

HP Email Archiving software for Microsoft Exchange

Version 2.1

Administrator Guide

Legal and notice information

© Copyright 2004-2009 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® and Windows® are US registered trademarks of Microsoft Corporation. Outlook™ is a trademark 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	9
Intended audience	9
Related documentation	9
Document conventions and symbols	10
HP technical support	11
Subscription service	11
Other Web sites	11
1 System overview	13
IAP and HP EAs Exchange	13
Character support	14
HP EAs Exchange system requirements	15
Prerequisites	15
Creating the archive service account	16
Configuring the archive credentials	16
Common administration tasks	19
2 Configuring Compliance Archiving	21
Overview of Compliance Archiving	21
Creating journal user accounts	21
Enabling Compliance Archiving on mailbox stores	22
Exchange 2007	22
Pre-2007 Exchange servers	23
Setting the registry key for Compliance Archiving (Exchange 2000)	23
Configuring Compliance Archiving events	23
Creating a Compliance Archiving event	24
Editing Compliance Archiving events	24
TNEF message capture	26
Copying a Compliance Archiving event	27
Deleting a Compliance Archiving event	27
Running Compliance Archiving events	27
3 Configuring Selective Archiving	29
Overview of Selective Archiving	29
Setting up Information Stores	30
Adding mailboxes	30
Adding public folders	32
Setting up Auto-Search	32
Configuring Selective Archiving events	33
Creating a Selective Archiving event	33
Editing Selective Archiving events	34
Copying a scheduled event	36
Deleting a scheduled event	36
Creating a team mailbox archiving event	37
Editing Selective Archiving rules	38
Information Stores tab	38
Folders tab	40
Conditions tab	41
Adding conditions	41

Determining how conditions are applied	43
Actions tab	43
Schedule tab	44
Editing local service processing settings	46
Starting the archiving process	47
Viewing event status	47
4 Archiving to a quota threshold	49
Configuring a Quota Archive Threshold event and rule	49
Selection tab	50
Messages tab	53
5 Using tombstone maintenance	55
Configuring tombstone maintenance events	55
Configuring Tombstone Maintenance events with folder capture	56
6 Configuring end-user delete	59
Location of deleted items	59
Deleted items tag	59
Enabling deletion retention on the Exchange server	60
Exchange 2007	60
Pre-2007 Exchange servers	61
Scheduling deletion from the IAP	61
Creating the event	61
Creating a Policy Engine rule	62
7 Working with folder capture	63
Introduction	63
Indexing folder information	63
Enabling folder capture	64
Enabling folder capture on the IAP	64
Enabling folder capture in the archiving global configuration file	64
Enabling folder capture for a specific event	64
Enabling folder capture in PST Import Tools	64
How folder capture works with archiving events	65
Folder capture and Selective Archiving events	65
Folder capture and Tombstone Folder Synchronization events	65
Folder capture and Synchronize Deleted Items events	65
Folder capture and PST Import Tools	65
Folder capture and the merging of duplicate messages	66
8 Archiving messages in public folders	67
Overview	67
Configuring the Exchange server	67
Exchange 2007	68
Pre-2007 Exchange servers	68
Configuring a public folder event	69
Adding public folders to Information Stores	69
Configuring the public folder rule	69
Enabling ACL expansion	70
9 Archiving with the PST Import Tools	71
PST Import Tools overview	71
Installing the PST Import Tools	72
Installation requirements	72
Installation procedure	72

The PST import process	72
Establishing archive credentials	73
Creating the Archive Request file	74
Archive Request file	74
Creating or revising an Archive Request file	74
Validating the file using the PST Loader	78
Validating the file from the command line	79
Using the PST Import Monitor	79
Processing PST files	79
Displaying reports and log files	82
PST Import report	82
PST Importer log file	82
10 Working with end-user applications	83
Overview of the applications	83
Using the IAP Web Interface	84
Using single sign-on	84
Installing and configuring the Outlook Plug-In	84
Verifying security settings	84
Installing the Outlook Plug-In for users	85
The Archive Options tab	86
Setting host information	86
Displaying the About dialog box	87
Configuring Archive Cache	88
HP EAsE Archive Cache status icon	90
Registry settings	90
Default registry settings	90
Manually creating other registry settings	90
Overriding the language in the Outlook Plug-In user interface	91
Using the plug-in with Citrix Presentation Manager	92
Exporting messages from the IAP	93
Overview of the export process	93
Exporting messages	93
Problems exporting messages	97
11 Working with HP OWA Extension	99
System requirements	99
Multiple mail stores	99
Multiple IAP systems	100
Temporary storage in Drafts folder	100
Deleting temporary Drafts copies using a rule	100
Making tombstoned mail items visible in OWA	101
Viewing the Web.config file in Exchange 2007 installations	101
Working with the asp.config file in Exchange 2000 and 2003 installations	102
IAP appliances	102
URL templates	102
ASP pages	102
Changing the ASP time-out in Exchange 2000 and 2003 installations	103
Browser functionality	103
Multi-user support	103
Large attachments	103
12 Troubleshooting	105
OWA 2007 users cannot open folders containing tombstoned messages	105
OWA 2007 users cannot retrieve tombstoned messages	105
Behavior in Microsoft Exchange Server 2007 impacts detection of message duplicates	105
Overview	105
HP RIM 1.x	106

HP EAs Exchange 2.x	106
Selective archiving does not process all folders in user mailbox	106
Changes not captured in email attachments	107
Users cannot find messages sent to a distribution list	107
DiskSpaceBuffer error	107
HP Batch Export error	107
A Indexed document and content types	109
Indexed document types	109
Message MIME types	110
Additional indexing detail/limitations for Microsoft Office	111
B PST Import Tools: Archive Request file specifications	117
Settings description	117
Sample Archive Request file	118
C Outlook Plug-In registry settings	121
Cache related registry settings	121
IAP retrieval related registry entries	123
Search and export related registry settings	123
Administrative registry settings	125
Index	127

Tables

1	Document conventions	10
2	IAP and EAs Exchange applications for users	13
3	IAP and HP EAs Exchange applications for administrators	14
4	HP IAP and EAs Exchange character support	14
5	Common administration tasks	19
6	Archive Cache settings	89
7	IAP indexed document and MIME types	110
8	Microsoft Office supported features	111
9	Microsoft Office supported properties	113
10	Tags in Archive Request file header	117
11	Tags in Archive Request FileSpec	118
12	[HKLM\Software\Hewlett-Packard\Outlook PlugIn\Cache] settings	121
13	[HKLM\Software\Hewlett-Packard\Outlook PlugIn\PlugInURLs] settings	123
14	[HKLM\Software\Hewlett-Packard\Outlook PlugIn\Search] settings	123
15	[HKLM\Software\Hewlett-Packard\Outlook PlugIn] settings	125

About this guide

HP Email Archiving software for Microsoft Exchange (HP EAs Exchange or EAsE) is mail administration software that archives messages from Outlook mail accounts and/or journals and places the messages in the HP Integrated Archive Platform (IAP) architecture. 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
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.

HP technical support

Telephone numbers for worldwide technical support are listed on the HP support Web site: <http://www.hp.com/support/>.

Collect the following information before calling:

- Technical support registration number (if applicable)
- Product serial numbers
- Product model names and numbers
- Applicable error messages
- Operating system type and revision level
- Detailed, specific questions

For continuous quality improvement, calls may be recorded or monitored.

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.

After subscribing, locate your products by selecting **Business support**, selecting **Storage** under Product Category, and then selecting **Storage Archiving**.

Other Web sites

For other product information, see the following HP Web sites:

- <http://www.hp.com>
- <http://www.hp.com/go/storage>
- http://www.hp.com/service_locator
- <http://www.hp.com/support/manuals>

1 System overview

This chapter provides an overview of the IAP system and HP EAs Exchange software. It contains the following topics:

- [IAP and HP EAs Exchange](#), page 13
- [HP EAs Exchange system requirements](#), page 15
- [Prerequisites](#), page 15
- [Common administration tasks](#), page 19

IAP and HP EAs Exchange

IAP is a fault-tolerant, secure system of hardware and software that archives email messages and attachments for your organization, and lets users search for archived documents. IAP provides the following main functions:

- Automatic, active email archiving that helps your organization meet regulatory requirements.
- Interactive querying to search for and retrieve archived email according to various criteria.

HP EAs Exchange is management and configuration software that is installed on the Archive Gateway. It includes three archiving methods:

- Compliance Archiving (journaling)
- Selective Archiving
- PST Import Tools

You can use any or all of these methods to archive Exchange items.

To interact with the system, users can access the following applications:

Table 2 IAP and EAs Exchange applications for users

Application	Description
IAP Web Interface	Employees can use a Web browser to search for and view email archived on the IAP, and save and reuse search-query definitions and results.
HP EAs Exchange client applications (customer option)	When the Outlook Plug-In is installed, users can search for and open archived messages from their Outlook mailbox, and use a cache to access archived messages offline. Users can also export messages from the IAP to a PST file.
OWA Extension	With OWA Extension, users can view and open archived messages using Outlook Web Access in their Web browser.

System administrators can use the following troubleshooting and administrative tools:

Table 3 IAP and HP EAs Exchange applications for administrators

Application	Description
HP EAs Exchange Selective Archiving software	Use the software to create Selective Archiving rules and archive user mailboxes.
HP EAs Exchange Compliance Archiving software	Use the software to archive journal mailboxes.
PST Import Tools	Use the software to perform batch imports of multiple PST files into the IAP. See “Archiving with the PST Import Tools” on page 71.
Audit Log	Enable the Audit Log for regulatory compliance. See the <i>HP Integrated Archive Platform Administrator Guide</i> .
IAP Platform Control Center (PCC)	Monitor and troubleshoot IAP system status and performance, and manage IAP user accounts using a Web browser. See the <i>HP Integrated Archive Platform Administrator Guide</i> .

Character support

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

Table 4 HP IAP and EAs Exchange character 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)

Supported character set	Description
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

HP EAs Exchange system requirements

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

- Compliance and Selective Archiving
- PST Import Tools
- Outlook Plug-In, 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 2.0.

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.
- Outlook user profiles should be set to synchronize all Outlook folders automatically and regularly.
- Exchange servers should be set up so that SMTP traffic does not directly enter the server where the mailbox stores are kept.
HP recommends a front end/back end configuration where:
 - The front end server does not have mailbox stores and handles the SMTP traffic.
 - The back end server has mailbox stores and does not handle the SMTP traffic.
 - HP EAs Exchange is configured to send email to the front end server only.

If messages are sent directly via SMTP to an Exchange server that also handles mailbox stores, the addresses could be resolved in an inconsistent manner between different servers. The same message might not be recognized as a duplicate and submitted again.
- 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](#)" on page 16.
- If you are implementing Compliance Archiving (journal mining), create and configure the journal mailbox(es) (See "[Creating journal user accounts](#)" on page 21.

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 HPAEServiceAccount.
2. Use the same name for the user logon name and mailbox alias: HPAEServiceAccount.
3. Ensure the user is a member of both Domain Users and Administrators.
4. Enter a password for the account.
5. In Exchange 2000 and 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.
6. In Exchange 2007, add the access rights and permissions for HPAEServiceAccount using the following command in the Exchange Management Shell:

```
get-MailboxDatabase | add-ADPermission -User HPAEServiceAccount  
-AccessRights GenericRead,GenericWrite,DeleteChild
```

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

```
get-MailboxDatabase | remove-ADPermission -User HPAEServiceAccount  
-AccessRights GenericAll
```

Configuring the archive credentials

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

The Archive Credentials program:

- Specifies HPAEServiceAccount as the logon account for the archiving services (HP EAsE Archive Engine, Mail Attender Enterprise Service and JBOSS).
- Specifies HPAEServiceAccount as the account to access the IAP.
- Specifies HPAEServiceAccount as the account to access the Exchange server mailboxes to be archived.

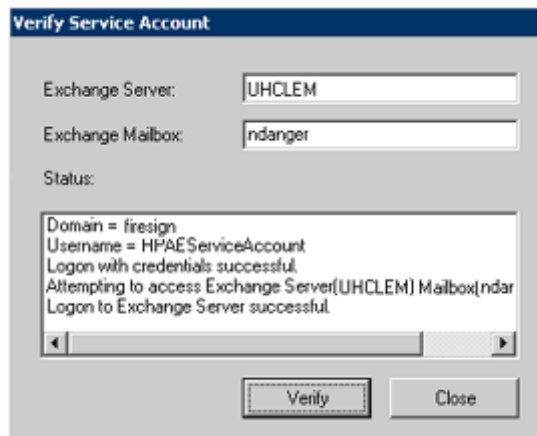
Whenever the HP EAs Exchange software is updated on the Archive Gateway, the archive credentials should be re-established automatically. You can verify the service account access by performing steps 3d and 5c-f in the procedure below.

This procedure is also used if you change the archive service account password periodically. When changing the password, make the change in Active Directory and the Archive Gateway, then change the password in Service/Exchange Account and IAP Credential Settings in Archive Credentials.

To review or change the archive credentials:

1. Log on to the Archive Gateway as the archive service account.
2. On the desktop, double-click the **Archive Credentials** icon.
The Archive Credentials window appears.
3. Change the Service/Exchange Account settings by following these steps:
 - a. In the Domain\Username box, enter *<Exchange domain>\HPAEServiceAccount*.
 - b. In the Domain Password box, enter the password for the archive service account.
The Verify Service Account window appears.
 - c. Enter the Exchange server name and the name of a user mailbox in the domain.
 - d. Click **Verify** to test the archive service account access to the Exchange server.

The results are shown in the status window.



- e. Click **Close** to return to the Archive Credentials window.
4. Click **Save** to save the credentials.

5. Change the IAP Credential Settings by following these steps:
 - a. In the IAP Admin Username box, enter the email address of the archive service account: `HPAEServiceAccount@<Exchange domain>`.
 - b. In the IAP Admin Password box, enter the password for the archive service account.
 - c. Click **Verify** to test the account access.

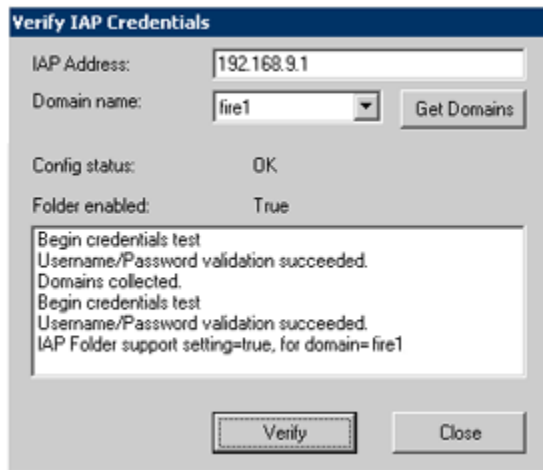
The Verify IAP Credentials window appears.
 - d. In the IAP Address box, enter the IAP HTTP portal address and click **Get Domains**.

You can enter any of the VIP addresses listed in the `ipToDomainInfo` field in the `Domain.jcm1` file, which is located on the IAP kickstart server.

The domains that are available in the IAP are added to the Domain name drop-down list in the archive credentials window.
 - e. In the Domain name box, select the IAP domain.
 - f. Click **Verify**.

The Archive Credentials program conducts a test access and logs the results in the status window.

The results also show the status of IAP folder capture support for the selected domain. (Information on folder capture is located in ["Working with folder capture"](#) on page 63.



- g. Click **Close** to return to the Archive Credentials window.

- Click **Save** to save the IAP credentials.

- Click **Close** to exit the program.

Common administration tasks

Table 5 Common administration tasks

Task	Go to
Configuring Compliance Archiving	Configuring Compliance Archiving , page 21
Configuring Selective Archiving	Configuring Selective Archiving , page 29
Archiving to mailbox quota threshold	Archiving to a quota threshold , page 49
Using folder capture	Working with folder capture , page 63
Using end-user delete reference	Configuring end-user delete , page 59
Batch loading PST files into the IAP	Archiving with the PST Import Tools , page 71
Archiving messages in public folders	Archiving messages in public folders , page 67
Accessing archived messages using the IAP Web Interface	Using the IAP Web Interface , page 84
Installing and configuring the Outlook Plug-In on client systems	Installing and configuring the Outlook Plug-In , page 84 Outlook Plug-In registry settings , page 121
Working with OWA Extension	Working with HP OWA Extension , page 99

2 Configuring Compliance Archiving

- [Overview of Compliance Archiving](#), page 21
- [Creating journal user accounts](#), page 21
- [Enabling Compliance Archiving on mailbox stores](#), page 22
- [Setting the registry key for Compliance Archiving \(Exchange 2000\)](#), page 23
- [Configuring Compliance Archiving events](#), page 23
- [Running Compliance Archiving events](#), page 27

Overview of Compliance Archiving

HP EAs Exchange Compliance Archiving captures the following Exchange items placed in a journal mailbox:

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

Attachments to these items are also archived.

Calendar items (IPM.Appointment) are not placed in the journal mailbox by Exchange. Therefore, archiving of calendar items is not supported in Compliance Archiving.

Standard email messages (IPM.Note) can be archived using MIME (Multipurpose Internet Mail Extensions) or TNEF (Transport Neutral Encapsulation Format). All other messages types are archived using TNEF. See "[TNEF message capture](#)" on page 26 for more information about archiving using TNEF.

Creating journal user accounts

Before Compliance Archiving is configured, it is your responsibility to create one or more journal user accounts and mailboxes in Active Directory.

