for the event.
5. Click **Update**, and then click **Save** to finalize the changes.

Enabling folder capture in PST Import Manager

In PST Import Manager, folder capture is enabled by default in the global configuration file (\Program Files\Hewlett-Packard\HP EAsE PST Importer\HP EAsE PST Importer.ini).

The UseFolderCapture value in the global configuration file can be overridden for individual PST imports. The Archive Request file specifies whether folder information is captured during PST import. See “Creating or editing an Import Description file” (page 81) for information on how to configure this file.

Import overrides are placed in the relevant .ini file in \Program Files\Hewlett-Packard\HP EAsE PST Importer\PSTLoad.

How folder capture works with archiving events

The following sections describe how scheduled archiving events behave when folder capture is enabled.

Folder capture and Selective Archiving events

When a message is sent to the IAP and folder capture is enabled, a Selective Archiving event submits folder information to the mailbox owner's repository. The tombstone that is created contains the folder location stored on the IAP.

If the Selective Archiving event finds a message that is already archived, the message is processed in the same way that Tombstone Folder Synchronization events are processed (see "Folder capture and Tombstone Folder Synchronization events" (page 72)). However, this situation should not occur when you use the pre-configured settings in the Selective Archiving rules.

Folder capture and Tombstone Folder Synchronization events

When folder capture is enabled, a Tombstone Folder Synchronization event determines if folder information for an archived message has been submitted previously to the IAP. If not, the event submits the folder information to the mailbox owner's repository. If folder information was previously submitted for the message, the current folder path is examined to determine if it has changed. When the path has changed, the folder information is updated in the mailbox owner's repository. See "Configuring tombstone maintenance events with folder capture" (page 64) for the procedure to use.

Folder capture and Synchronize Deleted Items events

Synchronize Deleted Items (also known as End User Delete) is an optional event that is described in "Configuring end-user delete" (page 66). This event coordinates deletion of tombstoned messages from user mailboxes with deletion of references to those tombstones in the IAP.

When folder capture is enabled, a Synchronize Deleted Items event determines if folder information was submitted for a tombstoned message. If it was submitted, a folder deletion request for the archived item is issued for the mailbox owner's repository. If folder information was not submitted, the event submits and then deletes folder information based on the item's parent folder.

To configure a Synchronize Deleted Items event and rule, see "Scheduling deletion from the IAP" (page 68).

NOTE: Currently, the Remove Folder Referenced In Item Only setting in the Synchronize Deleted Items event window is not operational.

Folder capture and PST Import Manager

When folder capture is enabled, items that have not been archived are processed like those in Selective Archiving events. Previously tombstoned items that are found in PST files are processed like those in Tombstone Folder Synchronization events. Folder information is submitted or updated based on the User Repository address (the <repository> tag) provided in the Archive Request file.

The PST Import Manager is described in "Archiving with PST Import Manager" (page 78). The Archive Request file is described in "PST Import Manager: Archive Request file specifications" (page 117).

Folder capture and the merging of duplicate messages

Duplicate Manager in the IAP software merges duplicate versions of an archived email into a single instance of the message. Before IAP 2.0, duplicates were often stored in the system. For example, a duplicate copy of a message was stored for each recipient of the message. Now, when Duplicate Manager is enabled on the IAP, a single merged message contains the aggregated data of the duplicates.

If you are upgrading your IAP system and plan to use both Duplicate Manager and folder capture, HP recommends running the initial merge job before enabling folder capture on the IAP. The first run of Duplicate Manager is a performance-intensive operation because it merges the duplicated

messages that are currently archived in the system and re-indexes the merged messages. It is much more efficient to start capturing folder data after messages are merged.

Enabling folder capture after the initial merge jobs also avoids:

- Document deletions not occurring if Synchronize Deleted Items (End User Delete) is enabled.
- Negative impact on search capability, whether from the Outlook Integrated Archive Search or the IAP Web Interface.

If folder capture is performed at the same time as duplicate merge, folder information might not be updated properly, making it difficult to search using the folder name.

12 Monitoring performance

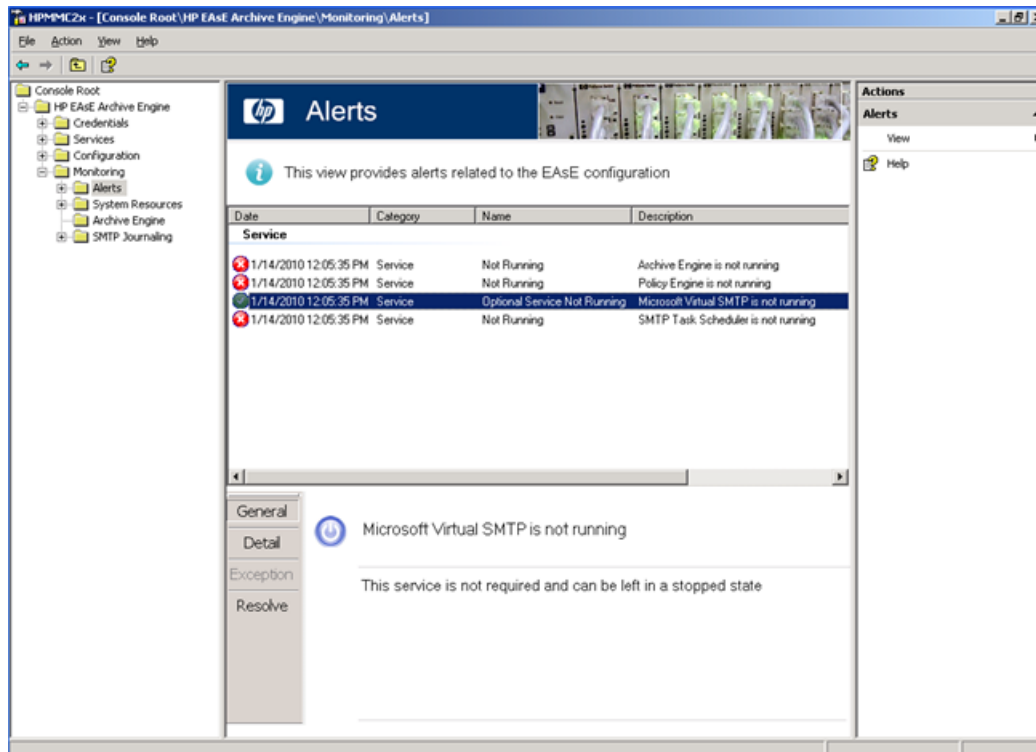
The EAsE software gives you several tools to monitor the health and performance of your system. To access the monitoring tools:

1. Log on to the Archive Gateway using the archive service account and launch the HP EAsE software (see “Launching EAsE software” (page 16).
2. Navigate to **Monitoring**. To learn about navigating see “Navigating in the HP EAs Exchange software” (page 16).

The Monitoring page gives you an overall status of your system's performance. You can click on the individual links on this page or the corresponding items on the tree control in the left pane to get more detail.

Monitoring alerts

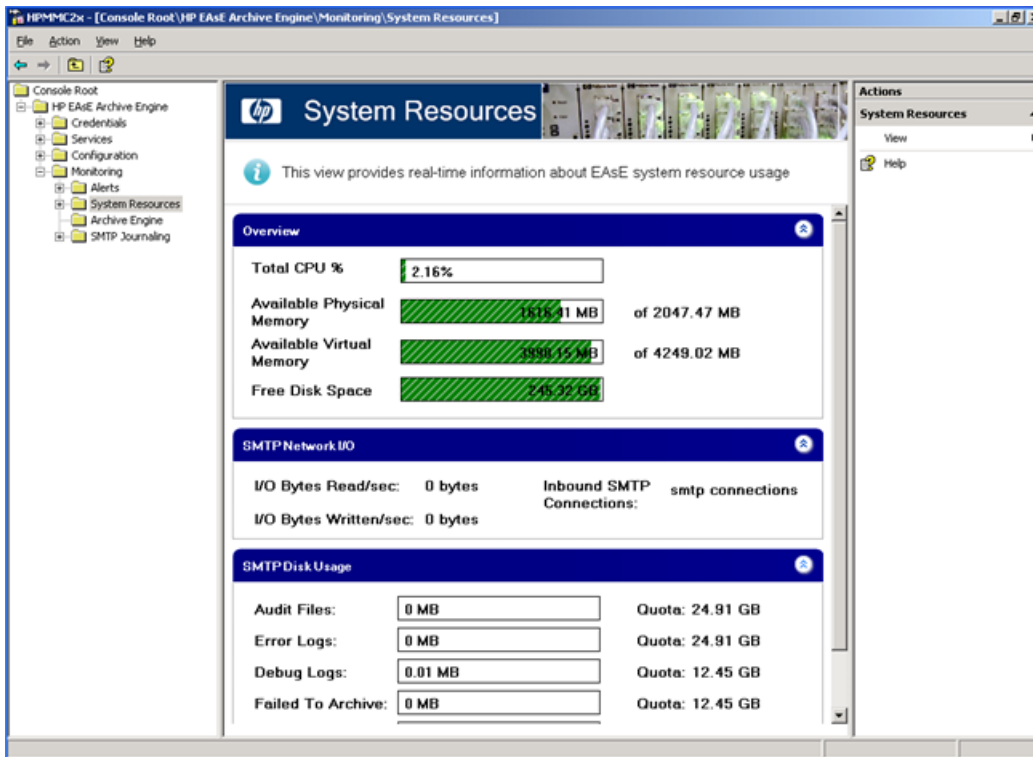
The Alerts panel gives you a historical view of events in the Archive Engine. Click an event to see more details about it.



Monitoring system resources

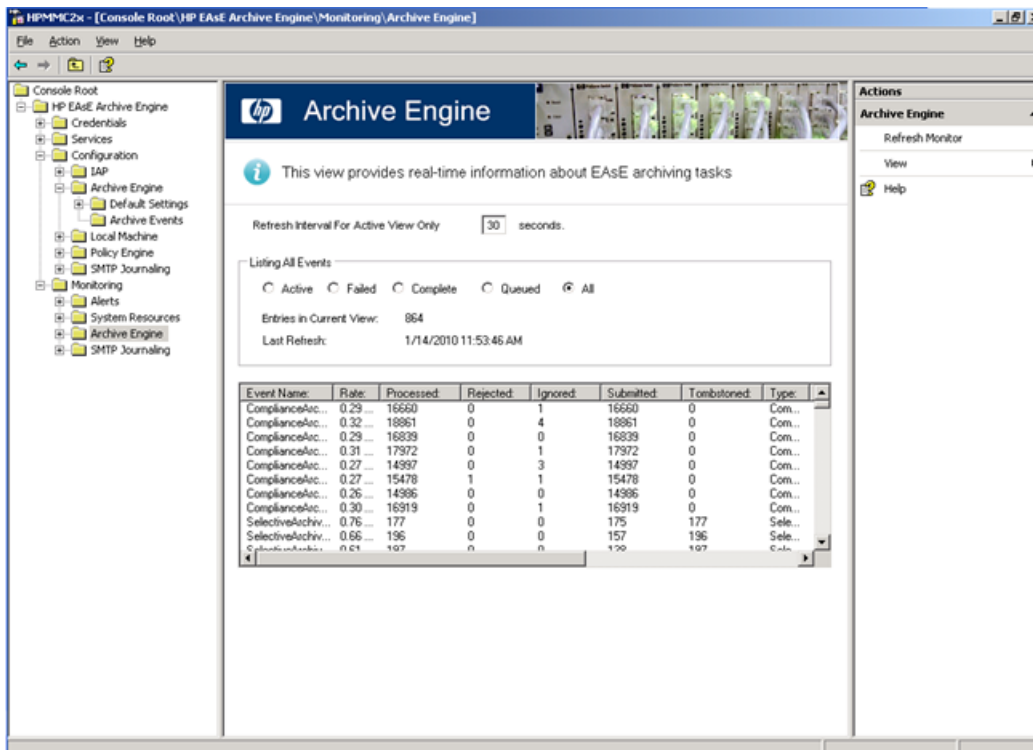
This pane gives you basic information about the Archive Gateway including:

- CPU usage
- Memory usage
- Disk usage
- SMTP connections
- SMTP disk usage



Monitoring Archive Engine status

The Archive Engine monitor shows the status of all scheduled events. A series of radio buttons let you filter the display according to different conditions. Various statistical data is provided for each event displayed.



The top area of the pane lets you set the refresh interval of the display.

The middle area of the window contains radio buttons that allow the displayed data to be filtered by processing status.

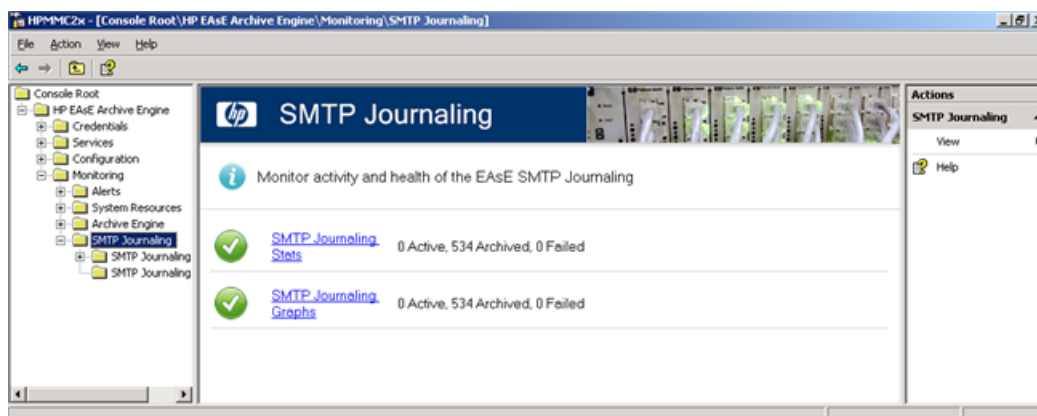
- **Active:** Only scheduled events that are currently active are displayed.
- **Failed:** Only events that have a failed status are displayed.
- **Complete:** Only events that have a complete status are displayed.
- **Queued:** Only events that have a queued status are displayed.
- **All:** All events are displayed.

The bottom area of the pane displays the event data according to the selected filter type. The data for each event is broken down into twelve different columns. Note that some columns may be irrelevant for certain event types (for example, Compliance Archiving events will never display a value in the Tombstoned column).

Field	Description
Event Name	The name of the event.
Rate	The processing rate. The way the processing rate is calculated depends on the way the events are filtered. For the Active filter, the processing rate is the average rate since the last refresh. For other filters, it is the aggregate rate of processing for the entire run.
Processed	The accumulated number of items processed by this event.
Rejected	The accumulated number of items rejected for processing by this event.
Ignored	The accumulated number of items ignored for processing by this event.
Submitted	The accumulated number if items submitted to the IAP for archiving by this event.
Tombstoned	The accumulated number of items that were tombstoned by this event.
Type	The type of event.
Elapsed Time	The accumulated amount of time, in seconds, that the event has run.
Last Run	The last time the event was successfully completed.
Log Information	The current status of the event.
File Name	The name of the data file that the event is processing.

