HP Email Archiving software for IBM Lotus Domino

Version 2.0

Administrator Guide

Part number: PDF
Third edition: July, 2009

Legal and notice information

© Copyright 2007-2009 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. Lotus®, Domino®, Lotus Notes®, LotusScript®, AIX®, AS/400®, iSeries®, RS/6000®, pSeries®, OS/390®, and zSeries® are U.S.-registered trademarks of IBM Corporation. iNotes™ is a U.S. trademark of IBM Corporation. Java™ is a U.S. trademark of Sun Microsystems, Inc.

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 EAs . . . 13
System requirements and prerequisites . . . 14
IAP requirements . . . 14
System requirements . . . 14
Domino server requirements . . . 14
Supported operating systems and Domino versions . . . 14
Supported Lotus Notes clients . . . 16
IAP Web Interface . . . 16
Character support . . . 16
Architecture . . . 18
Common administration tasks . . . 18

2 Preparing to run HP EAs Domino . . . 19
Remote and local mining . . . 19
How HP EAs Domino works with your current system and configuration . . . 20
Pre-installation tasks . . . 20
Configuring the HP gateway server . . . 20
Installing HP EAs Domino . . . 21
Permissions . . . 21
Editing the Agent Manager parameter values . . . 21
Setting the JavaMaxHeapSize . . . 22

3 HP EAs Domino configuration basics . . . 23
HP EAs-D API . . . 23
Editing the Global Configuration document . . . 24
General Settings tab . . . 25
Additional Modules tab . . . 25
Address Conversion Settings (global) . . . 25
Profile Agent Settings (global) . . . 25
DWA Index Settings . . . 26
Error Messages tab . . . 26
Administration Alert tab . . . 27
Configuring the Server Definition document . . . 27
Server Settings tab . . . 28
Archiving Options tab . . . 29
Address Conversion Settings . . . 30
SMTP Alias tab . . . 30
Multiple Domino Domain tab . . . 31
Multiple Domino Domain (Group) tab . . . 31
Profile Agent Settings . . . 32

Execution Settings . . . 33
DWA Settings . . . 34
Debug Options . . . 35
Preprocessing messages . . . 35
Preprocessing and reference databases . . . 35
Configuring the Preprocessing Control documents . . . 36
Databases Location tab . . . 37
Encapsulation Settings . . . 37
Agent Log Settings . . . 39
Execution Settings . . . 39
Debug Settings . . . 40
Viewing references . . . 40
Viewing the message reference log . . . 40
Reference database troubleshooting tools . . . 41
Working with log files . . . 41
HP EAs-D Log database . . . 41
Viewing archiving log files . . . 42
Purging log entries . . . 44

4 Configuring DWA Extension . . . 47
DWA Extension configuration steps . . . 47
Configuring the Proxy Gateway document (optional) . . . 49
Configuring the Tombstone Prototype document . . . 51
Editing the Tombstone Settings tab . . . 53
Purging cached messages . . . 54
Purging tombstone conversion requests . . . 54

5 Configuring selective archiving . . . 55
Overview . . . 55
Configuring mining rules . . . 56
Time Conditions tab . . . 58
Folders Settings tab . . . 59
Exceptions Settings . . . 60
Special Fields . . . 60
Attachments & Doc size tab . . . 61
Other Macro Formula tab . . . 61
User Membership tab . . . 62
Defining wildcard patterns . . . 63
Reference Database tab . . . 64
Tombstone Settings tab . . . 65
Session Settings tab . . . 67
User Notification tab . . . 68
Administration Alert tab . . . 68
Scheduling the mining job . . . 69
Editing a rule or schedule . . . 71
Enabling the mining agents . . . 71
Enabling the preprocessing agent . . . 72
HP EAs-D Users database . . . 73
Scheduling and enabling the Profile Agent . . . 73
Viewing Mail Detail records . . . 74
Enabling other HP EAs-D Users agents . . . 75
Statistics User Activity Alert agent . . . 75
Editing agent values . . . 75
Scheduling the agent . . . 76
Purge Not Synchronized person document agent . . . 76
Purge Selective Archive Log agent . . . 76
Running the mining job . . . 77

6 Configuring compliance (journal) archiving 79
Overview 79
Encrypted messages 79
Calendar notices 79
Mail-To-Me messages 80
Journaling recommendations 80
Advanced Filtering (HP EAs Domino journaling) 80
Domino native journaling 81
Defining an IAP exception in the native journaling rules 81
Configuring HP EAs Domino journaling and native journaling on the same server 82
The journaling process 82
Creating HP EAs Domino journaling rules 85
Traffic Definition tab 86
Sender/Receiver Exceptions tab 87
Content Exceptions tab 87
Journal Database tab 88
Rules Status tab 88
Editing journal rules 89
Mail.box issue 89

7 Using bulk upload 91
Editing the bulk upload mining rule 91
Editing the Preprocessing Control document 92
Enabling the agents 92
Discovering the databases 92
Forcing a database owner 93
Reviewing the Mail Detail records 93
Mining the databases 93

8 Configuring IAP single sign-on 95
Copying the SSO templates 95
Configuring the HP EAs-D SSO database and the Generate SSO Tokens agent 96
Configuring the Search The IAP Archive agent 99
The implementation process 100
Copying design elements from the template 101
Modifying the Search The IAP Archive agent 102
Configuring SSO on the IAP 102
Installing the secret key 102
Modifying the UID 103
Configuring the client computers 103

9 Working with HP EAs Domino client applications 105
Using the IAP Web Interface 105
Creating an IAP Web Interface link in Lotus Notes 106
Creating a link to the Web Interface 106
Using Export Search 107
Using the client to extract messages 107
Using the server to extract messages 109
Modifying files for server-side Export Search 109
Exporting the messages 110
Extracting the messages 110
Removing requests from the log 112
Using Local Cache 113
Installing Local Cache 113
Configuring Local Cache 115
Deleting messages from the cache 119
Uninstalling Local Cache 119
Using the Windows Notes Client Plug-In 120

Configuring the plug-in installer . . . 120
Installing the plug-in . . . 122
Using the Windows Notes Client Plug-In with Local Cache . . . 123
Adding the tombstone icon (optional) . . . 123
Retrieving and viewing encapsulated messages . . . 124
Retrieving and opening encapsulated messages in Lotus Notes and DWA . . . 124
Opening encapsulated messages in the IAP Web Interface . . . 124
Opening encapsulated messages . . . 124
Adding MS Office 2007 MIME type support to HP EAs Domino . . . 125

10 Collecting held messages for HP technical support . . . 127
Using the application . . . 127

11 Troubleshooting and performance improvement . . . 129
Preventing mail server instability . . . 129
Mining program shuts down . . . 129
JVM panic gc0 error . . . 130
Large Mail Detail log records . . . 131
Message attachments named ATTxxxxx . . . 131
Compacting databases . . . 131
Editing server configuration . . . 132
Monitoring the gateway . . . 132
Limiting the server log file size . . . 133

A Indexed document and content types . . . 135
Indexed document types . . . 135
Message MIME types . . . 135
Additional indexing detail/limitations for Microsoft Office . . . 137

B Configuring the HP EAs-D Tools database . . . 141
Creating the database . . . 141
Configuring the database . . . 142
Enabling the cleanup agent . . . 142

C Creating reference and preprocessing databases . . . 145
Creating a new preprocessing database . . . 145
Creating a new reference database . . . 146

D Account Synchronization . . . 149
Account Synchronization overview . . . 149
Creating and running DAS jobs . . . 149
Creating LDAP server connections . . . 149
Creating jobs . . . 150
Mapping advanced options . . . 151
Assigning HTTP portals . . . 152
Starting, scheduling, and stopping DAS jobs . . . 152
Viewing DAS history logs . . . 153

Index . . . 155

Tables

1 Document conventions 10
2 IAP and EAs applications for users 13
3 IAP and EAs applications for administrators 14
4 Supported platforms and operating systems 15
5 HP EAs Domino character support 17
6 Common administration tasks 18
7 New MS Office 2007 MIME types 126
8 IAP indexed document and MIME types 135
9 Microsoft Office supported features 137
10 Microsoft Office supported properties 138

About this guide

HP Email Archiving software for IBM Lotus Domino (HP EAs Domino) is mail administration software that mines messages from Lotus Notes mail databases and/or journal databases and places the messages in the HP Integrated Archive Platform (IAP) architecture. This guide explains how to configure and administer HP EAs Domino to enable mining of Notes databases.

NOTE:

The Integrated Archive Platform was formerly known as the Reference Information Storage System, or RISS. HP Email Archiving software for IBM Lotus Domino was formerly known as HP Reference Information Manager for Domino, or RIM for Domino.

Intended audience

This guide is intended for:

- HP IAP administrators
- HP EAs Domino administrators

Related documentation

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

For administrators and installers:

- *HP Email Archiving software for IBM Lotus Domino Installation Guide* (available to HP personnel installing IAP and EAs)
- *HP Email Archiving software for IBM Lotus Domino Release Notes*
- *HP Integrated Archive Platform Installation Guide* (available to HP personnel installing IAP and EAs)
- *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 IBM Lotus Domino 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	• 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
Italic font	Text emphasis
`Monospace font`	• File and directory names • System output • Code • Text typed at the command line
`Monospace, italic font`	• 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.

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 Domino software. It contains the following topics:

- IAP and EAs, page 13
- System requirements and prerequisites, page 14
- Character support, page 16
- Architecture, page 18

IAP and EAs

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.

EAs Domino is management and configuration software available for IAP.

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

Table 2 IAP and EAs applications for users

Application	Description
IAP Web Interface	Employees can use a Web browser to search for, view, and send email archived on the IAP, and save and reuse search-query definitions and results.
HP EAs Domino client applications (customer option)	When the Windows Notes client plug-in and/or local cache is installed, users can view and open archived messages in their Lotus Notes mailbox. Windows users can also export messages from the IAP to a Notes database.
HP EAs DWA Extension (customer option)	When Domino Web Access (iNotes) support is enabled, users can view and open archived messages from DWA.

System administrators can use the following troubleshooting and administrative tools:

Table 3 IAP and EAs applications for administrators

Application	Description
HP EAs Domino server software	System administrators can use the software to create selective archiving and journaling rules and configure agents for archiving email messages.
IAP Platform Control Center (PCC)	Administrators can monitor and troubleshoot system status and performance, and manage IAP user accounts using their Web browser.

System requirements and prerequisites

Your system must meet the following requirements to deploy HP EAs Domino 2.0.

IAP requirements

IAP is the only compatible archiving platform for EAs Domino.

IAP version 1.6 (or later) hardware and software is required.

If your company uses IAP single sign-on, IAP version 1.6.1 or later is required. (See "Configuring IAP single sign-on" on page 95.

System requirements

Domino server requirements

- If you are using Advanced Filtering (EAs Domino journaling) or are locally mining a mail server, the server must meet IBM system requirements plus the following:
  - Additional 512 MB RAM per server
  - Additional 200 MB free disk space per server
- If you are using remote mining or Domino native journaling, there are no additional memory requirements.
- Signed and encrypted message validation requires additional free space on message processing servers (either for local or remote mining). Space requirements vary, depending on the quantity and size of signed and encrypted messages processed by a message processing server. To avoid server instability and ensure sufficient disk space, determine the data volume of signed and encrypted messages and double that value.

Supported operating systems and Domino versions

The following platforms, operating systems, and Lotus Domino releases are supported by HP EAs Domino 2.0.

Table 4 Supported platforms and operating systems

Platform	OS	EAs–D advanced filtering	Support via local mining or Active Gateway (remote mining)	Support only via Active Gateway (remote mining)
		Lotus Domino release		
Intel 32 bit	Windows server 2003	6.5.6, 7.x, 8.0.x, 8.5.x	6.5.6, 7.x, 8.0.x, 8.5.x	
	Windows server 2000	6.5.6, 7.x	6.5.6, 7.x	
	Red Hat Enterprise Linux 5	8.0.x	8.0.x	
	Red Hat Enterprise Linux 4	7.x	7.x	
	SUSE Linux Enterprise Server 10	7.x	7.x, 8.0.x	
	SUSE Linux Enterprise Server 9	7.x	7.x	
Intel 64 bit	Windows server 2003	8.0.x, 8.5.x	8.0.x, 8.5.x	
	Red Hat Enterprise Linux 5	8.0.x	8.0.x	
	Red Hat Enterprise Linux 4	7.x	7.x	
	SUSE Linux Enterprise Server 10	7.x, 8.0.x	7.x, 8.0.x	
Sun SPARC	Sun Solaris 10	7.x, 8.0.x	7.x	8.0.x
	Sun Solaris 9	7.x		7.x
IBM pSeries (RS6000)	AIX 5.3 (32–bit)	6.5.x, 7.x, 8.0.x	6.5.x, 7.x	8.0.x
	AIX 5.3 (64–bit)	6.5.x, 7.x, 8.0.x	6.5.x, 7.x	8.0.x
	AIX 5.2 (32–bit)	7.x		7.x
	AIX 5.2 (64–bit)	7.x		7.x
IBM iSeries (AS/400)	I5/OS V6 Release 1	8.0.x		8.0.x
	I5/OS V5 Release 4	7.x		7.x, 8.0.x
IBM zSeries	Any	Contact HP		Contact HP
IBM OS/390	Any	Contact HP		Contact HP

Supported Lotus Notes clients

- Windows 2000: Lotus Notes 7.0.x and 8.0.x (Standard and Basic)
- Windows XP: Lotus Notes 6.5.x, 7.0.x, 8.0.x, 8.5.x (Standard and Basic)
- Windows Vista: Lotus Notes 7.0.x, 8.0.x, 8.5.x (Standard and Basic)
- Red Hat Linux and Macintosh OS: 8.0.x (Standard) by request to HP

IAP Web Interface

The Web Interface can be accessed with the following browsers:

- Microsoft Internet Explorer (Windows) 6.x and 7.x
- Mozilla Firefox 2.x and 3.x

Character support

HP EAs Domino supports all character sets that are supported by both Domino and the IAP.

IAP 1.6.2 or later must be installed.

Table 5 HP EAs Domino 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)
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

Architecture

The HP EAs Domino software can be installed on a mail server or it can be installed on a separate processing server such as the HP gateway.

Common administration tasks

Table 6 Common administration tasks

Task	Go to
Configuring selective archiving	"Configuring selective archiving" on page 55
Archiving "on demand"	"Folders Settings tab" on page 59
Archiving to mailbox quota	"Session Settings tab" on page 67
Mining policy exceptions	"Exceptions Settings" on page 60
Domino Web Access (iNotes) support	"Configuring DWA Extension" on page 47
Configuring journaling (compliance archiving)	"Configuring compliance (journal) archiving " on page 79
Loading old mail files into the IAP	"Using bulk upload" on page 91
Accessing archived messages using the IAP Web Interface	"Using the IAP Web Interface" on page 105
Installing and configuring the Windows Notes Client Plug-in	"Using the Windows Notes Client Plug-In" on page 120
Using a local cache	"Using Local Cache" on page 113

2 Preparing to run HP EAs Domino

This chapter contains information about preparing your environment to install and run HP EAs Domino. It covers these topics:

- Remote and local mining, page 19
- How HP EAs Domino works with your current system and configuration, page 20
- Pre-installation tasks, page 20
- Configuring the HP gateway server, page 20
- Installing HP EAs Domino, page 21
- Permissions, page 21
- Editing the Agent Manager parameter values, page 21
- Setting the JavaMaxHeapSize, page 22

Remote and local mining

EAs Domino software can be installed on:

- HP gateway servers
  This type of configuration is known as remote mining. All archiving operations occur on the gateway server in the external domain. Messages are mined from mail files and/or journal mail-in databases on Domino servers in the Domino domain. In remote mining, the gateway may be referred to as the HP Active Gateway, since it processes messages and routes them to the IAP. Remote mining provides a zero or near-zero* footprint on your production mail servers, because no archiving code is required on the mail servers.
  * If you implement Advanced Filtering (HP EAs Domino journaling) to meet compliance requirements, a subset of the EAs files is installed on each server from which journal mail-in files are archived.
- Domino journal or application servers
  This configuration supports:
  - Remote mining of mail files
  - Remote or local mining of journal mail-in databases

  All archiving operations occur on the journal server, which must be within the Domino domain. Messages are routed to the IAP by the HP gateway server.
- Domino production mail servers
  This type of configuration is known as local mining. Archiving operations occur on the same Domino servers where the mail files and journal mail-in databases are located. In local mining, the HP gateway server may be referred to as the HP Passive Gateway. Its main task is to route messages to the IAP.