Make sure the following conditions are met:

1. Ensure the user is a member of Domain Users.
2. Name each user account whatever you choose; for example, LocalJournalUser or [Domain]JournalUser.
The user logon name and mailbox alias should use the same name (for example, LocalJournalUser).
3. Create a password for the account.
4. Ensure that the HPAEServiceAccount has access to the mailbox.

The following permissions must be granted to the archive service account:

- Exchange 2000 and 2003:
 - Delete mailbox storage
 - Read permissions
 - Change permissions
 - Take ownership
 - Full mailbox access
- Exchange 2007:
 - GenericRead
 - GenericWrite
 - DeleteChild

(For more information about the HPAEServiceAccount, see [“Creating the archive service account”](#) on page 16.)

Your HP representative configures the credentials on the Archive Gateway that allow the journaled messages to be sent to the IAP.



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

Set the mailbox store properties to enable Compliance Archiving on a journal mailbox.

Exchange 2007

To enable Compliance Archiving:

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:

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 pop-up 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.

Setting the registry key for Compliance Archiving (Exchange 2000)

NOTE:

Set the registry key only for Exchange 2000. This task does not need to be performed if a later version of Exchange is installed on the server.

Set the registry key to implement envelope journaling on the Exchange server. Envelope journaling captures all recipient information including BCC and distribution lists. It **must** be used to correctly expand distribution lists.

For the procedure to follow, see the following Web site: <http://support.microsoft.com/default.aspx?scid=kb;en-us;843105&Product=exch2k>.

Configuring Compliance Archiving events

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

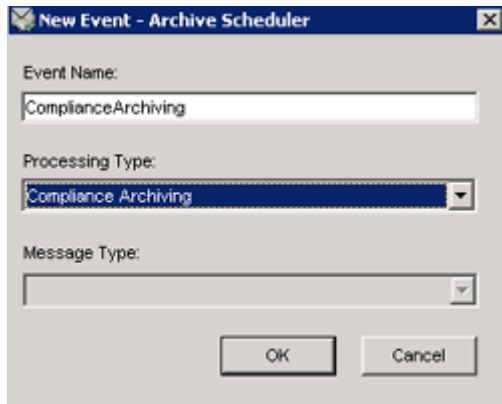
After messages are archived on the IAP, they are automatically deleted from the journal Inbox.

Creating a Compliance Archiving event

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

To create a new event:

1. Log on to the Archive Gateway using the archive service account.
2. Double-click the Archive Scheduler icon on the desktop.
3. In the Archive Scheduler window, select **New** to display the New Event window.
4. Enter a descriptive name for the event in the Event Name box.
The name should not contain any special characters.
5. In the Processing Type drop-down list, select **Compliance Archiving**.



6. Click **OK** to close the window.
7. Verify that the journal mailbox is excluded from Selective Archiving.
See ["Adding mailboxes"](#) on page 30.

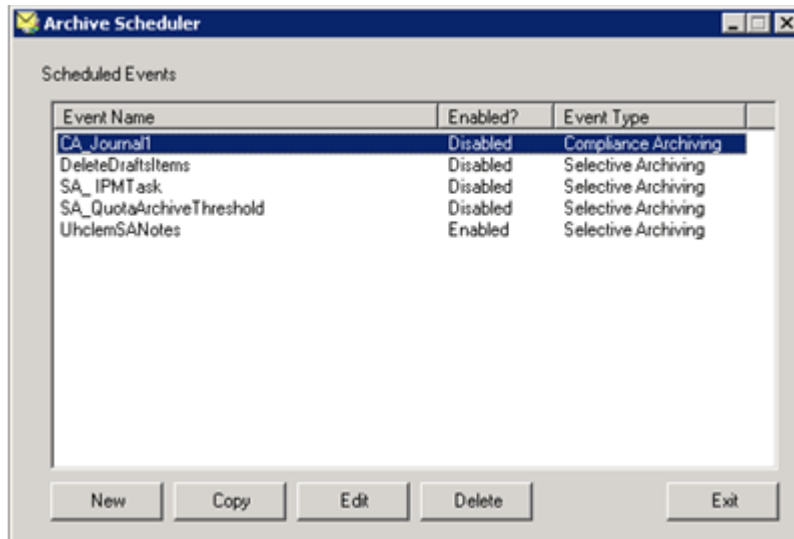
Editing Compliance Archiving events

When the HP EAs Exchange software is installed, your HP service representative configures global archiving settings in the G:\Mining>Selective Archiving\HPAE.ini file on the Archive Gateway. Events in the Archive Scheduler are populated with these values. The global values can be overridden in a scheduled event, but should be changed only under the supervision of HP technical support. Event overrides are placed in separate .ini files in G:\Mining>Selective Archiving\Events.

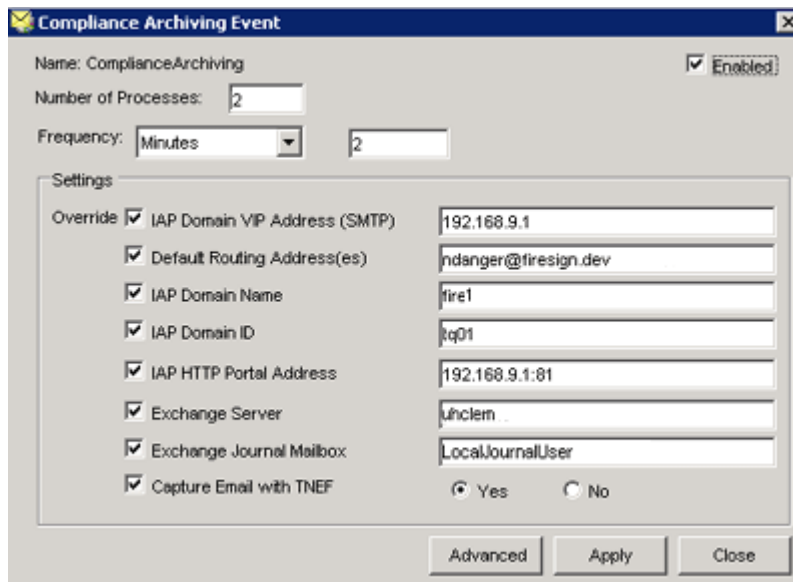
In most cases, you will open the event window only to enable or disable an event.

To edit an event:

1. Open Archive Scheduler.
2. Select the event in the Archive Scheduler window, and click **Edit**.



3. In the event window, select the **Enabled** check box to enable the event. Disable the event by clearing the check box.
4. If you are editing a setting (under the guidance of HP technical support), select the **Override** check box in front of the setting, and then enter a new value.



Field	Description
Number of Processes	Do not change. This field defines number of processes for each event. HP engineering sets the number of processes after reviewing several factors, including scalability.
Frequency	Use the two Frequency check boxes to change the archiving time interval from the default value of 2 minutes.
IAP Domain VIP Address (SMTP)	The IAP Virtual IP (VIP) used for SMTP. The VIP is the internal IAP domain that stores documents and is the same value as the ipToDomainInfo attribute used in Domain.jcml on the IAP.
Default Routing Address(es)	<user>@<iap-domain.com> Replace <user> with either a fictitious user or a real user name. If a fictitious user is entered, the undeliverable messages are routed to the catchall repository on the IAP. If a real user is entered, the undeliverable messages are sent to that user's repository. One or more users can be specified, with the user addresses separated by commas. Replace <iap-domain.com> with the domain name specified in Domain.jcml.
IAP Domain Name	The name of the internal IAP domain to which the email from the journal mailbox should be stored. The Domain Name must match exactly the domain name attribute specified in Domain.jcml.
IAP Domain ID	The domain ID that matches the domain name specified above. The Domain ID must match exactly the domain ID attribute in Domain.jcml.
IAP HTTP Portal Address	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 in a round-robin fashion, message-by-message.
Exchange Server	The name of the Exchange server for which Compliance Archiving is configured. This server name must be resolvable by DNS in the IAP.
Exchange Journal Mailbox	The journal account name specified when the journal mailbox is set up.
Capture Email with TNEF	For Compliance Archiving, keep the default value of Yes . For more information about TNEF, see " TNEF message capture " on page 26.

5. Click **Apply**, and then click **Close** to finalize the changes.

Clicking the **Advanced** button in the event window displays the settings in text format.

 **NOTE:**

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

TNEF message capture

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 listed below 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 non-standard 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.

Copying a Compliance Archiving event

Each journal mailbox that is archived requires a separate 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.

Copy an event by following these steps:

1. Select the relevant event and click **Copy**.
2. In the Copy Event window:
 - a. Enter a name for the new event.
 - b. Click **OK** to create the event copy.

The event window appears.
3. Select the **Enabled** check box to enable the event.
Edit other settings under the direction of HP technical support.
4. Click **Apply** and then **Close** to finalize the changes.

Deleting a Compliance Archiving event

To delete a scheduled Compliance Archiving event:

1. Select the appropriate event and click **Delete**.
A dialog box appears asking you to confirm the delete request.
2. Click **Yes** to complete the delete process.
The event is removed from the Archive Scheduler database.
3. Click **Exit** to close Archive Scheduler.

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

A Compliance Archiving event starts running as scheduled as soon as it is enabled.

You can track the status of the event in the Archive Monitor. (See "[Viewing event status](#)" on page 47.)

During system setup, your HP representative configured the archive credentials to allow the HP EAsE Archive Engine, Mail Attender Enterprise, and JBOSS services access to the mailboxes, and started those services on the Archive Gateway.

3 Configuring Selective Archiving

Selective Archiving uses rules, or policies, to archive email messages and other Exchange items from the Exchange server to the IAP. A request to the IAP is sent to determine if a message in a user's mailbox is already archived. If so, a tombstone (or stub) is created on the Exchange server. The tombstone is a link to the original message that is stored in the IAP. If the message is not already archived, it is archived, and a tombstone is created.

- [Overview of Selective Archiving](#), page 29
- [Setting up Information Stores](#), page 30
- [Configuring Selective Archiving events](#), page 33
- [Editing Selective Archiving rules](#), page 38
- [Editing local service processing settings](#), page 46
- [Starting the archiving process](#), page 47
- [Viewing event status](#), page 47

Overview of Selective Archiving

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 can be archived.
- Only completed tasks can be archived.

When an Exchange item attached to a standard email (IPM.Note) is captured, message behavior varies depending on whether TNEF (Transport Neutral Encapsulation Format) is enabled in the HP EAs Exchange configuration file (`HPAE.ini`). If TNEF is enabled, these items are stored with full fidelity so the original item content is maintained. If TNEF is not configured, the item is converted into an embedded email message. In this case, all internal message properties associated with the particular item are lost.

Only standard email messages (IPM.Note) can be archived without TNEF enabled. For all other message types (documents, appointments, tasks), TNEF is enabled automatically. See ["TNEF message capture"](#) on page 26 for information about TNEF.

Items archived in the IAP can be searched for using the Outlook Integrated Archive Search or the IAP Web Interface. (See ["Working with end-user applications"](#) on page 83.) All items except secure or encrypted messages (and their attachments) are indexed, allowing for a search on the message contents. For secure and encrypted messages, searches can only be made on header information. See ["Indexed document types"](#) on page 109 for more information.

Setting up Information Stores

Before archiving rules can be created and implemented, the information stores that contain items to be archived must be specified. HP EAs Exchange can selectively archive email, calendar items, task items, and documents in Exchange mailboxes and messages in public folders.

When the EAs Exchange environment is configured, your HP service representative adds all mailboxes and public folders that can be selectively archived and then 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 taken 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](#)” on page 30. 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.

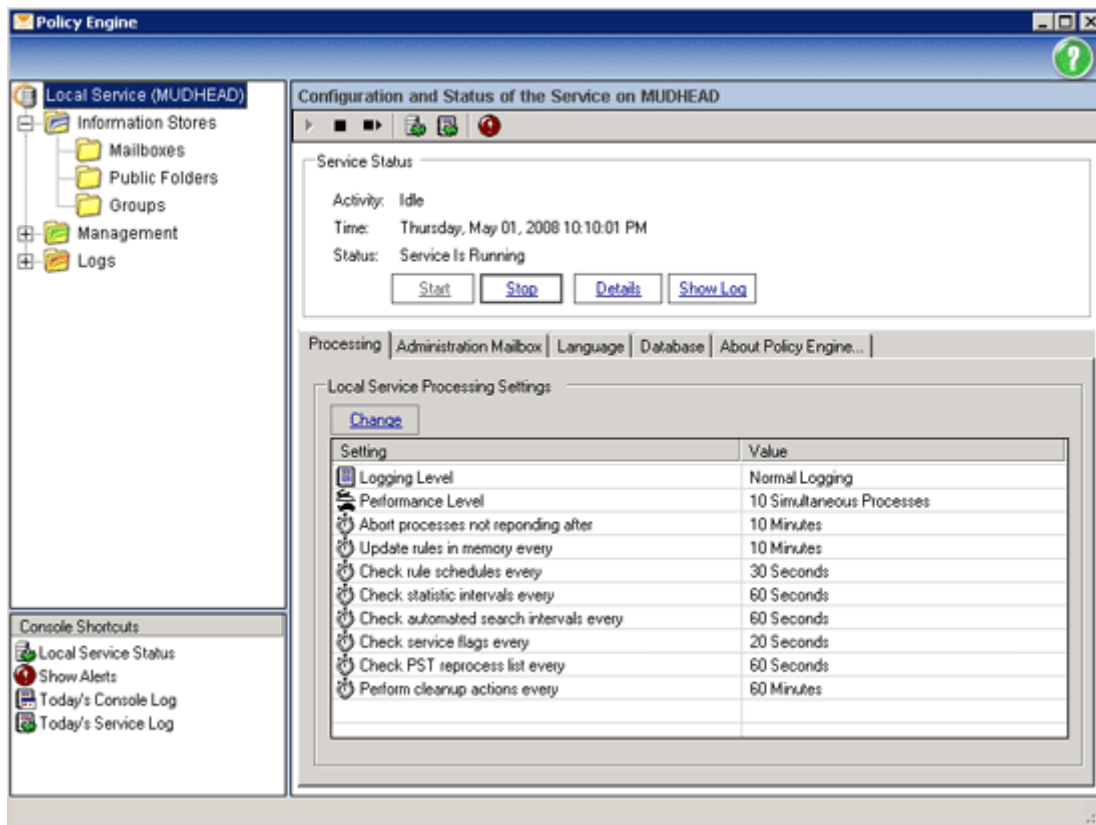
Adding mailboxes

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

1. Log on to the Archive Gateway as the archive service account.
2. Double-click the Policy Engine icon on the desktop.

The Policy Engine window appears.

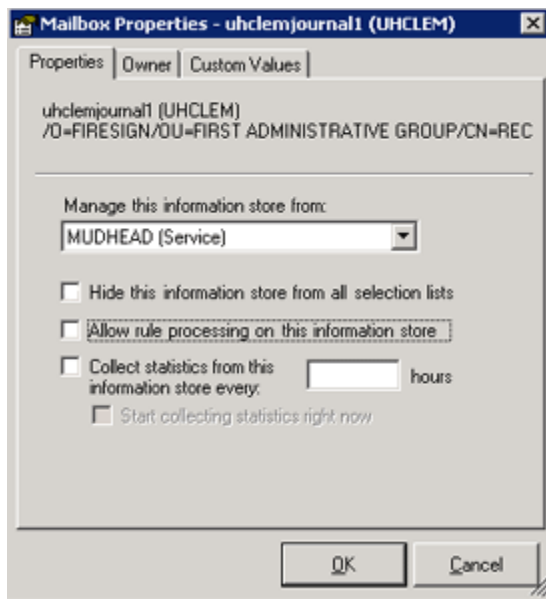
3. In the left pane, expand the Information Stores folder.



4. In the left pane, select **Mailboxes**.
5. Right-click in the right pane and select **Add Mailboxes > From an Exchange Server > Browse Network**.
6. From the window that appears, select the appropriate Exchange Server, and click **OK** to continue.
7. 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.
8. Exclude all journal mailboxes and the SMTP and System Attendant information stores from processing:
 - a. Verify that **Mailboxes** is selected in the left pane.
 - b. Click the settings view button to change to the Settings View.



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



- e. Click **OK** when finished.
- f. Repeat steps c–e for any other journal mailboxes and for the SMTP and System Attendant information stores.

Adding public folders

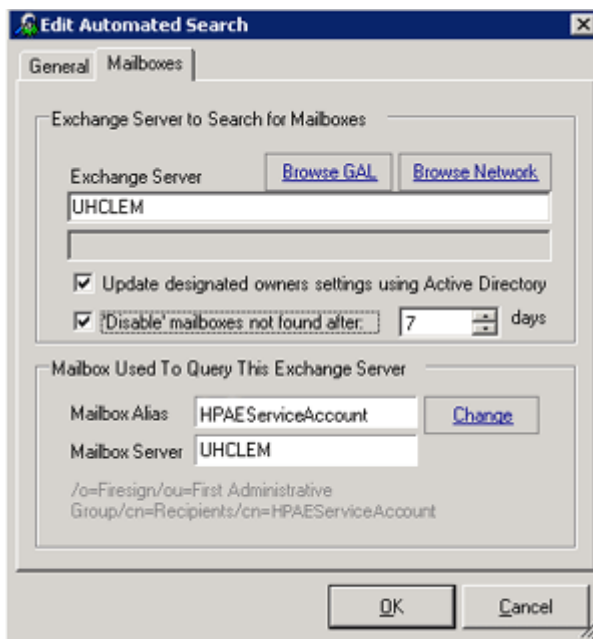
See “Archiving messages in public folders” on page 67.