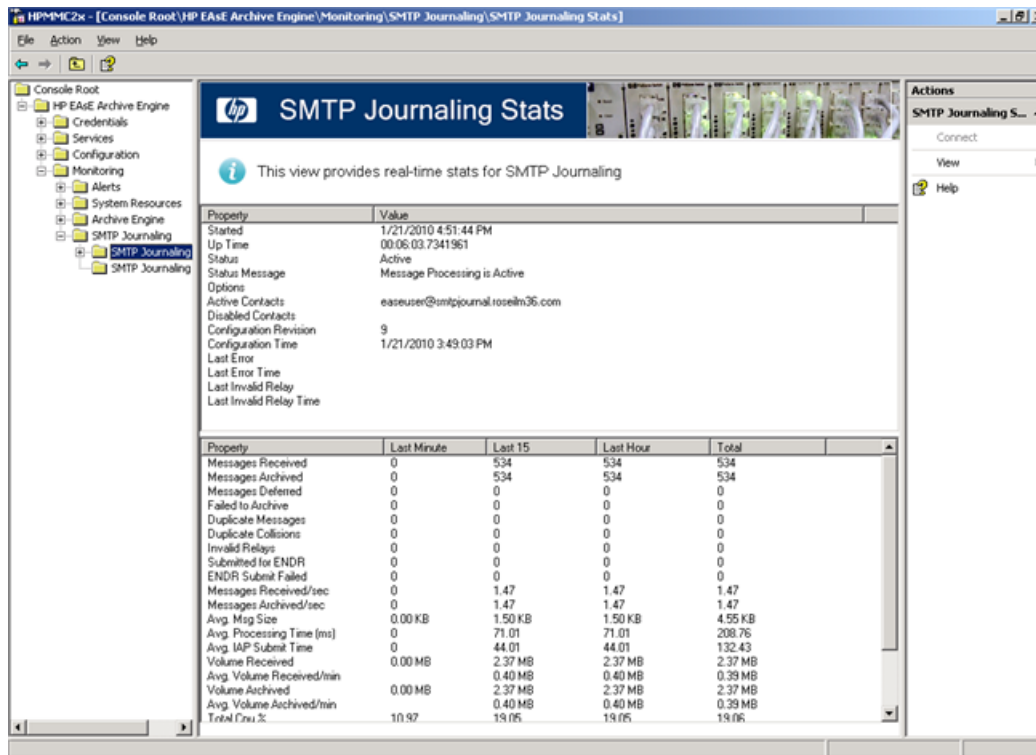
Monitoring SMTP Premium Journaling status

The SMTP Journaling pane shows you the status of each Archive Gateway that is being used for SMTP Premium Journaling.



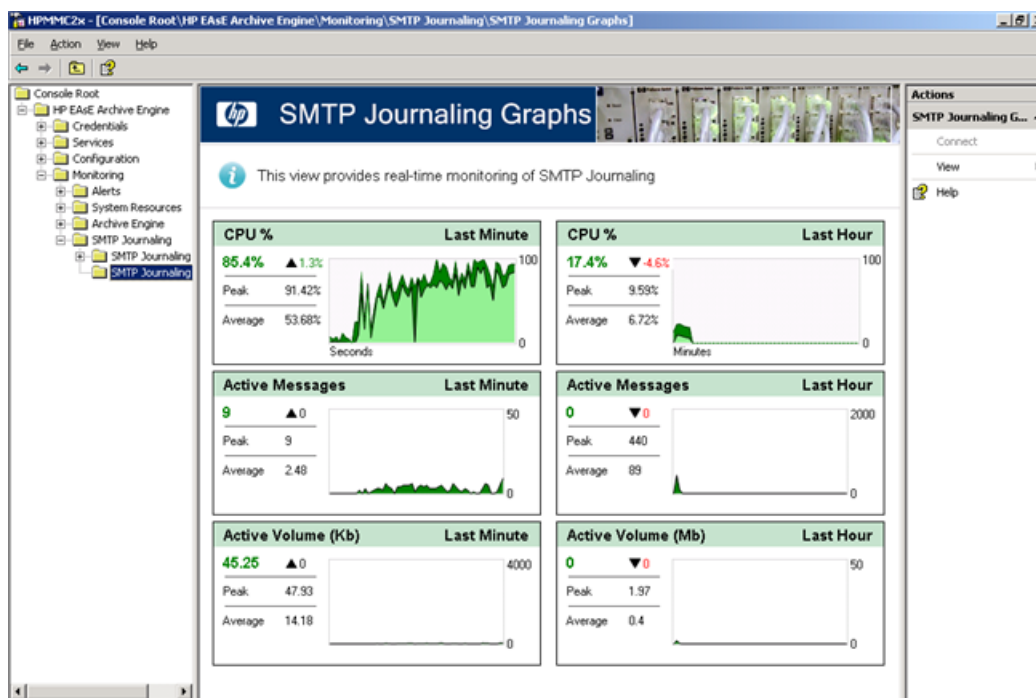
SMTP Journaling Stats

The SMTP Journaling Stats pane displays statistics about the state of SMTP Premium Journaling. You can use these statistics to monitor the health of your system.



SMTP Journaling Graphs

The SMTP Journaling Graphs pane displays information about the state of SMTP Premium Journaling. You can use these graphs to see at a glance whether your system is working as expected.



13 Archiving with PST Import Manager

The PST Import Manager tool allows you to:

- Archive legacy PST files into the IAP.
- Scan PST files to find and archive new messages.
- Optionally tombstone messages in the PST file after archiving them.

See the HP EAs Exchange Support Matrix for the system requirements to install and run the PST Import Manager.



IMPORTANT:

Antivirus programs, especially those that inspect email messages, may interfere with the proper operation of the PST Import Manager. This is because the PST Import Manager modifies every message as it is archived, and the antivirus program may interpret this modification as an infection. To avoid this problem, disable antivirus programs while the PST Import Manager is running.

In some cases, disabling the antivirus program is not sufficient. If you have disabled your antivirus program, and you are still having trouble importing PST files, you may have to uninstall the antivirus program.

Installing the PST Import Manager

This section describes the installation requirements and steps to take to install the PST Import Manager.

Installation requirements

Before installation, verify that the client machine on which you are installing the PST Import Manager meets the system requirements listed in the HP EAs Exchange Support Matrix. Your HP representative can provide you with a copy of the support matrix.

The following requirements must also be met.

Requirements on client machine

- Microsoft Management Console 3.0
 - Access to the IAP HTTP portal without proxy
 - Access to Exchange mailbox for Global Address List (GAL) name resolution
 - Read/Write access to PST files containing messages to be imported
 - Access to Outlook and Exchange without logon prompts
-

NOTE: The PST Import Manager does not run on 64-bit platforms.

IAP software requirements

- Audit repository that receives log files and status reports
 - SMTP access for client machine
-

Installation procedure

Always install the PST Import Manager on a client machine. Do not install it on the Archive Gateway.

NOTE: Microsoft's .NET Framework 2.0 must be installed on the client machine before you install the PST Import Manager.

To install or update the tools on the client:

1. Verify that client machine meets the installation requirements.
2. Run Setup.exe in the PST Importer folder on the HP EAsE Extensions CD.
3. Follow the instructions in the installation wizard, and accept all defaults.

Launching the PST Import Manager

To launch the PST Import Manager:

- Double-click its icon on the desktop
- Choose it from the **Start** menu

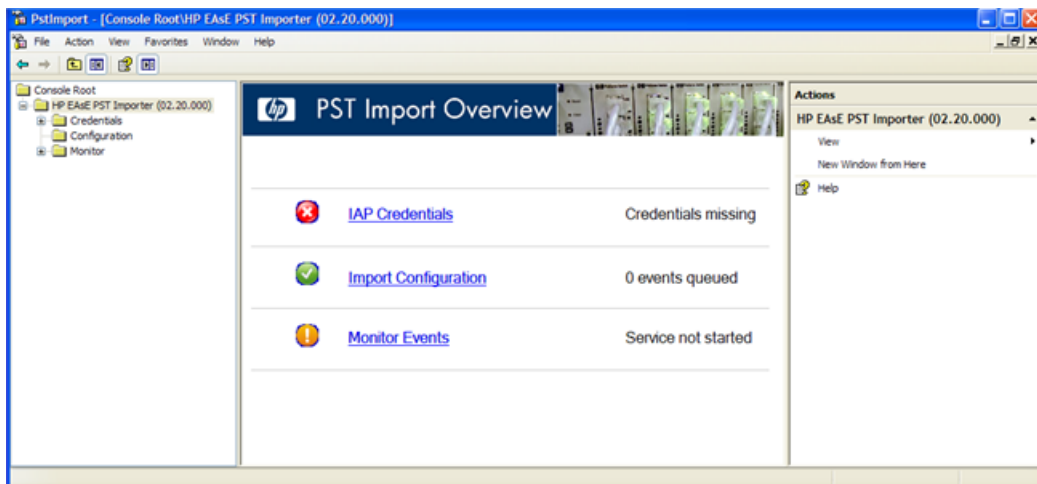
Establishing archive credentials

The archive service account needs access to the IAP so that messages in the PST files can be archived.

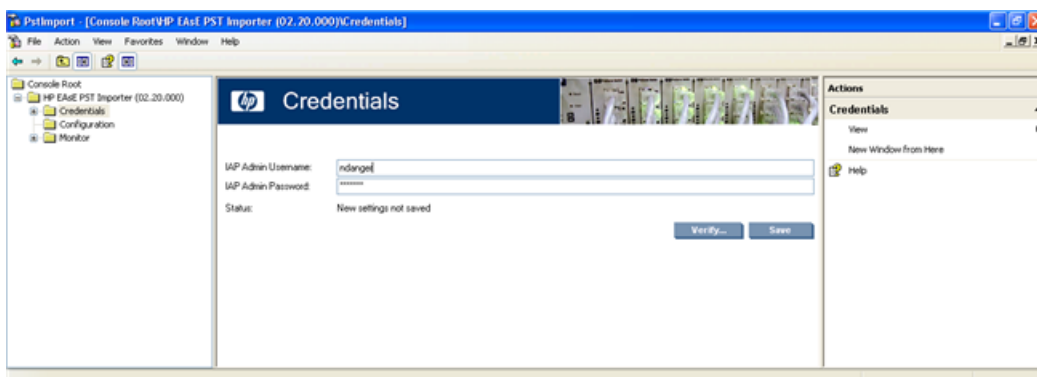
Follow these steps to set the archive credentials:

1. Launch the PST Import Manager from the desktop or select **Start**→**All Programs**→**Hewlett-Packard**→**Email Archiving software for Exchange**→**PST Import Tools**→**PST Import Manager**.

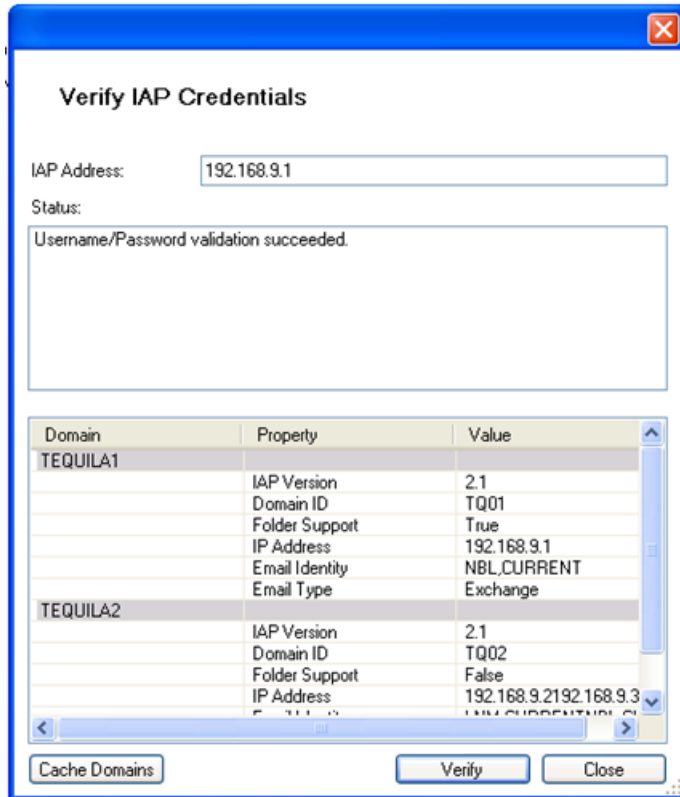
The PST Import Manager console appears.



2. Click the **Credentials** link in the main pane, or select **Credentials** from the tree control on the left side of the PST Import Manager console.



3. In the **IAP Admin Username** box, enter the email address of the service account: HPAEServiceAccount@<domain>.
For more information about the service account, see “Creating the archive service account” (page 13).
4. In the **IAP Admin Password** box, enter the password that was established for the service account.
5. Click **Verify** to test the account access.
The Verify IAP Credentials window appears.



6. In the **IAP Address** box, enter the IAP HTTP portal address.
The HTTP portal address can be any of the VIP addresses listed in the ipToDomainInfo field in the Domain.jcml file on the IAP kickstart server.
7. Click **Verify**.
The PST Import Manager tests access and displays the results in the status window.
If folder capture is enabled in the IAP, the results also show the status of IAP folder support for the selected domain.
8. In the Domain name box, select the domain in which the messages will be stored.
9. Click **Cache Domains** to have the PST Import Manager store information about IAP domains locally. This will make future rule creation faster.
10. Click **Close** to finish entering the credentials.
11. Click **Save**.

Creating and queuing the Import Description

PST Import Manager uses Import Description files to specify which PST files to import and how they will be imported.

NOTE: You can create the Import Description file manually, see “PST Import Manager: Archive Request file specifications” (page 117) for a description of the XML tags to use and a sample XML file.

Before adding a file to the import database, PST Import Manager performs the following tasks:

- Verifies that the PST file can be accessed with the appropriate access rights.
- Obtains a computed signature, or hash, that uniquely identifies the file to be inserted into the import database.
- Queries the import database, `AEDB.mdb`, for duplicate entry using the computed signature.
- Queries the IAP for duplicate entry.
- If no duplicate entry is found on the IAP, proceeds with insertion into the database.

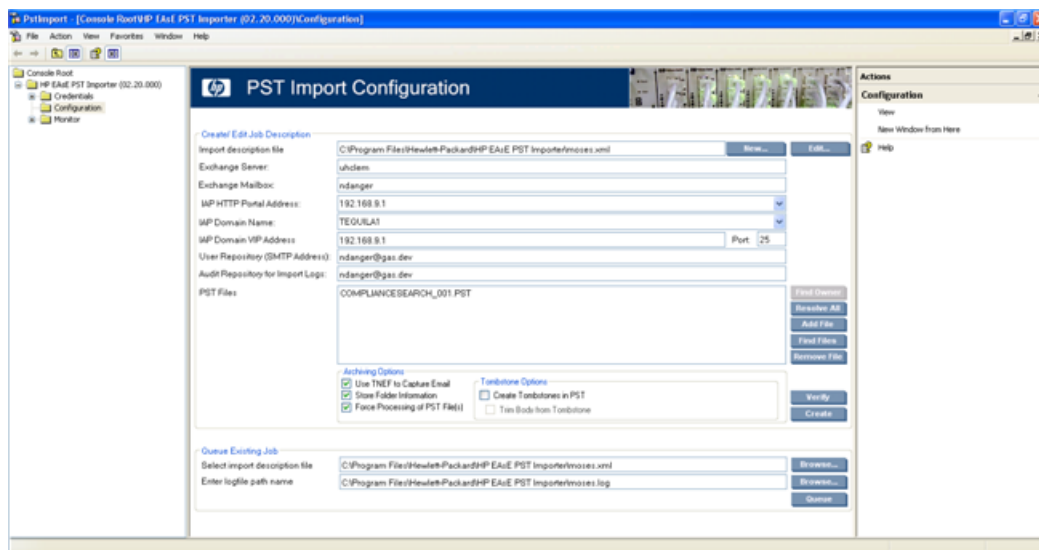
Creating or editing an Import Description file

Follow these instructions to create or edit an Import Description file.