NOTE:

Servers that mine and process messages for archiving can also be called *message processing servers*, or MP servers, a term that you will see frequently in this guide. Message processing servers can be gateway servers, journal or application servers, or mail servers, depending on your archiving configuration.

How HP EAs Domino works with your current system and configuration

- Clustering does not affect EAs Domino.
- Partitioning has no affect on EAs Domino.
- Shared mail has no effect on EAs Domino.
- A replica of your Domino Directory(ies) is installed on the HP gateway server(s) and is modified during the DAS process (synchronization of user information with the IAP). EAs Domino does not update the Domino Directory itself.
- Any mail template that is supplied by Lotus is functional with EAs Domino. Customized mail templates that add functionality to the standard Lotus mail template can be a problem. Any customizations that re-save a message or remove or alter data values, data types, or standard design elements are likely to cause problems in Lotus Notes and Domino, and will also cause problems in EAs Domino.

Pre-installation tasks

Before the HP EAs Domino software installation begins, you will work with the HP service representative to:

- Install Windows software on the HP gateway server(s).
- Install Domino server software on the HP gateway servers.
- Install Lotus Notes administrator and designer clients on the gateway servers.

As Domino administrator, you must also do the following:

- Generate a server ID for each gateway server using your company's certifier.
  HP recommends that you create a special organizational unit certifier to generate the ID.
  For example: **/ou=hparchive/o=acme** where *hparchive* is the organizational unit within the organization *acme*.
  If there were two gateway servers, you would need two server IDs. For example: **gateway1/hparchive/acme**; **gateway2/hparchive/acme**.
- Using the same organizational unit certifier, create a gateway administrator ID. For example: **hpadmin/hparchive/acme**.
- Set security in the server document for each gateway server, in conformance with your organization's site standards. This includes ensuring that agent signing IDs (or the gateway administrator) have appropriate access.
- Perform cross-certification of the gateway server ID(s) with the mail servers being mined.
- Configure Domino Web Access (iNotes) if you plan to implement the HP EAs Domino DWA Extension. This feature allows users to view archived messages in DWA.

Configuring the HP gateway server

After Windows and the Domino server software are installed on the HP gateway server(s), you will work with the HP service representative to configure the gateway to send messages from your servers to the IAP.

Installing HP EAs Domino

EAs Domino can be loaded on and signed by the HP gateway server(s) for remote mining, installed directly on the mail servers for local mining, or installed on Domino journal or application servers for local or remote mining. Your HP service representative performs the installation of the EAs server software on the servers.

The Agent Manager, Router, and Replicator server tasks must be running while the EAs Domino software is installed.

If you install the EAs Domino client software on end user systems, the HP representative will work with you to install and configure the software. For more information, see "Working with HP EAs Domino client applications" on page 105. Installing the client software is optional.

Permissions

- The HP EAs Domino installer must have rights to create new databases and create replica databases.
- The EAs Domino agent signer must have rights for the following:
  - Run restricted LotusScript/Java agents
  - Run Simple and Formula agents
  - Run unrestricted methods and operations
- EAs Domino requires Editor access to the mail databases.
- EAs Domino requires Editor with Delete access to the journal databases.
- EAs Domino agents can be signed with a server ID or an administration ID.
- Whatever ID (server/user) signs the EAs Domino agents is the ID used to process the mail databases.

Editing the Agent Manager parameter values

After the EAs software is installed and configured, work with the HP service representative to set the EAs–recommended options in the Agent Manager.

IMPORTANT:

Set the Agent Manager values correctly to avoid server instability.

1. In the Administrator client, click the **Configuration** tab.
2. Expand **Server**, and click **All Server Documents**.
3. Double-click the server document for the current mail server.
4. Click the **Server Tasks** tab.
5. Click the **Agent Manager** tab, and then click **Edit Server**.

6. Change the Daytime Parameter values as shown in the table below.

   (In some circumstances, your HP representative or HP support might recommend increasing these values.)

Field	Description
Start time	Enter **08:00 AM**.
End time	Enter **08:00 PM**.
Max concurrent agents	Enter **5**.
Max LotusScript/Java execution time	Enter **240 minutes**.
Max % busy before delay	Enter **50**.

7. Change the Nighttime Parameter values as shown in the table below.

   (In some circumstances, your HP representative or HP support might recommend increasing these values.)

Field	Description
Start time	Enter **08:00 PM**.
End time	Enter **08:00 AM**
Max concurrent agents	Enter **5**.
Max LotusScript/Java execution time	Enter **480 minutes**.
Max % busy before delay	Enter **70**.

8. Click **Save & Close**.
9. Repeat steps 4–8 for each mail server in the domain.

Setting the JavaMaxHeapSize

Work with the HP service representative to set the correct JavaMaxHeap size configuration in the `notes.ini` file on message processing servers.

IMPORTANT:

Set the JavaMaxHeapSize value correctly to avoid server instability and memory problems.

When the JavaMaxHeapSize value is changed, the Agent Manager, Router, and Replicator server tasks must be restarted. IBM recommends restarting the server rather than restarting each task.

The Domino default setting for JavaMaxHeapSize is 64 MB. Revise the size according to the guidelines below:

- Organizations with fewer than 5,000 users and 10,000 groups, set to 128 MB:
  `set config JavaMaxHeapSize=134217728`
- Organizations with up to 20,000 users and 20,000 groups, set to 256 MB:
  `set config JavaMaxHeapSize=268435456`
- Organizations with up to 40,000 users and 40,000 groups, set to 512 MB:
  `set config JavaMaxHeapSize=536870912`

If your organization has other Java processes running on the server, the value should be adjusted upward. The HP service representative will consult with the HP engineering staff for the correct value to use.

3 HP EAs Domino configuration basics

- HP EAs–D API, page 23
- Editing the Global Configuration document, page 24
- Configuring the Server Definition document, page 27
- Preprocessing messages, page 35
- Viewing references, page 40
- Working with log files, page 41

HP EAs-D API

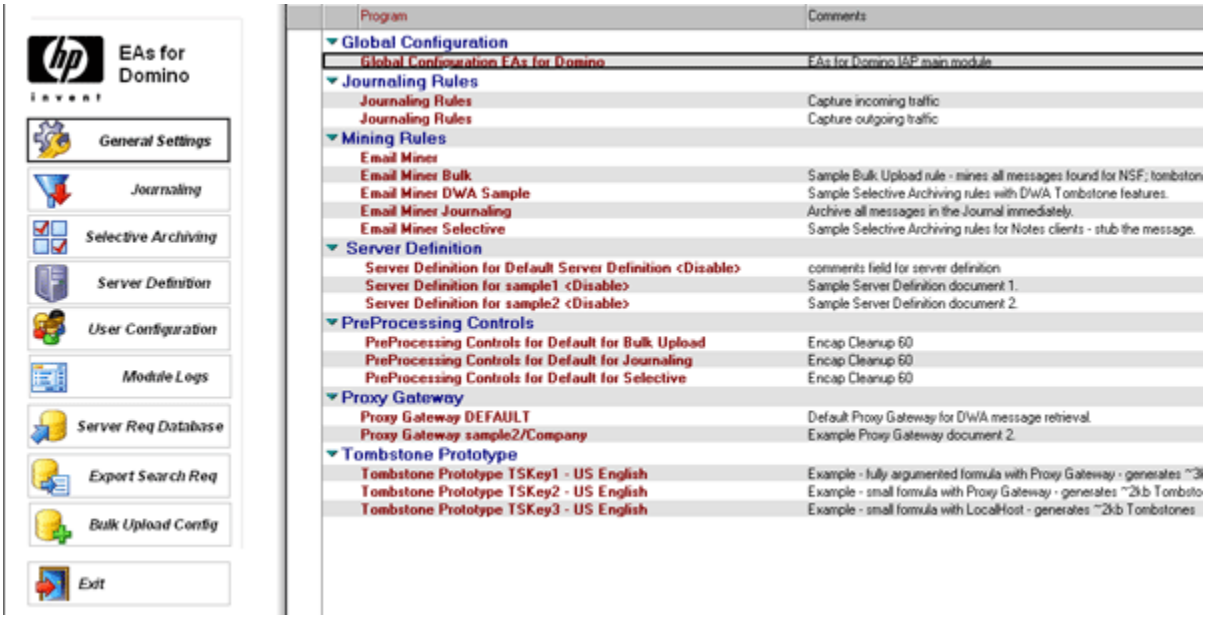
The EAs databases are installed in the `hprim` folder of the Domino `data` directory or `notesdata` directory.

All EAs Domino modules are registered into the main configuration database, HP EAs-D API (`hp_rissapi.nsf`). This database is the main entry point for administering the application and is replicated across all message processing servers.

To open the HP EAs-D API database:

1. Open the Domino Administrator client.
2. Select the domain and mail server.
3. Click the **Files** tab and open the `hprim` folder.
4. Double-click the **HP EAs-D API** database file.

   The main view appears. The Global Configuration document is listed in the view, along with mining and journaling rules and other documents needed to configure archiving.



Editing the Global Configuration document

The Global Configuration document registers the HP EAs-D API database and configures the EAs Domino binaries on servers where the EAs software is installed.

To configure the Global Configuration document:

1. Open the HP EAs-D API database.
2. Double-click **Global Configuration EAs Domino** in the EAs-D API main view.

The Global Configuration document appears.

If the Global Configuration document does not exist, you can create a new one by selecting **Create** > **API Global Config** > **1. Main**.

3. View the databases that were created during installation of EAs Domino:
   - "General Settings tab" on page 25
   - "Additional Modules tab" on page 25
4. Edit the fields on the remaining global configuration tabs:
   - Address Conversion Settings (global), page 25
   - Profile Agent settings (global), page 25
   - "DWA Index Settings" on page 26
   - "Error Messages tab" on page 26
   - "Administration Alert tab" on page 27
5. To save changes to the Global Configuration document, select **File** > **Save**.

General Settings tab

View the standard databases that were created during installation of the software.

User's Mail file details database	Database containing the EAs user mail records on the mail server (`hprim/hp_rissuser.nsf`).
Journaling filtering rules database	Filtering rules for EAs journaling (`hprim/hp_rissapi.nsf`).
Module's log database	The mining log database (`hprim/hp_risslog.nsf`).

Additional Modules tab

View the additional databases that were created during installation of the software. You might not use all of these databases.

Domino Directory database (for Journaling and Mining rules)	The Names and Address book database (`names.nsf`), containing all groups and associated Black and Red lists.
Bulk Upload database	A database (`hprim/hp_rissblkupd.nsf`) used in loading messages from old mail files into the IAP.
Server request database	A database (`hprim/hp_rissreq.nsf`) used in retrieving tombstoned messages in Domino Web Access.
Export Search request database	A database (`hprim/hp_rissexportsearch.nsf`) used to retrieve messages exported from the IAP Web Interface. Generally, this database is used for compliance purposes.

Address Conversion Settings (global)

The address conversion settings resolve SMTP aliases and allow for resolution of groups from multiple Domino domains.

- If the address conversion settings apply for all servers, complete the fields in this tab.
- If the settings vary by server, do not complete the address conversion settings in the Global Configuration document. Instead, configure address conversion in the Server Definition document.

A description of the address conversion settings is located in the Server Definition section, "Address Conversion Settings" on page 30.

Profile Agent Settings (global)

Configure the Profile Agent settings if an alternate Domino Directory (such as a Directory Assistance database) identifies users and groups for selective archiving.

- If the Profile Agent settings apply for all servers, complete the fields in this tab.
- If the settings vary by server, do not complete the Profile Agent settings in the Global Configuration document. Instead, configure these settings in the Server Definition document.

A description of the Profile Agent settings is located in the Server Definition section, "Profile Agent Settings" on page 32.

DWA Index Settings

EAs Domino's DWA Extension feature allows users to access tombstoned messages in Domino Web Access.

If you plan to use DWA Extension, edit the Retention field in this tab and configure DWA support. See "Configuring DWA Extension" on page 47.

Field	Description
DWA Index database	Leave the default: `hprim\hp_dwaindex.nsf`. This database contains the software to accept and process requests to retrieve archived messages from the IAP and return them to the request user's browser.
Retention (days)	Enter the number of days to retain retrieved messages in the user cache. The message copies are purged after this time. **Note**: If a DWA user deletes a message that has been cached, only the cached version of the message is deleted. The tombstone remains in the mail file and is not deleted. For more information, see "Purging cached messages" on page 54.

Error Messages tab

Edit the address and other settings where messages are sent if the system encounters errors with mail files.

Field	Description
Sender address	For example: HP EAs Domino
From	For example: HP IAP system
To	For example: LotusNotesAdministrator
Subject	Add a subject for the message. When an error occurs, one of the listed messages appears, depending on the cause of the error. Do not modify these messages.

Administration Alert tab

Edit the settings for email alerts to be sent to the administrator if an EAs Domino task is not running properly.

Field	Description
From	Enter a value such as Global Config or IAP system.
SendTo	You can change the default value (LotusNotesAdministrator) by: • Clicking the arrow. • Removing the default value. • Adding a name from the address list. • Clicking **OK**.
Subject	You can change the subject from the default.

Configuring the Server Definition document

The Server Definition document defines the path to the IAP and other archiving parameters.

A default Server Definition document is located in the HP EAs-D API database. The same document can be used for both compliance and selective archiving. You have the option of creating additional Server Definition documents. For example, you might want to create a separate server definition for servers that require special options, such as longer query timeout settings.

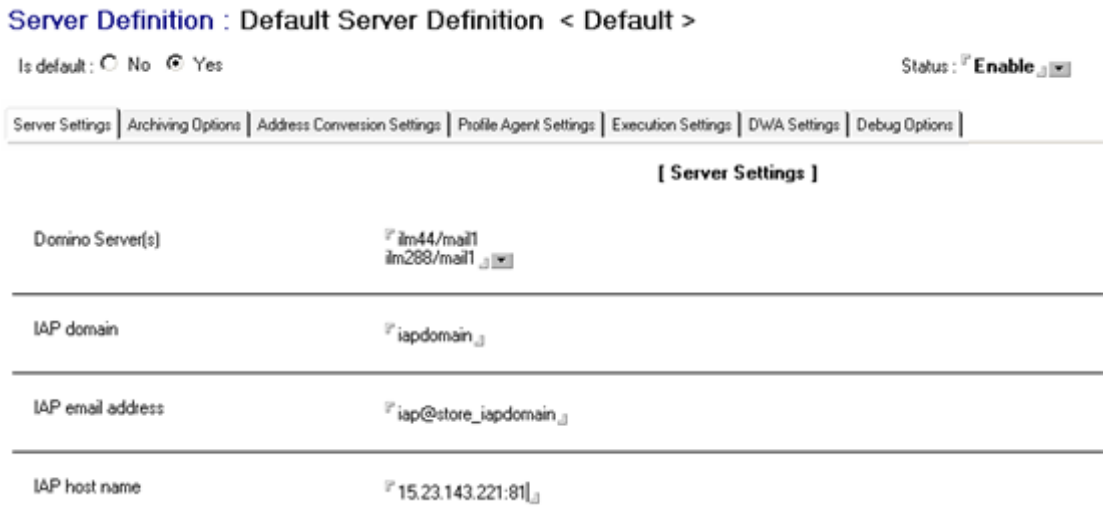
NOTE:

If you implement DWA Extension and use one or more proxy servers to process message retrievals, a separate Server Definition document must be created for the Proxy Gateway(s).