Setting up Auto-Search

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**.

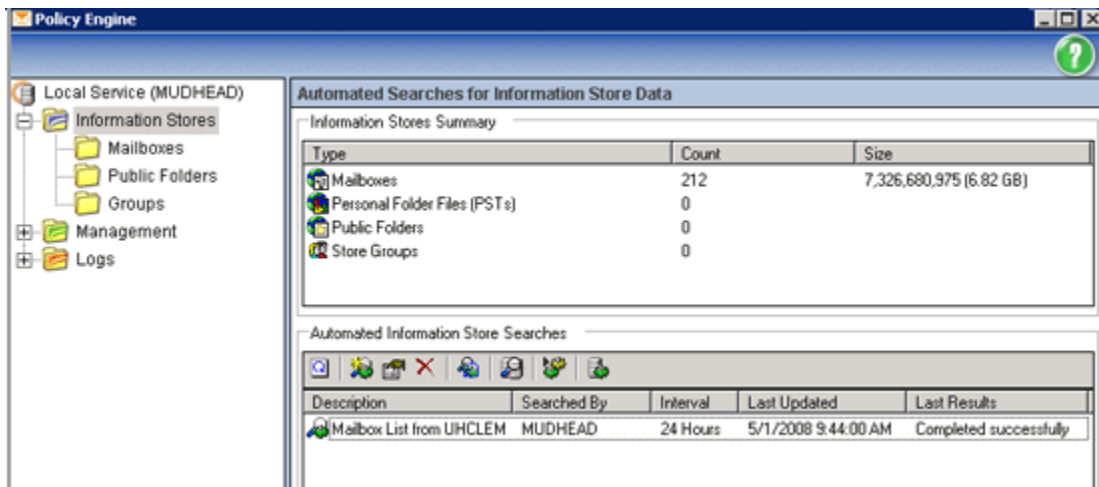
The Edit Automated Search window appears.

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” on page 16 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.



Configuring Selective Archiving events

Use the Archive Scheduler to create events for archiving data within the Exchange environment. When Selective Archiving events are defined, companion rules are created in the Policy Engine.

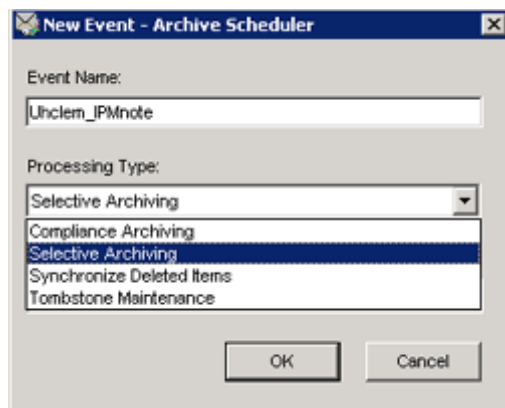
Creating a Selective Archiving event

To create a Selective Archiving event:

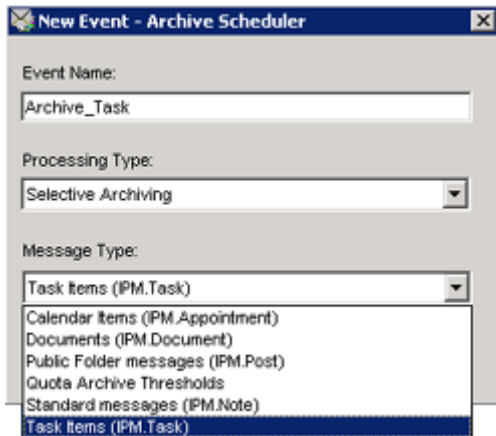
1. Log on to the Archive Gateway as the archive service account.
2. Open Archive Scheduler by clicking the Archive Scheduler icon on the desktop.
3. In the Archive Scheduler window, select **New** to display the New Event window.

If you are creating the first event, the New Event window appears automatically when you start Archive Scheduler.

4. Enter a descriptive name for the event in the Event Name box.
The name should not contain any special characters.
5. Select the **Selective Archiving** processing type in the **Processing Type** drop-down list.



6. Select the type of message from the **Message Type** drop-down list:
 - Calendar items (IPM.Appointment)
 - Documents (IPM.Document)
 - Standard email messages (IPM.Note)
Includes secure and encrypted email.
 - Task Items (IPM.Task)



 **NOTE:**

For the steps required to archive messages in Public Folders (IPM.Post), see [“Archiving messages in public folders”](#) on page 67.

For the steps required to archive messages to a mailbox quota threshold, see [“Archiving to a quota threshold”](#) on page 49.

For the steps required to archive messages in team (shared) mailboxes, see [“Creating a team mailbox archiving event”](#) on page 37.

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 **OK** to close the dialog box.

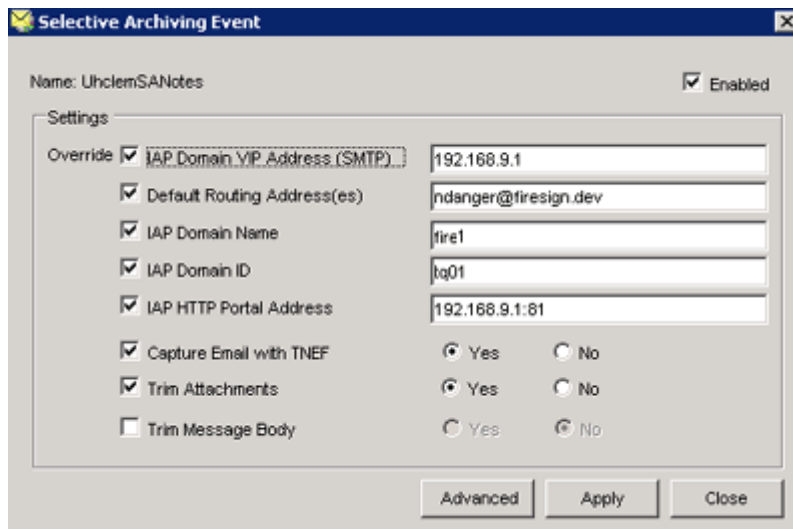
Editing Selective Archiving events

When the HP EAs Exchange software is installed, your HP service representative configures global archiving settings in the `G:\Mining>Selective Archiving\HPAE.ini` file on the Archive Gateway. Events in the Archive Scheduler are populated with these values. The global values can be overridden in a scheduled event, but should be changed only under the supervision of HP technical support. Event overrides are placed in separate .ini files in `G:\Mining>Selective Archiving\Events`.

In most cases, you will open the event window only to enable or disable an event.

To edit a Selective Archiving event:

1. Open Archive Scheduler.
2. Select the event in the Archive Scheduler window, and click **Edit**.
3. In the event window, select the **Enabled** check box to enable the event.
Disable the event by clearing the check box.
4. If you are editing a setting (under the guidance of HP technical support), select the **Override** check box in front of the setting, and then enter a new value.



Field	Description
IAP Domain VIP Address (SMTP)	The IAP Virtual IP (VIP) used for SMTP. The VIP is the internal IAP domain that stores documents and is the same value as the ipToDomainInfo attribute used in Domain.jcml.
Default Routing Address(es)	<p><code><user>@<iap-domain.com></code></p> <p>Replace <code><user></code> with either a fictitious user or a real user name. If a fictitious user is entered, the undeliverable messages are routed to the catchall repository on the IAP. If a real user is entered, the undeliverable messages are sent to that user's repository. One or more users can be specified, with the user addresses separated by commas.</p> <p>Replace <code><iap-domain.com></code> with the domain name specified in Domain.jcml.</p>
IAP Domain Name	The name of the internal IAP domain to which the email should be stored. The Domain Name must match exactly the domain name attribute specified in Domain.jcml.
IAP Domain ID	The domain ID that matches the domain name specified above. The Domain ID must match exactly the domain ID attribute in Domain.jcml.
IAP HTTP Portal Address	The VIP of the IAP domain for which archiving is set up, followed by the non-sticky port number. For example, 192.168.9.8:81. This enables load balancing message-by-message. For the VIP, use the ipToDomainInfo attribute in Domain.jcml.
Capture Email with TNEF	TNEF is enabled automatically for all message types except IPM.Note. For IPM.Note events, select Yes to send messages to the IAP in TNEF format or No to send messages in MIME format.
Trim Attachments	<p>Selecting Yes removes attachments when messages are archived and replaces the attachments with a proxy file in the tombstoned messages.</p> <p>In Outlook the proxy appears under its filename, ArchiveInfo.htm. In OWA the proxy appears under its display name, Attachment Info.htm.</p>
Trim Message Body	Selecting Yes removes the message body from tombstones.

5. Click **Apply**, and then click **Close** to finalize the changes.

Clicking the **Advanced** button in the event window displays the settings in text format.

Processes that are currently being executed are not affected by any modifications you make.

Copying a scheduled event

Copy a scheduled Selective Archiving event by following these steps:

1. Select the relevant event and click **Copy**.
2. In the Copy Event window:
 - a. Enter a name for the new event.
 - b. Select a **Message Type** from the drop-down list.
 - c. Click **OK** to create the event copy.

The event window appears.

3. Select the **Enabled** check box to enable the event.
Edit other settings under the direction of HP technical support.
4. Click **Apply** and then **Close** to finalize the changes.

A dialog box appears indicating that a companion rule for the event has been created in the Policy Engine.

5. Edit the rule in the Policy Engine.

Deleting a scheduled event

To delete a scheduled Selective Archiving event:

1. Select the appropriate event and click **Delete**.

A dialog box appears asking you to confirm the delete request.

2. Click **Yes** to complete the delete process.

A dialog box appears asking if the companion rule for this event in the Policy Engine should also be deleted.

3. Click **Yes** to delete the companion rule from the Policy Engine database.

Creating a team mailbox archiving event

In general, only users who are listed in the To/From/CC/BCC fields of a message have access to the message when it is stored in the IAP. However, if the ExpandACL setting is enabled for certain Selective Archiving events, the message is sent to the repositories of all users listed in the original mailbox user's Access Control List (ACL).

ACL expansion should not be enabled for most Selective Archiving events, to avoid archiving messages to repositories where they do not belong. ACL expansion can, however, be enabled for two types of events:

- Public folder events (see “[Archiving messages in public folders](#)” on page 67).
- Shared (team) mailbox events, so that all users listed in the mailbox ACL have access to archived messages.

Follow the steps below to expand the ACL in team mailbox events.



NOTE:

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

1. Verify that ACL expansion is not enabled in the global configuration file:
 - a. On the Archive Gateway, open the global configuration file `G: \Mining\Selective Archiving\HPAE.ini`.
 - b. Locate the `ExpandACL` parameter in the `[ExchSelectiveArchiving]` section.
 - c. Ensure the value is set to `False`.
If this parameter does not appear in the file, the value has automatically been set to `False`, the default.



IMPORTANT:

ACL expansion should never be enabled in the global configuration file. Doing so sets ACL expansion globally for Selective Archiving.

2. In Archive Scheduler, create an event to specifically archive team mailboxes:
 - **Processing type:** Selective Archiving
 - **Message type:** Standard messages (IPM.Note)
3. Open the team mailbox event for editing.
4. In the event window, click **Advanced** to display the advanced settings for the event.
5. Locate the `[ExchSelectiveArchiving]` section.
6. Add the statement `ExpandACL=True` directly under the `[ExchSelectiveArchiving]` section header.

The section now begins:

```
[ExchSelectiveArchiving]
ExpandACL=True
```

7. Click **Apply**, and then click **Close** to finalize the changes.

Changing the `ExpandACL` setting overrides the global configuration file for the event. The event override `.ini` file is placed in `G: \Mining\Selective Archiving\Events` on the Archive Gateway.

8. Open Policy Engine and select the archiving rule that was created for the event.
For information on opening and configuring the rule, see [“Editing Selective Archiving rules”](#) on page 38.
9. In the **Information Stores** tab, select the team mailboxes to be covered by the rule.
Be sure to select only the relevant team (shared) mailboxes.
10. Configure the settings in the remaining tabs, and then save the rule.
11. In Archive Scheduler, enable the team mailbox event.

 **NOTE:**

You can give users access to a team’s archived messages through ACL expansion (as shown in the procedure above) or through the IAP software (by granting access to a team repository).

Users added via ACL expansion can access the team’s archived messages in their personal repositories only while they are members of the team. They must have access to the team repository to retrieve messages archived before they joined the team (or after they left the team).

Editing Selective Archiving rules

When an event is created, a corresponding rule is set up in the Policy Engine. You can add information to a rule, but do not delete or change any items that are already configured.

To edit Selective Archiving rules:

1. Log into the Archive Gateway as the archive service account.
2. Double-click the Policy Engine icon on the desktop.
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 (created by Archive Scheduler) to be modified.
The General tab appears with the rule description, category, and rule type.
5. Modify the settings as necessary:
 - [Information Stores tab](#), page 38
 - [Folders tab](#), page 40
 - [Conditions tab](#), page 41
 - [Actions tab](#), page 43
 - [Schedule tab](#), page 44
6. Click **OK** to save the modifications to the Policy Engine rule.

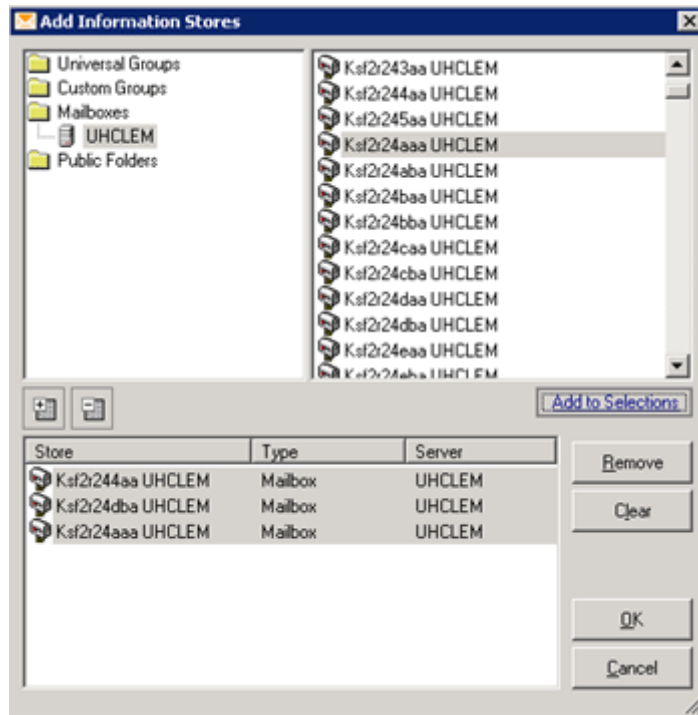
Information Stores tab

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

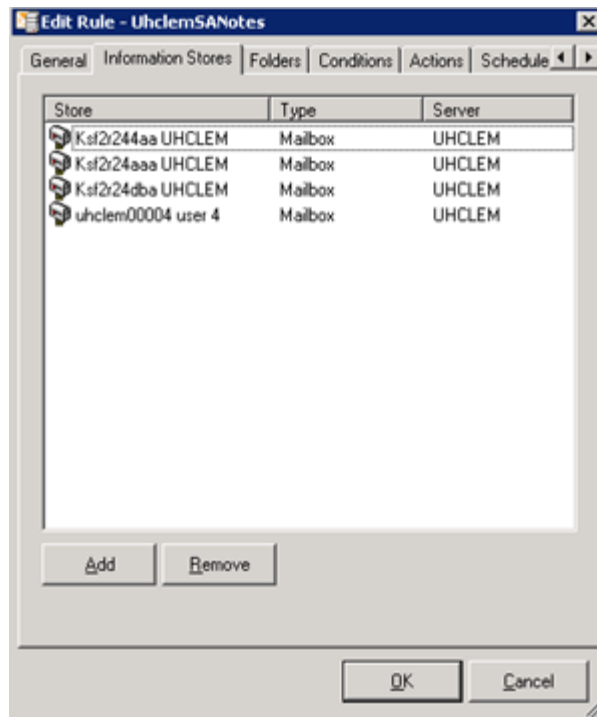
To add information stores:

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. To archive mailbox items:
 - a. Click **Mailboxes** to process either specific mailboxes or all mailboxes on the Exchange server.
 - b. After making a selection, click **Add to Selections**.



- c. Click **OK** when you have finished adding mailboxes.
The mailboxes are added to the Information Stores tab.



Folders tab

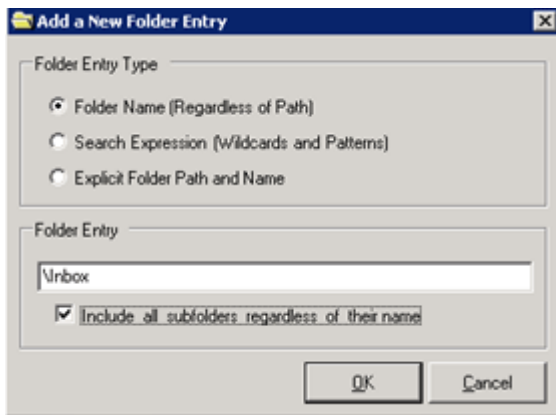
Use the Folders tab to select the Outlook folders to which a rule applies.