1. Launch the PST Import Manager from the desktop or select **Start**→**All Programs**→**Hewlett-Packard**→**Email Archiving software for Exchange**→**PST Import Tools**→**PST Import Manager**.

The PST Import Manager console appears.

2. Click the **Configuration** link in the main pane, or select **Configuration** from the tree control on the left side of the PST Import Manager console.



3. Click **New** to create a new Import Description file.
To edit an existing Import Description file, click **Edit** and browse to the location of the file you want to modify.
4. Enter the following values.
Note that the values entered override the settings configured in the global configuration file, `\Program Files\Hewlett-Packard\HP EAsE PST Importer\HP EAsE PST Importer.ini`.

Import overrides are placed in the relevant .ini file in \Program Files\Hewlett-Packard\HP EASE PST Importer\PSTLoad.

Field	Description
Exchange Server	The address of the Exchange server or Client Access Server (CAS) used when accessing the Global Address List (GAL) for address resolution. The XML tag is <Server>.
Exchange Mailbox	The mailbox on the Exchange server used when accessing the GAL for address resolution. The XML tag is <Mailbox>. If this address is on an Exchange 2010 server, be sure to use the address of the Client Access Server instead of the address of the mailbox server in the Exchange Server field above.
IAP HTTP Portal Address	The VIP of the IAP domain for which archiving is being set up. The XML tag is <HTTPServer>. This field will be filled in with an appropriate value after you have configured credentials. You can also find the VIP, use the ipToDomainInfo attribute in Domain.jcml.
IAP Domain Name	The IAP domain used when checking for duplicate messages to be submitted. The IAP domain is case-sensitive and must match the domain name in the Domain.jcml file on the IAP. The XML tag is <IAPDomain>. This field will be filled in with an appropriate value after you have configured credentials.
IAP Domain VIP Address (SMTP)	DNS name or IP address of the IAP SMTP portal used to submit messages to the IAP. This is the same value as the ipToDomainInfo attribute used in Domain.jcml. The XML tag is <SMTPServer>. This field will be filled in with an appropriate value after you have configured credentials.
Port	SMTP port number. This setting is optional and the default is 25. The XML tag is <SMTPPort>.
User Repository (SMTP Address)	Repository into which documents in the Select Files To Process list are delivered. The XML tag is <Repository>.
Audit Repository for Import Logs	Name of the audit repository that receives the log file created during the import process. (See "Working with log files" (page 84).) The XML tag is <AuditRepository>.

- Click **Add File**, and select the PST files to be loaded into the IAP.

To search for PST files on your disk, click **Find Files**.

To remove files, select one or more files from the list and click **Remove File**.

NOTE: The PST Import Manager can process PST files even if they are password protected.

- The **Find Owner** button scans SMTP addresses in the PST file to try to determine a likely owner. You can use this information to select a repository to archive the messages into, or you can supply your own.

You can choose the owner from the list of candidates or supply your own.

- To configure archiving and tombstone settings, select the applicable check boxes:

Field	Description
Use TNEF to Capture Email	If selected, messages are stored using Transport Neutral Encapsulation Format. Otherwise, messages are stored using MIME format. See “TNEF message format” (page 20) to learn more about TNEF.
Store Folder Information	If selected, information about the folder where the message resides is stored along with the message. The XML tag is <UseFolderCapture>. Note: Folder capture must also be enabled in the global configuration file (HP EASE PST Importer.ini) and the Domain.jcm1 file on the IAP for folder information to be stored.
Force Processing of PST File(s)	If selected, messages in a previously processed PST file are tombstoned. Under normal circumstances, a PST file is not processed again unless it changes. This option forces PST Loader and PST Import Utility to process the file again. The XML tag is <ForceProcessing>.
Create Tombstones in PST Trim Body from Tombstone	If selected, tombstoning for attachments is enabled. To tombstone the message body and attachments, also select the Trim Body from Tombstone check box. The XML tag is <Tombstone>.

- Click **Verify** to confirm that the settings are correct.
 - The Verify Settings window opens. Click **Start**.
 - After verification is complete, click **Close**.
- Click **Create** to create the Import Description file.

Queuing the Import Description file

Once you have created or edited an Import Description file, the next step is to place it on the queue to be processed. You can specify several PST files in one Import Description file, or you can use multiple Import Description files to import PST files with different settings.

- Click **Browse** next to the Select import description file field.
- Select the Import Description file to queue and click **Open**.
- Click **Browse** next to the Enter logfile path name field.
- Give the log file a name and click **Save**.
The log file contains the results of queuing the Import Description file.
- Click **Queue** to queue the Import Description file

Importing and monitoring

Use the PST Import Monitor pane to:

- Start and stop the file import.
- Display an overview of running tasks, message counts, and other status information showing import progress.
- Draw attention to potential error conditions.
- Generate reports.
- Reset failed processes.

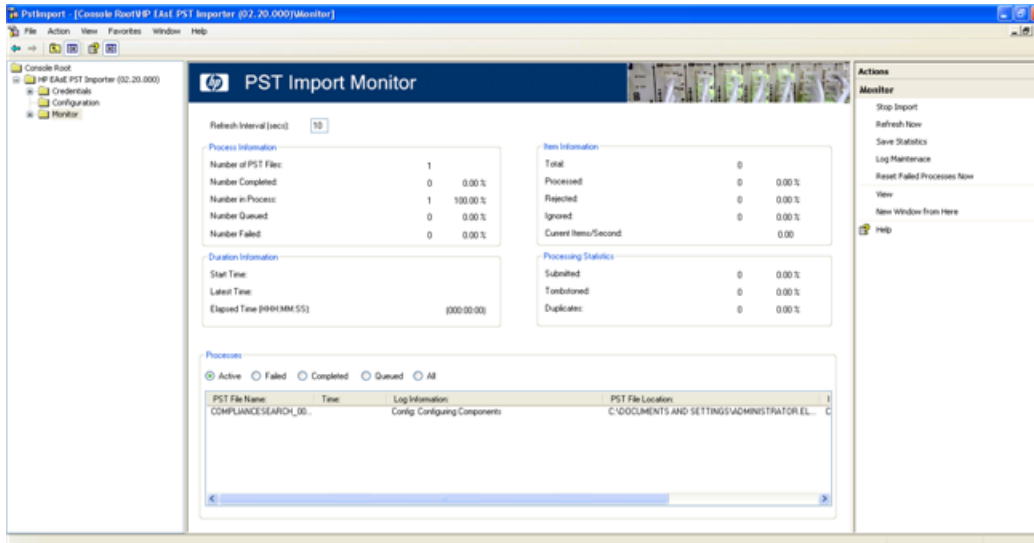
Importing PST data

Follow these steps to start importing data from the PST files to the IAP.

1. Launch the PST Import Manager from the desktop or select **Start**→**All Programs Hewlett-Packard**→**Email Archiving software for Exchange**→**PST Import Tools**→**PST Import Manager**.

The PST Import Manager console appears.

2. Click the **Monitor** link in the main pane, or select **Monitor** from the tree control on the left side of the PST Import Manager console.



3. Click **Start Import** in the Actions pane of the PST Import Manager.

The PST Import Manager starts processing the Import Description files that you queued. If you need to stop the import process, click **Stop Import** in the Actions pane.

Monitoring progress

You can monitor the PST Import Manager's progress. The top part of the PST Import Monitor pane gives you the current status of the process. This information is refreshed according to the value in the Refresh Interval field. If you want to refresh the information immediately, click **Refresh Now** in the Actions pane of the PST Import Manager console.

The lower part of the PST Import Monitor pane displays the each of the PST files being processed. You can use the buttons to display:

- only the active processes,
- only the failed processes,
- only the completed processes,
- the pending processes in the queue,
- all the processes.

Click **Save Statistics** in the Actions pane of the PST Import Manager to save a summary of all the processes.

Working with log files

Each archiving process creates a log file containing warnings, errors, and completion statistics about the process. The log file, sent to the IAP as an email attachment, is delivered to the repository specified by <AuditRepository> in the Import Description file. Once the log file is sent to the IAP, it is deleted from the local machine.

The log files are stored in the directory specified in the Log Maintenance window. To open the Log Maintenance window click **Log Maintenance** in the Actions pane of the PST Import Manager console.

From the Log Maintenance window, you can change the location of the log files, delete all the log files, delete log files older than the maximum retention time.

If an archiving process terminates and is retried, a separate log file is generated. To determine the processing history of a PST file, log into the IAP Web Interface and search the <AuditRepository>.

14 Working with end-user applications

This chapter describes how to use HP EAs Exchange applications.

For information on the client operating systems that HP EAs Exchange supports, see the EAs Exchange Support Matrix.

Overview of the applications

Your company's employees can view and retrieve copies of archived messages from the IAP in several ways, depending on the HP EAs Exchange applications that are installed.

- **IAP Web Interface:** The IAP Web Interface is available for all online clients. Users can view and open archived messages using their Web browser, and export message copies to their mailboxes. These functions do not require software to be installed on client systems. If single sign-on (SSO) is configured, users can open the Web Interface without logging in.
- **Outlook Plug-In:** When the Outlook extension is installed, Outlook users have instant access to archived messages when they are online. When users select an archived message, it is retrieved from the IAP and viewed in memory.

For information on the Outlook extension, see “Installing and configuring the Outlook extension” (page 87).

The Outlook extension also installs the following functions:

- **Outlook Integrated Archive Search:** Integrated Archive Search allows users to search the IAP from Outlook. When single sign-on is configured, users can conduct a search without first logging into the IAP.
See the *HP Email Archiving software for Microsoft Exchange User Guide* for information on using the integrated search function.
- **Archive Cache:** A cache can be installed on clients (normally on mobile computers) so that users can access archived messages offline using Outlook.
- **PST Export Utility:** The export utility lets compliance officers export messages from the IAP Web Interface to PST files.
- **OWA Extension:** When OWA Extension is installed, users can access archived messages using Outlook Web Access. The integrated search function is not available in OWA Extension. For information on OWA Extension, see “Working with HP OWA Extension” (page 100).

Using the IAP Web Interface

The IAP Web Interface lets employees use their Web browser to search for messages archived in their user repositories and any other repositories to which they have access.

The Web Interface portal is set up during system installation and supports HTTPS by default. Users must be logged into your organization's network (either locally or through a VPN) and use a supported Web browser. (See “HP EAs Exchange system requirements” (page 13).)

The IAP Web Interface is most commonly used when compliance officers export messages to a PST file using the PST Export function. The Outlook extension must be installed on the client system to export messages from the IAP. For more information, see “Exporting messages from the IAP” (page 95).

Using single sign-on

IAP single sign-on (SSO) allows logged-on Windows users to search for and view archived messages without logging in to the IAP, either from their Web browser or from Outlook.

If your organization wants to use single sign-on, your HP service representative will set up the application and handle the necessary configuration on the IAP.

Installing and configuring the Outlook extension

Installing and configuring the Outlook extension provides seamless integration to the IAP and facilitates retrieval of tombstoned messages and search results.

To install the Outlook extension, complete all the procedures described in this section for each person using the extension.

NOTE: HP strongly recommends that you always use the latest version of the Outlook extension. The current version of HP EAs Exchange always supports the previous version of the Outlook extension.

Installing the Outlook extension for users

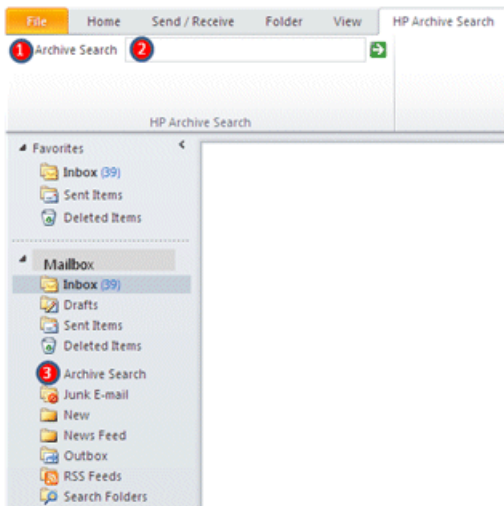
The Outlook extension is a COM Add-In for Microsoft Outlook. You must have local administration privileges to install the extension.

These instructions can be used for either new or updated extension installations.

To install or update the extension on a client:

1. Ensure that Microsoft's .NET Framework 2.0 is installed on the user's machine.
2. Close Outlook if it is open.
3. Install the Outlook extension by running `HP_EAsE_Outlook_Plug-In.msi` in the Outlook Plug-In folder on the HP EAsE Extensions CD.
4. Follow the Install Shield wizard instructions.
5. (Optional) Change the language used in the extension interface by following the steps in "Overriding the language in the Outlook extension user interface" (page 93).
6. Open Outlook and configure the archive options.
See "The Archive Options tab" (page 88).
7. Click **OK**.

8. In Outlook, click **Archive Search** in the Archive Search toolbar.



To display the Archive Search toolbar, click **View**→**Toolbars**→**HP Archive Search**.

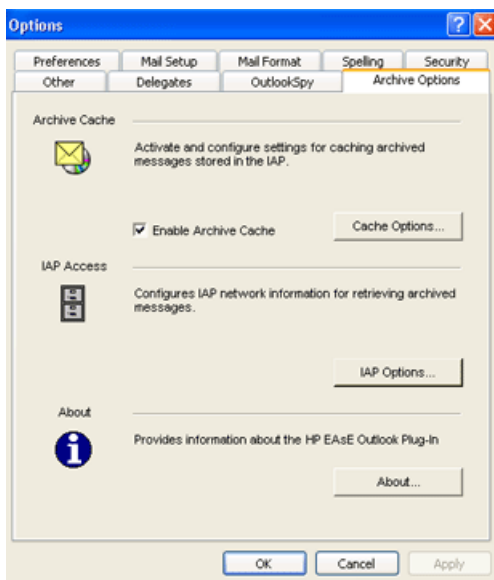
- If SSO has been configured, the Archive Search window appears. If there are problems with the configuration, the Archive Search logon window appears instead.
- If SSO has not been configured, the Archive Search logon window appears. The user must then supply a valid username and password to search the IAP.
- If the IAP hostnames or IP addresses specified in the Archive Options tab are incorrect, a message appears indicating that the Archive Search cannot connect to any of the configured hosts.

The Archive Options tab

The Outlook extension installs an Archive Options tab in the Outlook Options window. Use the options on this tab to configure the Archive Cache, set the IAP host information for message retrieval, and view information about the extension.

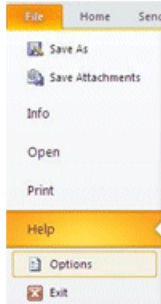
Using the Archive Options tab in Outlook 2003 and 2007

To open Archive Options in Outlook 2003 and 2007, select **Tools**→**Options**, and then click the **Archive Options** tab.