To configure a Server Definition document:

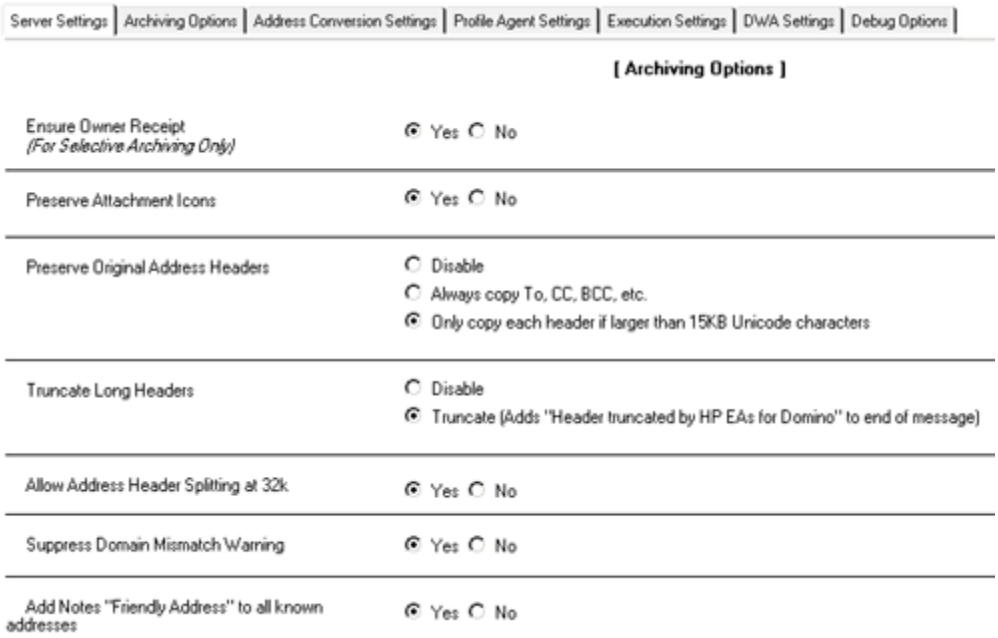
1. In the Domino Administrator client, click the **Files** tab and open the `hprim` folder.
2. Open the **HP EAs-D API** database.
3. Under **Server Definition**, double-click the default server definition to open the document.
4. If this will be the default Server Definition document for the domain, click **Yes**. Otherwise, leave the default of **No**.
5. Configure the settings in each tab:
   - "Server Settings tab" on page 28
   - "Archiving Options tab" on page 29
   - "Address Conversion Settings" on page 30
   - Profile Agent Settings, page 32
   - "Execution Settings" on page 33
   - "DWA Settings" on page 34
   - "Debug Options" on page 35
6. In Status, click **Enable** when you are ready to enable the server definition.
7. Select **File** > **Save** to save the server definition.
8. To create additional Server Definition documents, in the EAs-D API main view select **Create** > **Archiving** > **1. Server Definition** and follow steps 4–7.

Server Settings tab



Field	Description
Domino Server(s)	Click the arrow and select the message processing server(s) **or** the DWA Proxy Gateway server(s) to be included in the server definition. Only DWA proxy servers or servers that run the EAs Domino code should be listed in this field. In a remote mining configuration, add the HP gateway(s) or the journal or application servers. Do not add the mail servers or the servers on which the journal mail-in databases reside.
IAP domain	Obtain the domain name from your HP service representative. This name (the foreign SMTP domain name) is set up when the HP gateway server is configured.
IAP email address	Enter **[unique administrator name]@[complete address including foreign domain]**. For example, iap@store_iapdomain. Make sure that the name is unique and not admin or administrator.
IAP host name	Enter the IAP VIP as defined in `Domain.jcml`. The VIP is defined in the ipToDomainInfo field and name field for the store group assigned for Lotus Domino. Append :81 after the VIP. (For example, 15.23.143.221:81.)

Archiving Options tab



Field	Description
Ensure Owner Receipt	When a message is sent to a user's mailbox via a distribution list, the user is not specifically included in the recipient list. Clicking **Yes** allows the email to be archived in the user's mailbox repository. Note that when Duplicate Manager is enabled on the IAP, this does not result in a duplicate copy of the message. This option is used only for selective archiving. It does not apply to compliance archiving and, if enabled, is ignored.
Preserve Attachment Icons	Select **Yes** to preserve attachment icons in archived messages.
Preserve Original Address Headers	Lotus Notes message headers can only store up to 32 KB of data. In the process of creating an email message, Lotus Notes and Domino restrict recipient lists to enforce this limitation. During the archive process, recipient lists are expanded to include the fully qualified Internet address. This expansion means the 32 KB limitation can be exceeded on messages with large distribution lists. Use this field to expand the original message headers during archiving. You can choose whether headers should always be expanded or whether they should be expanded only if they are larger than 15 KB Unicode characters.
Truncate Long Headers	Select **Truncate** to truncate message headers for large distribution lists during archiving. Otherwise, select **Disable**.
Allow Address Header Splitting at 32 K	Select **Yes** to allow message headers to be split into multiple fields if the headers exceed 32 KB. Otherwise, select **No**.
Suppress Domain Mismatch Warning	Leave the default of **Yes**. If set to No, a warning prints to the server's `log.nsf` file if the recipient's domain cannot be found in the Domino Directory.
Add Notes "Friendly Address" to all known addresses	Select whether to expand headers to include Notes "friendly" addresses when messages are archived.

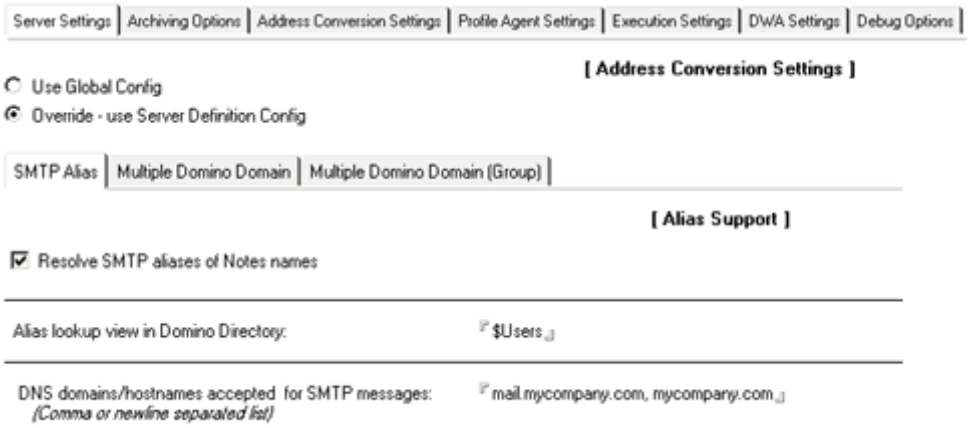
Address Conversion Settings

The address conversion settings:

- Resolve SMTP aliases.
- Allow for resolution of groups from multiple Domino domains.
- Allow configuration of a single additional Domino Directory for resolution of group names.

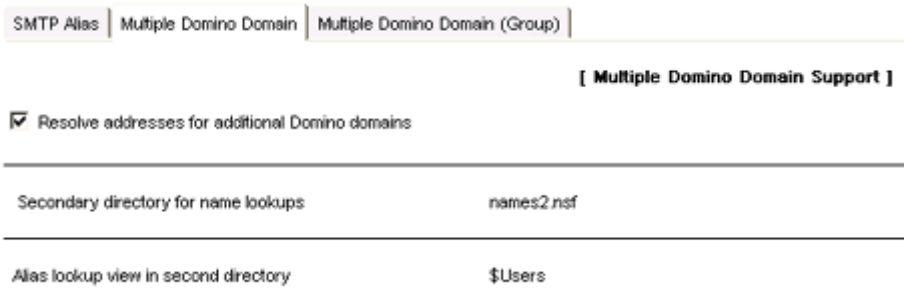
Field	Description
Use Global Config Override — use Server Definition Config	• If the address conversion settings apply to all Domino servers in the domain, select **Use Global Config** and configure address conversion in the Global Configuration document. See "Address Conversion Settings (global)" on page 25. • If the address conversion settings apply only to the server(s) listed in this Server Definition document, select **Override — use Server Definition Config**, and then complete the address conversion settings.

SMTP Alias tab



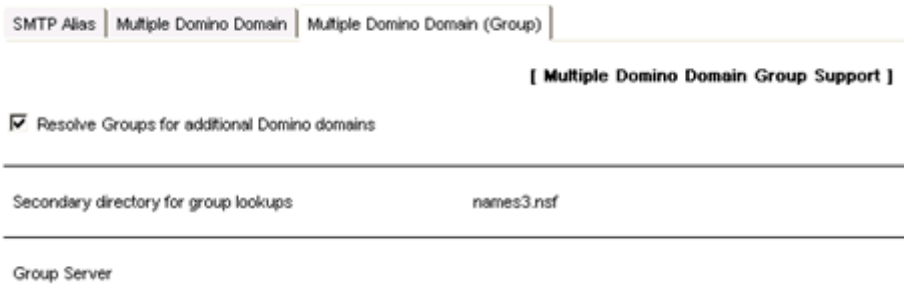
Field	Description
Resolve SMTP aliases of Notes names	Select the check box to resolve SMTP aliases.
Alias lookup view in Domino Directory	Leave **$Users** (the default).
DNS domains/hostnames accepted for SMTP messages	Enter a comma- or newline-separated list of DNS domains and hostnames for which the mail server will accept SMTP messages. For example, if there are MX records for mycompany.com and mycompany.net, and both records point to a server with the hostname `mail`, the list should include four entries: `mail.mycompany.com, mail.mycompany.net, mycompany.com, mycompany.net`.

Multiple Domino Domain tab



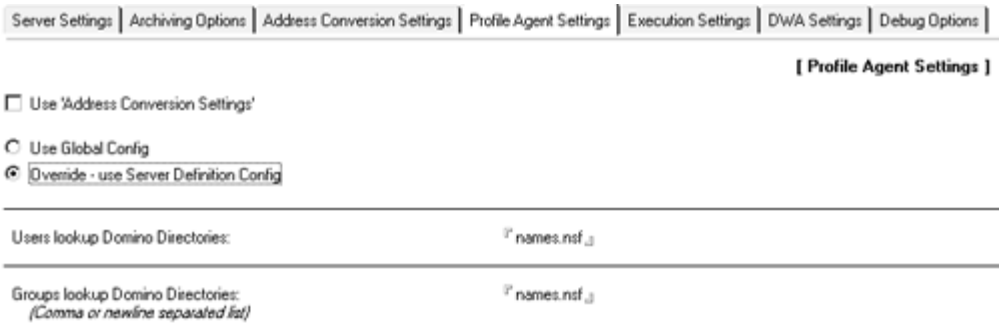
Field	Description
Resolve addresses for additional Domino domains	Select the check box to resolve addresses.
Secondary directory for name lookups	Enter the filename of an additional Domino Directory for name resolution. A Directory Catalog can be used if the configuration includes more than two Domino mail domains.
Alias lookup view in second directory	Leave **$Users** (the default).

Multiple Domino Domain (Group) tab



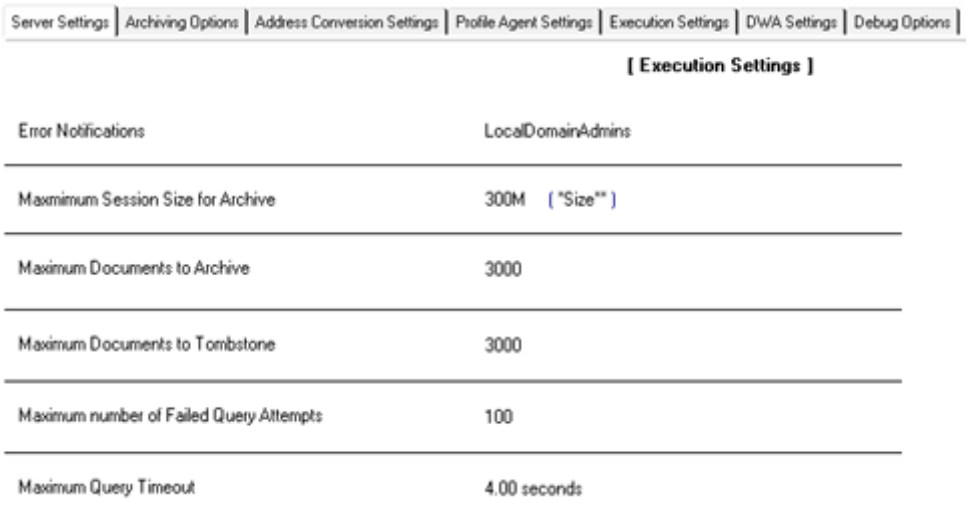
Field	Description
Resolve Groups for additional Domino Domains	Select the check box to resolve groups.
Secondary directory for group lookups	Enter the filename of an additional Domino Directory for resolution of group names. A Directory Catalog can be used if the configuration includes more than two Domino mail domains.
Group Server	If the Domino Directory containing secondary group information is on a different server, list that server here. Otherwise, leave this field blank.

Profile Agent Settings



Field	Description
Use 'Address Conversion Settings'	Leave the default (with the check box selected) unless you plan to use an alternate Domino Directory to identify users for selective archiving. (For example, if you have set up a Directory Assistance database.) If you plan to use an alternate Domino Directory to identify users, deselect the check box and complete the remaining fields in this tab.
Use Global Config Override — use Server Definition Config	• If the settings on this tab apply to all Domino servers in the domain, select **Use Global Config** and configure the Profile Agent settings in the Global Configuration document. See "Profile Agent settings (global)" on page 25. • If the settings apply only to the server(s) listed in this Server Definition document, select **Override — use Server Definition Config**, and then complete the Profile Agent Settings.
Users lookup Domino Directories	Enter the name(s) of the alternate Domino Directory(ies) used to select individual users.
Groups lookup Domino Directories	Enter the name(s) of the alternate Domino Directory(ies) used to select groups. Entries can be separated with commas or newlines.

Execution Settings



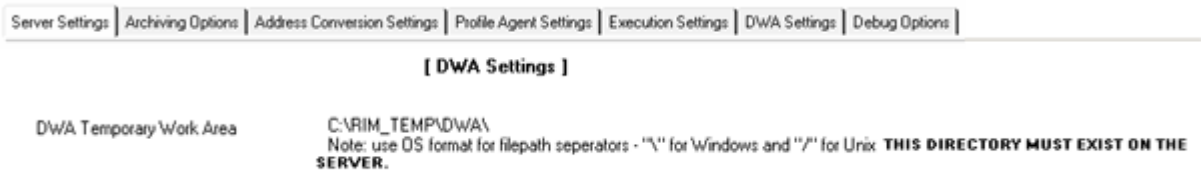
Field	Description
Error Notifications	Select the user or group from the list who should be notified when there are errors executing the Archive or Tombstone mining agents. For example, LocalDomainAdmins.
Maximum Session Size for Archive	For local mining, leave the default (300M). For remote mining, increase to 500M on an Active Gateway or journal server.
Maximum Documents to Archive	For local mining, leave the default (3000). For remote mining, increase to 10,000 on an Active Gateway or journal server.
Maximum Documents to Tombstone	For local mining, leave the default (3000). For remote mining, increase to 10,000 on an Active Gateway or journal server.
Maximum number of Failed Query Attempts	Leave the default (100).
Maximum Query Timeout	Leave the default (4.00 seconds) unless you find that the timeout is not long enough.

DWA Settings

During archive processing, a signed or encrypted message is *encapsulated*, or encased in its own database, to keep message data intact. The database with the encapsulated message is then attached to the original message and sent to the IAP.

When the message is retrieved in DWA, it needs to be unencapsulated for the user to view it. If you are implementing DWA Extension, a directory must be created to temporarily store the unencapsulated files when DWA users retrieve signed or encrypted messages from the IAP. This directory is listed in the DWA Settings tab.

For more information on DWA Extension, see "Configuring DWA Extension" on page 47.



Field	Description

Temporary Work Area	This field lists the directory that temporarily stores the unencapsulated files. The directory can be on the mail server or the Proxy Gateway, if a proxy is used. Alternatively, you can create a file share on an application server and map a drive to the share. The share must have read/write access.
	If the server definition lists more than one Proxy Gateway, the directory for the work area should have the same name and path on each server.
	The size of the directory depends on your environment (how often users send or receive signed or encrypted messages).
	Important! Always create a new directory for the work area, making sure the following conditions are met:
	• Do not create a sub-directory within the operating system's temporary directory, or use the temporary directory for the work area.
	• Ensure the work area refers to a drive different than the one holding user mail files.
	• For security reasons, make sure the work area is not contained in the Domino data directory, or in any subdirectory- or directory-linked area that is visible to Notes clients or browser users. For example, do not enter `D:\Lotus\Domino\Data\RIM_TEMP` if that is the path to your Domino data root. Do not share this directory in your network.
	Using Windows Remote Desktop, Telnet, or another terminal window, connect to the server and issue the appropriate commands to create the directory identified in this field.
	For example, on a Windows-based Domino server, enter:
	`C:`
	`CD\`
	`MKDIR RIM_TEMP`
	`CD RIM_TEMP`
	`MKDIR DWA`
	Ensure that security settings on the server allow access to the directory that you create. On UNIX-based servers, make sure that the owner, group, and permissions for the directory are the same as the owner, group, and permissions for the server's data root directory. Typically, the following commands accomplish this:
	`chown domino:domino RIM_TEMP`
	`chmod 755 RIM_TEMP`

Debug Options

Debug options are used by HP support to help diagnose problems that might occur during message archiving.

- The Archive tab enables debugging for the Archive agent.
- The Tombstone tab enables debugging for the Tombstone agent.
- The Field Remapper tab enables debugging for message headers.
- The Body Parser tab enables debugging for the unique message ID (hash).