You can choose to archive:

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

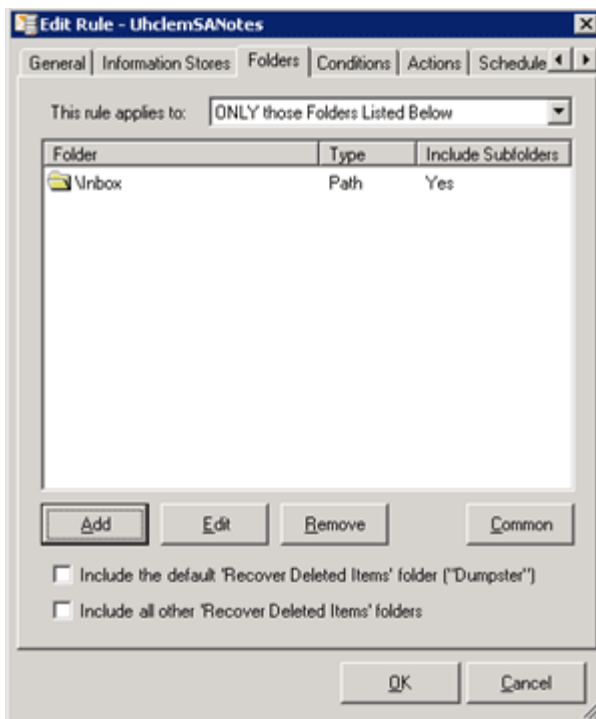
For example, to archive only items in users' Inbox folders:

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.



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

 **NOTE:**

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

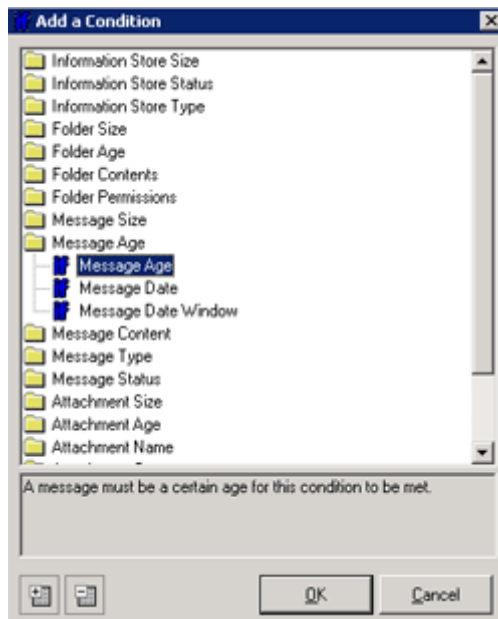
Add new conditions to a Condition List by following these steps:

1. Click **Add**.

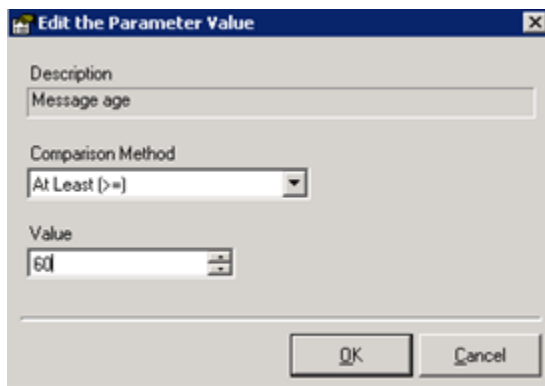
A window containing a list of all the possible conditions appears.

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

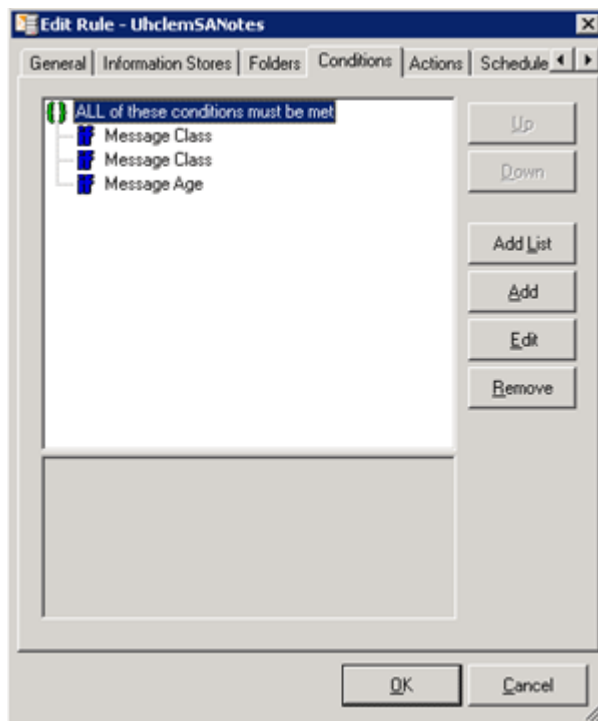
For example, to add the condition to archive messages more than 60 days old, select **Message Age** in the Message Age folder.



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**.



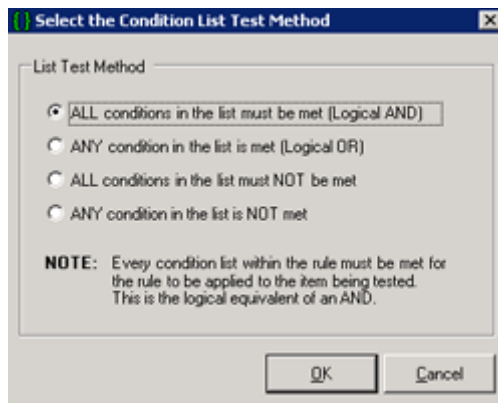
4. In the Edit the Condition window, click **OK** to add the condition.
The condition now appears in the Condition List.



Determining how conditions are applied

Determine how the conditions listed are applied during archiving.

1. Select the Condition List, and click **Edit**.
2. Select one of the following test methods:
 - All conditions in the list must be met.
 - Any condition in the list must be met.
 - All conditions in the list must **not** be met.
 - Any condition in the list must **not** be met.



3. Click **OK**.

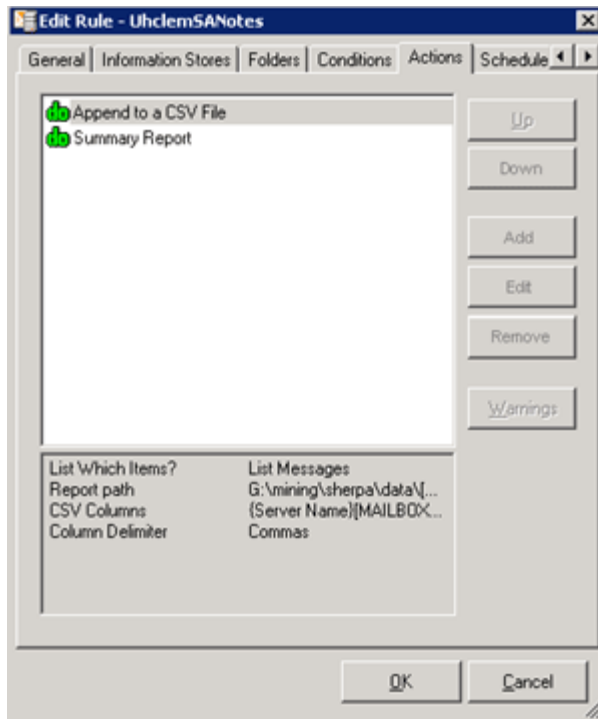
The method selected appears in the Condition List.
4. To create a Condition List with a different test method, click **Add List**, select the test method, then add conditions to the list.

For example, in the same rule you can create a list where all conditions must be met, and another list where any condition in the list can be met.

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.

If you need an action to be added or edited (for example, if you want to change reporting or logging criteria), discuss your requirements with the HP service representative or with HP support.



Schedule tab

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

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

You can choose to schedule the rule so that

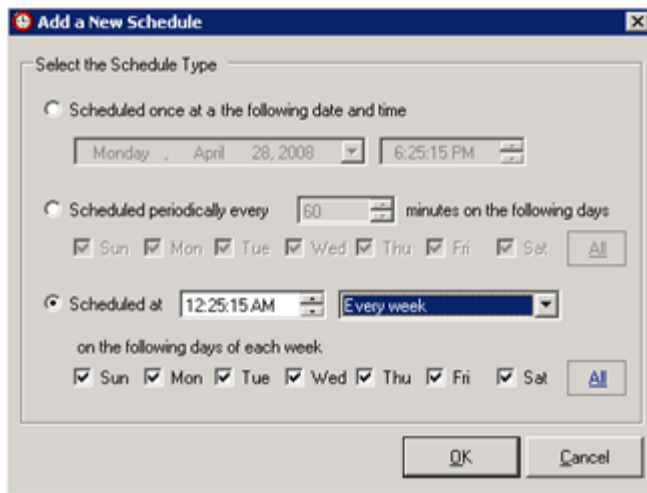
- It only occurs once.
- It occurs periodically throughout the day on specified days.
- It occurs at specified times on specified days and weeks.



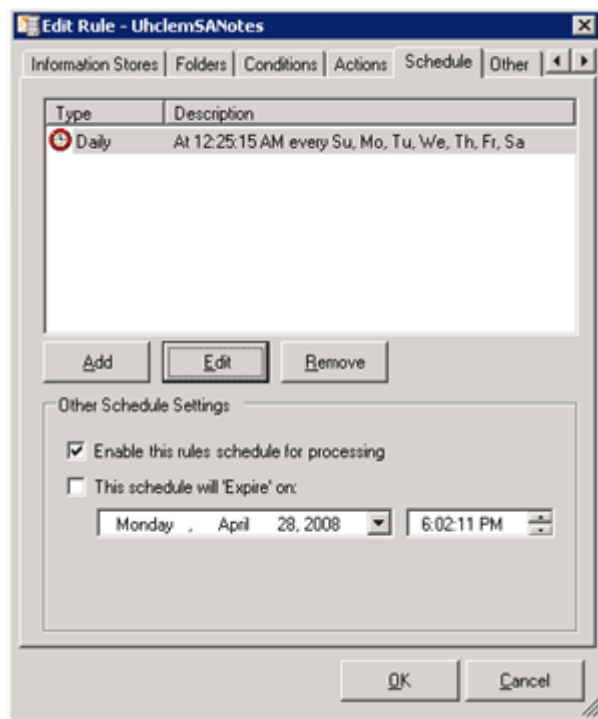
NOTE:

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

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



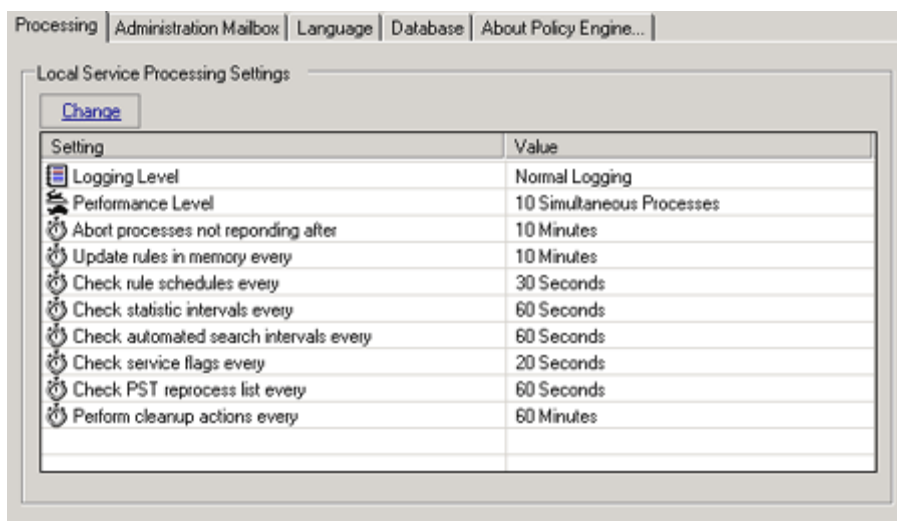
3. On the Schedule tab, select the check box to enable the rule for processing.



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

Editing local service processing settings

The local service processing settings are defined in the right pane of the Policy Engine window. You can change the logging level and service time-out settings by clicking **Change** on the Local Service Processing Settings tab.



△ CAUTION:

Consult HP technical support before changing the number of Performance Level processes.

Configure the administration mailbox settings by clicking **Change** in the Administration Mailbox tab and creating an Outlook profile. The administration mailbox is used by the local service to perform tasks such as sending messages and notifications, looking up addresses in the GAL, and copying or moving content.

Starting the archiving process

After a Selective Archiving event is enabled and its corresponding rule is scheduled for processing, the event is executed automatically.

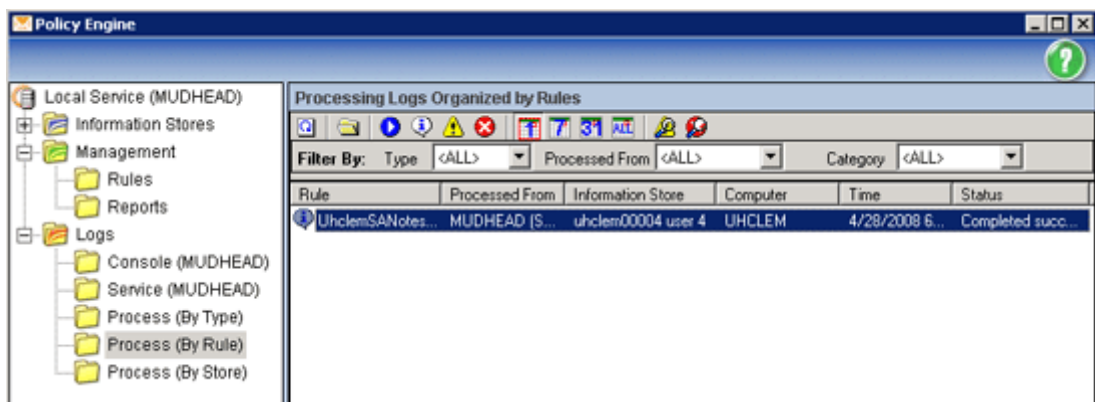
To execute a Policy Engine rule manually, without scheduling:

1. On the Archive Gateway, select **Start > Administrative Tools > Services**.
2. In the Services list:
 - Ensure the logon for the HP EAsE Archive Engine, JBOSS, and Mail Attender Enterprise services is set to <domain>\HPAEServiceAccount.
 - Ensure that each service has been started.
3. Open Policy Engine.
4. 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.

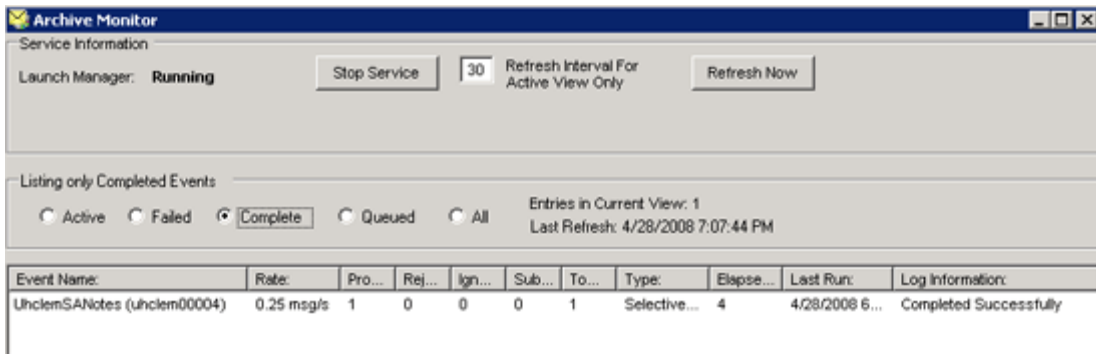


3. Double-click the entry to display the log information.

Viewing event status

The Archive Monitor on the Archive Gateway shows the status of all scheduled events. A series of radio buttons allow the information to be filtered by different conditions. Various statistical data is provided for each event displayed.

To open the Archive Monitor, double-click the Archive Monitor icon on the desktop.



The top area of the window shows the status of the HP EAsE Archive Engine service. This service launches the enabled events that are defined in Archive Scheduler. From this area, you can start or stop the service. You can also set the refresh interval. The Archive Engine service must be running for any event to be processed.

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 Archive Monitor window 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 created in Archive Scheduler.
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 of 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 that was created in Archive Scheduler.
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.

4 Archiving to a quota threshold

A Quota Archive Threshold event and its corresponding rule mine information stores so that their size falls below a particular threshold. The threshold can be a percentage of the mailbox storage limit, or quota, that is set in Active Directory, or it can be determined by mailbox size. The rule also determines the conditions under which messages are selected for archiving.

- [Configuring a Quota Archive Threshold event and rule](#), page 49
- [Selection tab](#), page 50
- [Messages tab](#), page 53

Configuring a Quota Archive Threshold event and rule

To create and configure a Quota Archive Threshold event and corresponding rule:

1. Start Archive Scheduler.
2. Click **New** to create a Selective Archiving event, and then configure the event in the New Event window:
 - Event Name: Enter a name for the event
 - Processing Type: Select **Selective Archiving**
 - Message Type: Select **Quota Archive Thresholds**
3. Click **OK**.

A dialog box appears stating that a corresponding rule for the event has been created in the Policy Engine database.
4. Click **OK** to close the dialog box.