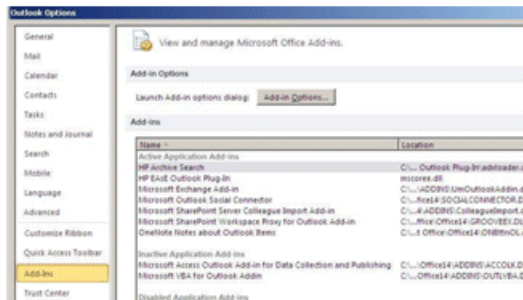


Using the Archive Options tab in Outlook 2010

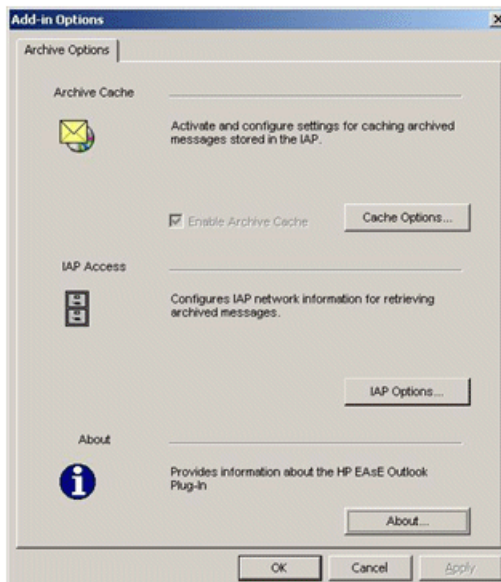
1. Select **File**→**Options**.



2. Select **Add-Ins**→**Add-Ins Options**.



3. On the Add-in Options tab, you can configure caching settings and IAP network information.



Setting host information

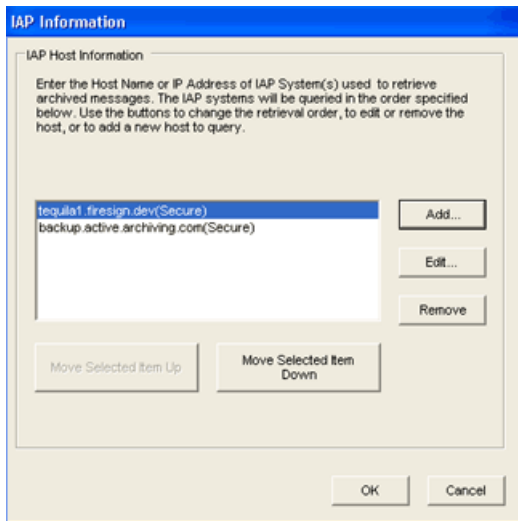
To set the host information, complete the procedure described in this section. Integrated Archive Search, Archive Cache, and PST Export Utility must have certain host information to function correctly.

To configure the host information:

1. In Outlook, select **Tools**→**Options**, and then click the **Archive Options** tab.

2. Click **IAP Options**.

The IAP Information window is displayed.



3. To add a new host (an IAP used to access archived messages), click **Add**. To edit a host, select the host and click **Edit**.

Complete the following steps:

- a. Enter or edit the host name or IP address in the dialog box that appears.
 - b. If the host is using a secure HTTPS connection, select the **Use Secure Connection** check box.
 - c. Click **OK**.
4. To remove a host, select the host and click **Remove**.
 5. To change the order in which the hosts are queried, select a host and click **Move Selected Item Up** or **Move Selected Item Down**.
 6. Click **OK** to apply the settings. Click **OK** again to close the Options dialog box.

Displaying the About dialog box

Use the About dialog box to display the Outlook extension version and administrative mode and turn logging on and off.

To display the About options:

1. In Outlook, select **Tools**→**Options**, and then click the **Archive Options** tab.
2. Click **About**.

The About dialog box displays the following information:

- **Version:** Version of the installed Outlook extension
- **Admin Mode:** Indicates whether the client is running in administrative mode, which is set externally. If set to True, the client is locked and users cannot change most configuration settings on the client. If set to False, the client is unlocked and users are able to change many configuration settings.

The Admin Mode is set in the registry. See “Administrative registry settings” (page 123).

- **Logging Enabled:** Select the check box to allow diagnostic information to be stored for HP support purposes.
3. Click **OK** to apply any changes and close the About dialog box. Click **OK** again to close the Archive Options tab.

Configuring Archive Cache

Archive Cache is a client application that gives Outlook users offline access to their archived messages. It is most useful for employees who use a mobile computer and travel frequently on business.

Archive Cache runs in the background when Outlook is open. When client machines are online, archived messages are pulled from the IAP into the cache, as long as the messages fall within the parameters that are configured for the cache.

When client machines are offline, users can access any archived messages that are in the cache.

If an archived message is not stored in the cache and the client is offline, users see text stating that the message has been archived when they open the tombstone.

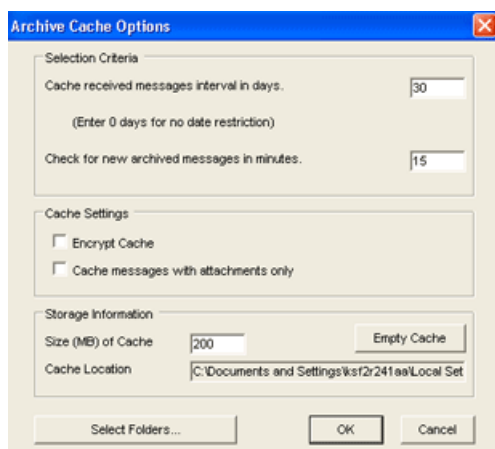
Users might not have access to the most recent messages that have been archived, depending on how often you set archiving to run.

The following steps explain how to enable Archive Cache as well as how to set the Archive Cache options. You may also need to set the host information before you can retrieve tombstoned messages. See [Setting host information](#).

To set the Archive Cache options:

1. In Outlook, select **Tools**→**Options**, and then click the **Archive Options** tab.
2. In the Archive Cache area, click **Cache Options**.

The Archive Cache Options window is displayed.



3. Use the Archive Cache Options window to configure the settings described in the following table:

Table 2 Archive Cache settings

Setting	Description
Cache messages received within the last x days	Selects tombstoned messages received within the specified number of days. Enter 0 to retrieve all tombstoned messages regardless of the received date. Archive Cache deletes previously cached messages that fall outside of this range. This option is based on the date the message was received, not the date it was tombstoned.
Check for new archived messaged every x minutes	Enter how often (in minutes) Archive Cache should inspect the user's mailbox for newly tombstoned messages and messages that have been deleted from the cache.

Table 2 Archive Cache settings (continued)

Setting	Description
Encrypt Cache	Select this check box to use encryption when storing the messages in the cache location on the client machine's file system. Depending on how the user's computer is configured, only the current user can read encrypted messages. Also, depending on how the user's Folder Options are set, the encrypted cached message is likely to appear green in Windows Explorer. NOTE: Archived messages are only encrypted in the cache if Encrypting File System (EFS) is properly configured on the client. If you want to implement this option, consult Microsoft's documentation for information on configuring EFS.
Cache messages with attachments only	Select this check box to retrieve only messages that have attachments. Clearing this check box retrieves all messages. Selecting this option saves space on the user's system and the time necessary to load the Archive Cache. Unless archiving is set to Trim Message Bodies, the message body is visible in the preview pane, and therefore, storing messages without attachments in the Archive Cache is not necessary.
Size (MB) of Cache	Sets the maximum size (in megabytes) of a user's cache. This setting takes precedence over the number of days set above. For example, if the messages selected according to the number of days setting cause the cache to exceed the maximum size, Archive Cache retains only the most recent messages that comply with the configured size.
Empty Cache	Click to delete all messages stored in the cache.
Cache Location	This read-only setting indicates where the Archive Cache is stored on the user's system. For example, on Windows XP the archive cache is in <code>\Documents and Settings\CurrentUser\Local Settings\Application Data\Hewlett-Packard\Cache</code>
Select Folders	Click to select which folders in the user's mailbox Archive Cache inspects for messages.

4. Click **OK** to apply the settings.
5. Select the **Enable Archive Cache** check box. If you want to save the options, but not enable Archive Cache at this time, clear this check box.
6. Click **OK** to save your changes and close the Archive Cache Options window.

NOTE: Users can change these settings unless they are prevented from doing so in the AdminMode registry setting. See "Administrative registry settings" (page 123).

Other cache options can be set in the registry. See "Cache related registry settings" (page 120) for more information.

HP EAsE Archive Cache status icon






Archive Cache provides a status by displaying an icon in the system tray.



Users can hold the cursor over the icon to display status information.

Users can also display a status report or stop Archive Cache from caching archived messages by clicking the icon.

The following icons are used:

Icon	Description
	Default icon.
	Archive Cache is analyzing the mailbox for messages to download and/or downloading them.
	Archive Cache has completed downloading archived messages and is waiting for the next time it should scan for messages.
	Warning. Double-click the icon to display more information.
	Alert. Double-click the icon to display more information.

Registry settings

Default registry settings

Installing the Outlook extension registers the necessary components in the client's `\Program Files\Hewlett-Packard\HP EAsE Outlook Plug-In` folder. Initial registry settings are made in HKEY_LOCAL_MACHINE (HKLM). The first time a user runs Outlook on a machine that has the extension installed, these registry settings are copied from HKLM to HKEY_CURRENT_USER (HKCU).

The settings are maintained on a user-by-user basis in HKCU by selecting **Tools**→**Options**→**Archive Options** in Outlook.

To change default settings for all users, use `regedit` to make changes in HKLM so they are copied and saved to HKCU when each user first runs Outlook.

See “Outlook extension registry settings” (page 120) for the default registry settings that are created when the Outlook extension is installed.

Manually creating other registry settings

Contact HP support if you need to repackage the installation for use with software management tools that do not support the MSI provided with Outlook extension. Note that the SMS file in the Outlook extension folder on the EAsE Extensions CD is a sample only.

Overriding the language in the Outlook extension user interface

When the Outlook extension is installed, the user interface automatically assumes the language that is set in Microsoft Office.

However, there might be cases where you want to change the language in the extension interface. For example, the language in Microsoft Office might be set to English, but a particular user might prefer to search for and/or export archived messages using a German user interface.

The user interface language can be overridden for the Integrated Archive Search and, separately, for the other extension components: Archive Options tab, Archive Cache, and PST Export Utility.

Changing the language in Archive Options tab, Archive Cache, and PST Export Utility

The language override is registered in `HKCU\Software\Hewlett-Packard\Outlook PlugIn\LangID`. `LangID` is a combination of language and locale. For example, a `LangID` of `0816` signifies Portuguese as the language and Portugal as the locale. If Brazil was the locale, the `LangID` would simply be `XX16` because the extension is not currently localized into Brazilian Portuguese. The locale would be dropped and the setting would be neutral.

To add the LangID, follow these steps:

1. Close Outlook.
2. Open `regedit` and navigate to `HKCU\Software\Hewlett-Packard\Outlook Plugin`.
3. In the left pane, select **Outlook Plugin**.
4. In the right pane, right-click and select **New**→**String Value**, and then enter **LangID** for the name.
5. In the right pane, right-click **LangID** and select **Modify**.
6. Change the LangID to a specific or neutral code listed in “Localized languages in Outlook extension” (page 94).
The table contains all languages in which the extension is currently localized.
7. Exit the registry.
8. Open Outlook and observe the changes.

Changing the language in Integrated Archive Search

A registry key must be created to override the language used in Integrated Archive Search.

The code for this key, called `UICultureOverride`, also combines language and locale and is neutral if a particular language/locale combination is not localized.

Follow these instructions to create the key:

1. Close Outlook.
2. Open `regedit` and navigate to `HKCU\Software\Hewlett-Packard\Outlook Plugin\Search`.
3. In the left pane, right-click **Search** and select **New**→**Key**.
4. Name the key **UICultureOverride**.
5. In the right pane, right-click the new **UICultureOverride** key and select **Modify**.
6. Enter the specific or neutral code for the key.

The Integrated Archive Search columns in the table on page “Localized languages in Outlook extension” (page 94) contain the codes that can be used.

7. Exit the registry.
8. Open Outlook and observe the changes.

Localized languages in Outlook extension

Language	Outlook Integrated Archive Search		Archive Options tab/Archive Cache/PST Export Utility	
	UICultureOverride (specific)	Neutral	LangID (specific)	Neutral
English	en-US	en	0409	XX09
French	fr-FR	fr	040C	XX0C
German	de-DE	de	0407	XX07
Spanish	es-ES	es	0C0A	XX0A
Portuguese	pt-PT	pt	0816	XX16
Japanese	ja-JP	ja	0411	XX11
Korean	ko-KR	ko	0412	XX12
Chinese (Simplified)	zh-CHS	zh	0804	XX04
Chinese (Traditional)	zh-CHT	zh	0404	XX04

Using the extension with Citrix Presentation Manager

The Outlook extension supports Citrix Presentation Manager in the configurations listed in the HP EAs Exchange support matrix. (Your HP service representative can provide a copy of the support matrix.)

When Outlook and the extension are installed on a Citrix server, the following conditions apply:

- The extension's logging function should be disabled in the registry to avoid space problems on the server.

Logging is disabled by default when the extension is installed.

Check each of the following locations to verify the logging status:

- In `HKLM\Software\Hewlett-Packard\Outlook PlugIn`, ensure that a path is not listed in `LogFilePath`.
- In `HKLM\Software\Hewlett-Packard\Outlook PlugIn\Cache`, ensure that `LogToDisk` is set to `False`. If this setting is not listed in the registry, cache logging has automatically been set to `False` (the default).
- In `HKLM\Software\Hewlett-Packard\Outlook PlugIn\Search`, ensure that `TraceLevelToLog` is set to `0`. If this setting is not listed in the registry, logging has automatically been set to `0` (the default).
- The export function does not work if users access Outlook via a Citrix session. Outlook and the extension must be installed on a user's local machine for messages to be successfully exported from the IAP Web Interface. Otherwise, the user receives an error message. (See "HP Batch Export error" (page 107).)

For more information on the registry settings, see "Outlook extension registry settings" (page 120).

For more information on the export function, see "Exporting messages from the IAP" (page 95).

Exporting messages from the IAP

The PST Export Utility is installed as part of the Outlook extension. It is an application that is used by a company's compliance officers or system administrators to export copies of archived messages from the IAP to an Outlook PST (Personal Folder) file. The original messages remain on the IAP.

Messages can only be opened in Outlook. They cannot be exported to Outlook Web Access (OWA) or viewed in OWA.

Additionally, messages can only be exported when Outlook and the extension are installed on the machine where the export is performed. For example, users cannot export messages from the IAP if they access Outlook remotely through a Citrix server session.

For information on the registry settings that are used by the PST Export Utility, see "Search and export related registry settings" (page 122).

Overview of the export process

Messages can be exported to a single, default PST folder, or to a set of folders in the PST file.

When messages are exported to a set of folders:

- The following folders are created in the PST file: Inbox, Sent Items, Calendar, Tasks, Journal, Junk E-mail, Contacts, and Drafts.
- Messages are exported to folders with the same name as the folders where the messages were originally located. For example, if a message was located in the Inbox folder before it was archived, it is exported to the Inbox folder in the PST file.