Under normal operation all debug options should be disabled, as certain options write additional entries to the Domino log database (`log.nsf`) for each message processed. Ensure that all options on the Debug tabs are set to **No** unless you are asked by HP support to enable an option.

Preprocessing messages

Several types of messages must be preprocessed so they can be archived in a format that preserves all message data intact:

- Lotus Notes PKI and S/MIME signed and encrypted messages
- Journaled items such as calendar notices, tasks or other messages that are not Memo, Reply
- Messages with ATT attachments
  See "Message attachments named ATTxxxxx" on page 131 for a description of these messages.

During preprocessing, a copy of the message is *encapsulated*—encased in a encapsulation database that is attached to the original message. The message and attachment are then routed to the IAP. "Preprocessing and reference databases" on page 35 describes what can be viewed in the preprocessing database as the message is being processed.

When encapsulated messages are retrieved in Lotus Notes or DWA, or are exported from the IAP using the Web Interface, they can be opened just like any other message. However, if users send copies of encapsulated messages from the IAP Web Interface to their mailbox (Mail-To-Me messages), the message is still inside the encapsulation database. "Opening encapsulated messages" on page 124 explains how to open these messages.

There is a significant storage penalty on the IAP for encapsulating messages because of the extra processing involved. The size of an encapsulated message stored on the IAP is approximately 8 KB.

Preprocessing and reference databases

Three EAs Domino preprocessing databases are installed in the `hprim` folder on message processing servers. An Encapsulate agent in these databases performs message encapsulation.

Each preprocessing database is paired with a corresponding reference database, which contains temporary pointers to the messages that have been flagged for archiving. The Archive and Tombstone agents in each reference database create and remove these pointers as needed. After a mining job is run, you can open a reference database to view a log of the message references that are being processed. The reference database also contains tools to troubleshoot encapsulation problems; these tools should only be used under the direction of HP support. See "Viewing references" on page 40 for more information.

You can view the encapsulated messages as they are being processed in the preprocessing databases:

- For signed messages, ATT file attachments, and calendar notices you can view the messages, including header, body and all attachments, in their original format (RTF or HTML/MIME).
- For encrypted messages, you can view the headers but cannot view the message body.
- Encapsulated messages are 84 KB when they are routed to the IAP. That size is reduced to 8 KB when they are stored on the IAP.

Function	Preprocessing database name	Reference database name
Selective archiving	`hprim\hp_preproc_miner.nsf`	`hprim/hp_riss_minerrefer-enc.nsf`
Compliance archiving	`hprim\hp_preproc_journal.nsf`	`hprim/hp_riss_journalrefer-enc.nsf`
Bulk upload	`hprim\hp_preproc_blk.nsf`	`hprim/hp_riss_blkupdrefer-enc.nsf`

NOTE:

The preprocessing and reference databases should not be replicated. To create a new preprocessing and reference database on message processing servers, see "Creating a new preprocessing database " on page 145 and "Creating a new reference database" on page 146.

Configuring the Preprocessing Control documents

A Preprocessing Control document must be configured for each preprocessing database that is used during archiving. Three default documents have been created: for selective archiving, journaling, and bulk upload.

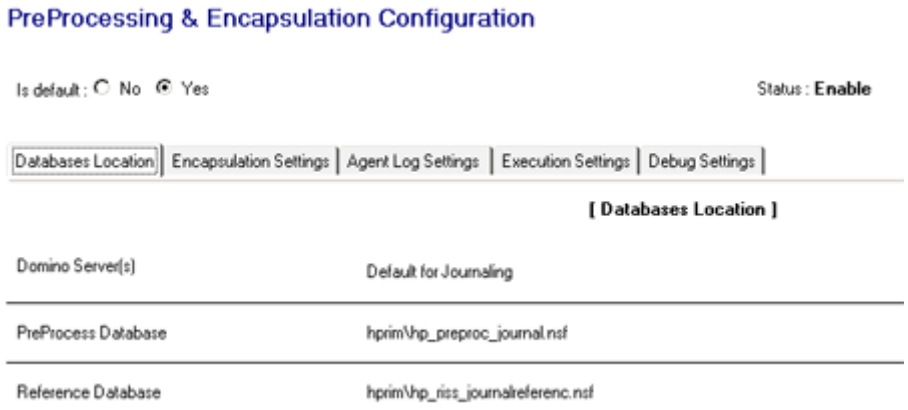
To configure a Preprocessing Control document:

1. In the Domino Administrator client, click the **Files** tab and open the HP EAs-D API database.
2. In the main view, under **PreProcessing Controls**, double-click the default document for journaling, selective archiving, or bulk upload to open the document.
3. If this will be the default Preprocessing Control document for the domain, click **Yes**. Otherwise, leave the default of **No**.
4. Configure the settings in each tab:
   - "Databases Location tab" on page 37
   - "Encapsulation Settings" on page 37
   - "Agent Log Settings" on page 39
   - "Execution Settings" on page 39
   - "Debug Settings" on page 40
5. In Status, click **Enable** when you are ready to enable the Preprocessing Control document.
6. Select **File** > **Save** to save the document.

IMPORTANT:

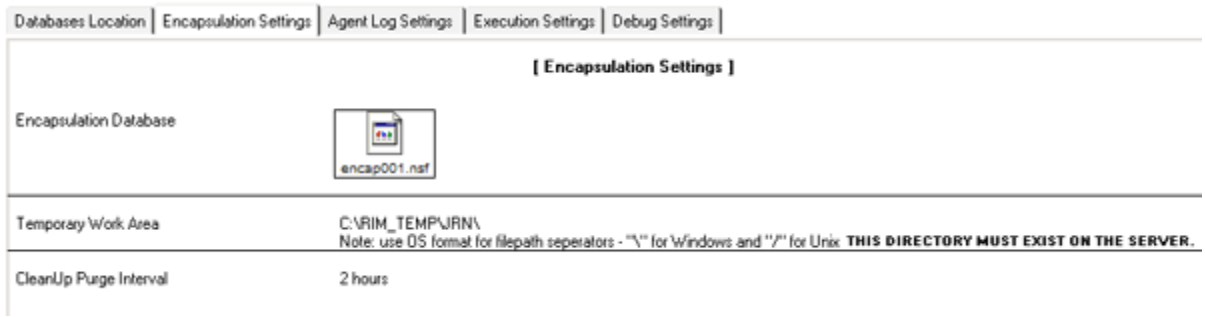
To create a new Preprocessing Control document, copy one of the existing documents in the main view. This ensures that the encapsulation database is copied into the new document. Do not use the Create menu.

Databases Location tab



Field	Description
Domino Server(s)	Enter the name of the server running the Encapsulate agent. For local mining, this would be the local mail server(s). For remote mining, this would be the HP gateway server(s) or application/journal server(s).
PreProcess Database	The path and filename are pre-set in the default documents: • `hprim\hp_preproc_miner.nsf` for selective archiving • `hprim\hp_preproc_journal.nsf` for journaling • `hprim\hp_preproc_blk.nsf` for bulk upload
Reference Database	The path and filename are pre-set in the default documents: • `hprim\hp_riss_minerreferenc.nsf` for selective archiving • `hprim\hp_riss_journalreferenc.nsf` for journaling • `hprim\hp_riss_blkupdreferenc.nsf` for bulk upload

Encapsulation Settings

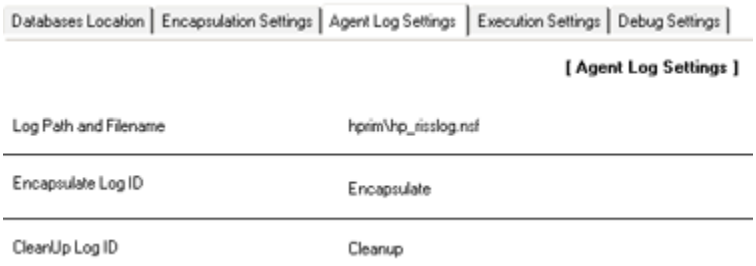


Field	Description
Encapsulation Database	Do not edit this field. A copy of the message is encased in the encapsulation database. The database is then renamed (for example, `encap001.nsf`, `encap002.nsf`) and added as an attachment to the message.

Temporary Work Area	This field lists the directory on the message processing server that temporarily stores the encapsulation databases while the messages are being encapsulated.
	Use the following formula to compute the amount of disk space required for each work area. Note that each message is 320 KB while it is being encapsulated.
	320 KB x 2 x number of messages
	(To determine the number of messages, monitor router traffic for several days, and note the traffic size and approximate number of encapsulated messages per 24–hour period.)
	Important! Always create a new directory for the work area, making sure the following conditions are met:
	• Ensure that each preprocessing database (for journaling, selective archiving, and bulk upload) has a separate directory or sub-directory in order to avoid file name collisions.
	• Do not use the temporary directory for the work area or create subdirectories within the operating system's temporary directory.
	• Make sure the work area refers to a drive different than the one holding user mail files.
	• For security reasons, make sure the work area is not contained in the Domino data directory, or in any subdirectory- or directory-linked area that is visible to Notes clients or browser users. For example, do not enter `D:\Lotus\Domino\Data\RIM_TEMP` if that is the path to your Domino data root. Do not share this directory in your network.
	Using Windows Remote Desktop, Telnet, or another terminal window, connect to the server and issue the appropriate commands to create the directory identified in this tab.
	For example, on a Windows-based Domino server, enter:
	`C:`
	`CD\`
	`MKDIR RIM_TEMP`
	`CD RIM_TEMP`
	`MKDIR MNR`
	Ensure that security settings on the server allow access to the directory that you create. On UNIX-based servers, make sure that the owner, group, and permissions for the directory are the same as the owner, group, and permissions for the server's data root directory. Typically, the following commands accomplish this:
	`chown domino:domino RIM_TEMP`
	`chmod 755 RIM_TEMP`

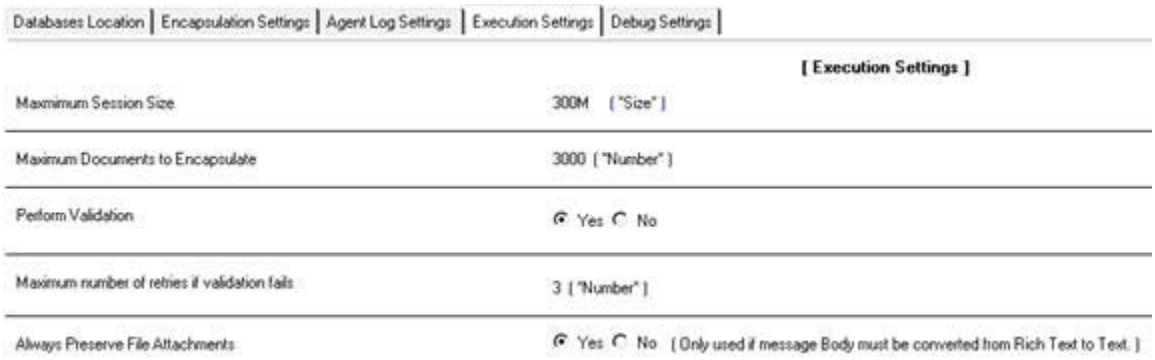
CleanUp Purge Interval	The temporary files in the work area are automatically purged after they are processed successfully. This field sets the interval between purges. Keep the default of 2 hours.

Agent Log Settings



Field	Description
Log Path and Filename	Leave the default.
Encapsulate Log ID	Leave the default.
CleanUp Log ID	Leave the default.

Execution Settings



Field	Description
Maximum Session Size	The size of the total number of messages that can be processed by the Encapsulate agent in a session. The default is 300M; this size can be increased to 500M for remote mining.
Maximum Documents to Encapsulate	The maximum number of messages that can be processed by the Encapsulate agent in a session. The default is 3000 (documents), which is adequate for most environments.
Perform validation	Leave the default of **Yes** to ensure that a valid encapsulation database is attached to a message.
Maximum number of retries if validation fails	Enter the number of validation retries. The default is three retries.
Always Preserve File Attachments	Leave the default of **Yes**. In some cases, encapsulation is required if there is a problem with the Rich Text content in the message Body field. To fix the problem, the body is converted from RTF to text and the Body field is rewritten. While the conversion occurs, file attachments are temporarily detached and placed in the same temporary work area that is used by the encapsulation databases (see "Encapsulation Settings" on page 37. **Yes** must be selected so that attachments can be preserved and reattached to the message.

Debug Settings

The debug option is used by HP support to help diagnose problems that might occur during message preprocessing.

Under normal operation this option should be disabled. Ensure that the Debug Level is set to **None**, unless you are asked by HP support to enable debugging.

Viewing references

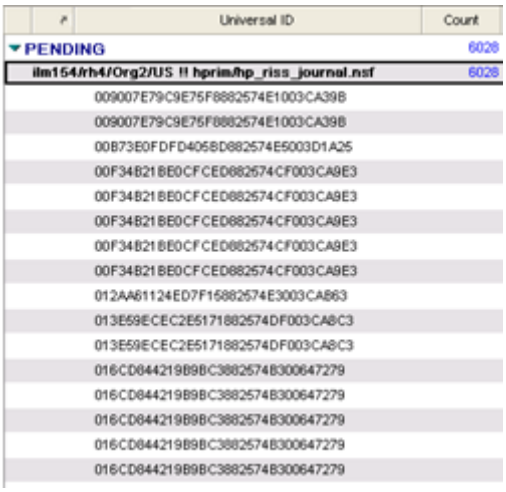
Reference databases contain pointers to messages that are eligible for archiving. The EAs agents create and remove these pointers as needed. After a mining job is run, you can open the reference database to view a log of the message references that are being processed.

Viewing the message reference log

To open the message reference log:

1. In the Domino Administrator client, open the relevant reference database in the `hprim` folder.
   - Selective archiving: HP EAs-D Reference (mnr) (`hp_riss_minerreferenc.nsf`)
   - Journaling: HP EAs-D Reference (jrl)`hp_riss_journalreferenc.nsf`)
   - Bulk upload: HP EAs-D Reference (blk)`hp_riss_blkupdreferenc.nsf`)
2. Click one of the buttons in the left menu to view references by server or status.

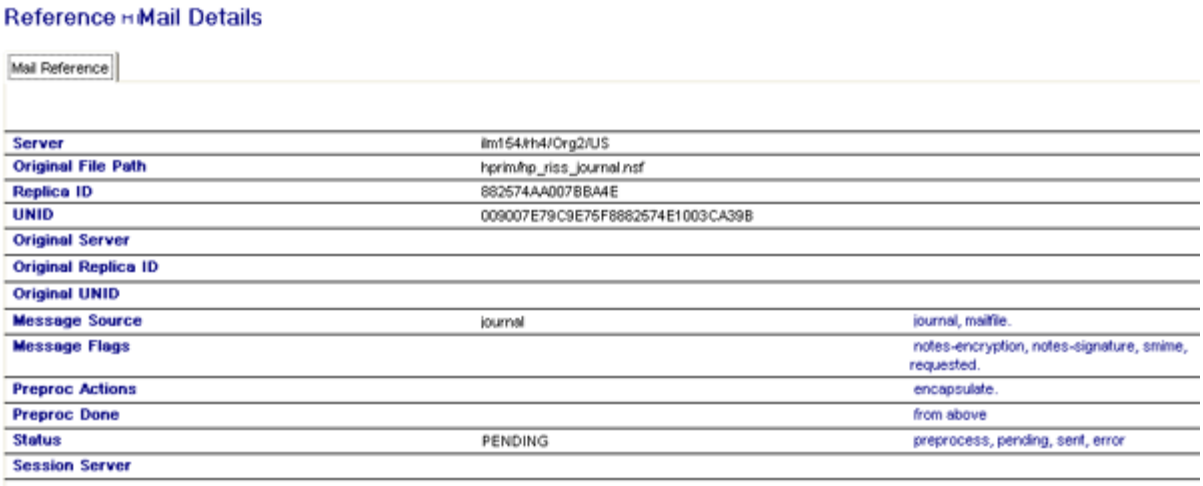
   The log shows the message references for each mailbox on a server.



3. Double-click the message entry for more information about a reference. Each message has a universal ID (UNID).

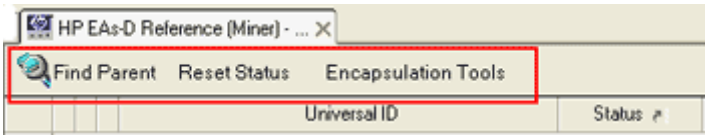
   Messages can be in one of the following states:

   - Preprocess: An encapsulated message is being processed.
   - Pending: A message has not been sent to the IAP. It is pending on a mail server or on the HP gateway server.
   - Sent: A message has been sent to the IAP from the gateway server.
   - Error: An error occurred and the message was not processed.