The event appears in the Archive Schedule window.
5. Select the event and click **Edit**.
6. In the event window, select the **Enabled** check box.
7. If you are editing a setting (under the guidance of HP technical support), select the **Override** check box in front of the setting, and then enter a new value.

For a description of each of the event settings, see [“Editing Selective Archiving events”](#) on page 34.
8. Click **Apply**, and then click **Close** to finalize the changes.
9. Click **Exit** to close Archive Scheduler.

10. Open Policy Engine.
11. In the left pane of the Policy Engine window, expand the Management folder, and then select **Rules**.
12. Double-click the Quota Archive Threshold rule in the right pane.
13. Configure the rule:

Tab	Configuration
Information Stores	Select the mailbox stores to be archived. See “ Information Stores tab ” on page 38.
Folders	Select the Outlook folders containing the messages to be processed. See “ Folders tab ” on page 40.
Selection	Configure the qualifications that determine which messages are selected for archiving. See “ Selection tab ” on page 50.
Messages	Determine which message types are processed by the rule. See “ Messages tab ” on page 53.
Actions	Do not edit.
Schedule	Schedule the rule. See “ Schedule tab ” on page 44.

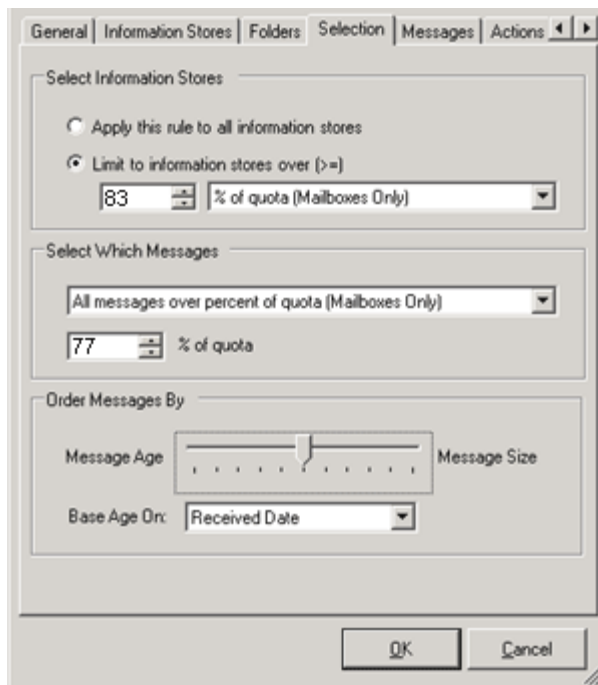
14. Click **OK**.

Selection tab

NOTE:

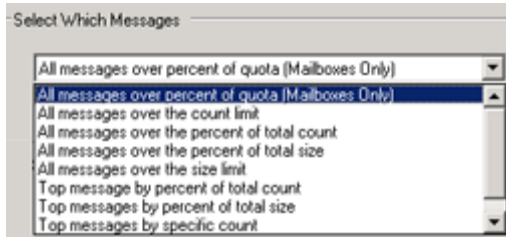
The Selection tab is only available for Quota Archive Threshold events.

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. This is the most commonly-used 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 weighed 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. 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 below 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. For example, if you select 100 messages, 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. 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>

Item	Description
All messages over the percent of total size	Determine the percentage of messages to remain in 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 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.
All messages over the size limit	Process messages when the mailbox exceeds a certain size. Enter the size in megabytes. 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.
Top messages by percent of total count	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. 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.
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. Weigh messages according to age or size to establish the order for processing.

The items that can be weighed 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



4. Determine how the date is defined for 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.

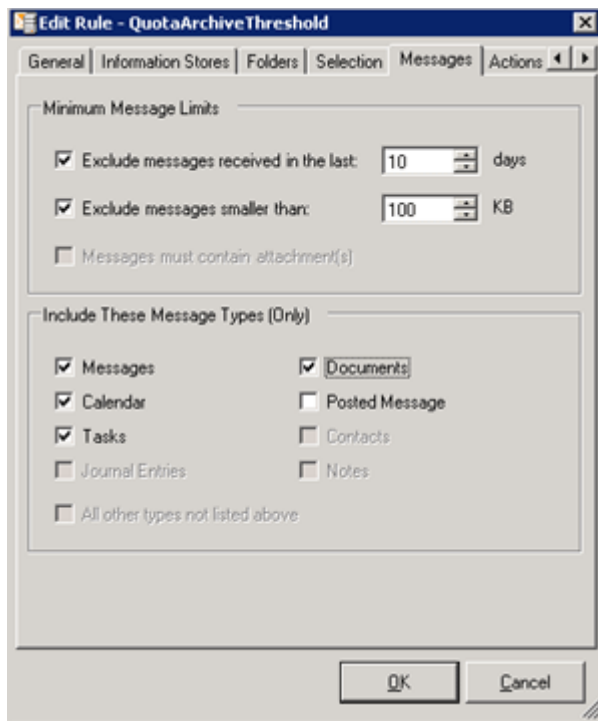
In fact, it is possible to exclude so many items that mining will not take place at all. For example, if you are archiving to a percentage of the quota, it is possible that the upper limit might not be reached and mining will not occur.

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.



1. 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)

5 Using tombstone maintenance

When a message is selectively archived, or is imported into the IAP using PST import, a tombstone can be created in the user's mailbox or 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 55
- [Configuring Tombstone Maintenance events with folder capture](#), page 56

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 the event is run once after a software upgrade, so the tombstoned items are compliant with the newly-installed version of the software. After that, HP recommends that the event is only run every few months.

To create the event and corresponding rule:

1. Log on to the Archive Gateway as the archive service account.
2. Start Archive Scheduler.
3. Click **New** to create the event, and then configure the event in the New Event window:
 - Event Name: Enter **TombstoneMaintenance**
 - Processing Type: Select **Tombstone Maintenance**
 - Maintenance Option: **Tombstone Maintenance**
4. Click **OK**.

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

5. Click **OK** to close the dialog box.
The event appears in the Archive Scheduler window.
6. Select the event and click **Edit**.
7. Select the **Enabled** check box, and then click **Apply** and **Close**.
8. Click **Exit** to close Archive Scheduler.
9. Open Policy Engine.

10. In the left pane, expand **Management**, select **Rules**, and then double-click **TombstoneMaintenance** in the right pane.

11. Configure the rule:

Tab	Configuration
Information Stores	Select the mailboxes to be archived. See " Information Stores tab " on page 38.
Folders	Select the Outlook folders containing the messages to be archived. See " Folders tab " on page 40.
Conditions	Do not edit the Message Class.
Actions	Do not edit.
Schedule	Schedule the rule. See " Schedule tab " on page 44.

12. Click **OK**.

Configuring Tombstone Maintenance events with folder capture

When folder capture is enabled in the IAP and EAs, 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.

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. In Archive Scheduler, click **New** to create the event.
2. Configure the event in the New Event window:
 - Event Name: Enter **TombstoneMaintenance**
 - Processing Type: Select **Tombstone Maintenance**
 - Maintenance Option: **Tombstone Folder Synchronization**
3. Click **OK**.

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

4. Click **OK** to close the dialog box.

The event appears in the Archive Scheduler window.
5. Select the event and click **Edit**.
6. Select the **Enabled** check box, and then click **Apply** and **Close**.
7. Click **Exit** to close Archive Scheduler.

8. Open Policy Engine.
9. In the left pane, expand **Management**, select **Rules**, and then double-click **Tombstone Folder Sync** in the right pane.
10. Configure the rule:

Tab	Configuration
Information Stores	Select the mailboxes to be archived. See " Information Stores tab " on page 38.
Folders	Select the Outlook folders containing the messages to be archived. See " Folders tab " on page 40.
Conditions	Do not edit the Message Class.
Actions	Do not edit.
Schedule	Schedule the rule. See " Schedule tab " on page 44.

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

6 Configuring end-user delete

Exchange supports a 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 tombstone (a “footprint” with a reference to the archived message on the IAP), 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.jcml` file on the IAP: `MinRegulatedRetentionPeriodDays` and `MinUnRegulatedRetentionPeriodDays`, which define the minimum data retention period for a user repository.

- [Location of deleted items](#), page 59
- [Enabling deletion retention on the Exchange server](#), page 60
- [Scheduling deletion from the IAP](#), page 61

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. 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 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

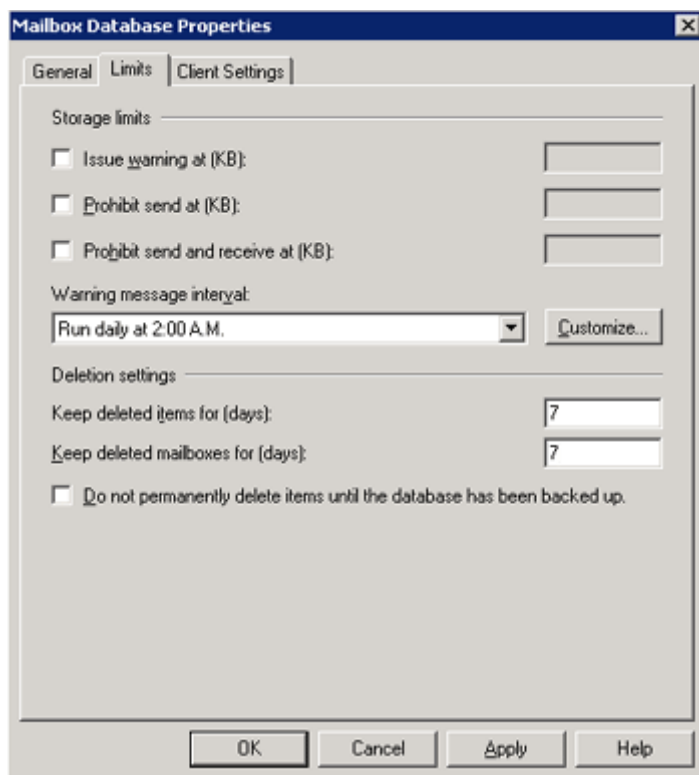
To enable deletion retention on the Exchange server, configure the following settings for each mailbox store.

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**.



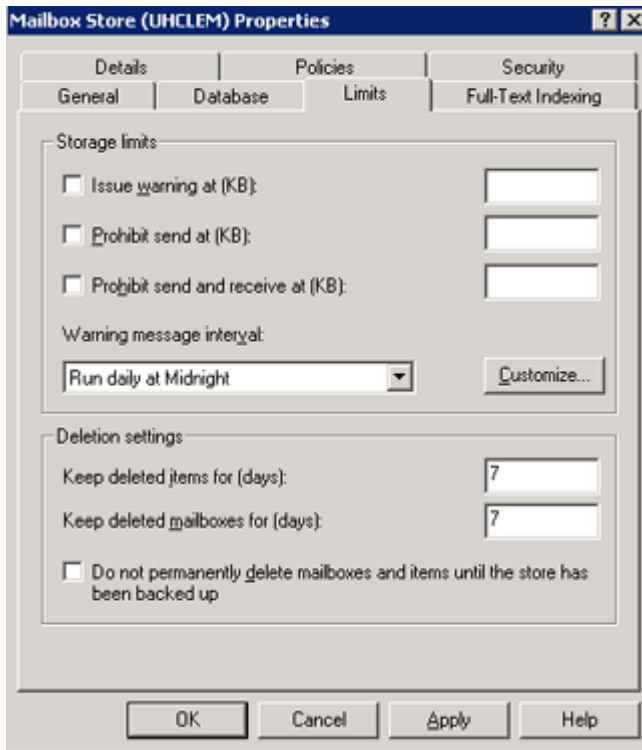
6. Click **Apply**, and then click **OK**.
7. Repeat steps 4–6 for each relevant Storage Group and Mailbox Database.

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 in Archive Scheduler and establish a corresponding rule in Policy Engine.

Creating the event

1. Log on to the Archive Gateway as the archive service account.
2. Open Archive Scheduler clicking the Archive Scheduler icon on the desktop.
3. In the Archive Scheduler window, select **New** to display the New Event window.
4. Enter a descriptive name for the event in the Event Name box.

The name should not contain any special characters.

5. Select the **Synchronize Deleted Items** processing type in the **Processing Type** drop-down list.

6. Click **OK**.
A dialog box appears stating that a corresponding rule for the event has been created in the Policy Engine database.
7. Click **OK** to close the dialog box.
8. Select the event in the Archive Scheduler window, and click **Edit**.
9. In the event window, select the **Enabled** check box to enable the event, and then click **Apply** and **Close**.
10. Click **Exit** to close Archive Scheduler.

Creating a Policy Engine rule

To create the Policy Engine rule:

1. Open Policy Engine.
2. In the left pane, expand **Management**, select **Rules**, and then double-click the Synchronize Deleted Items rule in the right pane.
3. In the Information Stores tab, select the mailboxes to be archived. See “[Information Stores tab](#)” on page 38.
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 causes 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 below, 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](#)” on page 44 for more information.

7 Working with folder capture

This chapter contains the following topics:

- [Introduction](#), page 63
- [Indexing folder information](#), page 63
- [Enabling folder capture](#), page 64
- [How folder capture works with archiving events](#), page 65
- [Folder capture and the merging of duplicate messages](#), page 66

Introduction

The folder capture feature captures the Outlook location of archived messages and updates the corresponding 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 in Archive Scheduler:
 - Selective Archiving
 - Tombstone Maintenance (Tombstone Folder Synchronization)
 - Synchronize Deleted Items
- PST Import Tools

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](#).

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](#)” on page 107. To prevent this error, HP recommends setting the cut off date to the date the system is upgraded.

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 set 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. Open Archive Scheduler on the Archive Gateway.
2. Select the event in the Archive Scheduler window, and click **Edit**.
3. Click **Advanced** in the event window.
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 **Apply**, and then click **Close**.
6. In the event window, click **Apply**, and then click **Close**.

Enabling folder capture in PST Import Tools

In PST Import Tools, 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 revising an Archive Request file”](#) on page 74 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 below). 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”](#) on page 56 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”](#) on page 59. 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”](#) on page 61.



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 Tools

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.

PST Import Tools and the Archive Request file are described in [“Archiving with the PST Import Tools”](#) on page 71

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.

8 Archiving messages in public folders

This chapter describes HP EAs Exchange support for Selective Archiving of messages in public folders.

- [Overview](#), page 67
- [Configuring the Exchange server](#), page 67
- [Configuring a public folder event](#), page 69
- [Adding public folders to Information Stores](#), page 69
- [Configuring the public folder rule](#), page 69
- [Enabling ACL expansion](#), page 70

Overview

HP EAs Exchange offers limited support for the Selective Archiving of messages in public folders.

There are several limitations to archiving messages in public folders:

- Users with read access to the public folders are able to open and view archived messages when the HP EAs Exchange Outlook Plug-In is installed on their machines. However, they are not able to search for or retrieve the messages from the IAP.
- Only users listed in the To/From/CC/BCC fields of archived messages are able to search for or retrieve the messages from the IAP Web Interface or Outlook Integrated Archive Search. Storage is not applied to users in the public folders ACL unless ACL expansion is enabled. See [“Enabling ACL expansion”](#) on page 70.
- If a tombstone is deleted from a public folder, only a user listed in the To/From/CC/BCC field or a super-user (administrator) can search for and retrieve the email.
- Appropriate Editor permissions must be assigned to the archive service account for all public folders on the Exchange server that are processed by Selective Archiving. The next section describes this process. The remaining sections cover the creation of the events and rules used by the Selective Archiving process.

Configuring the Exchange server

Before messages in public folders can be archived, the Exchange server must be configured so the archive service account (HPAEServiceAccount) has the appropriate permissions to archive and tombstone messages in public folders.

Exchange 2007

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.

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.

Pre-2007 Exchange servers

 **NOTE:**

The appropriate Editor permissions must be assigned to the archive service account for **every** public folder to be archived.

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**, 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.

Configuring a public folder event

To configure a public folder event.

1. Log on to the Archive Gateway as the archive service account.
2. Start Archive Scheduler.
3. Click **New** to create a Selective Archiving event, and then configure the event in the New Event window:
 - Event Name: Enter a descriptive name; for example, servername_PublicFolders.
 - Processing Type: Select **Selective Archiving**
 - Message Type: **Public Folder messages (IPM.Post)**
4. Click **OK**.

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

5. Click **OK** to close the dialog box.

The event appears in the Archive Schedule window.
6. Select the event and click **Edit**.
7. In the event window, select the **Enabled** check box.
8. If you are editing a setting (under the guidance of HP technical support), select the **Override** check box in front of the setting, and then enter a new value using the guidelines in [“Editing Selective Archiving events”](#) on page 34.
9. Click **Apply**, and then click **Close** to finalize the changes.
10. Click **Exit** to close Archive Scheduler.

Adding public folders to Information Stores

1. Start Policy Engine.
2. In the left pane, expand the Information Stores folder.
3. In the left pane, select **Public Folders**.
4. Right-click in the right pane and select **Add Public Folders > From the Global Address List**.
5. Select an Outlook profile that can access the Global Address List (GAL), and click **OK**.

If a profile does not exist, create a new Outlook profile:

- a. Select **New**.
 - b. In the wizard, select **Microsoft Exchange Server**, and click **Next**.
 - c. Enter a profile name, and click **Next**.
 - d. In the server box, enter the IP address or name of the Exchange server, and then click **Next**.
6. 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.