- Messages archived from user-created folders are exported to folders of the same name in the PST file. For example, if you created an Outlook folder named Folder 1, messages that were located in Folder 1 before they were archived are exported to Folder 1 in the PST file.
Note: If you copy a message to another Outlook folder after it has been archived, the message is exported to the folder where it was copied. For example, if a message was archived while it was in Folder 1 and then moved to Folder 2, it would be exported to Folder 2.
- Messages archived from an Outlook Data File (such as an Archive Folder or other Personal Folder File) are exported to a structure that corresponds to the original data file.
- Archived calendar items such as appointments and meetings are exported to the Calendar folder in the PST file. Archived task lists are exported to the Tasks folder in the PST file.
- Messages archived without a folder name are exported to the default PST folder.

Deleting a message removes it from the PST file, but does not delete it from the IAP.

Exporting messages

To export copies of archived messages:

1. Log into the IAP Web Interface and search for the relevant messages.
For search instructions, see the *HP Integrated Archive Platform User Guide*.
2. On the query results page, select the check box next to each item you want to export. Skip this step if you are exporting all items in the query results.
3. Click **More Options** to open the options menu.



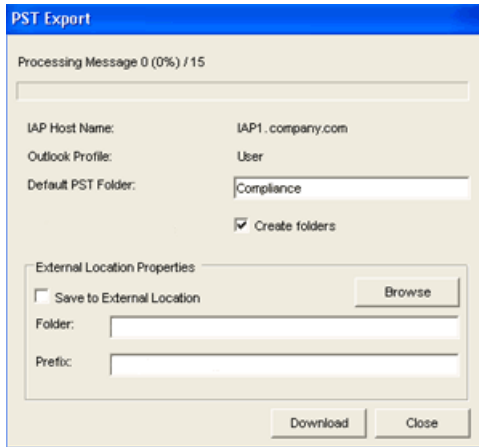
4. To export all results, click **Export All Items**. To export selected items, click **Export Checked Items**.

If this is the first time you are exporting messages, the File Download dialog box is displayed.

5. Click **Open** in the File Download dialog box.

(You might want to make sure that the file download box does not appear when you export messages from the IAP in the future. For example, you can clear the **Always ask before opening this type of file** check box if it is displayed in Internet Explorer.)

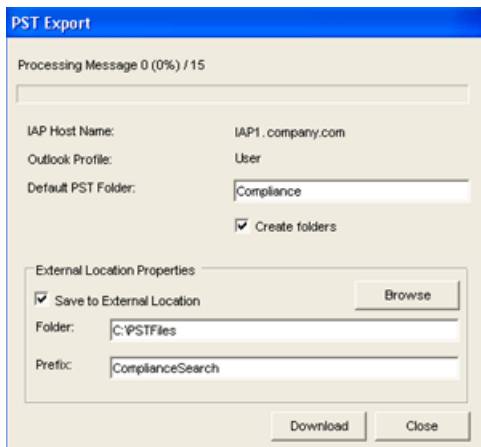
The PST Export window appears.



6. In the **Default PST Folder** box, enter a new name for the default folder.
The default folder name is `Default`. Any messages previously exported to the `Default` folder are deleted unless you change the folder name. A new PST folder is created automatically when a new name is specified in the Default PST Folder box.
Messages are automatically exported to the default folder if the **Create folders** check box is not selected.
7. (Optional) Select the **Create folders** check box for messages to be exported to folders in the PST file.
The folders will have the same name as the folders where the messages were originally located. For more information on the folder option, see [“Overview of the export process” \(page 95\)](#). Note that any messages archived without a folder name are exported to the default PST folder.

8. (Optional) To export messages to an external location (such as a folder on your hard drive or network), follow steps a–c .

If you do not specify an external location, messages are automatically exported to IAP Search Results (IAP Search Results.pst), which you can view in the Outlook Folders List. (See step 13.)



- a. Select the **Save to External Location** check box.
- b. In the **Folder** box, specify a location for the PST file. Enter a path manually or click **Browse** to select a location.

Note: If you add a folder that doesn't currently exist, a dialog box appears at the time the messages are downloaded. Click **Yes** to create the new folder.

- c. In the **Prefix** box, enter a name for the PST file to be generated when you export the messages.

If the PST file contains more than 64,000 messages or the file size exceeds 1.7 GB, a new PST file is created and the files are numbered sequentially (for example, XYZ_001.pst, XYZ_002.pst, and so forth). If there is one file, it is numbered _001 (for example, XYZ_001.pst)

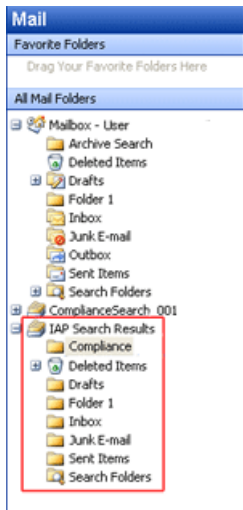
9. Click **Download** to begin the export process.

A progress bar is displayed while the results are downloading.

If you exported the messages to an external location, the Message Export Facility dialog box appears when the download is complete. Click **OK** to review the export log.

10. Click **Close** to close the PST Export window.
11. Click **Close Options** to close the options menu in the IAP Web Interface.

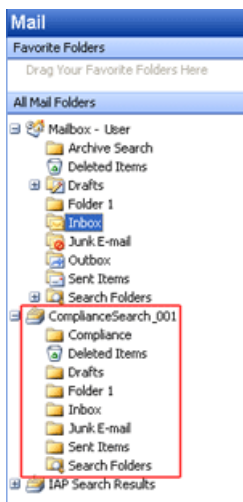
12. If the messages were not exported to an external location:
 - a. Open Outlook.
 - b. Expand **IAP Search Results** in the Folder List, then open the folders to view the messages.



13. If the messages were exported to an external location:
 - a. Open Outlook.
 - b. Select **File**→**Open Outlook Data File**.
 - c. Browse to the location where you exported the PST file.
 - d. Select the PST file, and then click **OK**.

The folder containing the exported messages appears in the navigation pane Folder List.

- e. Expand the PST folder, then open the subfolders to view the messages.



Problems exporting messages

If you receive an error while attempting to export messages, see “HP Batch Export error” (page 107).

15 Working with HP OWA Extension

Microsoft Outlook Web Access is a Web application that provides access to a user's mailbox from any desktop connected to the Internet. OWA Extension provides the same transparent access to a mailbox, and allows users to view tombstoned messages in OWA.

After you have installed OWA, your HP service representative will install and configure OWA Extension. This chapter describes additional configuration options.

System requirements

The following minimum requirements must be met for HP OWA Extension to work on Microsoft Exchange Server 2007:

- Microsoft Exchange Server 2007 Service Pack 1, Update Rollup 5 or later
- OWA Premium service
- Internet Explorer 7.0 and later (Windows) browser

For Microsoft Exchange Server 2010, the HP OWA Extension is supported on the following browsers:

- Internet Explorer 7.0 and later (Windows)
- Safari 3.0 and later (Macintosh)
- Firefox 3.0 and later (Windows 98 and later)
- Chrome 1.0 and later (Windows NT and later)

Exchange 2003, 2007, 2010 all require .NET Framework 2.0 with Service Pack 1 or later.

See the HP EAs Exchange Support Matrix for the complete list of system requirements to install and use OWA Extension with Exchange 2003, 2007, 2010.

NOTE: To ensure that HP OWA Extension work on Microsoft Exchange Server 2007, you must connect to a CAS server, open Microsoft Exchange PowerShell console, and enter the following commands:

```
Get-ExchangeServer | where {$_.IsClientAccessServer -eq $TRUE} |  
ForEach-Object {Add-ADPermission -Identity $_.distinguishedname -User  
"NT AUTHORITY\SYSTEM" -extendedRight ms-Exch-EPI-Impersonation}  
Get-MailboxDatabase | ForEach-Object {Add-ADPermission -Identity  
$_.DistinguishedName -User "NT AUTHORITY\SYSTEM" -ExtendedRights  
ms-Exch-EPI-May-Impersonate}
```

See "Installing on Exchange 2007 and later servers" in the *HP Email Archiving software*

for *Microsoft Exchange Version 2.2 Installation Guide, Second Edition* for detailed information about the procedure in which to run these commands.

Multiple mail stores

The OWA Extension install procedure performed by your HP service representative can configure multiple mail stores. OWA Extension allows access to any number of mail stores configured through a given Exchange server. Typically, a user mailbox is completely within one IAP. OWA Extension determines automatically which IAP store applies to any given user.

The list of Exchange mail servers is entered by the HP service representative in the installation configuration file. The install procedure extracts the System Mailbox information and saves it back into the configuration file.

Multiple IAP systems

Your HP service representative can initially set the OWA Extension configuration for multiple IAP appliances, and set standard and specialized IAP URL templates. Any number of IAPs can be listed. Installed IAP systems have standard URL addresses. To accommodate both standard and special IAP systems, the URL template for any given IAP can be added to the configuration file.

A mail item does not contain a reference to a specific IAP and the user is not aware of the archival state of a selected mail item. For this reason, the location of physical storage is discovered automatically. For a given user, the complete mail store is located in one IAP. During a session, OWA Extension determines automatically which IAP store applies to that user and caches that information for the duration of the session.

Temporary storage in Drafts folder

During normal operation, OWA requires temporary storage for rendering mail parts. For each archived mail item opened in OWA to view or forward, a working copy of the email is created in the user's Drafts folder. This working copy remains after the item is closed. It can be manually deleted or, alternatively, a Policy Engine rule can be scheduled to periodically delete the archived copies from Drafts.

The temporary life of the Drafts copy can only be determined by your individual customer environment. There are some built in constraints in OWA. For example, there is a built in session time out if the user is inactive for about 30 minutes. The actual time out is determined by your OWA setup and users' mode selection when they log in.

The Drafts copy is saved in the `/Drafts/RissTemp` subfolder. If the folder doesn't exist, it is created. If the subfolder cannot be created, the Drafts folder is used.

Deleting temporary Drafts copies using a rule

A Policy Engine rule defines clean up of temporary items in the Drafts folder. This rule is for external housekeeping only. It should be configured only in the Policy Engine; an event should **not** be created in the EAsE software.

To create the rule:

1. Log on to the Archive Gateway.
2. Open Policy Engine.
3. In the left pane, expand **Management**, and select **Rules**.
4. In the right pane, right-click and select **Other Tasks**→**Import Rule**.
5. Select `EASE_Cleanup_OWA_Drafts_Template.mr` and click **Open** to import the rule into Policy Engine.
6. Click the Information Stores tab and select the mailboxes to be covered by the rule.
7. Click **OK** to save the rule.

It is not necessary to make any other changes. The rule is predefined to search the Drafts folder and subfolders for OWARISS temporary items and delete them.

8. Schedule the rule, or run it immediately.

Creating a rule with the `EASE_Tombstone_Delete` template

The `EASE_Tombstone_Delete_Template.mr` is a Policy Engine template. It resides in the `templates` folder in the installation directory.

Use this template and rule to remove unwanted tombstoned messages. To create a rule using this template:

1. Log on to the Archive Gateway.
2. Open the Policy Engine.

3. In the left pane, expand Management, and select **Rules**.
4. Right-click in the right pane and select **Other Tasks**→**Import Rule** .
5. Select **EAsE_Tombstone_Delete_Template.mr** from the Selective Archiving\Templates folder and click **Open** to import the rule into the Policy Engine
6. Click the Information Stores tab and select the mailboxes to be included in the rule.
7. Click the Folders tab and specify which folders to include (or exclude) if the entire mailbox should not be scanned.
8. Click the Conditions tab to add criteria for selection of tombstoned messages (For example, Received Date older than 2 years).
9. Click the Schedule tab to establish when the rule will run, and enable it for scheduling.
10. Click **OK** to save the rule.

Making tombstoned mail items visible in OWA

If your system contains items tombstoned prior to EAsE 1.5.x, execute the Tombstone Maintenance event and associated rule to make tombstoned messages visible in OWA.

See “Configuring tombstone maintenance events” (page 63) for instructions on creating a Tombstone Maintenance event and rule.

NOTE: For OWA 2007 and later, OWA Premium is required to retrieve tombstoned messages. OWA Extension does not support retrieval of archived appointment/calendar items in OWA 2007 and later.

Viewing the Web.config file in Exchange 2007 and later installations

The following OWA Extension configuration settings are added to \Exchange Server\ClientAccess\Owa\forms\PERSISTMailItem\Web.config.

- <IAPServers>

A typical system can have one or more IAPs. The <IAPServers> section of Web.config contains a list of IAP appliances. The syntax for an entry is a keyname followed by the protocol and IAP name. The keyname identifies the IAP and appears in the error page if a document fails to load. If there is a special template in the <appSettings> section, the keyname must be the same for the appliance and its corresponding template.

For example:

```
<IAPServers>
  <add key="000001" value="http://15.43.213.6" />
  <add key="000002" value="https://15.43.10.231" />
</IAPServers>
```

- <appSettings> which includes:

- The Exchange server where OWA Extension is deployed.

For example:

```
<add key="Exchange Server" value="ILM205" />
```

- The domain name of the Exchange server.

For example:

```
<add key="Domain" value="ROSEILM36.COM" />
```

- The IAP URL template.

For standard installations, the only setting in this section is the default setting:

```
<add key="IAPDOCTEMPLATEURL" value="#PHOST#/externalAPI/servlet/
DocumentRetrievalServlet?documentURL=#REF#" />
```

If a custom template is defined, the template keyname must be the same as the corresponding IAP appliance keyname. Do not add a custom template unless instructed to do so by your HP service representative.

Working with the asp.config file in Exchange 2003 installations

The `asp.config` file, used in OWA Extension for Exchange 2003, contains several configuration settings. It is located in the Install folder, usually in the `owariss` directory.

IAP appliances

A typical system can have one or more IAPs. The RISS section of `asp.config` contains a list of IAP appliances. The syntax for an entry is a keyname followed by the protocol and IAP name. The keyname identifies the IAP. If there is a special template in the next section, the keyname must be the same for the appliance and its corresponding template. The keyname also shows up in the error page if a document fails to load.

The syntax is: `Symbol=<protocol>://<IAP>` where `<protocol>` can be `http` or `https`.

For example:

```
[RISS]
mbarney=http://mbarney
papoon=http://papoon
```

URL templates

The Template section of `asp.config` contains custom OWA Extension URL templates. For standard installations, the only setting in this section is the default setting.

If a custom template is defined, the template keyname must be the same as the corresponding IAP appliance keyname.

-
- ❗ **IMPORTANT:** Do not add a custom template unless instructed to do so by your HP service representative.
-

ASP pages

Use the ASP section of `asp.config` to change the appearance of IAP tombstoned items, and to set the `UsePropertyTemplate` flag.

For OWA Extension, a message that is archived on the IAP optionally displays the IAP icon. You can disable the appearance of the icon by changing the `Icon` configuration setting.

```
[ASP]
;Icon allows the IAP icon to be turned on/off
;Default=On
Icon=On
;UsePropertyTemplate causes the unset flag to be corrected for Exchange 2000
;Default=TRUE
;Set to FALSE for Exchange 2003
UsePropertyTemplate=TRUE
```

Changing the ASP time-out in Exchange 2003 installations

The amount of time it takes to retrieve and reconstruct an email with large attachments is directly related to the CPU size of the Exchange server. The default attachment limit for a 500 MHz server is about 3 MB. The default attachment limit for a 3 GHz server is about 10 MB. (These limits are the default based on the configuration of the OWA Extension site in the IIS Manager.) If the maximum attachment size is exceeded, the retrieval times out.