Reference database troubleshooting tools

New tools have been added in HP EAs Domino version 2.0.1 to help HP troubleshoot archiving problems. The tools are located in each reference database and should only be used under the direction of HP support.



- Find Parent tool: If there is a problem with archiving a message, this tool locates the message in a journal or user mail file.
- Reset Status tool: This tool changes the processing status of a message and reference. The Hold status (for pending documents) and the Hold-P status (for documents being preprocessed) remove messages and their associated references out of the archiving execution path.
- Encapsulation Tools: The three flag message options find a source message and stamp it with the appropriate flag for HP support. The revert option finds and deletes the transport copy of a message.

Working with log files

You can view a log of mining activity and change the number of days that log entries are kept.

HP EAs-D Log database

The HP EAs-D Log database (`hprim\hp_risslog`) records:

- Activity of the mining program (rissminer) and the EAs Domino agents
- Any debugging that you are asked to perform by HP support

- Output generated from the API database's Actions >- Tools > 2. Export configuration (used by HP support to examine the HP EAs-D API database configuration)

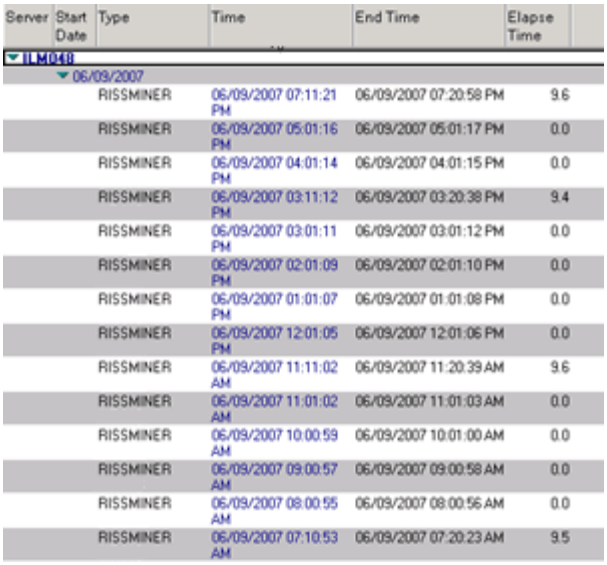
The Domino server log (`log.nsf`) also records the execution of rissminer and the agents, and any debugging output. However, items are much easier to locate in the EAs-D log than the server log, and the EAs-D log contains more information about the mining activity.

Viewing archiving log files

To view mining logs:

1. Click **Module Logs** in the left menu of the HP EAs-D API main view.

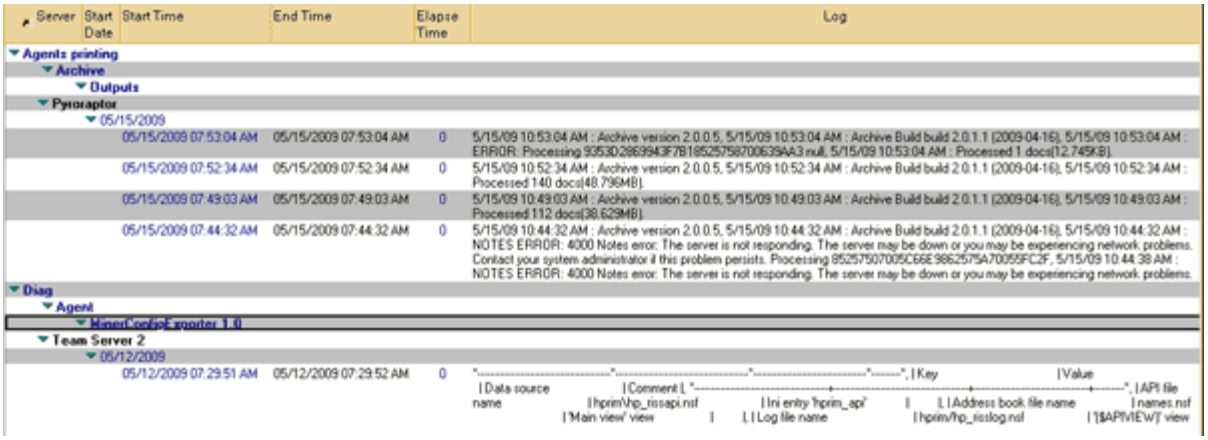
   The All Log view appears.



Server	Start Date	Type	Time	End Time	Elapse Time
ILM04B					
	06/09/2007				
		RISSMINER	06/09/2007 07:11:21 PM	06/09/2007 07:20:58 PM	9.6
		RISSMINER	06/09/2007 05:01:16 PM	06/09/2007 05:01:17 PM	0.0
		RISSMINER	06/09/2007 04:01:14 PM	06/09/2007 04:01:15 PM	0.0
		RISSMINER	06/09/2007 03:11:12 PM	06/09/2007 03:20:38 PM	9.4
		RISSMINER	06/09/2007 03:01:11 PM	06/09/2007 03:01:12 PM	0.0
		RISSMINER	06/09/2007 02:01:09 PM	06/09/2007 02:01:10 PM	0.0
		RISSMINER	06/09/2007 01:01:07 PM	06/09/2007 01:01:08 PM	0.0
		RISSMINER	06/09/2007 12:01:05 PM	06/09/2007 12:01:06 PM	0.0
		RISSMINER	06/09/2007 11:11:02 AM	06/09/2007 11:20:39 AM	9.6
		RISSMINER	06/09/2007 11:01:02 AM	06/09/2007 11:01:03 AM	0.0
		RISSMINER	06/09/2007 10:00:59 AM	06/09/2007 10:01:00 AM	0.0
		RISSMINER	06/09/2007 09:00:57 AM	06/09/2007 09:00:58 AM	0.0
		RISSMINER	06/09/2007 08:00:55 AM	06/09/2007 08:00:56 AM	0.0
		RISSMINER	06/09/2007 07:10:53 AM	06/09/2007 07:20:23 AM	9.5

   Depending on the view you select from the left menu, the log lists the following data:

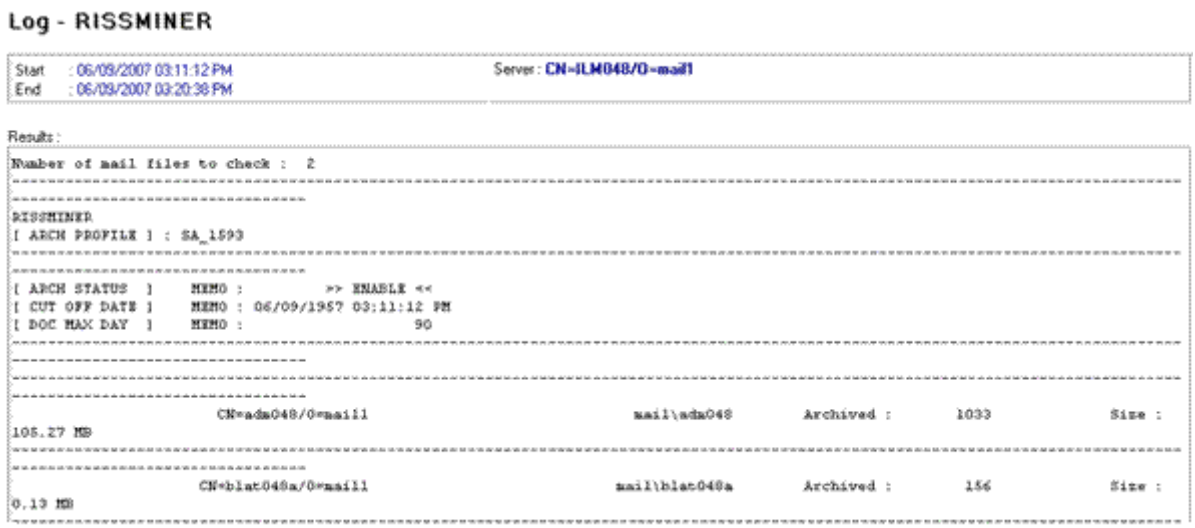
   - The mail server on which the activity was performed
   - The date the activity took place
   - The type of activity
   - The start time and end time of the session
   - The time, in minutes, that it took to process each journal or mail database
   - The total number of databases and documents processed
   - The total size (in MB) of the databases processed
   - Errors that occurred during the session



Server	Start Date	Start Time	End Time	Elapse Time	Log
Agents printing					
Archive					
Outputs					
Pyroraptor					
	05/15/2009				
		05/15/2009 07:53:04 AM	05/15/2009 07:53:04 AM	0	5/15/09 10:53:04 AM : Archive version 2.0.0.5, 5/15/09 10:53:04 AM : Archive Build build 2.0.1.1 (2009-04-16), 5/15/09 10:53:04 AM : ERROR: Processing 9353D2863943F7B185257587006394A3.null, 5/15/09 10:53:04 AM : Processed 1 docs(12.745KB).
		05/15/2009 07:52:34 AM	05/15/2009 07:52:34 AM	0	5/15/09 10:52:34 AM : Archive version 2.0.0.5, 5/15/09 10:52:34 AM : Archive Build build 2.0.1.1 (2009-04-16), 5/15/09 10:52:34 AM : Processed 140 docs(48.796MB).
		05/15/2009 07:49:03 AM	05/15/2009 07:49:03 AM	0	5/15/09 10:49:03 AM : Archive version 2.0.0.5, 5/15/09 10:49:03 AM : Archive Build build 2.0.1.1 (2009-04-16), 5/15/09 10:49:03 AM : Processed 112 docs(38.629MB).
		05/15/2009 07:44:32 AM	05/15/2009 07:44:32 AM	0	5/15/09 10:44:32 AM : Archive version 2.0.0.5, 5/15/09 10:44:32 AM : Archive Build build 2.0.1.1 (2009-04-16), 5/15/09 10:44:32 AM : NOTES ERROR: 4000 Notes error: The server is not responding. The server may be down or you may be experiencing network problems. Contact your system administrator if this problem persists. Processing 85257507005C66E9862575A70055FC2F, 5/15/09 10:44:38 AM : NOTES ERROR: 4000 Notes error: The server is not responding. The server may be down or you may be experiencing network problems.
Diag					
Agent					
HinerConfigExporter 1.0					
Team Server 2					
	05/12/2009				
		05/12/2009 07:29:51 AM	05/12/2009 07:29:52 AM	0	"----------","----------","----------","----------", | Key | Value | Data source name | hprim\hp_rissapi.nsf | 'Main view' view | Comment | "----------+----------+----------", | Ini entry 'hprim_api' | | Log file name | API file | Address book file name | hprim\hp_isslog.nsf | names.nsf | '($APIVIEW)' view

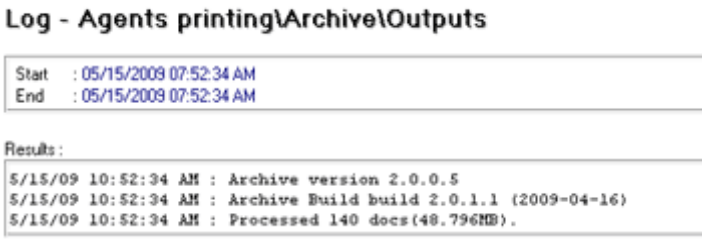
2. Double-click a log entry for more information about the particular entry.

For the rissminer program, the entry shows the following information:



- The number of mailboxes in the database
- The name and version of the mining rule used for mining the database
- The cutoff date set in the rule for the Memo, Reply time condition
- The name of each mailbox that was mined, the number of messages processed in the mailbox, and the size of the processed messages

For a successful run, an agent log entry displays:



- The start time and end time of the session
- The agent version and EAs Domino build version
- The total number of documents processed
- The total size (in MB) of the documents processed

If an error occurs during processing, the log entry displays information about the error:

Log - Agents printing\Archive\Outputs

Start : 05/15/2009 07:44:32 AM
End : 05/15/2009 07:44:32 AM
Server : CN=Pyroraptor/O=EASDomino

Results :

```
5/15/09 10:44:32 AM : Archive version 2.0.0.5
5/15/09 10:44:32 AM : Archive Build build 2.0.1.1 (2009-04-16)
5/15/09 10:44:32 AM : NOTES ERROR: 4000 Notes error: The server is not responding. The server may be down or you may be experiencing network problems. Contact your system
administrator if this problem persists. Processing 85257507005C66E986257SA70055FC2F
5/15/09 10:44:38 AM : NOTES ERROR: 4000 Notes error: The server is not responding. The server may be down or you may be experiencing network problems. Contact your system
administrator if this problem persists. Processing 85257507005C66E986257SA70055F969
5/15/09 10:44:43 AM : NOTES ERROR: 4000 Notes error: The server is not responding. The server may be down or you may be experiencing network problems. Contact your system
administrator if this problem persists. Processing 85257507005C66E986257SA70055F8E4
5/15/09 10:44:48 AM : NOTES ERROR: 4000 Notes error: The server is not responding. The server may be down or you may be experiencing network problems. Contact your system
administrator if this problem persists. Processing 85257507005C66E986257SA70055F843
5/15/09 10:44:53 AM : NOTES ERROR: 4000 Notes error: The server is not responding. The server may be down or you may be experiencing network problems. Contact your system
administrator if this problem persists. Processing 85257507005C66E986257SA70055F961
5/15/09 10:44:58 AM : NOTES ERROR: 4000 Notes error: The server is not responding. The server may be down or you may be experiencing network problems. Contact your system
administrator if this problem persists. Processing 85257507005C66E986257SA70055F871
5/15/09 10:45:03 AM : NOTES ERROR: 4000 Notes error: The server is not responding. The server may be down or you may be experiencing network problems. Contact your system
administrator if this problem persists. Processing 85257507005C66E986257SA70055FB32
5/15/09 10:45:08 AM : NOTES ERROR: 4000 Notes error: Operation stopped at your request Processing 85257507005C66E986257SA70055F9F9
5/15/09 10:45:12 AM : NOTES ERROR: 4000 Notes error: Operation stopped at your request Processing 85257507005C66E986257SA70055F735
5/15/09 10:45:12 AM : NOTES ERROR: 4000 Notes error: Operation stopped at your request Processing 85257507005C66E986257SA70055F497
5/15/09 10:45:12 AM : NOTES ERROR: 4000 Notes error: Operation stopped at your request Processing 85257507005C66E986257SA70055F800
5/15/09 10:45:12 AM : NOTES ERROR: 4000 Notes error: Operation stopped at your request Processing 85257507005C66E986257SA70055F7FF
5/15/09 10:45:12 AM : NOTES ERROR: 4000 Notes error: Operation stopped at your request Processing 85257507005C66E986257SA70055FB48
```

When you select Actions >- Tools > 2. Export configuration in the EAs-D API database, information about the database configuration settings is displayed in the log entry:

Log - Diag\Agent\MinerConfigExporter 1.0

Start : 05/12/2009 07:29:51 AM
End : 05/12/2009 07:29:52 AM
Server : CN=Team Server 2/O=HP EAs

Results :

Key	Value	Data source	Comment
API file name	hprim\hp_rissapi.nsf	Ini entry 'hprim_api'	
Address book file name	names.nsf	'Main view' view	
Log file name	hprim/hp_risslog.nsf	'($APIVIEW)' view	
All debug	false	Hard coded	
Sleep interval	0		
Tombstone settings debug	false	Ini entry 'HPRIM_DebugTombstone'	
Mining rules	4 rule(s) and 5 action(s)	'ModuleProfileDefView' view	
Profile name	DNA Sample	Mining rules	
> Minimum message size :	0 byte(s)		
> Enabled	true		
Action bevavior			
> Removes message	false		
> Removes body	true		
> Removes attachments	true		
Style	Rich text		
Profile name	Bulk	Mining rules	
> Minimum message size :	0 byte(s)		
> Enabled	true		
Action bevavior			
> Removes message	true		
> Removes body	true		
> Removes attachments	true		
Style	Simple text		

Purging log entries

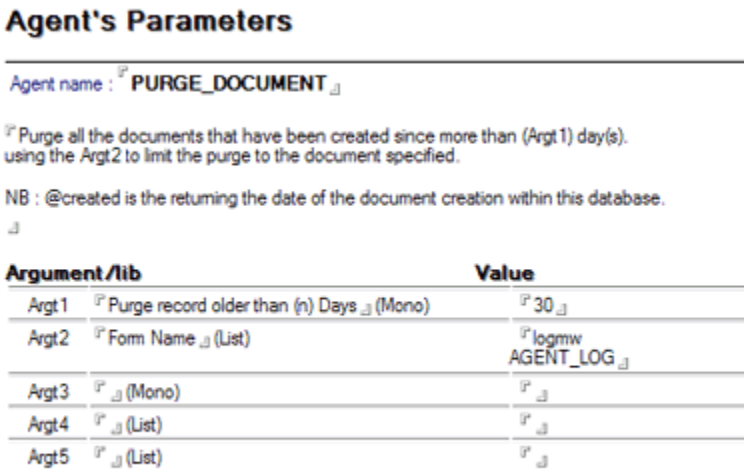
The Purge_Document agent is used by the HP EAs-D Log to remove log records that are older than a certain number of days. The default removes records that are more than 30 days old.