Configuring the public folder rule

To configure the public folder rule:

1. Open Policy Engine.

2. In the left pane, expand **Management**, select **Rules**, and then double-click the public folder rule in the right pane.
3. In the Information Stores tab, click **Add** and then follow these steps:
 - a. In the left pane, select **Public Folders**.
 - b. Select each public folder to be archived, and click **Add to Selection**.
 - c. Click **OK** when you have finished adding public folders.
 - d. Click **OK**.
4. In the Folders tab, select **All Folders** or any specific public folders.
5. Click the Conditions tab.
Two Message Class entries are listed. Do not remove these entries.
6. In the Conditions tab, add a Message Age condition:
 - a. Click **Add**.
 - b. Select **Message Age > Message Age** and click **OK**.
 - c. In the Edit the Condition window, select **Message Age** and click **Edit Value**.
 - d. In the Value box, select **1** and click **OK**.
 - e. Select **Age units** and click **Edit Value**.
 - f. In the Parameter value box, select **Minutes** and click **OK**.
 - g. Click **OK** to save the new condition.
7. Click the Schedule tab and schedule the rule.
See “[Schedule tab](#)” on page 44 for more information.
8. Click **OK** to save the rule modifications.

Enabling ACL expansion

Unless the access control list (ACL) is expanded, only users who are listed in the To/From/CC/BCC fields of archived messages in public folders can search for or retrieve the messages from the IAP. If you want to enable ACL expansion for public folders, follow these steps.

1. Open Archive Scheduler.
2. In the Archive Scheduler window, locate the public folder event and click **Edit**.
3. Click the **Advanced** button to display the advanced settings for the event.
4. Find the [ExchSelectiveArchiving] section.
5. Add the statement `ExpandACL=True` directly under the [ExchSelectiveArchiving] section header.

The section now begins:

```
[ExchSelectiveArchiving]
```

```
ExpandACL=True
```

6. Click **Apply**, and then click **Close** to finalize the changes.

ACL expansion is now enabled in the event.

An event override `.ini` file is created for the public folder event and placed in `G:\Mining\Selective Archiving\Events`.

9 Archiving with the PST Import Tools

This chapter contains the following topics:

- [PST Import Tools overview](#), page 71
- [Installing the PST Import Tools](#), page 72
- [The PST import process](#), page 72
- [Establishing archive credentials](#), page 73
- [Creating the Archive Request file](#), page 74
- [Using the PST Import Monitor](#), page 79

PST Import Tools overview

The PST Import Tools are installed on client systems and consist of:

- PST Loader
- PST Import Monitor
- Archive Credentials

These tools allow you to:

- Load legacy PST files into the IAP.
- Scan PST files to ensure that new messages are found and archived.
- Provide optional tombstoning of messages in PST files.
The PST Import Tools can modify messages by removing attachments and body content. These altered messages are referred to as *tombstones*. You might be more familiar with the term *stub*. Outlook users see a stub icon next to tombstoned messages.
- Grant the archive service account access to the IAP.

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

IMPORTANT:

The PST Import Tools might cause a problem with anti-virus programs that are configured to inspect for email changes. This is because the tools modify every email that is archived. Symantec AntiVirus has this conflict; other anti-virus programs might have a similar conflict.

To resolve the issue, disable the anti-virus program while the PST Import Tools are running.

Symantec AntiVirus only: On the desktop that is running the PST Import Tools, open the Symantec client and turn off the Internet Email Auto Protect Option.

Installing the PST Import Tools

Follow these instructions to install the PST Import Tools on client systems.

Installation requirements

Before installation, verify that the client machine on which you are installing the tools 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.

Network requirements on client machine

- 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

IAP software requirements

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

Installation procedure

Always install the PST Import Tools on a client machine. Do not install the tools on the Archive Gateway.



NOTE:

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

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.

The PST import process

Follow these steps to import messages from PST files into the IAP:

1. Use Archive Credentials to generate the necessary permissions for archiving to the IAP. See [“Establishing archive credentials”](#) on page 73.
2. Use PST Loader to create an Archive Request file. See [“Creating or revising an Archive Request file”](#) on page 74.
3. Validate that each PST file in the Archive Request file is available. The validated files are added to the PST import database, `AEDB.mdb`, for processing. See [“Validating the file using the PST Loader”](#) on page 78.
4. Use the PST Import Monitor to launch the import process. The HP EAsE Archive Engine service reads the PST file and archives messages that have not been tombstoned or previously archived. See [“Using the PST Import Monitor”](#) on page 79.

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. Click the Archive Credentials icon on the desktop or select **Start > All Programs > Hewlett-Packard > Email Archiving software for Exchange > PST Import Tools > Archive Credentials**.

The Archive Credentials window appears.

2. 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](#)” on page 16.

3. In the IAP Admin Password box, enter the password that was established for the service account.

4. Click **Verify** to test the account access.

The Verify IAP Credentials window appears.

5. In the IAP Address box, enter the IAP HTTP portal address, and then click **Get Domains**.

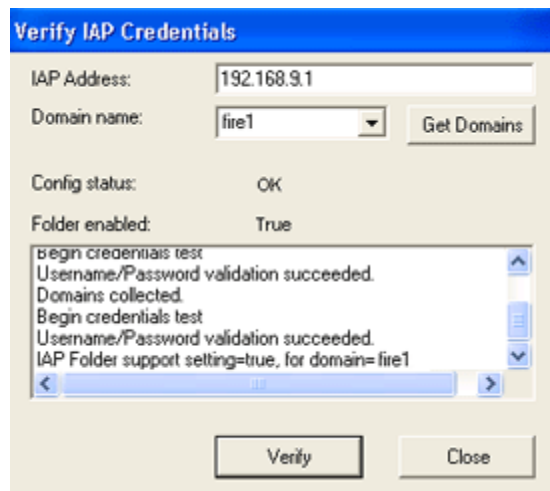
The HTTP portal address can be any of the VIP addresses listed in the ipToDomainInfo field in the Domain.jcm1 file on the IAP kickstart server.

The domains available in the IAP are added to the Domain name drop-down list.

6. In the Domain name box, select the domain in which the messages will be stored.

7. Click **Verify**.

The Archive Credentials program conducts a test access and logs the results in the status window. This example shows the results of a successful test.

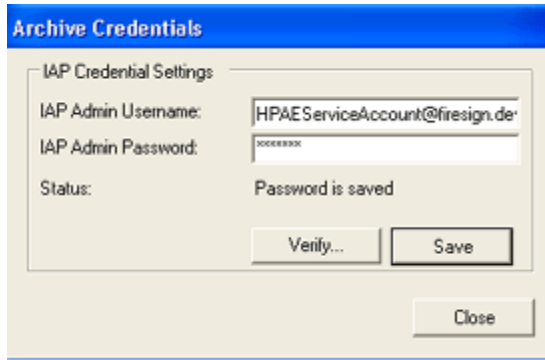


If folder capture is enabled in the IAP, the results also show the status of IAP folder support for the selected domain.

8. Click **Close** to return to the Archive Credentials window.

9. Click **Save** to save the credentials.

The status is changed, as shown in this example.



10. Click **Close** to exit the program.

Creating the Archive Request file

Use PST Loader to create or revise and validate an Archive Request file. This tool also generates an output log file, detailing issues that occurred during the load process.

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

- Verifies 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.

Archive Request file

The Archive Request file defines the set of documents to be archived. It is an XML file that is generated with PST Loader. You can also create the request file manually.

Creating or revising an Archive Request file

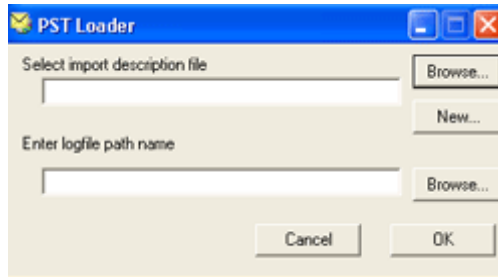
Follow these instructions to create an Archive Request file. Use the same procedure to revise a file, which you can then resubmit for subsequent processing.

If you plan to create an Archive Request file manually, see ["PST Import Tools: Archive Request file specifications"](#) on page 117 for a description of the XML tags to use and a sample XML file.

To create a new Archive Request file:

1. Click the PST Loader icon on the desktop or select **Start > All Programs > Hewlett-Packard > Email Archiving software for Exchange > PST Import Tools > PST Loader**.

The PST Loader window appears.

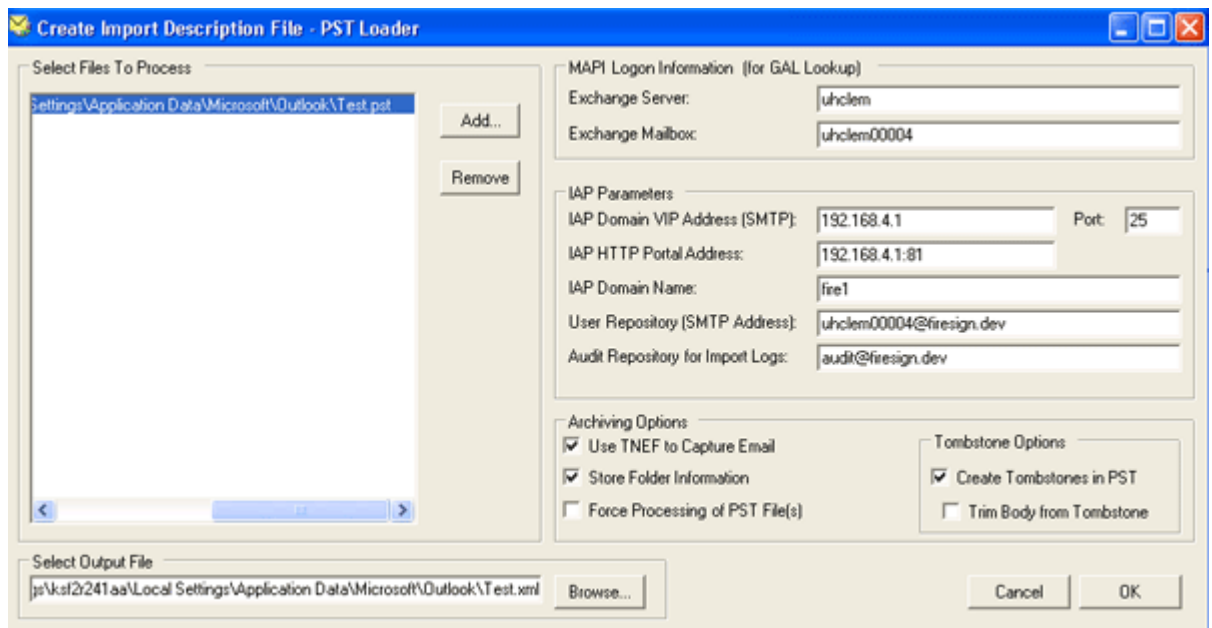


2. Click **New**.

If you are revising an existing Archive Request file, browse to the file, and then click **New** in the PST Loader window.

The Create Import Description File window appears.

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



Only files in the Select Files To Process list are imported. In the Archive Request file you are creating, the corresponding XML tags are <FileSpeclist> and <FileSpec>.

4. If necessary, select PST files you do not want to process, and click **Remove**.
5. In the **Select Output File** box, enter the path and file name of the file you are creating or revising, or click **Browse** to navigate to a location.
6. 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.

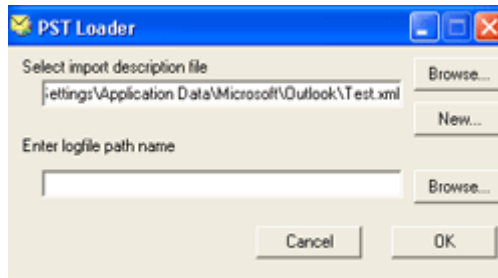
Field	Description
Exchange Server	The Exchange server used when accessing the Global Address List (GAL) for address resolution. The XML tag is <Server>.
Exchange Mailbox	The mailbox on the Exchange server used when accessing the GAL for address resolution. The XML tag is <Mailbox>.
IAP Domain VIP Address (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>.
Port	SMTP port number. This setting is optional and the default is 25. The XML tag is <SMTPPort>.
IAP HTTP Portal Address	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. The XML tag is <HTTPServer>. For 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>.
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 PST Importer log file created during the import process. (See " PST Importer log file " on page 82.) The XML tag is <AuditRepository>.

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

Field	Description
Use TNEF to Capture Email	TNEF is enabled automatically for all message types except standard email (IPM.Note). Select this check box for standard email to be archived using 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.jcml 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>.

8. Click **OK**.

The PST Loader window appears. The **Select Input File to Process** text box contains the path and file name of the Archive Request file.



To validate the file from this point, continue to the next section. You can validate the file from the PST Loader window or from the command line.

For a complete description of each XML tag in the Archive Request file and a sample file, see ["PST Import Tools: Archive Request file specifications"](#) on page 117.

 **NOTE:**

To import PST files larger than 150 MB, navigate to \Program Files\Hewlett-Packard\HP EAsE PST Importer\HP EAsE PST Importer.ini.

Edit the MaxProcesses variable as shown to reduce performance degradation and increase throughput:

```
[LaunchMgr]
```

```
MaxProcesses=1
```

Validating the file using the PST Loader

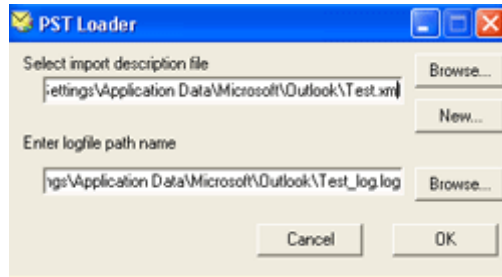
To validate the Archive Request file:

1. Open PST Loader.

The Archive Request file you created or revised in [Creating or revising an Archive Request file](#) appears in the **Select input description file** box. If it does not, browse to the file and click **Open**.

2. In the **Enter logfile path name** box, enter a path and file name for a new PST Loader log file, or click **Browse** to locate an existing log file.

The log file contains processing and error information generated while loading the Archive Request file. If the log file already exists, PST Loader appends processing and error information to the existing file.



3. Click **OK**.
4. Open the PST Import Monitor to start the import process.

In the monitor window, the file appears in Queued Processes at the bottom of the monitor window. An entry also appears in the Number Queued field in the Process Information area of the window.

See [“Using the PST Import Monitor”](#) on page 79.

NOTE:

The log file’s verbosity level is set to the default, which is 3 (information). To change the level, navigate to `\Program Files\Hewlett-Packard\HP EASE PST Importer\HP EASE PST Importer.ini`. Edit the default verbosity value to the level of your choosing:

```
[HPPSTInit]  
Verbosity=<x>
```

See [“Validating the file from the command line”](#) on page 79 for an explanation of verbosity levels.

Validating the file from the command line

Enter the HPPSTInit command with the following parameters to validate an Archive Request file:

```
<install_path>/HPPSTInit /i <ArchiveRequestFileName.xml> /o  
<LoadLogFileName.log> [/c] [/v<x>]
```

Parameter	Description
/i	Required. Name of input file to be processed. Replace <i>ArchiveRequestFileName.xml</i> with the full UNC path and XML file name.
/o	Required. Name of PST Loader log file to which diagnostic and processing information is written. Replace <i>LoadLogFileName.log</i> with the full UNC path and log file name.
/c	Optional. Parses XML structure in input file for syntax and file accessibility only. No records are added to PST.MDB for processing.
/v	Optional. Verbosity level used when processing Archive Request file. Enter a number from 0 to 5 following the /v to indicate verbosity level, with 5 containing the most detail. <ul style="list-style-type: none">• 0: Fatal• 1: Alert• 2: Warning• 3: Information• 4: Trace• 5: Debug

Using the PST Import Monitor

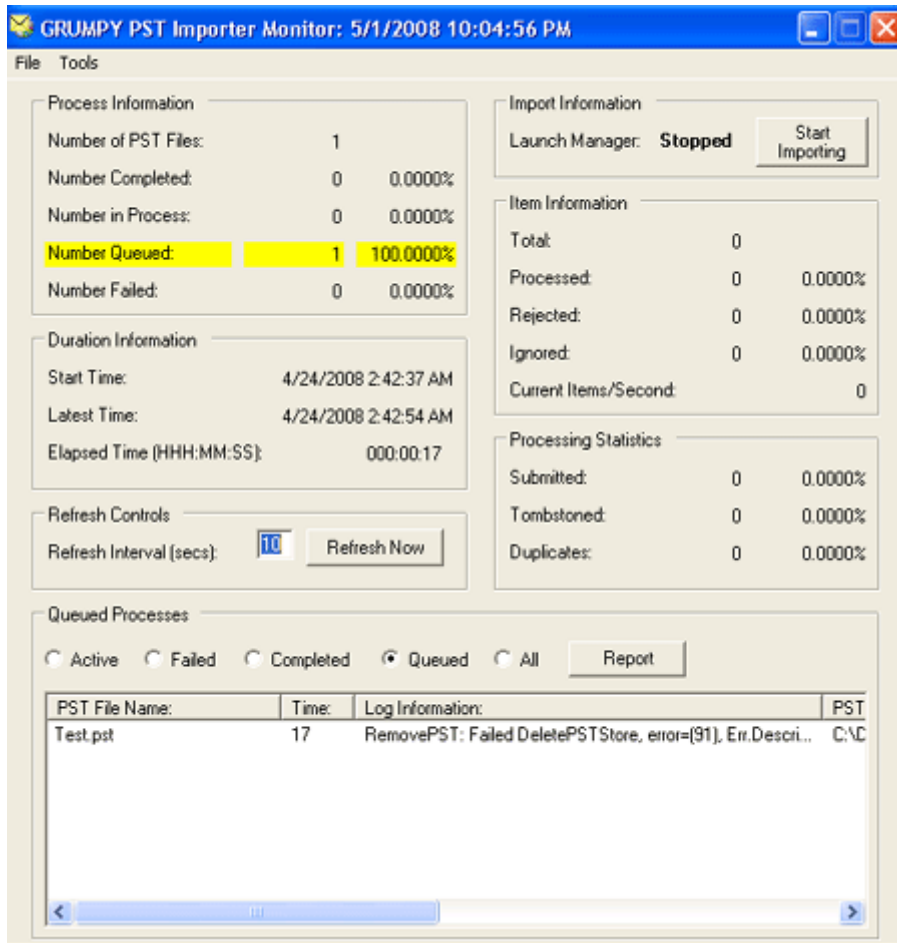
Use the PST Import Monitor to:

- 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.