If you anticipate attachments to be larger than these limits, the default ASP time-out can be adjusted.

1. On the Exchange server, open the IIS Manager.
2. Navigate to **Web Sites**→**Default Web Site**, and right-click the OWA Extension (OWA RISS) site.
3. Select **Properties**.
4. In the **Virtual Directory** tab, click **Configuration**.
5. Click the **Options** tab.
6. Look for the ASP Script Timeout adjustment.
The default is 90 seconds. The setting can be increased to allow larger attachments.
7. After changing the setting, click **OK**.
It is not necessary to restart IIS.

NOTE: The time-out settings do not need to be manually adjusted for OWA 2007 and later.

Browser functionality

OWA has two modes of operation, Premium and Basic. The mode of operation and configuration is an enterprise decision and is described in the Microsoft OWA install manual. Premium operation has the look and feel of Microsoft-Outlook. Basic operation is similar, but might have reduced functionality.

For Microsoft Exchange Server 2003, HP strongly recommends use of OWA Premium on Microsoft Internet Explorer.

For Microsoft Exchange Server 2007 and later, OWA Premium is required to retrieve tombstoned messages.

Multi-user support

Any number of users can access their email through OWA at the same time. Limits are only dependent on the size and performance of the underlying Microsoft Exchange servers and corresponding hosting Web site. Because this is a Web access script, there are expected small delays that typically occur during Web site access.

Large attachments

OWA 2007 and later users might not be able to retrieve messages in OWA if the messages contain attachments larger than 70 MB. This situation can occur whether there is one attachment or several smaller attachments totalling 70 MB or more.

16 Troubleshooting

This chapter describes HP EAs Exchange troubleshooting information.

OWA 2007 users cannot open folders containing tombstoned messages

Microsoft Exchange Server 2007 SP1, Update Rollup pack 5 must be installed for OWA Extension to work properly with OWA 2007.

Otherwise, OWA users receive an error message when they open folders containing tombstoned messages (IPM.Note).

Folders with a mix of tombstoned and non-tombstoned messages can sometimes be opened, but the tombstoned email is not shown on screen. A dialog box appears saying, "OWA can not complete your request."

This problem does not occur for folders containing other tombstoned items, such as documents or tasks.

OWA 2007 and later users cannot retrieve tombstoned messages

OWA Premium is required for OWA 2007 and later users to retrieve tombstoned messages from the IAP.

Any appointment or calendar items that were selectively archived cannot be retrieved in OWA 2007 and later. However, they can be retrieved using Outlook or the IAP Web Interface.

Behavior in Microsoft Exchange Server 2007 and later impacts detection of message duplicates

Overview

Microsoft Exchange stores the client submit time (the sent date) of each message in a MAPI date property. This property is granular to the millisecond.

In pre-2007 versions of Exchange, any message that was sent, journaled, or received in a recipient mailbox had equivalent values—to the millisecond—in each instance of the message.

In Exchange 2007 and later, however, only Sent messages retain the millisecond portion of the client submit time. Journaled messages and items received in a recipient mailbox do not provide millisecond granularity. The value is truncated.

This difference between the two Exchange versions impacts calculation of the hash, the computed signature that uniquely identifies a message in EAs Exchange and the IAP. The same message could have different hashes, and therefore not be detected as a duplicate when archived in the IAP.

HP RIM 1.x

1.x versions of the archiving software (known as Reference Information Manager or RIM) read the client submit time MAPI property and rounded the milliseconds to the nearest second (≥ 500 milliseconds caused the second to be rounded upward). This rounded date value was used in computation of the message hash.

- If you performed compliance archiving in a mixed Exchange 2003/2007 and later environment, duplicate messages with different hashes might have been created if multiple journal mailboxes were hosted on different versions of Exchange.
- If you performed selective archiving of Exchange 2007 and later mailboxes, messages archived from the Sent Items folder might have introduced duplicates (with different hashes) into the IAP system.

HP EAs Exchange 2.x

In HP EAs Exchange 2.x, the message hash is computed in the following ways:

- Standard email messages (IPM.Note) archived from Exchange 2007 and later servers:
 - All Sent items have the hash computed with the milliseconds truncated. This includes Sent items that are archived from an Exchange 2007 and later server and Sent items in an Exchange 2007 and later server mailbox that are imported using the PST Import Manager.
 - All non Sent items use the hash logic from HP RIM 1.x, which includes millisecond values.
- Non-standard messages (non IPM.Note) archived from Exchange 2007 and later servers:
Non-standard messages such as calendar items, tasks, etc. have the hash computed with milliseconds truncated, regardless of the sent state or server location.

Any Sent items archived from an Exchange 2007 and later server might not be seen as hash equivalents of Sent items received or archived from previous versions of Exchange. If you are planning to migrate to Exchange 2007 and later, we suggest that you archive all messages in the Sent Items folder before migration. This will minimize the number of duplicates entering the system.

In mixed Exchange 2003/2007 and later environments, HP cannot guarantee hash equivalency because of the inconsistent date values generated between the two Exchange versions. We do not recommend maintaining a mixed environment for a prolonged period because of this inconsistency.

HP is working with Microsoft on this behavior. We will consider making further modifications in a future EAs Exchange release, depending on the resolution of this issue.

Selective archiving does not process all folders in user mailbox

By default, Policy Engine keeps mailbox folders open after querying them during the Selective Archiving process. In Exchange Server 2003 SP2, no more than 500 folders can be open at the same time on a client. Therefore, on servers running Exchange 2003 SP2, user mailboxes that contain more than 500 folders are not completely processed during Selective Archiving.

To allow all user mailboxes to be mined completely, follow these steps on each Archive Gateway:

1. Log on to the Archive Gateway as the archive service account.
2. Open `regedit`.
3. In the Registry Editor, navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Sherpa Software Group\Mail Attender for Exchange Enterprise Edition\Service`.
4. Add the following string value: `Keep Mailbox Folders Open`
5. Set the value to `False`.
6. Exit the registry.
7. Restart the Mail Attender Enterprise service for the registry setting to take effect.

Changes not captured in email attachments

In Microsoft Outlook it is possible for end users to modify email attachments on Exchange servers "in-place" without saving the attachment to their desktop/server or sending the message through the Exchange MTA (Reply, Forward, etc.). HP EAs Exchange does not automatically capture these changes. The intent of the software is to capture transactional messages and not privately modified attachments. If in-place attachment modification is common practice in your organization, contact HP support for information on how to capture these changes. If you are running both Compliance Archiving and Selective Archiving, in-place modifications to attachments might not be saved.

Users cannot find messages sent to a distribution list

In EAs Exchange Selective Archiving and PST Import, distribution lists are not expanded during archiving. (Distribution lists are only expanded during Compliance Archiving, if envelope journaling

is implemented.) For messages with distribution lists to be archived in each recipient's IAP repository, the EnsureOwnerReceipt parameter in the global configuration file must be set to `True`.

EnsureOwnerReceipt ensures a message is archived whenever the mailbox owner's SMTP address is not shown in the recipient list.

In EAs Exchange 2.0 and 2.1, EnsureOwnerReceipt is automatically enabled for Selective Archiving and PST Import. However, if this parameter was not enabled in earlier versions of the software, messages sent via a distribution list were not selectively archived to each recipient's repository, and users will not find these messages when searching their IAP repository.

To assign previously-stored messages to IAP user repositories, contact HP Support.

Note that reprocessing the messages on the IAP does not solve this issue, because the mailbox owner is not specified.

DiskSpaceBuffer error

If a "DiskSpaceBuffer Threshold has been reached" error is reported during Selective Archiving and folder capture is enabled, the IAP is attempting to update folder information on messages that are in a closed smart cell. Messages impacted by the error cannot be processed by the HP EAs Exchange software.

An example of a folder update would be a user moving archived messages from one Outlook folder to another. The next time the folders were archived, the IAP would attempt to update the folder name on the previously-archived messages.

Folder changes can be made in a closed smart cell until the available disk space drops under an established watermark. At that point, the IAP rejects the folder changes with a disk full error.

An override to the disk full behavior can be configured on the IAP by HP technical support.

HP Batch Export error

If the following error message appears when exporting messages from the IAP Web Interface:



Confirm that:

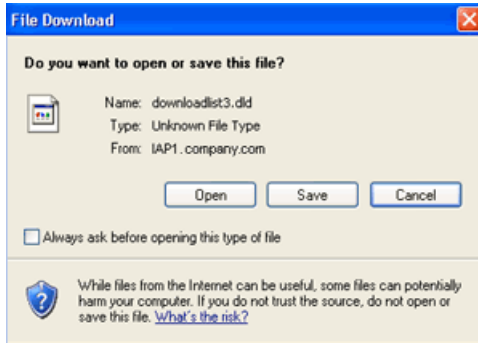
- The user is not accessing Outlook through a remote application session, for example a Citrix server session.
The export function does not work if users open the IAP Web Interface from a browser on the local computer, but Outlook and the extension are installed on a remote server.
- The Outlook extension is installed on the local computer.
Outlook and the extension must be installed on the local computer for the export function to work.

If Outlook and the extension are installed on the local computer, verify that the Windows system has associated the `.ald` file type with HPBatchExport, which is used to export archived messages.

To verify the file type:

- (Windows Vista) In the Control Panel, select **Default Programs**, and then click **Associate a file type or protocol with a program** to view the file type list.
- (Other Windows operating systems) In the Control Panel, select **Tools** → **Folder Options**, and then click the **File Types** tab to view the file type list.

If the DLD file type is not shown in the file type list or is not associated with HPBatchExport , *Unknown File Type* appears in the dialog box when you export messages from the IAP.



Creating a file type association

Create an association for the DLD file type if DLD is not shown in the file type list.

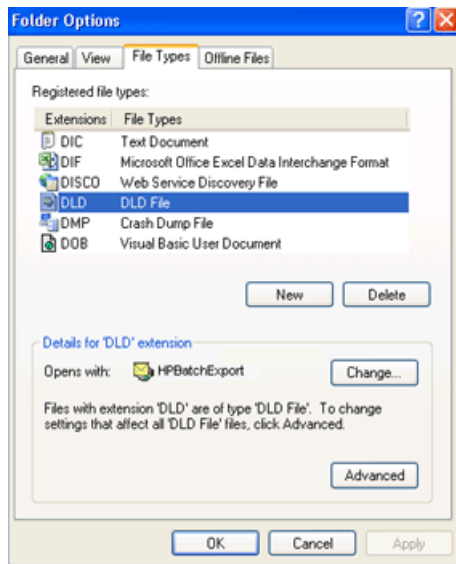
Windows Vista:

1. Right-click the download list file that is created in the temporary Internet file folder.
When you select **Export All Items** or **Export Checked Items** in the IAP Web Interface, links to the archived messages you select are placed in a special download file called a DLD file. The export tool uses these links to export copies of the messages.
For example, in Internet Explorer the path would be Documents and Settings\[user id]\Local Settings\Temporary Internet Files\downloadlist2.dld).
2. Select **Properties**.
3. In the **General** tab, click **Change**.
4. Click **Browse**, and then browse to the following location:
`\Program Files\Hewlett-Packard\HP EAsE Outlook Plug-In.`
5. Select **HPBatchExport.exe**, and then click **Open**.
6. Click **OK** to associate the DLD file type with HPBatchExport.

Other Windows operating systems:

1. In the Control Panel, select **Tools** → **Folder Options**, and then click the **File Types** tab.
2. Click **New**.
3. In the File Extension box, enter **DLD**, and then click **OK**.
4. In the Details for 'DLD' extension area, click **Change**.
5. Click **Select the program from a list** in the dialog box that appears, and then click **OK**.
6. Click **Browse** in the Open With dialog box.
7. Browse to the following location:
`\Program Files\Hewlett-Packard\HP EAsE Outlook Plug-In.`
8. Select **HPBatchExport.exe**, and then click **Open**.

9. Click **OK** to associate the DLD file type with HPBatchExport.



Changing the file type association

If DLD is listed as a file type, but is associated with another program, change the association:

Windows Vista:

1. In the Control Panel, select **Default Programs** and then click **Associate a file type or protocol with a program**.
2. Select the **.dld** extension, and then click **Change program**.
3. Click **Browse** in the Open With dialog box.
4. Browse to the following location:
`\Program Files\Hewlett-Packard\HP EASE Outlook Plug-In.`
5. Select **HPBatchExport.exe**, and then click **Open**.
6. Click **OK** to associate the DLD file type with HPBatchExport.

Other Windows operating systems:

1. In the Control Panel, select **Tools** → **Folder Options**, and then click the **File Types** tab.
2. Select the **DLD** extension in the File Types tab, and then click **Change**.
3. In the **Open With** dialog box, click **Browse**.
4. Browse to the following location:
`\Program Files\Hewlett-Packard\HP EASE Outlook Plug-In.`
5. Select **HPBatchExport.exe**, and then click **Open**.
6. Click **OK** to associate the DLD file type with HPBatchExport.

A Indexed document and content types

This appendix describes document and message types.

Indexed document types

You can search the contents of a message and attachment only if the contents have been indexed. Indexing catalogs the words in a message and attachment to prepare them for later searching.

Exchange items

In Compliance Archiving, HP EAs Exchange indexes the following types of Exchange items:

- Standard Email (IPM.Note)
Secure and encrypted email is not indexed
- Non-Delivery Reports (REPORT.IPM)
- Meeting Requests (IPM.Schedule)
- Task Requests (IPM.TaskRequest)

In Selective Archiving and PST Import, HP EAs Exchange indexes the following types of Exchange items:

- Standard Email (IPM.Note)
Secure and encrypted email is not indexed
- Calendar items (IPM.Appointment)
- Tasks (IPM.Task)
- Documents (IPM.Document)
- Public Folder Items (IPM.Post)

Indexed file types

In addition to email messages, the following types of message attachments are indexed:

- Plain text files
- Rich text files (.rtf)
- HTML (HyperText Markup Language) files
- Files used by the following Microsoft Office programs, including Office 2007: Word, Excel, and PowerPoint
- PDF (Portable Document Format) files viewed with Adobe Acrobat Reader
- Zip files
For zip files and embedded messages, the content inside the files is expanded and indexed.
- Embedded messages (RFC 822 messages)

Invisible source-code words, such as HTML markup tags, are ignored in indexing.

Document formatting usually has no bearing on indexing, and only the words you see in an email or attachment are indexing candidates. However, when a dropped cap (a large initial capital letter) is used in a Microsoft Word document, the word with the dropped cap is indexed as two separate words. This is because Word puts a dropped cap into a text box to set it off from the surrounding paragraph. In the following example, XYZcorp would be indexed as "X" and "yzcorp."

XYZcorp has posted strong results in the second quarter. Chief Executive Officer Bob Brown announced today that the company is on track to beat

The following types of attachments are not indexed:

- Graphic files
- Music files
- Video files
- Any other file type that is not included in the list of indexed file types

These files can be archived, but can be searched only by using external identifying information, such as the file name or file extension.