You can change the number of days that log records are kept by editing the Agent Parameters document.

1. Using the Domino Administrator client, open the HP EAs-D Log database (`hp_risslog`) in the `hprim` folder on any mail server with a copy of the database.
2. In the **View** menu, select **Go To**, and then select **Agent**.
3. Expand **Agent**, select **Parameters**, and then click **OK**.

   The Agent\Parameters view appears.
4. Double-click the document listed in PURGE_DOCUMENT.

5. Double-click the value in **Argt1: Purge record older than (n) Days** and change the number of days. Do not change the Form Name value in Argt2.



Agent's Parameters

Agent name : **PURGE_DOCUMENT**

Purge all the documents that have been created since more than (Argt1) day(s).
using the Argt2 to limit the purge to the document specified.

NB : @created is the returning the date of the document creation within this database.

Argument/lib		Value
Argt1	Purge record older than (n) Days (Mono)	30
Argt2	Form Name (List)	logmw AGENT_LOG
Argt3	(Mono)	
Argt4	(List)	
Argt5	(List)	

6. Click **File** > **Save**, and then close the document.
7. In the Designer client, schedule and enable the Purge_Document agent.
   a. Open the HP EAs-D Log database in the `hprim` folder on any mail server with a copy of the database.
   b. In the Design pane, select **Shared Code** > **Agents**.
   c. Double-click **Purge_Document**.

      The Properties for Agent dialog box appears.
   d. Make sure the Trigger is set to **On schedule** and the Target is set to **All documents in database**.
   e. Set the schedule, selecting **Any server** in the Where agent runs box.

      The agent can be scheduled to run as needed, but is usually run once a day. (The default is set for daily at 1:00 a.m.)
   f. Click **Enable** to enable the agent.

4 Configuring DWA Extension

Tombstones, or links in mail files to messages archived on the IAP, can be retrieved in Lotus Notes and Domino Web Access (DWA), or iNotes. This chapter explains the steps required to retrieve messages in DWA.

For information on retrieving messages in Notes clients, see "Working with HP EAs Domino client applications" on page 105.

- DWA Extension configuration steps, page 47
- Configuring the Proxy Gateway document, page 49
- Configuring the Tombstone Prototype document, page 51
- Editing the Tombstone Settings tab, page 53
- Purging cached messages, page 54
- Purging tombstone conversion requests, page 54

DWA Extension configuration steps

When users open a tombstoned message in DWA, text such as "Click here to retrieve the full message" is displayed. This text is a live URL that submits a retrieval request to the IAP. The request is executed by the EASWEB agent in the HP EAs-D DWA Index database (`hp_dwaindex.nsf`). The messages that are retrieved from the IAP are cached for the number of days that you specify.

All mail functionality, including reply and forward, applies for each message retrieved in DWA.

Older tombstoned message that were created using earlier versions of EAs Domino are converted automatically when they are opened in DWA.

NOTE:

Retrieved DWA messages are cached in the user's mail file for the period of time specified in the Global Configuration document. These cached messages are hidden from all standard views provided by the Lotus Notes Mail templates. If you want to add a custom view to your mail template to display the cached messages, use the following selection formula: SELECT @IsAvailable(HP_DWA_CACHE_DATE) | @IsAvailable(HP_DWA_CACHE)

To configure DWA Extension, follow these steps:

1. Verify the file installation.

   On each Domino server where messages are retrieved from the IAP (including the proxy, if used):

   - A replica of the API database should be installed using the following file path: `hprim\hp_rissapi.nsf`.
     This database is used to support the lookup operations that are performed when a user clicks a tombstone URL in DWA.
   - A unique instance of the DWA Index database should be installed using the following file path: `hprim\hp_dwaindex.nsf`.
     This database contains the software to accept and process requests to retrieve archived messages from the IAP and return them to the request user's browser.
   - If your installation has been upgraded from a pre-2.0 version of EAs Domino: A replica of the HP EAs-D Server Requests database should be installed using the following file path: `hprim\hp_rissreq.nsf`.
     The HP EAs-D Server Requests database is used to convert pre-EAs Domino 2.0 tombstoned messages to the Rich Text format required by DWA Extension.

2. If a proxy server is used, ensure the following settings are configured on the proxy:

   - A trust relationship is established with the mail servers that the proxy is servicing.
   - SSL is configured to service encrypted message requests.
   - Domino single sign-on is configured with the mail server(s) to avoid users being prompted to authenticate.

3. On each server where the DWA Index database is installed, verify the EASWEB agent security settings in the database.

   Ensure the Run on behalf of security setting in the agent is set to a Notes ID that is listed in the Server document's Security > Programmability Restrictions > Run restricted LotusScript/Java agents field. HP recommends specifying the server on which the agent will run.

4. Ensure the ACL is set as follows:

   - In the DWA Index database, each Notes ID that is used in step 3 must have Editor access. This Notes ID, with Editor access, should also be listed in the mail file ACL of all DWA users.
   - In the HP EAs-D API database, DWA users require Reader access. Each Notes ID used in step 3 must be listed, with Reader access. **Note**: If the Notes ID is the same as the Server ID, the ID should have Manager access with delete rights.
   - If the HP EAs-D Server Requests database is used, the LocalDomainAdmins (or substitute) should have Manager access with delete rights.

5. (Optional) Configure a Proxy Gateway document.

   This document allows the message retrieval process to be executed on an alternate server in the domain.

   See "Configuring the Proxy Gateway document" on page 49.

6. (Optional) If you are using proxy servers to retrieve messages, create a new Server Definition document for the Proxy Gateway(s).

   See "Configuring the Server Definition document" on page 27.

7. In the Server Definition document, create a temporary work area for unencapsulating signed and encrypted messages that are retrieved from the IAP.

   This work area must be configured whether or not you use a Proxy Gateway.

   See "DWA Settings" on page 34.

8. Configure the Tombstone Prototype document.

   See "Configuring the Tombstone Prototype document" on page 51.

9. (Optional) If there are user groups that only access messages via DWA, create a DWA mining rule. Use Email Miner DWA Sample in the HP EAs-D API Mining Rules as the basis for the rule.
10. Configure the Tombstone Settings tab in the mining rule(s).

    This tab must be configured whether you use a DWA mining rule or a mining rule for mail files accessed by both DWA and Notes user communities.

    See "Editing the Tombstone Settings tab" on page 53.
11. Configure the remaining settings in the mining rule according to the steps in "Configuring mining rules" on page 56.
12. In the Global Configuration document, set the amount of time to retain retrieved messages in a cache in the user's mail file.

    See "DWA Index Settings" on page 26.
13. Schedule and enable the Purge agent in the HP EAs-D DWA Index database.

    This agent deletes the cached messages in the user's mail file after the configured number of days.

    See "Purging cached messages" on page 54.
14. Schedule and enable the Purge_Document agent in the HP EAs-D Server Requests Database.

    The agents in this database automatically convert older tombstoned messages when they are opened in DWA. The purge agent deletes the conversion requests in the database.

    See "Purging tombstone conversion requests" on page 54.

Configuring the Proxy Gateway document (optional)

A Proxy Gateway can be any Domino server that is in the same Domino domain as the mail server(s) that are being supported. HP recommends the use of a Proxy Gateway if you support a DWA user community where performance and server stability are critical.

If a Proxy Gateway is used, you will work with your HP representative to configure it for DWA Extension:

- A unique instance of the HP DWA Index database (`hp_dwaindex.nsf`) is installed on the proxy. It contains the software to accept and process requests to retrieve archived messages from the IAP and return them to the request user's browser.
- A replica copy of the HP EAs-D API database is installed on the proxy. The EAs-D API database must contain a Server Definition document for the Proxy Gateway server.
- The following settings are configured on the proxy:
  - A trust relationship is established with the mail servers that the proxy is servicing.
  - SSL is configured to service encrypted message requests.
  - Domino single sign-on is configured with the mail server(s) to avoid users being prompted to authenticate.

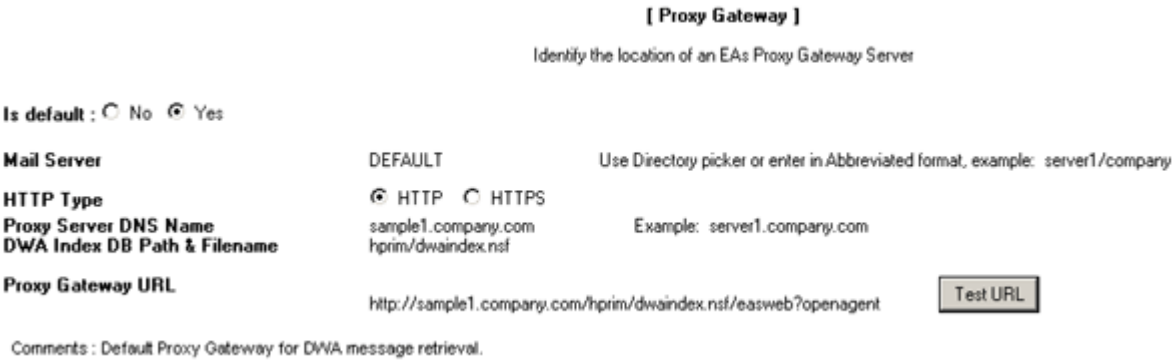
The Proxy Gateway document specifies the server that is being used as the proxy. By itself, this document has no effect on DWA message retrieval. It must be leveraged by a Tombstone Prototype document, which is created in "Configuring the Tombstone Prototype document" on page 51.

NOTE:

The Proxy Gateway document is not required if you plan to process DWA message requests on a local mail server.

To configure the Proxy Gateway document:

1. Open the HP EAs-D API database file.
2. Under Mining Rules in the main view, open **Proxy Gateway Default**, the default Proxy Gateway document.



3. Complete the following settings.

Field	Description
Is default	Select **Yes** if there is one Proxy Gateway or if this Proxy Gateway acts as the default for all mail servers listed in the Mail Server field below.
Mail Server	Click the arrow and select the name of the mail server(s) that are redirecting user requests to the proxy server. **Note**: Always use the picker to select the mail servers. This allows the hierarchy information to be properly stored with the server name.
HTTP Type	Select the HTTP type: HTTP or HTTPS. If DWA users are allowed to read encrypted email, select HTTPS. This setting is required to display encrypted mail messages.
Proxy Server DNS Name	Enter the DNS name of the Proxy Gateway server. For example, `server1.company.com`.
DWA Index DB Path & Filename	Enter `hprim/hp_dwaindex.nsf`.
Proxy Gateway URL	(Do not edit) This is the URL that points to the proxy server and DWA Index database. This field is updated automatically when you save the document. To verify the URL after saving, click **Test URL**.

4. Save the document.
5. To create a new document from the API main view, select **Create** > **Retrieval** > **1. Proxy Gateways**.

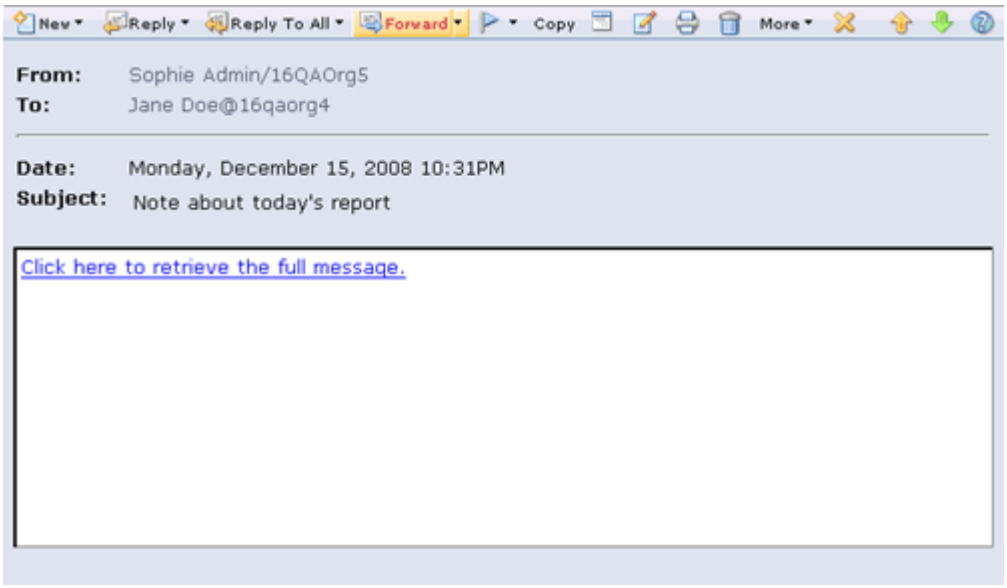
Configuring the Tombstone Prototype document

A Tombstone Prototype document must be configured for tombstoned messages to be retrieved in DWA. It must also be configured if users access messages in both DWA and the Notes client.

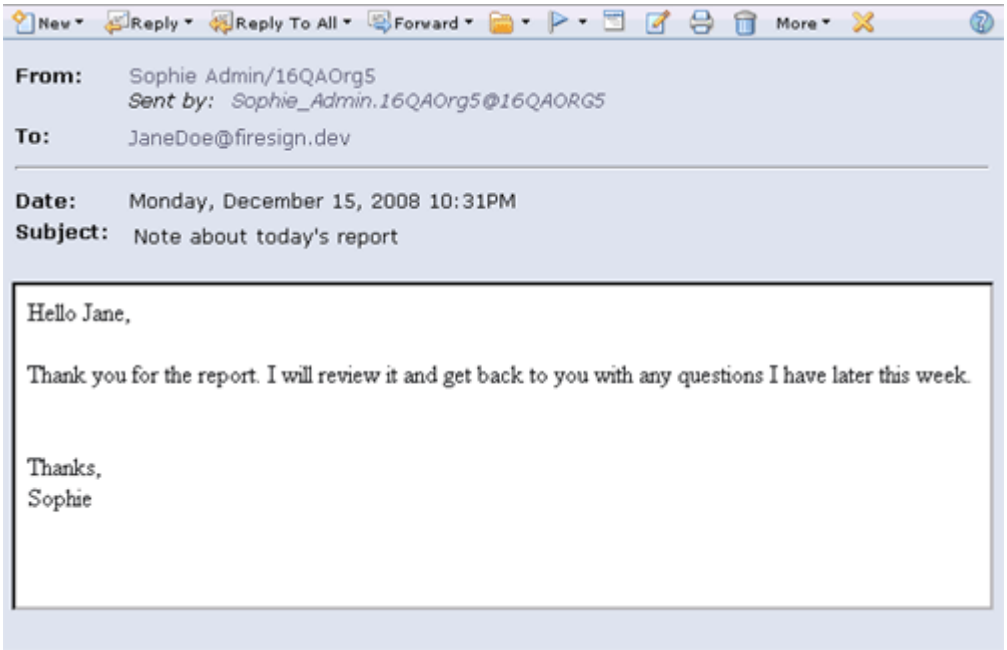
The prototype document includes a Rich Text field with a Computed Text element. The element contains a Formula Language function that is used to generate the link used during DWA tombstone retrieval.

The clickable link message that is created in the document replaces or appends the message body, depending on the tombstone action specified in the Tombstone Settings tab. (See "Editing the Tombstone Settings tab" on page 53). The link's URL is controlled by this document and the Proxy Gateway document (when used) and inserted into the message by the Tombstone agent.

The graphic below shows how a tombstoned message appears to DWA users.



When the link is clicked, the retrieved message is displayed. It appears in a separate window or tab depending on the browser.



NOTE:

If users access messages only in the Notes client, do not configure a Tombstone Prototype document. See "Tombstone Settings tab" on page 65 for the settings to use.