Processing PST files

1. To open PST Import Monitor, click the Import Monitor icon on the desktop or select **Start > All Programs > Hewlett-Packard > Email Archiving software for Exchange > PST Import Tools > PST Import Monitor**.

The monitor window appears. Files that are waiting in queue to be processed are shown in Queued Processes at the bottom of the monitor window. Queued entries also appear in the Number Queued field in the Process Information area of the window.



2. Start the import process by clicking **Start Importing**.
This starts the archive service.
Stop the import process by clicking **Stop Importing**.
3. View specific processing information as follows:

Item	Description
Item Information area	
Total	The total number of items found in the PST files so far.
Processed	The number and percentage of items processed and submitted to the IAP.
Rejected	The number and percentage of items that the Archive Engine could not process due to errors. The PST Loader log file contains error information explaining why the item was rejected.
Ignored	The number and percentage of items that were not processed because they could not be submitted to the IAP. These Items might include tombstoned messages, IPM.Contacts, Sticky Notes, or custom items. The PST Loader log file explains why an item was rejected.

Item	Description
Processing Statistics area	
Submitted	The number and percentage of items processed and submitted to the IAP.
Tombstoned	The number and percentage of items submitted to the IAP and replaced by tombstones in the PST files. This number is not cumulative and resets per run.
Duplicates	The number and percentage of items not submitted to the IAP because duplicate items already exist in imported PST files or duplicate items are already archived to the IAP.
Processing area	
Processing radio buttons	Click the radio buttons to filter the file imports by processing status. <ul style="list-style-type: none"> • Active: Files that are currently being processed. • Failed: Files with a failed status. • Complete: Completed file imports. • Queued: Files that are in queue for import. • All: All processes.
Report button	Click Report to view a report on the PST import. See " PST Import report " on page 82

4. To collect import statistics immediately, click **Refresh Now**.

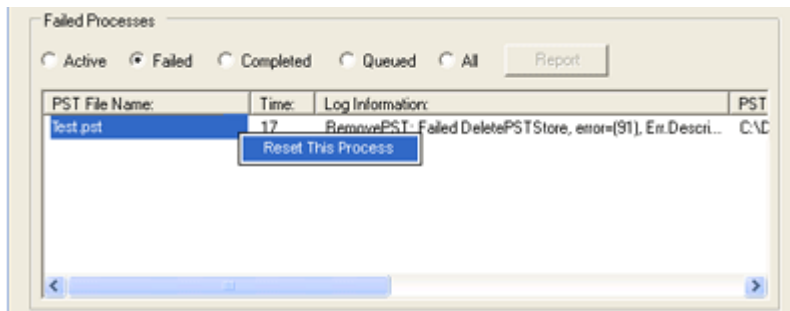
The PST Import Monitor displays statistics according to the Refresh Interval specified. The default is 10 seconds. You can change the automatic refresh interval to any whole number between 1 and 60 seconds.



NOTE:

Collecting statistics impacts performance.

5. To reset a failed process, click **Failed** in the Processes area at the bottom of the window. Right-click the failed process, then click **Reset this Process**.



Depending on the reasons the process failed, resetting a failed process might not correct the problem. However, the PST Loader tries to reprocess it as directed.

Displaying reports and log files

PST Import report

Use the PST Import Monitor to generate a PST Import report in HTML format. You can then import the report into a spreadsheet for analysis or progress tracking if needed.

1. In the Processes area of the PST Import Monitor, select a radio button and then click **Report**.
2. In the dialog box that appears, specify where to save the report, and enter a file name.

The default directory is `\Program Files\Hewlett-Packard\HP EASE PST Importer\Reports`.

3. Click **Save**.

PST Importer log file

Each archiving process is assigned a unique PST file and creates a PST Importer 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 Archive Request file. Upon successful submittal, the file is deleted on the local disk.

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>`.

To change the verbosity level of the logging, modify the `Verbosity` value in the `[HPAPPST]` area of `HP EASE PST Importer.ini`.

The default verbosity level is 3 (information). See “[Validating the file from the command line](#)” on page 79 for an explanation of verbosity levels.

10 Working with end-user applications

This chapter contains the following topics:

- [Overview of the applications](#), page 83
- [Using the IAP Web Interface](#), page 84
- [Using single sign-on](#), page 84
- [Installing and configuring the Outlook Plug-In](#), page 84
- [Exporting messages from the IAP](#), page 93

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 Plug-In 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 Plug-In, see ["Installing and configuring the Outlook Plug-In"](#) on page 84.

The Outlook Plug-In 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"](#) on page 99.

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" on page 15.)

The IAP Web Interface is most commonly used when compliance officers export messages to a PST file using the PST Export function. The Outlook Plug-In must be installed on the client system to export messages from the IAP. For more information, see "Exporting messages from the IAP" on page 93.

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 Plug-In

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

To install the Outlook Plug-In, complete all the procedures described in this section for each person using the plug-in.



NOTE:

HP strongly recommends that you always use the latest version of the Outlook Plug-In. The current version of HP EAs Exchange always supports the previous version of the Outlook Plug-In.

Verifying security settings

For each client, verify that you have set the security correctly. You must enable specific ActiveX security settings on the client for the Outlook Plug-In to work.

1. In the Control Panel, double-click **Internet Options**.
2. Click the **Security** tab, and then click **Restricted Sites**.
3. Click **Custom Level**.
4. In the ActiveX controls and plug-ins section, enable the **Initialize and script ActiveX controls not marked as safe** option.
5. In the Scripting section, enable the **Active scripting** option.
6. Click **OK** until you have closed all the dialog boxes.

Installing the Outlook Plug-In for users

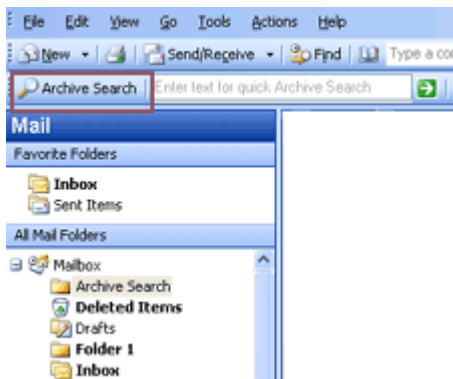
The Outlook Plug-In is a COM Add-In for Microsoft Outlook. You must have local administration privileges to install the plug-in.

These instructions can be used for either new or updated plug-in installations.

- Windows Vista or 64-bit clients: If an earlier version of the plug-in is installed, uninstall that version before executing the steps below.
- All other clients: If an earlier version of the software is installed, install the update on top of the existing installation.

To install or update the plug-in 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 Plug-In 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 plug-in interface by following the steps in ["Overriding the language in the Outlook Plug-In user interface"](#) on page 91.
6. Open Outlook and configure the archive options.
See ["The Archive Options tab"](#) on page 86.
7. Click **OK**.
8. In Outlook, click **Archive Search** in the Archive Search toolbar.



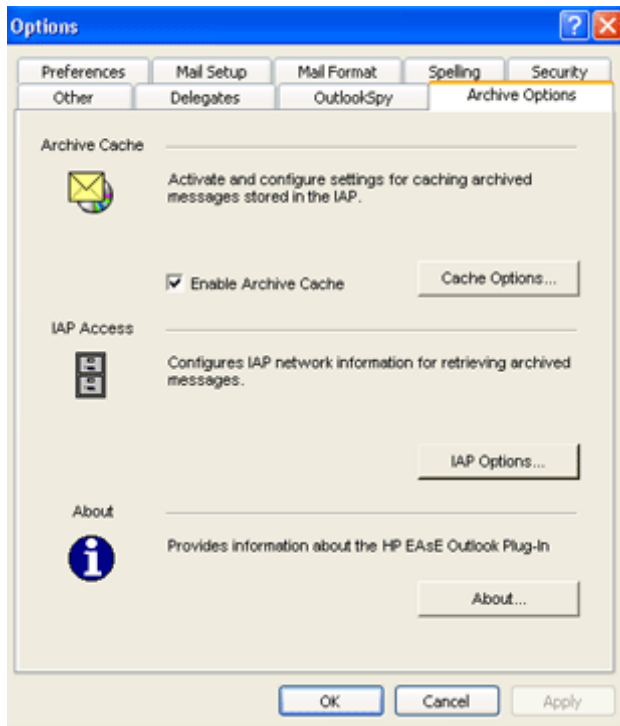
(To display the Archive Search toolbar, click **View > Toolbars > HP Archive Search**.)

- 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.
- 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 Plug-In 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 plug-in.

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



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 Plug-In 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 Plug-In.
- **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](#)" on page 125.
- **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.

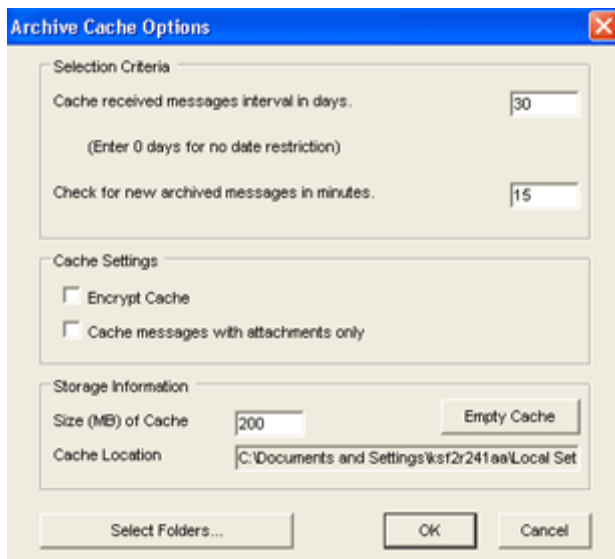
Users might not have access to the most recent messages that have been archived, depending on how often you set archiving to run.

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 6 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 messages 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.
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 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: <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](#)" on page 125.

Other cache options can be set in the registry. See "[Cache related registry settings](#)" on page 121 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 Plug-In 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 plug-in 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 Plug-In registry settings](#)" on page 121 for the default registry settings that are created when the Outlook Plug-In 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 Plug-In. Note that the SMS file in the Outlook Plug-In folder on the EAsE Extensions CD is a sample only.

Overriding the language in the Outlook Plug-In user interface

When the Outlook Plug-In 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 plug-in 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 plug-in 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 plug-in 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 the table on page 92.
The table contains all languages in which the plug-in 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 92 contain the codes that can be used.
7. Exit the registry.
8. Open Outlook and observe the changes.

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 plug-in with Citrix Presentation Manager

The Outlook Plug-In 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 plug-in are installed on a Citrix server, the following conditions apply:

- The plug-in’s logging function should be disabled in the registry to avoid space problems on the server.
Logging is disabled by default when the plug-in 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 plug-in 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](#)” on page 107.)

For more information on the registry settings, see “[Outlook Plug-In registry settings](#)” on page 121.

For more information on the export function, see [Exporting messages from the IAP](#), page 93.)

Exporting messages from the IAP

The PST Export Utility is installed as part of the Outlook Plug-In. 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 plug-in 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](#)" on page 123.

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

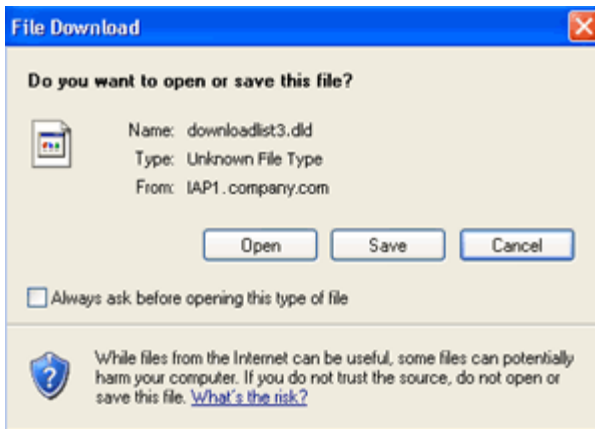
To export copies of archived messages:

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.

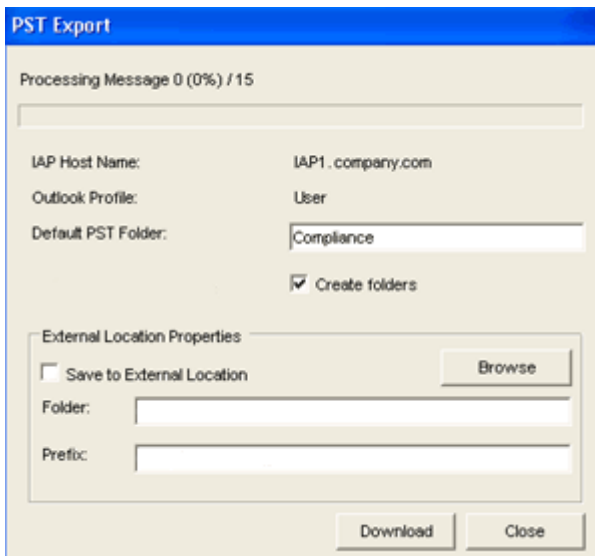


5. Clear the **Always ask before opening this type of file** check box if it appears. (This option depends on the version of Windows you are running and the security level you have set.)

When you clear the check box, the File Download box will not appear when you export messages in the future.

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

The PST Export window appears.



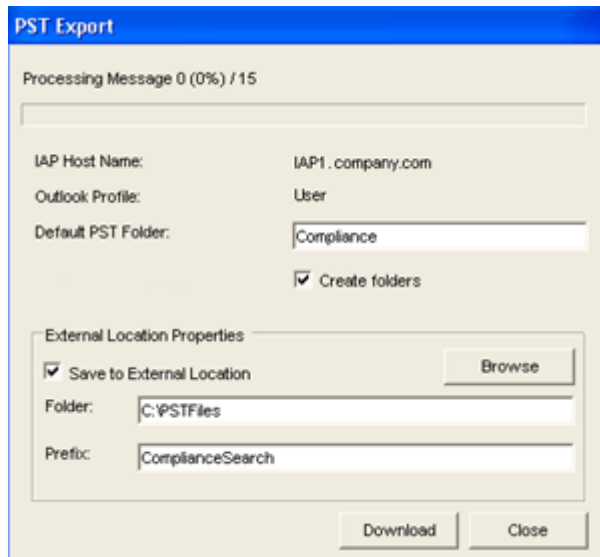
7. In the **Default PST Folder** box, enter a new name for the default folder.

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.

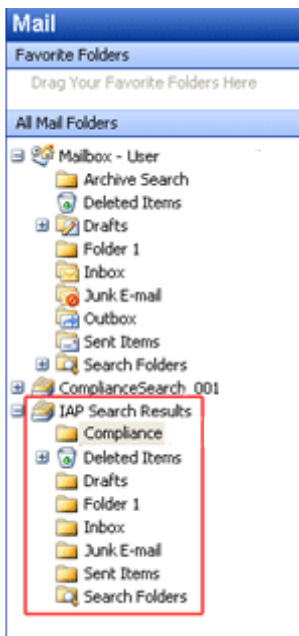
8. (Optional) Select the **Create folders** check box for messages to be exported to folders in the PST file.
The folders will have the same name as the folders where the messages were originally located. For more information on the folder option, see “[Overview of the export process](#)” on page 93. Note that any messages archived without a folder name are exported to the default PST folder.
9. (Optional) To export messages to an external location (such as a folder on your hard drive or network), follow steps a–c below.

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.)



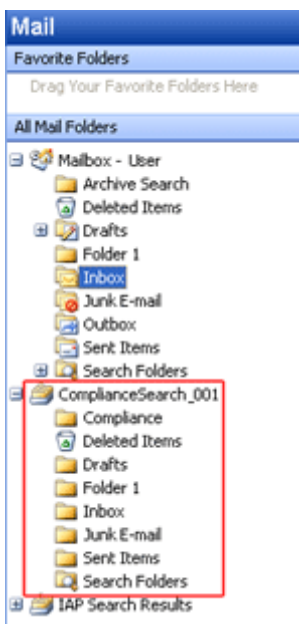
- a. Select the **Save to External Location** check box.
 - b. In the **Folder** box, specify a location for the PST file. Enter a path manually or click **Browse** to select a location.
Note: If you add a folder that doesn't currently exist, a dialog box appears at the time the messages are downloaded. 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`).
10. 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.
 11. Click **Close** to close the PST Export window.
 12. Click **Close Options** to close the options menu in the IAP Web Interface.

13. 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.



14. If the messages were exported to an external location:
 - a. Open Outlook.
 - b. Select **File > OpenOutlook 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”](#) on page 107.