Message MIME types

The MIME Content-Types shown in IAP indexed document MIME types are indexed and each corresponds to one of the indexed document types.

An email message that is entirely plain text, not MIME, is also indexed.

Table 3 IAP indexed file types and MIME types

File extension	File type	MIME content-type
.xml	XML document	text/xml
.txt	Plain text file; treated as ISO-8859-1 unless otherwise specified	text/plain
.htm, .html, .stm	HTML document	text/html, rtf/html
.rtf	Rich text format	rtf/text, application/rtf
.dat	TNEF (for Microsoft Exchange)	ms/tnef
.mht, .mhtml, .nws, .eml	Email message	message/RFC 822
.doc, .dot	Microsoft Word 97-2003 document	application/msword
.xla, .xlc, .xlm, .xls, .xlt, .xlw	Microsoft Excel 97-2003 document	application/vnd.ms-excel, application/ms-excel
.pot, .pps, .ppt	Microsoft PowerPoint 97-2003 document	application/vnd.ms-powerpoint, application/vnd.mspppt
.pdf	Adobe Portable Document format	application/pdf
.zip	ZIP archive	application/zip
.docx	Microsoft Word 2007 document	application/vnd.openxmlformats-officedocument.wordprocessingml.document
.docm	Microsoft Word 2007 macro-enabled document	application/vnd.ms-word.document.macroEnabled.12
.dotx	Microsoft Word 2007 template	application/vnd.openxmlformats-officedocument.wordprocessingml.template
.dotm	Microsoft Word 2007 macro-enabled document template	application/vnd.ms-word.template.macroEnabled.12
.xlsx	Microsoft Excel 2007 workbook	application/vnd.openxmlformats-officedocument.spreadsheetml.sheet

Table 3 IAP indexed file types and MIME types (continued)

File extension	File type	MIME content-type
.xlsm	Microsoft Excel 2007 macro-enabled workbook	application/vnd.ms-excel.sheet.macroEnabled.12
.xltx	Microsoft Excel 2007 template	application/vnd.openxmlformats-officedocument.spreadsheetml.template
.xltm	Microsoft Excel 2007 macro-enabled workbook template	application/vnd.ms-excel.template.macroEnabled.12
.xlam	Microsoft Excel 2007 add-in	application/vnd.ms-excel.addin.macroEnabled.12
.pptx	Microsoft PowerPoint 2007 presentation	application/vnd.openxmlformats-officedocument.presentationml.presentation
.pptm	Microsoft PowerPoint 2007 macro-enabled presentation	application/vnd.ms-powerpoint.presentation.macroEnabled.12
.ppsx	Microsoft PowerPoint 2007 slide show	application/vnd.openxmlformats-officedocument.presentationml.slideshow
.ppsm	Microsoft PowerPoint 2007 macro-enabled slide show	application/vnd.ms-powerpoint.slideshow.macroEnabled.12
.potx	Microsoft PowerPoint 2007 template	application/vnd.openxmlformats-officedocument.presentationml.template
.potm	Microsoft PowerPoint 2007 macro-enabled presentation template	application/vnd.ms-powerpoint.template.macroEnabled.12
.wpd	Corel WordPerfect for Windows – versions through Version 12.0, X3	application/wordperfect, application/wpd
.qpw, .wb1, .wb2, .wb3	Corel Quattro Pro for Windows – versions through Version 12.0, X3	application/qpw, application/wb1, application/wb2, application/wb3
.shw	Corel Presentations – versions through Version 12.0, X3	application/presentations

Additional indexing detail/limitations for Microsoft Office 2007

Office 2007 supported features and properties

Table 4 Microsoft Office supported features

Feature	Microsoft Word	Microsoft PowerPoint	Microsoft Excel
Contents	Yes	Yes	Yes
Table	Yes	Yes	Yes
Textbox	Yes	Yes	Yes
Header/Footer	Yes	Yes	Yes
Comment	Yes	Yes	Yes
FootNote/EndNote	No	No	No
Signature	Yes	Yes	No
Chart	Yes	Yes	Yes
Object (Microsoft Office, WordPad ...)	Yes	No	Yes

Table 4 Microsoft Office supported features *(continued)*

Feature	Microsoft Word	Microsoft PowerPoint	Microsoft Excel
Embedded Objects (OLE)	Yes	Yes	Yes
Notes	N/A	Yes	N/A
WordArt	Yes	Yes	Yes
SmartArt	No	No	No
Sheet's name	N/A	N/A	Excel 2007: No Excel 97-2003: Yes

Table 5 Microsoft Office supported properties

Type	Property	Microsoft Word	Microsoft PowerPoint	Microsoft Excel
Document Properties	Author	Yes	Yes	Yes
	Title	Yes	Yes	Yes
	Subject	Yes	Yes	Yes
	Keywords	Yes	Yes	Yes
	Category	Yes	Yes	Yes
	Status	Yes	Yes	Yes
	Comments	Yes	Yes	Yes
	Location	No	No	No
Advanced Properties: General	Type	No	No	No
	Location	No	No	No
	Size	No	No	No
	MS-DOS name	No	No	No
	Created	No	No	No
	Modified	No	No	No
	Accessed	No	No	No
	Attributes	No	No	No
Advanced Properties: Statistics	Created	Yes	Yes	Yes
	Modified	Yes	Yes	Yes
	Accessed	Yes	Yes	Yes
	Printed	Yes	Yes	Yes
	Last saved by	Yes	Yes	Yes
	Revision number	Yes	Yes	Yes
	Statistics	Yes	Yes	Yes

Table 5 Microsoft Office supported properties *(continued)*

Type	Property	Microsoft Word	Microsoft PowerPoint	Microsoft Excel
Advanced Properties: Custom	Checked by	Yes	Yes	Yes
	Client	Yes	Yes	Yes
	Date completed	Yes	Yes	Yes
	Department	Yes	Yes	Yes
	Destination	Yes	Yes	Yes
	Disposition	Yes	Yes	Yes
	Division	Yes	Yes	Yes
	Document number	Yes	Yes	Yes
	Editor	Yes	Yes	Yes
	Forward to	Yes	Yes	Yes
	Group	Yes	Yes	Yes
	Language	Yes	Yes	Yes
	Mailstop	Yes	Yes	Yes
	Office	Yes	Yes	Yes
	Owner	Yes	Yes	Yes
	Project	Yes	Yes	Yes
	Publisher	Yes	Yes	Yes
	Purpose	Yes	Yes	Yes
	Received from	Yes	Yes	Yes
	Recorded by	Yes	Yes	Yes
	Recorded date	Yes	Yes	Yes
Reference	Yes	Yes	Yes	
Source	Yes	Yes	Yes	
Status	Yes	Yes	Yes	
Telephone number	Yes	Yes	Yes	
Typist	Yes	Yes	Yes	
Advanced Properties: Contents	Document Contents	Yes	Yes	Yes

Table 5 Microsoft Office supported properties *(continued)*

Type	Property	Microsoft Word	Microsoft PowerPoint	Microsoft Excel
Advanced Properties: Summary	Title	Yes	Yes	Yes
	Subject	Yes	Yes	Yes
	Author	Yes	Yes	Yes
	Manager	Yes	No	Yes
	Company	Yes	No	Yes
	Category	Yes	Yes	Yes
	Keywords	Yes	Yes	Yes
	Comments	Yes	Yes	Yes
	Hyperlink base	Word 2007: Yes Word 97–2003: No	Yes	Excel 2007: Yes Excel 97–2003: No
	Template	Word 2007: Yes Word 97–2003: No	Yes	No

Microsoft Office 2007 indexing limitations

Office 2007 documents that were archived before IAP 1.6.1 or 2.0 was installed are not indexed or content searchable.

In addition, some documents converted to Microsoft Office version 2007 by the Office File converter might not be properly indexed.

The following items are not yet supported:

- Notes within PowerPoint slides
- Spreadsheet names within Excel
- Some embedded OLE objects
- Certain text within Excel charts

B Character support

The following table lists the character sets that are supported for Exchange messages archived in the IAP.

Table 6 HP EAsE and IAP character set support

Supported character set	Description
ISO-8859-1	Western European, extended ASCII
ISO-8859-15	Western European, variant of ISO-8859-1
WINDOWS-1252	Western European (Windows variant of ISO-8859-1)
US-ASCII	7-bit American Standard Code for Information Interchange
UTF-8	Unicode/Universal Character Set (all modern languages)
ISO-8859-2	Eastern European
KOI8-R	Cyrillic (Russian and Bulgarian)
ISO-8859-5	Cyrillic (Bulgarian, Belarusian, Russian)
WINDOWS-1251	Cyrillic
WINDOWS-1254	Turkish (Windows variant of ISO-8859-9)
ISO-8859-9	Turkish
GB18030	Chinese (Mainland)
BIG5	Chinese (Taiwan)
GB2312	Chinese (Mainland)
GBK	Chinese, simplified extension of GB2312 (Mainland)
ISO-2022-KR	Korean
EUC-KR	Korean
KS_C-5601-1987	Korean
ISO-2022-JP	Japanese
EUC-JP	Japanese
SHIFT-JIS	Japanese

C PST Import Manager: Archive Request file specifications

The XML tags used in the Archive Request file are listed in this section. You can generate the file using the PST Import Manager interface or create the file manually using Sample Archive Request file as a guide.

- Settings description
- Sample Archive Request file

Settings description

All settings specified under <Header> can be overridden at the <FileSpec> level. All settings described in the Archive Request file are required in either the <Header> or <FileSpec> sections unless otherwise noted.

Table 7 Tags in Archive Request file header

Tag	Description
<Version>	Version number associated with this Archive Request format. The current version is 2.0.
<Server>	Exchange server used when accessing the GAL for address resolution.
<Mailbox>	Mailbox on Exchange server used when accessing the GAL for address resolution.
<SMTPServer>	DNS name or IP address of the IAP SMTP portal used to submit messages to the IAP. This is the same value as the ipToDomainInfo attribute used in Domain.jcml.
<SMTPPort>	(Optional) Port number used with <SMTPServer>. The default is 25.
<HTTPServer>	The VIP of the IAP domain for which archiving is being set up, followed by the non-sticky port number. For example, 192.168.9.8:81. This enables load balancing message-by-message.
<IAPDomain>	IAP domain used when checking for duplicate messages to be submitted. IAP domain is case-sensitive and must match the domain name in Domain.jcml.
<Repository>	Repository into which documents listed under <FileSpec> are delivered.
<AuditRepository>	Name of the repository that receives processing logs created during the PST import process.
<UseTNEF>	Specifies if submitted messages are stored in TNEF format. <i>True</i> indicates TNEF format is used for archiving standard email messages. <i>False</i> indicates TNEF format is not used for archiving standard email messages. All nonstandard messages (appointments, tasks, etc.) are archived automatically using TNEF. See "TNEF message format" (page 20) to learn more about TNEF.
<UseFolderCapture>	Specifies if folder information is stored with the messages. <i>True</i> indicates that folder information is captured. <i>False</i> indicates that folder information is not captured. Note: Folder capture must also be enabled in the global configuration file (HP EASE PST Importer.ini) and the Domain.jcml file on the IAP for folder information to be stored.
<ForceProcessing>	Specifies if messages in a PST file that has been previously processed are tombstoned. Under normal circumstances, a PST file is not processed again unless it changes. This option forces PST Loader and PST Import Utility to process the file again. The <ForceProcessing> tag is supported in the <Header> only. It cannot be applied to an individual <FileSpec> and is ignored if specified there.

Table 7 Tags in Archive Request file header *(continued)*

Tag	Description
<Tombstone>	Controls tombstoning: <ul style="list-style-type: none"> • 0: Tombstoning is not enabled. • 1: Only attachments are removed. The item is tombstoned. • 2: Both attachments and the message body are removed. The item is tombstoned.
<FileSpecCount>	(Optional) Number of <FileSpec> tags listed later in the file. If provided, this tag controls file integrity by comparing the specified number to the actual number of <FileSpec> tags found.

The <FileSpecList> contains a list of file specifications bounded by the <FileSpec> tag. The settings described for <FileSpec> are required unless otherwise noted.

Table 8 Tags in Archive Request FileSpec

Tag	Description
<FilePath>	Path and file name of the imported file. Wildcards are allowed and are expanded prior to processing. UNC paths are supported and highly recommended.
<ProcessingType>	Type of import processing to be performed on the <FilePath>. PST is the only processing type supported.
<Server> <Mailbox> <SMTPServer> <SMTPPort> <HTTPServer> <IAPDomain> <Tombstone> <UseTNEF> <UseFolderCapture> <Repository> <AuditRepository>	Optional. Use these tags at the <FileSpec> level only to override <Header> settings.

Sample Archive Request file

```
<?xml version="1.0" encoding="UTF-8"?>
<ArchiveRequest>
  <Header>
    <Version>2.0</Version>
    <Server>UHCLEM</Server>
    <Mailbox>dmontgomery</Mailbox>
    <SMTPServer>192.168.4.1</SMTPServer>
    <SMTPPort>25</SMTPPort>
    <HTTPServer>192.168.4.1:81</HTTPServer>
    <IAPDomain>fire1</IAPDomain>
    <Repository>user@firesign.dev</Repository>
    <AuditRepository>audit@firesign.dev</AuditRepository>
    <UseTNEF>True</UseTNEF>
    <UseFolderCapture>True</UseFolderCapture>
    <EnsureOwnerReceipt>True</EnsureOwnerReceipt>
    <ForceProcessing>True</ForceProcessing>
    <Tombstone>1</Tombstone>
    <FileSpecCount>3</FileSpecCount>
  </Header>
  <FileSpecList>
    <FileSpec>
      <FilePath>
        E:\PSTFiles\PSTImportTest.pst
      </FilePath>
      <ProcessingType>PST</ProcessingType>
    </FileSpec>
    <FileSpec>
      <FilePath>
        E:\PSTFiles\Compliance.pst
      </FilePath>
      <ProcessingType>PST</ProcessingType>
    </FileSpec>
    <FileSpec>
      <FilePath>
        E:\PSTFiles\Test2.pst
      </FilePath>
      <ProcessingType>PST</ProcessingType>
    </FileSpec>
  </FileSpecList>
</ArchiveRequest>
```

D Outlook extension registry settings

Installing the Outlook extension registers the necessary components in the client's \Program Files\Hewlett-Packard\HP EASE Outlook Plug-In folder.

Initial registry settings are made in HKEY_LOCAL_MACHINE (HKLM):
HKLM\Software\Hewlett-Packard\Outlook PlugIn.

The first time a user runs Outlook on a machine that has the extension installed, these registry settings are copied from HKLM to HKEY_CURRENT_USER (HKCU):
HKCU\Software\Hewlett-Packard\Outlook PlugIn.

NOTE: On Microsoft Vista 64 bit clients, the initial registry settings are made in HKLM\Software\Wow6432Node\Hewlett-Packard\Outlook PlugIn. When a user initializes Outlook, the settings are copied to HKCU\Software\Hewlett-Packard\Outlook PlugIn.

Outlook extension settings are maintained on a user-by-user basis in HKCU by selecting **Tools**→**Options**→**Archive Options** in Outlook.

To change default settings for all users, use *regedit* to make changes in HKLM so they are copied and saved to HKCU when each user first runs Outlook. The following defaults are set in the registry.