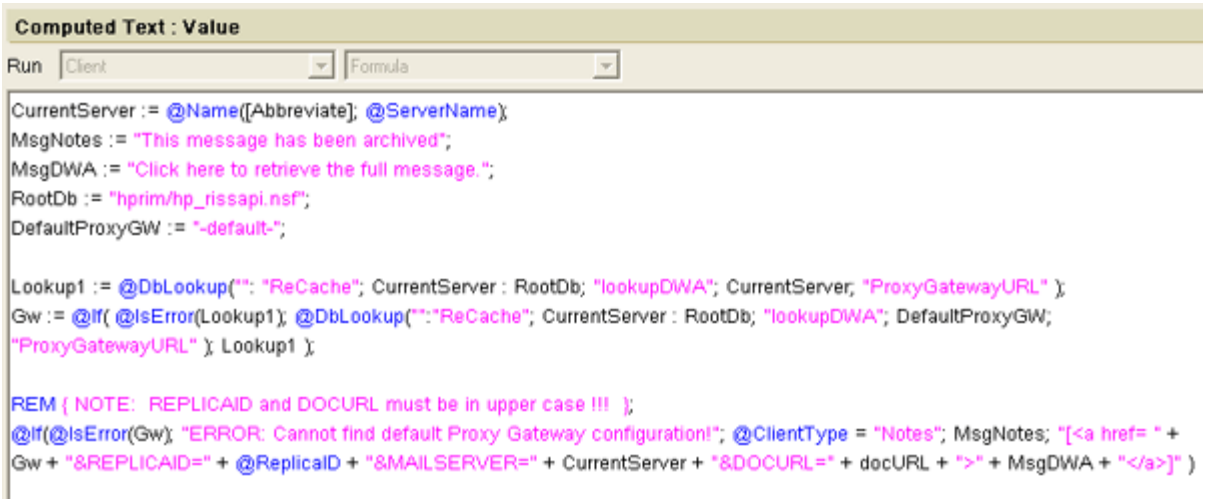
Follow this procedure to configure the document:

1. Open the HP EAs-D API database.
2. Under Tombstone Prototype in the main view, select one of the sample documents:
   - TSKey1, for use with a Proxy Gateway, generates tombstones that are approximately 3 KB. The formula in this document uses six variables to store the message retrieval parameters.
   - TSKey2, for use with a Proxy Gateway, generates tombstones that are approximately 2 KB. The formula in this document uses two hard–coded values (current server and lookup) for message retrieval.
     Whether you use TSKey1 or TSKey2 is a matter of preference.
   - TSKey3, for use with a local host, generates tombstones that are approximately 2 KB.
3. Use the copy and paste functions to make a working copy of the sample.
4. Double-click the working copy to open it for editing.
5. In the **Prototype key** field, change the name of the key to a new, unique name.

   The key name is used in the Tombstone Settings tab of the mining rule.
6. In the **Comments** field, enter any comments about the key or the document.
7. Place the cursor inside the **Tombstone Body** field, and in the **Computed Text** menu, select **Edit Computed Text**.

   The prototype formula appears. If a Proxy Gateway document has been configured, the values in the formula are imported from that document.

   The graphic below shows the formula that appears when a copy of TSKey1 is opened for editing. In this formula, the Lookup1 variable finds the Proxy Gateway document for the current server and retrieves the Proxy Gateway URL value. The @DbLookup function looks in the HP API database's lookupDWA view to find a Proxy Gateway document for the current mail server. (The lookupDWA view is the alias for a hidden view named ProxyGW.)



8. Edit the formula values:
   - (Proxy Gateway keys only) Edit the **CurrentServer** values if the mail server has spaces in its name. Change the spaces to either %20 or + so the URL can launch correctly. Otherwise, it stops at the first space.
   - Edit the **MsgNotes** value if you want to change the sample, "This message has been archived." This is the static message that appears in Lotus Notes.
   - Edit the **MsgDWA** value if you want to change the sample, "Click here to retrieve the full message."
     This is the clickable link message that appears in DWA when users open a tombstoned message.
   - If you make changes to the formula or create your own formula, ensure that the following parameters are always in upper case: REPLICAID, MAILSERVER, DOCURL. These URL parameters are case-sensitive.
     For example:
     https://<host_name>/hprim/hp_dwaindex.nsf/easweb?openagent&REPLICAID=<mail file_replicaID>&MAILSERVER=<mailserver_name>&DOCURL=<docURL>
9. Save the edited formula.

   An actual URL would look like this:

   http://rims2.usa.hp.com/hprim/hp_dwaindex.nsf/easweb?openagent&REPLICAID=852573DE:0078B7BC&MAILSEVER=Velociraptor/EASDomino&DOCURL=DWN03JI51C2lloMWpNmnAmaY1kIHikUWYWAme32EQekoce13WWnPKfdRJQ9w9MCjDHUqT21qcwn99SNb-I5vBqi5dUFpvpuoXQPlkAFWbKswEqMqw1RsEikjlcJXsHcX8J2qt4MTTqN9OYS7-uc23RuUqaVR4aKiNLHucf1J0M3U5ZoiNZ1TXeGmui3nTcOby1lXLmFjx4N6F6qDpc4ZAq
10. Save the edited Tombstone Prototype document.

NOTE:

For troubleshooting, append an optional DEBUG parameter to the URL configured in the document:

https://<prim/hp_dwaindex.nsf/easweb?openagent&REPLICAID=<mailfile_replicaID>&MAILSERVER=<mailserver_name>&DOCURL=<docURL>&DEBUG=true

Editing the Tombstone Settings tab

The key created in the Tombstone Prototype document is specified in the Tombstone Settings tab. The settings in this tab determine the action taken by the Tombstone agent and specify what content remains in the tombstone when a message is archived.

Three tombstoning choices are available:

- **Shrink Body and remove attachments** removes any attachments from the message and trims the length of the message body.
  The content created in the prototype document is appended to the message body.
  HP recommends that you choose this option.
- **Remove attachments only** removes any attachments, but leaves the message body intact.
  The content created in the prototype document is appended to the message body.
- **Clear body and remove attachments** removes both the body and any attachments from the message, leaving only the header.
  The content created in the prototype document replaces the message body.

To configure the tombstone settings:

1. Open the **HP EAs-D API** database file.
2. Under Mining Rules in the main view, open **Email Miner DWA Sample**.
3. Double-click inside the document to edit the rule.
4. Click the Tombstone Settings tab, and configure the settings according to the steps in "Tombstone Settings tab" on page 65.

Purging cached messages

The HP EAs-D DWA Index database (`hp_dwaindex.nsf`) contains the software to accept and process requests to retrieve archived messages from the IAP and return them to the request user's browser. These requests are cached in the user's mail file for the number of days specified in the Global Configuration document. (See "DWA Index Settings" on page 26.

The Purge agent in the DWA Index database must be scheduled and enabled so that the retrieved messages are deleted from the cache after the configured number of days.

To schedule and enable the agent using the Designer client:

1. Open the HP DWA Index database in the `hprim` folder.
2. In the Design pane, select **Shared Code** > **Agents**.
3. Double-click **Purge**, and then click **OK** to bypass the warning.

   The Properties for Agent dialog box appears.
4. Make sure the Trigger is set to **On schedule**, **Daily**, and the Target is set to **All documents in database**.
5. Set the schedule, selecting **Any server** in the **Where agent runs** box.
6. Click **OK**.
7. Close the Agent Properties dialog and the agent, and then click **Enable** to enable the agent.

Purging tombstone conversion requests

For DWA users to access messages that were archived using earlier versions of EAs Domino, the tombstones must be converted to Rich Text format. This conversion is handled automatically by agents in the HP EAs-D Server Requests database. A purge agent must be scheduled and enabled so that conversion requests are periodically deleted from the database.

Follow these steps to schedule and enable the agent:

1. In the Designer client, open the HP EAs-D Server Requests database (`hp_rissreq.nsf`).
2. In the Design pane, select **Shared Code** > **Agents**.
3. Double-click **Purge_Document**, and then click **OK** to bypass the warning.

   The Properties for Agent dialog box appears.
4. Make sure the Trigger is set to **On schedule**, **Daily**, and the Target is set to **All documents in database**.
5. Set the schedule, selecting **Any server** in the **Where agent runs** box.
6. Click **OK**.
7. Close the Agent Properties dialog and the agent, and then click **Enable** to enable the agent.

5 Configuring selective archiving

- Overview, page 55
- Configuring mining rules, page 56
- Scheduling the mining job, page 69
- Editing a rule or schedule, page 71
- Enabling the mining agents, page 71
- Enabling the preprocessing agent, page 72
- HP EAs–D Users database, page 73
- Scheduling and enabling the Profile Agent, page 73
- Viewing Mail Detail records, page 74
- Enabling other HP EAs-D Users agents, page 75
- Running the mining job, page 77

Overview

Selective archiving, also known as email mining, archives messages from Domino mail servers to the IAP. It can be used on both mail databases and journals. The system is first queried to determine if the email in a mailbox or journal is already archived. If the email is not already archived, it is archived. A tombstone, a link to the original email that is stored in the IAP system, can be created in the mail file.

To configure and enable selective archiving:

1. Create a mining profile, which contains the mining rules.

   See "Configuring mining rules" on page 56.
2. Schedule the mining job.

   See "Scheduling the mining job" on page 69.
3. Schedule and enable the Archive and Tombstone agents.

   See "Enabling the mining agents" on page 71.
4. Schedule and enable the Encapsulate agent.

   See "Enabling the preprocessing agent" on page 72.
5. Schedule and enable the Profile Agent.

   See "Scheduling and enabling the Profile Agent" on page 73.
6. Run the mining job.

   See "Running the mining job" on page 77.

NOTE:

The maximum supported size for messages to be archived is 100 MB. This includes any attachments to the message.

Configuring mining rules

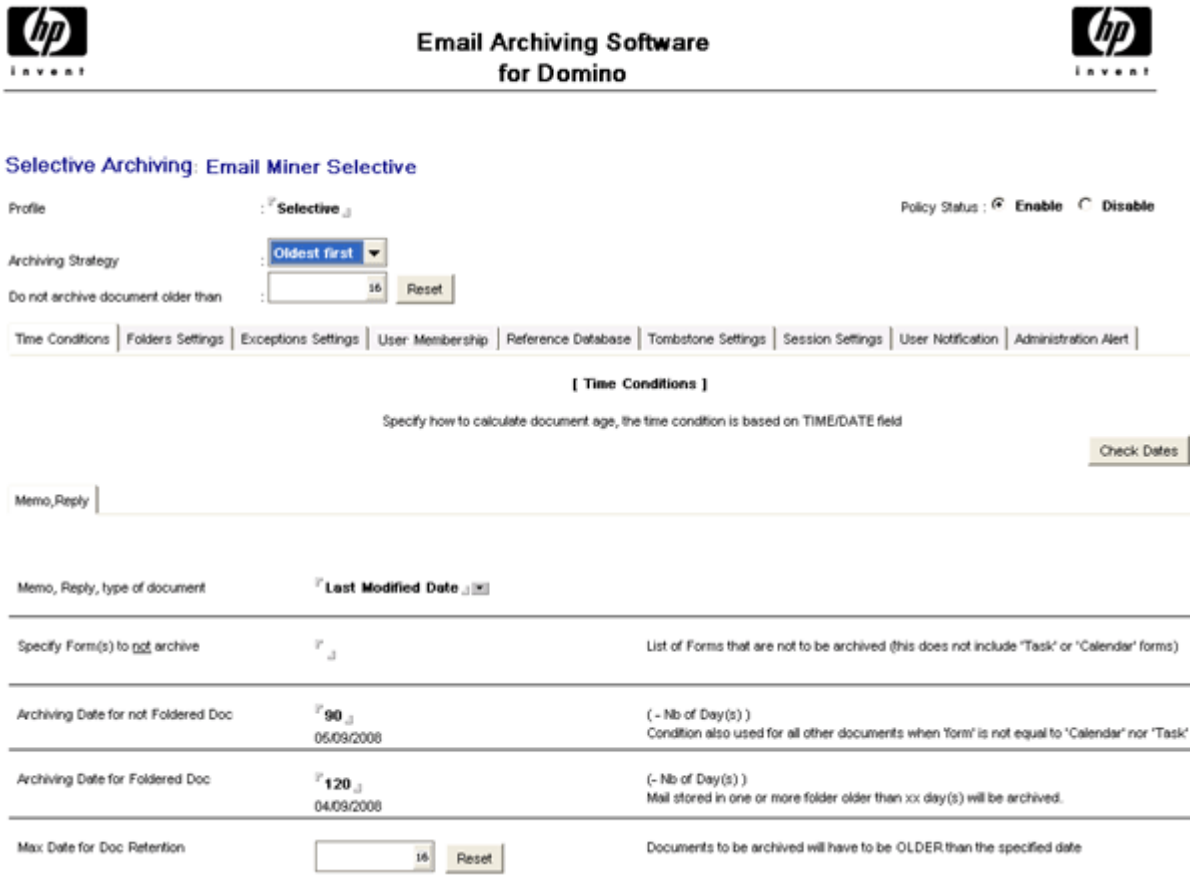
A mining rule must be configured in order to selectively archive messages in mail files or journals.

To configure the mining rule:

1. Double-click the **HP EAs-D API** database file.
2. In the HP EAs-D API main view, double-click one of the default rules under Mining Rules:
   - Use **Email Miner Selective** for archiving mail databases of current employees.
   - Use **Email Miner Journaling** for archiving messages in journals.
   - Use **Email Miner Bulk** for archiving older mail databases.

   If you need to create a new mining rule, select **Create** > **Archiving** > **3. Mining Rule**.

   The mining rules document appears.



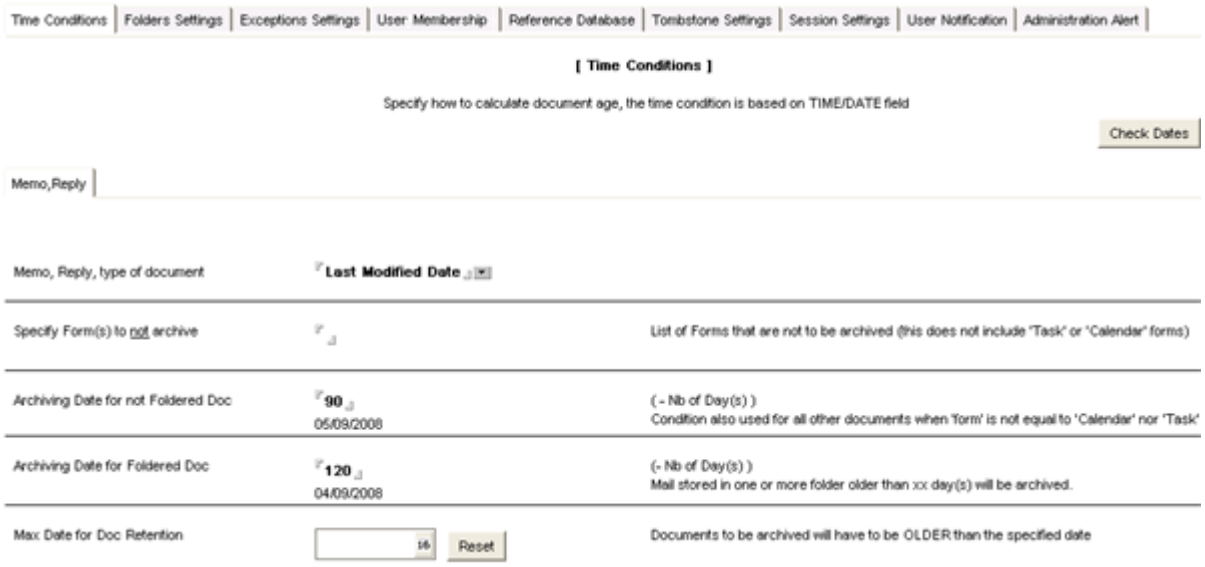
3. Complete the following fields at the top of the document:

Field	Description
Policy Status	Select **Enable** when you are ready to activate the rule and begin archiving.
Profile	The name of the rules profile. For example, Selective or Journaling.
Archiving Strategy	Select **Oldest first** or **Biggest first** from the drop-down menu.
Do not archive document older than	Enter a date by clicking the calendar icon. This date works with the date entered in the Time Conditions tab to establish a date range for archiving. For example, the value in this field could be 7 years, and the value in the Time Conditions tab could be one year. Messages that are between 1–7 years old would be archived.

4. Continue to configure the mining rule settings.
   - "Time Conditions tab" on page 58
   - "Folders Settings tab" on page 59
   - "Exceptions Settings" on page 60
   - "User Membership tab" on page 62
   - "Reference Database tab" on page 64
   - "Tombstone Settings tab" on page 65
   - "Session Settings tab" on page 67
   - "User Notification tab" on page 68
   - "Administration Alert tab" on page 68
5. When the profile is complete, click **Save**.