11 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. The full set of Outlook features is available through Microsoft Internet Explorer. Non-Microsoft browsers may have reduced functionality.

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

- [System requirements](#), page 99
- [Multiple mail stores](#), page 99
- [Multiple IAP systems](#), page 100
- [Temporary storage in Drafts folder](#), page 100
- [Making tombstoned mail items visible in OWA](#), page 101
- [Viewing the Web.config file in Exchange 2007 installations](#), page 101
- [Working with the asp.config file in Exchange 2000 and 2003 installations](#), page 102
- [Changing the ASP time-out in Exchange 2000 and 2003 installations](#), page 103
- [Browser functionality](#), page 103
- [Multi-user support](#), page 103
- [Large attachments](#), page 103

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
- .NET Framework 2.0 with Service Pack 1
- OWA Premium service

See the HP EAs Exchange Support Matrix for the complete list of system requirements to install and use OWA Extension with Exchange 2000, 2003, and 2007.

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 SystemMailbox 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 Archive Scheduler.

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.

Making tombstoned mail items visible in OWA

Use the Tombstone Maintenance event and associated rule to make tombstoned messages visible in OWA. See “[Configuring tombstone maintenance events](#)” on page 55 for instructions on creating a Tombstone Maintenance event and rule.

NOTE:

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

Viewing the Web.config file in Exchange 2007 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 2000 and 2003 installations

The `asp.config` file, used in OWA Extension for Exchange 2000 and 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
papoona=http://papoona
```

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.

The `UsePropertyTemplate` flag causes the `unset` flag to be corrected for Exchange 2000; this value should be set to `TRUE` only for Exchange 2000. Exchange 2003 performs the correct action by default. The `UsePropertyTemplate` flag setting is harmless for Exchange 2003, but set it to `FALSE` to save unnecessary steps.

```
[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 2000 and 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.

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, 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 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.

12 Troubleshooting

This chapter covers the following troubleshooting topics:

- [OWA 2007 users cannot open folders containing tombstoned messages](#), page 105
- [OWA 2007 users cannot retrieve tombstoned messages](#), page 105
- [Behavior in Microsoft Exchange Server 2007 impacts detection of message duplicates](#), page 105
- [Selective archiving does not process all folders in user mailbox](#), page 106
- [Changes not captured in email attachments](#), page 107
- [Users cannot find messages sent to a distribution list](#), page 107
- [DiskSpaceBuffer error](#), page 107
- [HP Batch Export error](#), page 107

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 users cannot retrieve tombstoned messages

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

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

Behavior in Microsoft Exchange Server 2007 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, 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 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 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 2.0 and 2.1, the message hash is computed in the following ways:

- Standard email messages (IPM.Note) archived from Exchange 2007 servers:
 - All Sent items have the hash computed with the milliseconds truncated. This includes Sent items that are archived from an Exchange 2007 server and Sent items in an Exchange 2007 server mailbox that are imported using PST Import Tools.
 - 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 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 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, 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 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 Exchange 2007 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 below 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. For more information, see the troubleshooting section of the *HP Integrated Archive Platform Administrator Guide*.

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 plug-in are installed on a remote server.
- The Outlook Plug-In is installed on the local computer.
Outlook and the plug-in must be installed on the local computer for the export function to work.

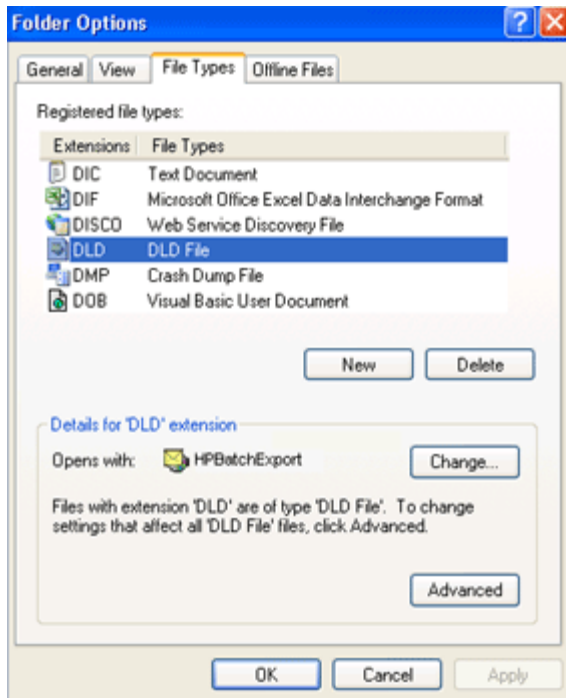
If Outlook and the plug-in are installed on the local computer, verify that the Windows system has not associated the .dld file type with another application.

To verify the file type:

1. Open My Computer.
2. Select **Tools > Folder Options**.
3. Click the **File Types** tab.

The .dld file type should be associated with HPBatchExport, which is used to export archived messages.

4. If .dld is associated with another application, change the association:
 - a. Select the **DLD** extension, and then click **Change**.
 - b. In the **Open With** dialog box, click **Browse**.
 - c. Browse to the following location:
`\Program Files\Hewlett-Packard\HP EAsE Outlook Plug-In.`
 - d. Select **HPBatchExport.exe**, and then click **Open**.
 - e. Click **OK** to associate the .dld file type with HPBatchExport.



A Indexed document and content types

- [Indexed document types](#), page 109
- [Message MIME types](#), page 110
- [Additional indexing detail/limitations for Microsoft Office](#), page 111

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.

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)
- Documents (IPM.Document)

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)

The following types of 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, PowerPoint, and Access
- 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)

The following types of attachments are not indexed:

- Graphic files
- Music files
- A file type that is not included in the list above

These attachments are archived, but users cannot search for them.

Message MIME types

The MIME Content-Types shown below 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 7 IAP indexed document and MIME types

File extension	File type	MIME 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
.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
.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

File extension	File type	MIME type
.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

Additional indexing detail/limitations for Microsoft Office

Table 8 Microsoft Office supported features

Type	Feature	Office 97–2003	Office 2007
Microsoft Word	Contents	Yes	Yes
	Table	Yes	Yes
	Textbox	Yes	Yes
	Header/Footer	Yes	Yes
	FootNote/EndNote	Yes	No
	Comment	Yes	No
	Signature	No	No
	Chart	No	Yes
	Object (Microsoft Office, WordPad)	No	No
	OLE	Yes	Yes
	WordArt	No	No

Type	Feature	Office 97–2003	Office 2007
Microsoft PowerPoint	Contents	Yes	Yes
	Table	Yes	Yes
	Textbox	Yes	Yes
	Header/Footer	Yes	Yes
	Comment	No	No
	Signature	No	No
	Chart	No	No
	Object (Microsoft Office, WordPad)	No	No
	OLE	Yes	Yes
	Notes	No	No
	WordArt	No	No
Microsoft Excel	Contents	Yes	Yes
	Table	Yes	Yes
	Textbox	No	Yes
	Header/Footer	No	No
	Comment	No	No
	Signature	No	No
	Chart	No	No
	Object (Microsoft Office, WordPad)	No	No
	OLE	Yes	Yes
	WordArt	No	No
	Sheet's name	No	No

Table 9 Microsoft Office supported properties

Type	Property	Microsoft Word, PowerPoint, and Excel
Document Properties	Author	Yes
	Title	Yes
	Subject	Yes
	Keywords	Yes
	Category	Yes
	Status	Yes
	Comments	Yes
	Location	No
Advanced Properties: General	Type	No
	Location	No
	Size	No
	MS-DOS name	No
	Created	No
	Modified	No
	Accessed	No
	Attributes	No
Advanced Properties: Summary	Title	Yes
	Subject	Yes
	Author	Yes
	Manager	No
	Company	No
	Category	Yes
	Keywords	Yes
	Comments	Yes
	Hyperlink base	No
	Template	No

Type	Property	Microsoft Word, PowerPoint, and Excel
Advanced Properties: Statistics	Created	No
	Modified	No
	Accessed	No
	Printed	No
	Last saved by	Yes
	Revision number	Yes
	Total Editing Time	No
	Statistics	Word, PowerPoint: No Excel: N/A
Advanced Properties: Contents	Document Contents	No
Advanced Properties: Custom	Checked by	Yes
	Client	Yes
	Date completed	Yes
	Department	Yes
	Destination	Yes
	Disposition	Yes
	Division	Yes
	Document number	Yes
	Editor	Yes
	Forward to	Yes
	Group	Yes
	Language	Yes
	Mailstop	Yes
	Office	Yes
	Owner	Yes
	Project	Yes
	Publisher	Yes
	Purpose	Yes

Type	Property	Microsoft Word, PowerPoint, and Excel
Advanced Properties: Custom (continued)	Received from	Yes
	Recorded by	Yes
	Recorded date	Yes
	Reference	Yes
	Source	Yes
	Status	Yes
	Telephone number	Yes
	Typist	Yes

B PST Import Tools: Archive Request file specifications

The XML tags used in the Archive Request file are listed below. You can generate the file using the PST Loader interface or create the file manually using “[Sample Archive Request file](#)” on page 118 as a guide.

- [Settings description](#), page 117
- [Sample Archive Request file](#), page 118

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 10 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 non-standard messages (appointments, tasks, etc.) are archived automatically using 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.

Tag	Description
<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.
<Tombstone>	Controls tombstoning: <ul style="list-style-type: none"> • 0: Tombstoning is not enabled. • 1: Only attachments are tombstoned. • 2: Both attachments and the message body are 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 11 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>
```


C Outlook Plug-In registry settings

Installing the Outlook Plug-In 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 plug-in 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 Plug-In 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 121
- [IAP retrieval related registry entries](#), page 123
- [Search and export related registry settings](#), page 123
- [Administrative registry settings](#), page 125

Cache related registry settings

These settings are used for configuring Archive Cache.

For more information, see "[Configuring Archive Cache](#)" on page 88.

Table 12 [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 <code>True</code> . Changing this to <code>False</code> 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 <code>True</code> . 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.

Registry key and default value	Description
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.
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 below 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 plug-in 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.

Registry key and default value	Description
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 plug-in 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 13 [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 HOSTNAME 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 plug-in fails to retrieve a tombstoned message using FetchURL0, it attempts to retrieve the message using FetchURL1 through FetchURL9 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” on page 93.

Table 14 [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 UseExternalFolderSupport=True. This is a user-configurable setting.
PSTFilePrefix=Compliance Search	Defines the file name prefix used when creating the individual PST files when UseExternalFolderSupport=True. Each file begins with the prefix specified here and has an ordinal appended to the file name. For example: ComplianceSearch_001.pst, ComplianceSearch_002.pst, and so forth. This is a user-configurable setting.

Registry key and default value	Description
UseExternalFolderSupport= True	Specifies whether the PST Export Utility allows the user to save PST files to an external location. The default is True. When UseExternalFolderSupport=True, the PST Export Utility saves the generated PST files prefixed with PSTFilePrefix to the folder specified by PSTFileFolder. This is a user-configurable setting.
AllowExternalFolderSupport=True	When set to False, 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.
<i>The following default settings do not appear in the registry and should be added only at the direction of HP technical support.</i>	
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 ResultSetLimit. • 2 = Allow only two attempts to get to the ResultSetLimit
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.
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 Plug-In administrative settings.

Table 15 [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	Plug-in version. This should never be modified.
LogFilepath=	A fully-qualified path name that instructs the plug-in to record certain diagnostic information to disk. This is a user-configurable setting.

Index

A

- ACL expansion
 - public folder events, 70
 - team mailbox events, 37
- Archive Cache, 83
 - defined, 88
 - system tray status icon, 90
- Archive Request file, 74, 117
 - file spec tags, 118
 - header tags, 117
- Archive Search, 85
- archive service account
 - specifying access, 16
- archiving services, 16
- assigning messages to IAP repositories, 107
- attachments
 - changes to, 107
 - proxy in tombstoned message, 35
- attachments, large, 103
- audit log, 14

B

- batch export error, 107

C

- changes not captured in email attachments, 107
- Citrix server, 92, 93, 107
- Compliance Archiving
 - copying events, 27
 - creating events, 23
 - deleting events, 27
 - editing events, 24
 - enabling on mailbox stores, 22
 - event status, 47
 - items archived, 21
 - running events, 27
 - setting registry key in Exchange 2000, 23
- Content-Type indexing, 110
- conventions
 - text symbols, 10
- credentials, archive, 16

D

- DiskSpaceBuffer error, 107
- distribution lists, 107
- DLD file type, 97, 107
- document conventions, 10
- duplicates, message, 105

E

- end user delete, 59
- EnsureOwnerReceipt, 107
- error opening folders in OWA 2007, 105
- export error, 107
- exporting
 - errors, 97
 - messages, 84, 93
 - search results, 93
- exporting messages
 - errors, 107

F

- FileSpec tag, PST Import Tools, 118
- folder capture, 63, 77, 93, 117
 - and Duplicate Manager, 66
 - and PST Import Tools, 65
 - and Selective Archiving events, 65
 - and Synchronize Deleted Items events, 65
 - and Tombstone Maintenance events, 56, 65
 - enabling, 64
 - indexing folder information, 63
- folders skipped during Selective Archiving, 106

G

- global configuration files, 107

H

- hash
 - , 105
 - and message duplicates, 105
 - computing, 105
- help, obtaining, 11
- HP
 - storage Web site, 11
 - Subscriber's choice Web site, 11
 - technical support, 11
- HP EAs Exchange, defined, 13

I

- IAP Web Interface, 13, 83
 - defined, 84
 - exporting messages, 83
- IAP, defined, 13
- indexed documents, 109
 - Microsoft Office, 110, 111
 - types, 111
- indexed Exchange items
 - types, 109

installation guide, 9
installing
 Outlook Plug-In, 85
 PST Import Tools, 72

J

journal mailboxes, creating, 21

L

logs
 PST Importer, 82

M

messages are not archived, 106
messages not being archived
 EnsureOwnerReceipt not enabled, 107
MIME Content-Type indexing; , 110

N

no archiving access to IAP, 16
no archiving access to mailboxes, 16

O

Outlook Integrated Archive Search, 85
Outlook Plug-In, 83
 Admin mode, 87
 and Citrix server, 92
 Archive Cache, 88
 Archive Options tab, 86
 installing, 85
 logging, 87
 overriding language, 91
 PST Export Utility, 93
 registry settings, 121
 security settings, 84
 setting host information, 86
Outlook Plug-In registry settings
 administrative, 125
 and Citrix server, 92
 Archive Cache, 121
 default settings, 90
 IAP retrieval, 123
 manually creating, 90
 overriding language, 91
 search and export, 123
OWA 2007
 error opening folders, 105

OWA Extension, 83
 asp config file, 102
 ASP time-out, 103
 browser functionality, 103
 making archived mail items visible in OWA,
 101
 multi-user support, 103
 multiple IAP system, 100
 multiple mail stores, 99
 system requirements, 99
 temporary copies in Drafts folder, 100
 Web config file, 101

P

PCC
 description, 14
Policy Engine
 Actions tab, 43
 Conditions tab, 41
 Folders tab, 40
 Information Stores tab, 38
 Messages tab, 53
 Schedule tab, 44
 Selection tab, 50
Policy Engine stops processing mailbox, 106
PST Export Utility, 83, 84
PST Import Monitor, 79
PST Import Tools
 about, 71
 creating Archive Request file, 74
 description, 14
 establishing archive credentials, 73
 features, 71
 FileSpec tag, 118
 import process, 72
 installing, 72, 72
 logs, 82, 82
 processing PST files, 79
 PST Import Monitor, 79
 sample Archive Request file, 118
 validating Archive Request file from
 command line, 79
 validating Archive Request file with PST
 Loader, 78
public folders, archiving messages, 67

Q

Quota Thresholds, 49
 configuring event, 49
 configuring rule, 50
 defining threshold, 50
 included and excluded messages, 53
 ordering message list, 52
 selecting data to process, 51

R

- registry keys
 - Microsoft Exchange 2000, 23
- registry settings
 - Outlook Plug-In, 90
- related documentation, 9
- reports
 - PST Import Tools, 82
- requirements
 - PST Import Tools, 72

S

- search results
 - exporting, 93
- Selective Archiving
 - archiving messages in public folders, 67
 - archiving to quota threshold, 49
 - copying events, 36
 - creating events, 33
 - deleting events, 36
 - editing events, 34
 - editing local service processing settings, 46
 - editing rules, 38
 - end user delete, 59
 - event status, 47
 - excluding journal mailboxes, 31
 - items archived, 29
 - processing rules, 47
 - setting up Auto Search, 32
 - setting up information stores, 30
- shared mailbox events, 37
- single sign-on, 84
- Smart Cells, 107
- stub, definition, 71
- Subscriber's choice, HP, 11

- symbols in text, 10
- system requirements, 15
 - OWA Extension, 99
 - PST Import Tools, 72

T

- team mailbox events, 37
- technical support
 - HP, 11
- text symbols, 10
- TNEF, 26, 26, 35, 77, 117
- Tombstone Maintenance
 - and folder capture, 56
 - events, 55
 - Tombstone Folder synchronization, 55
- Tombstone Maintenance events, 101
- tombstone, definition, 71
- tombstones, 55

U

- user guide, 9

V

- verifying
 - access to Exchange, 16
 - access to IAP, 16

W

- Web sites
 - HP documentation, 11
 - HP storage, 11
 - HP Subscriber's choice, 11