- “Cache related registry settings” (page 120)
- “IAP retrieval related registry entries” (page 122)
- “Search and export related registry settings” (page 122)
- “Administrative registry settings” (page 123)

Cache related registry settings

These settings are used for configuring Archive Cache.

For more information, see “Configuring Archive Cache” (page 91).

Table 9 [HKLM\Software\Hewlett-Packard\Outlook PlugIn\Cache] settings

Registry key and default value	Description
AttachmentsOnly=True	Indicates whether Archive Cache should cache only those archived messages that contain one or more attachments. The default is True. Changing this to False causes Archive Cache to cache all messages, whether or not attachment(s) exist. This is a user-configurable setting.
EncryptCache=True	Encrypts files in the Archive Cache location using Microsoft's Encrypting File System (EFS). The default is True. Depending on the computer's security settings, only the current user can read files stored in the cache. Depending on the Folder options on the user's computer, files may appear as green in Windows Explorer. This is a user-configurable setting. Note: Archived messages will only be stored encrypted in the cache if EFS is properly configured on the client. If you want to implement this option, consult Microsoft's documentation for information on configuring EFS.
Location	Folder where Archive Cache is located. Cached files are then stored in this location according to the current Outlook profile. Do not assign a value to this registry value in HKLM. It is initialized in HKCU to \Documents and Settings\CurrentUser\Local Settings\Application Data\Hewlett-Packard\Cache upon first execution for a user. This is a read-only setting.

Table 9 [HKLM\Software\Hewlett-Packard\Outlook PlugIn\Cache] settings (continued)

Registry key and default value	Description
MaxDays=30	Maximum number of days archived messages are contained within Archive Cache. This is based on the received date of the message, not the date it was archived or tombstoned. The Archive Cache retrieves and caches any archived message where the received date is more recent than the number of days specified. Note that the MaxSize setting takes precedence over the MaxDays setting. Setting MaxDays to 0 causes all archived messages that can be contained by the MaxSize setting to be cached regardless of the received date. This is a user-configurable setting.
MaxSize=100	Size, in megabytes, of the Archive Cache folder. If this size is exceeded, the cached .eml files are deleted in reverse chronological order until the size of the cache is once again under the limit specified by this setting. Note that this setting overrides the MaxDays setting. This is a user-configurable setting.
ScanInterval=15	Number of minutes the Archive Cache waits before instigating a scan for new archived messages. The timer for this setting does not begin until after all queued retrieval requests are complete. Therefore, if the Archive Cache is busy retrieving archived messages this setting is inactive. This is a user-configurable setting.
UseCache=True	Indicates whether the extension should use Archive Cache to cache messages that have been archived in the IAP. The default is True. Changing this to False prevents Archive Cache from starting and downloading archived messages, and messages are only cached per Outlook session. This is a user-configurable setting.
CacheEML	Do not change. Reserved for future functionality.
CacheMSG	Deprecated and no longer used.
<i>The following default settings do not appear in the registry and should be added only at the direction of HP technical support.</i>	
UseCacheManager=True	Indicates that archived messages are downloaded to and managed by Archive Cache. When this value is set to False, only archived messages that the user specifically accesses from the IAP are placed in the Archive Cache. This cache on demand feature should not be used for mobile users.
RetrieveSimpleMessage=True	Indicates that Archive Cache should retrieve only simple messages (messages with no attachments) from the IAP. This is required if message bodies have been removed from the archived messages. Network bandwidth and Archive Cache disk space can be saved by setting this to False.
ConnectRetryInterval=5	Number of minutes Archive Cache waits before resuming the retrieval of archived messages after a dropped connection or other network failure occurs.
MaxConnectRetryCount=2	Number of times Archive Cache tries to recover from a network failure before exiting.
MaxFetchCount=50	Number of archived messages that are retrieved from the IAP at one time.
LogToDisk=False	Replicates the status information reported in the Cache Status window to a log file on the local file system. The file that contains this information is stored in the extension installation folder with a CacheMgr_YYYYMMDD_HHMMSS.log file name.
ShowSysTrayIcon=True	Indicates to the Archive Cache whether the status icon should be displayed in the system tray. By default, the system tray icon is displayed.

IAP retrieval related registry entries

These settings are used for retrieval of archived messages in Archive Cache and Outlook.

Table 10 [HKLM\Software\Hewlett-Packard\Outlook PlugIn\PluginURLs] settings

Registry key and default value	Description
FetchURL0=http://HOSTNAME	Specifies the IAP host name or IP address (together with the HTTP protocol) used to retrieve tombstoned messages. The <code>HOSTNAME</code> must be changed to indicate the IAP host name or IP address. The IAP host name and HTTP protocol are user-configurable settings.
FetchURLX=X	Represents a number in the range of 1 to 9. If the extension fails to retrieve a tombstoned message using <code>FetchURL0</code> , it attempts to retrieve the message using <code>FetchURL1</code> through <code>FetchURL9</code> sequentially.

Search and export related registry settings

These settings are used for the Outlook Integrated Archive Search and for the PST Export function. For information on exporting messages from the IAP, see “Exporting messages from the IAP” (page 95).

Table 11 [HKLM\Software\Hewlett-Packard\Outlook PlugIn\Search] settings

Registry key and default value	Description
DefaultFolder=Default	The PST Export Utility downloads archived messages into a folder with this name within the generated PST file(s). This is a user-configurable setting.
PSTFileFolder=C:\PSTFiles	File system folder used to store the individual PST files when <code>UseExternalFolderSupport=True</code> . This is a user-configurable setting.
PSTFilePrefix=Compliance Search	Defines the file name prefix used when creating the individual PST files when <code>UseExternalFolderSupport=True</code> . Each file begins with the prefix specified here and has an ordinal appended to the file name. For example: <code>ComplianceSearch_001.pst</code> , <code>ComplianceSearch_002.pst</code> , and so forth. This is a user-configurable setting.
UseExternalFolderSupport= True	Specifies whether the PST Export Utility allows the user to save PST files to an external location. The default is <code>True</code> . When <code>UseExternalFolderSupport=True</code> , the PST Export Utility saves the generated PST files prefixed with <code>PSTFilePrefix</code> to the folder specified by <code>PSTFileFolder</code> . This is a user-configurable setting.
AllowExternalFolderSupport=True	When set to <code>False</code> , the user is restricted from saving PST files to an external location. This is an administrator/diagnostic setting and should be modified only at the direction of HP technical support.

The following default settings do not appear in the registry and should be added only at the direction of HP technical support.

DefaultSearchMonths=6	The default search range for the Integrated Archive Search is constructed based on this value (current date – number of months in this registry setting).
ResultSetAttempts=0	For the Integrated Archive Search: <ul style="list-style-type: none"> • 0 = Keep going until result set is complete. • 1 = Allow only one attempt to get to the <code>ResultSetLimit</code>. • 2 = Allow only two attempts to get to the <code>ResultSetLimit</code>
ResultSetLimit=0	For the Integrated Archive Search: <ul style="list-style-type: none"> • 0 = Default to back end result set size. • Other number = Limit of results to display from result set.

Table 11 [HKLM\Software\Hewlett-Packard\Outlook PlugIn\Search] settings *(continued)*

Registry key and default value	Description
SingleSignonEnabled=0	<ul style="list-style-type: none">• 1 = True; single sign-on is enabled.• 0 (or any other number) = Single sign-on is not enabled.
TraceLevelToLog=0	<p>If the user has selected the Enable Logging check box in the About window and this flag is added, logging occurs as follows:</p> <ul style="list-style-type: none">• 0 = Off• 1 = Error• 2 = Warning• 3 = Info• 4 = Verbose <p>If the user has selected the Enable Logging check box and this flag is not added, logging occurs as if it was set to level 4 (verbose).</p>

Administrative registry settings

These settings define the Outlook extension administrative settings.

Table 12 [HKLM\Software\Hewlett-Packard\Outlook PlugIn] settings

Registry key	Description
AdminMode=False	Indicates the machine is in Administrative mode. The default is <code>False</code> . When set to <code>True</code> , users (including the administrator) are restricted from changing user-configurable settings. This value should be set to <code>True</code> only if you do not want the end user to make any configuration changes.
Version=X.XXXX	extension version. This should never be modified.
LogFilePath=	A fully-qualified path name that instructs the extension to record certain diagnostic information to disk. This is a user-configurable setting.

Index

A

- antivirus programs
 - and PST Import Manager, 78
- Archive Cache, 86
 - defined, 91
 - system tray status icon, 92
- archive engine
 - defaults, 20
- archive gateway
 - joining to Exchange domain, 31
- Archive Request file, 117
 - see also Information Description file
 - file spec tags, 118
 - header tags, 117
- Archive Search, 88
- archive service account
 - creating, 13
 - specifying access, 18
- archiving event
 - Advanced tab, 28
 - Configuration tab, 27
 - IAP Domain tab, 28
 - Schedule tab, 27
- archiving services, 18
- assigning messages to IAP repositories, 106
- attachments
 - changes to, 106
 - proxy in tombstoned message, 46, 58
- attachments, large, 104

B

- batch export error, 107

C

- Capture Email in TNEF
 - default, 22
- CAS server
 - setting for Selective Archiving, 40
- changes not captured in email attachments, 106
- Citrix server, 95, 107
- Compliance Archiving
 - configuring Exchange server, 24
 - copying events, 28
 - creating events, 26
 - defaults, 22
 - deleting events, 28
 - editing events, 26
 - enabling on mailbox stores, 25
 - event status, 75
 - events, 26
 - items archived, 24
 - overview, 10, 24
 - running events, 29
- console, 16
- Content-Type indexing, 111

- conventions
 - text symbols, 9
- credentials, archive, 18

D

- Default Routing Address(es)
 - default, 21
- defaults
 - Compliance Archiving, 22
 - configuring, 20
 - delete synchronization, 22
 - general, 21
 - maintenance, 23
 - Selective Archiving, 22
 - tombstone maintenance, 22
- delete synchronization
 - defaults, 22
- DiskSpaceBuffer error, 107
- distribution lists, 106
- DLD file type, 99, 107
- DNS records, 32
- document conventions, 8
- dropped caps, 110
- duplicates, message, 105

E

- EAsE Archive Engine console, 16
- EAsE software
 - launching, 16
 - navigating, 16
- EAsE VIP, 32
- EASE_Tombstone_Delete_Template.mr , 101
- end user applications, 12
- end user delete, 66
- ENDR mailbox, 34
- EnsureOwnerReceipt, 106
- error opening folders in OWA 2007, 105
- Excel, 112, 113, 115
- Exchange domain, joining archive gateway to, 31
- export error, 107
- exporting
 - errors, 99
 - messages, 86, 95, 107
 - search results, 95

F

- FileSpec tag, PST Import Manager, 118
- folder capture, 70, 83, 95, 117
 - and Duplicate Manager, 72
 - and PST Import Manager, 72
 - and Selective Archiving events, 72
 - and Synchronize Deleted Items events, 72
 - and Tombstone Maintenance events, 72
 - and tombstone maintenance events, 64
- enabling, 70
- indexing folder information, 70

folders skipped during Selective Archiving, 106

G

global configuration files, 106

H

hash

- and message duplicates, 105
- computing, 105

HP

- Subscriber's choice Web site, 9

HPAEServiceAccount, 13

HTML formatting, 110

hub transport, 32

- configuring settings, 33
- creating journal rule, 34

I

IAP Web Interface, 86

- defined, 86
- exporting messages, 86

indexed documents, 110

- Microsoft Office, 111

indexed Exchange items

- types, 110

Information Store Groups, 60

installation guide, 8

installing

- Outlook extension, 87
- PST Import Manager, 78

J

journal mailboxes, creating, 24

L

Launch Manager Log Verbosity

- default, 21

M

mail contact record, 33

maintenance defaults, 23

messages are not archived, 106

messages not being archived

- EnsureOwnerReceipt not enabled, 106

Microsoft Office applications, 112, 113, 115

Microsoft Word, 112, 113, 115

MIME Content-Type indexing, 111

Monitoring

- alerts, 74
- Archive Engine status, 75
- SMTP Premium Journaling status, 76
- system resources, 74

MX records, 32

N

no archiving access to IAP, 18

no archiving access to mailboxes, 18

O

Outlook extension, 86

- installing, 87

Outlook extension registry settings

- administrative, 123
- and Citrix server, 95
- Archive Cache, 120
- default settings, 93
- IAP retrieval, 122
- manually creating, 93
- overriding language, 93
- search and export, 122

Outlook Integrated Archive Search, 88

Outlook Plug-In

- Admin mode, 90
- and Citrix server, 95
- Archive Cache, 91
- Archive Options tab, 88
- logging, 90
- overriding language, 93
- PST Export Utility, 95
- registry settings, 120
- setting host information, 89

overview, 10

OWA Extension, 86

- asp config file, 103

- ASP time-out, 103

- browser functionality, 104

- error opening folders in 2007, 105

- making archived mail items visible in OWA, 102

- multi-user support, 104

- multiple IAP system, 101

- multiple mail stores, 100

- temporary copies in Drafts folder, 101

- Web config file, 102

P

Policy Engine

- Actions tab, 55

- Conditions tab, 54

- configuring rules, 46

- EASE_Tombstone_Delete_Template.mr, 101

- Folders tab, 48

- Information Store Groups rules, 60

- Information Stores tab, 47

- manually executing rules, 59

- Messages tab, 53

- Schedule tab, 56

- Selection tab, 50

- stops processing mailbox, 106

PowerPoint, 112, 113, 115

PST Export Utility, 86

PST files

- importing to IAP, 78

PST Import Manager

- antivirus programs conflict with, 78

- creating Import Description file, 81

- establishing archive credentials, 79

- FileSpec tag, 118

- importing, 78
- installing, 78
- overview, 12
- PST Import Monitor, 83
- sample Archive Request file, 119

PST Import Monitor, 83

Q

Quota Thresholds

- defining threshold, 50
- included and excluded messages, 53
- ordering message list, 52
- selecting data to process, 50

R

registry settings

- Outlook extension, 93

related documentation, 8

requirements

- PST Import Manager, 78

S

search results

- exporting, 95

Selective Archiving

- copying events, 59
- creating events, 44
- defaults, 22
- deleting events, 59
- editing events, 57
- editing local service processing settings, 40
- editing rules, 46
- end user delete, 66
- event status, 75
- excluding journal mailboxes, 43
- items archived, 39
- overview, 11, 39
- running, 59
- setting CAS servers, 40
- setting up Auto Search, 43
- setting up information stores, 40

single sign-on, 87

Smart Cells, 107

SMTP Premium Journaling, 30

- configuring Archive Gateway, 31
- configuring Exchange server for, 32
- creating journaling event, 34
- creating mail contact record, 33
- ENDR mailbox, 34
- hub transport journal rule, 34
- monitoring status, 76
- overview, 11, 30

Subscriber's choice, HP, 9

symbols in text, 9

system requirements, 13

- OWA Extension, 100
- PST Import Manager, 78

T

text symbols, 9

TNEF, 20, 117

tombstoned

- visible in OWA, 102

tombstones

- events, 63
- folder synchronization, 63
- maintenance and folder capture, 64
- maintenance defaults, 22

U

user guide, 8

V

verifying

- access to Exchange, 18
- access to IAP, 18

W

Web sites

- HP Subscriber's choice, 9

Word, 112, 113, 115