Time Conditions tab

Time Conditions establishes the age of email to be archived. To configure Time Conditions, complete the Memo, Reply settings using the instructions in the table below.

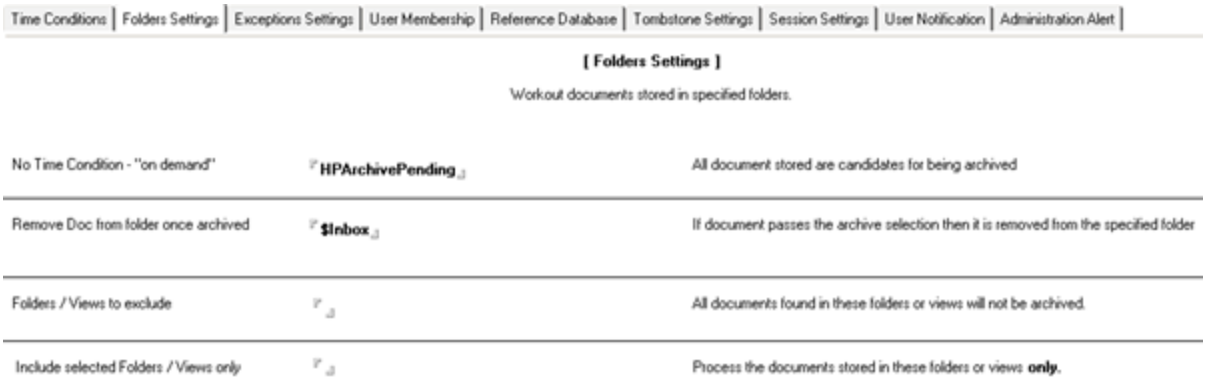


Field	Description
Memo, Reply type of document	Click the arrow and select the way to define an email's date: Creation Date, Last Modified Date, or Posted Date.
Specify Form(s) to not archive	List any forms your organization uses that should not be archived. Form names can be separated by commas, semicolons, or newlines.
Archiving Date for not Foldered Doc *	Email that is not stored in folders must be older than the number of days specified. Enter the number of days, and then click **Check Dates** to view the corresponding calendar date.
Archiving Date for Foldered Doc *	Email that is stored in folders must be older than the number of days specified. Enter the number of days, and then click **Check Dates** to view the corresponding calendar date.
Max Date for Doc Retention *	Click the calendar icon and select a maximum date for email retention. To be archived, all email must be older than the specified date. **Note**: If you selected archive dates for Foldered Docs and non Foldered Docs, leave this field blank.
Comments	Enter any comments about the configuration.

* This date works with the date entered at the top of the mining rules document to establish a date range for archiving. For example, the value in this field could be one year, and the value in the top of the document could be 7 years. Messages that are between 1–7 years old would be archived.

Folders Settings tab

These settings define specific archiving treatment for user folders.

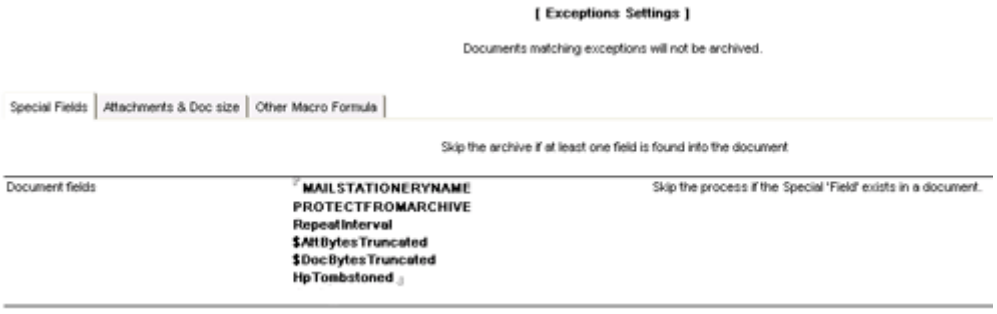


Field	Description
No Time Condition — "on demand"	When you list a folder in this field, all messages stored in the folder are archived no matter what value is set in the Time Conditions tab. (The upper limit set at the top of the mining rules document still applies.) The folder can include nested folders. You can list more than one folder. Folder names can be separated by commas, semicolons, or newlines. **Note**: HPArchivePending is simply an example and can be removed from this field.
Remove Doc from folder once archived	When you list a folder in this field, messages are removed from the specified folder after they are successfully archived. The folder can include nested folders. In addition, you can list more than one folder. Folder names can be separated by commas, semicolons, or newlines. HPArchivePending is simply an example and can be removed from this field. **Tip**: For mailbox management, you could list the $Inbox folder.
Folders/Views to exclude	Enter any views or folders containing messages that should not be archived. $Drafts is automatically excluded during selective archiving. Names can be separated by commas, semicolons, or newlines. The folders listed can include nested folders.
Include selected Folders/Views only	Use this field to list specific folders or views to be mined. Only the messages that are contained in these folders or views are archived. If you complete this field, do not complete the Folders/Views to exclude field. Names can be separated by commas, semicolons, or newlines. The folders listed can include nested folders.
Comments	Enter any comments about the configuration.

Exceptions Settings

Use the Exceptions Settings to define exceptions to the overall mining rules, or to limit the amount of archive traffic per session.

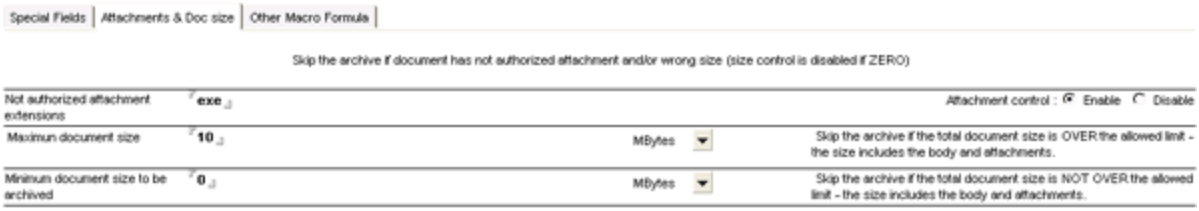
Special Fields



Field	Description
Document fields	If one of the fields listed is found in a message, the message is not archived. A default list of special fields is shown. Delete those that do not apply. Do **not** delete the **HPTombstoned** field. You can add other fields. Field names can be separated by commas, semicolons, or newlines. **Note**: Invitations, calendar notices and other non-Memo, Reply messages are automatically excluded during selective archiving. (However, these messages are always journaled.)
Comments	Enter any comments about the configuration.

Attachments & Doc size tab

To complete the Attachments & Doc size settings, use the instructions in this table.



Field	Description
Attachment control	Click **Enable** to enable these settings.
Not authorized attachment extensions	To exclude documents with certain types of extensions, list the extensions. You can prevent the system from mining attachments containing calendar-related notices by entering **.ics**. Extensions can be separated by commas, semicolons, or newlines.
Maximum document size	If documents over a certain size should not be archived, enter the cutoff size. Enter **0** if there are no restrictions. The size includes both the body of the message and any attachments. **Important**: The maximum supported size for messages to be archived is 100 MB. This includes any attachments to the message.
Minimum document size to be archived	If documents below a certain size should not be archived, enter the size. Enter **0** if there are no restrictions.
Comments	Enter any comments about the configuration.

Other Macro Formula tab

You can implement other exception criteria using macros written in the Notes formula language.

Most valid formulas that return True/False values can be used. However, avoid the following formulas so that mining performance is not impacted:

- @Abstract, or @DbLookup, @For, @While and related functions
- Overly complex formulas

Enable or disable these settings by clicking **Enable** or **Disable**.

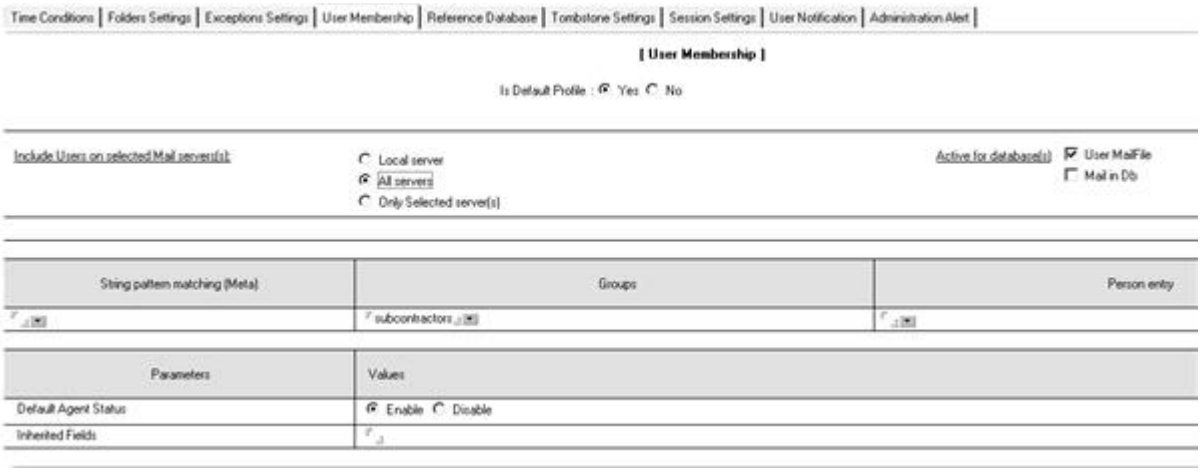
Field	Description
Filter rules to be evaluated	Enter any additional formulas defining documents that should not be archived. If the formula returns True, the document is not archived. You can test the formula by clicking **Check Syntax**.
Comments	Enter any comments about the configuration.

User Membership tab

Complete this tab to associate users with the mining rule. Users can be added from standard Domino Directory mail databases and mail-in databases.

When users are added in this tab and the Profile Agent is run, a Mail Detail record is created for each user in the HP EAs-D Users database (`hp_rissuser.nsf`) and the user is associated with the mining rule.

For more information, see "Scheduling and enabling the Profile Agent" on page 73 and "Viewing Mail Detail records" on page 74.



Field	Description
Is Default Profile	Click **Yes** if you want to make the mining rule the default rule that is associated with users in the domain. **Note**: One mining rule must be designated as the default.
Include Users on selected Mail server(s)	Select the mail servers to be mined with the rule. **Note**: For local mining, select **Local server**. For remote mining, select either **All servers** or **Only selected servers**. • **Local server** • **All servers** (all mail servers in the domain) When the Profile Agent runs, it adds any users who match the value set in the Membership Conditions field, regardless of the user's home (mail) server. • **Only selected servers** The Profile Agent adds a user to the mining rule when the user matches the value set in Membership Conditions and the user's home (mail) server is listed in this field. Click the arrow and add the relevant servers from the list that is displayed. **Note**: Use this setting to filter the mining rule to a specific server or set of servers.
Active for databases	Select **User MailFile** and/or **Mail in Db**. Users can be selected from standard Domino mailboxes (User MailFile) and Mail-in databases (Mail in Db).

Field	Description
Membership conditions	Define the user mailboxes or journals to be mined with this rule. Select any or all of the following: • **String pattern matching (Meta)**: Use a wildcard to define members of an organization or organizational unit. For information on the syntax to use, see "Defining wildcard patterns" on page 63. • **Groups**: A group within the organization. **Important!** EAs does not support group types that are set to Access Control List. • **Person entry**: Individual mailboxes.
Default Agent Status	Click **Enable** to enable the Profile Agent for the specified users. (The Profile Agent itself is enabled in a separate process. See "Scheduling and enabling the Profile Agent" on page 73.)
Inherited Fields	EAs Mail Detail records contain several values from Domino Person or Mail-In documents, which allow users to be synchronized with the Domino Directory. (See "Viewing Mail Detail records" on page 74. If you want the Mail Detail records to inherit other, specific fields from users' Person documents or Mail-In database documents, enter them here. Field names can be separated by commas, semicolons, or new lines.
Comment	Enter any comments about the document.

Defining wildcard patterns

Wildcards can be used to define users who are associated with a mining or journaling rule.

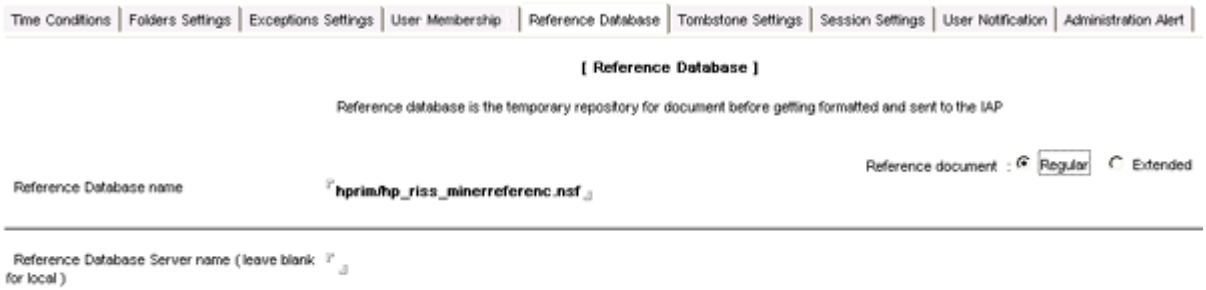
EAs Domino supports a subset of standard regular expression syntax, modified for compatibility with the wildcard conventions used in Lotus Notes and Domino administration.

You can use wildcards to define members of an organization in two ways:

- */org unit/organization
- */organization

Reference Database tab

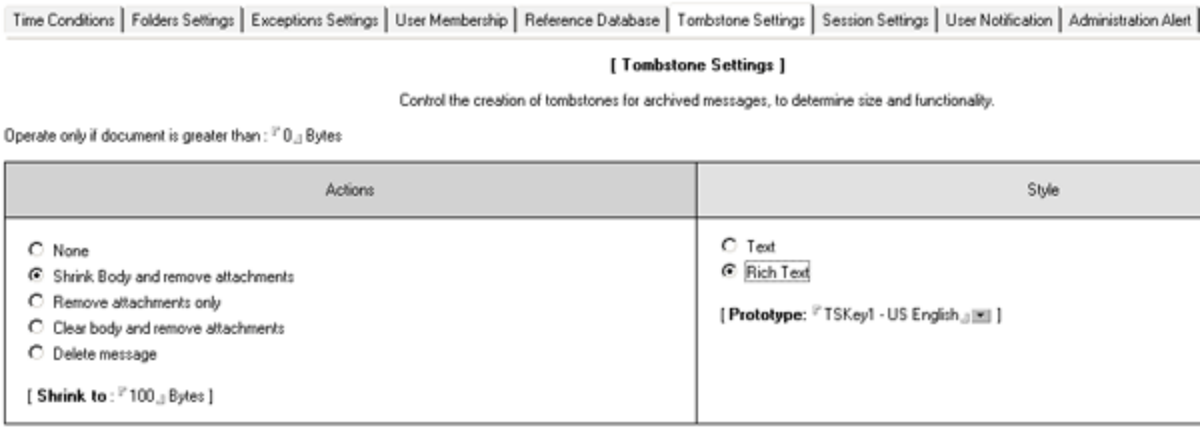
The reference database is a temporary repository that contains pointers to messages in mail boxes while the messages are being processed and sent to the IAP. Use this tab to enter the name and location of the reference database.



Field	Description
Reference document	Select **Regular** unless HP support asks you to select Extended for troubleshooting purposes. An Extended reference document appends the following fields to a message: • HP_SessionInfo: Identifies which server remotely mined the message. Adds values for the session server name, API database Replica ID, and mining document UNID. • HP_ReferenceInfo: Identifies which reference database contains the pointer to the message. Adds values for the reference server name, reference database Replica ID, and Reference document UNID. These fields are especially helpful in troubleshooting a remote mining configuration when you suspect two servers are trying to mine the same database. Only one server should ever mine a given database.
Reference Database name	Enter `hprim/hp_riss_minerreferenc.nsf` unless: • The mining rule is being used for journaling. Change the path and name to `hprim/hp_riss_journalreferenc.nsf`. • The mining rule is being used for bulk upload. Change the path and name to `hprim/hp_riss_blkupdreferenc.nsf` • Another reference database has been created. Change the path and name to `hprim/hp_<anotherdb>_referenc.nsf`.
Reference Database Server name (leave blank for local)	Enter the server name if the reference database is not on the local server.
Comments	Enter any comments about the reference database.

Tombstone Settings tab

Use this tab to specify the action the Tombstone agent takes when a mail file is mined. There are several actions available: the full message can be retained in the mail file, the message can be deleted from the mail file, or the message can be replaced with a link, or tombstone, to the archived message on the IAP.



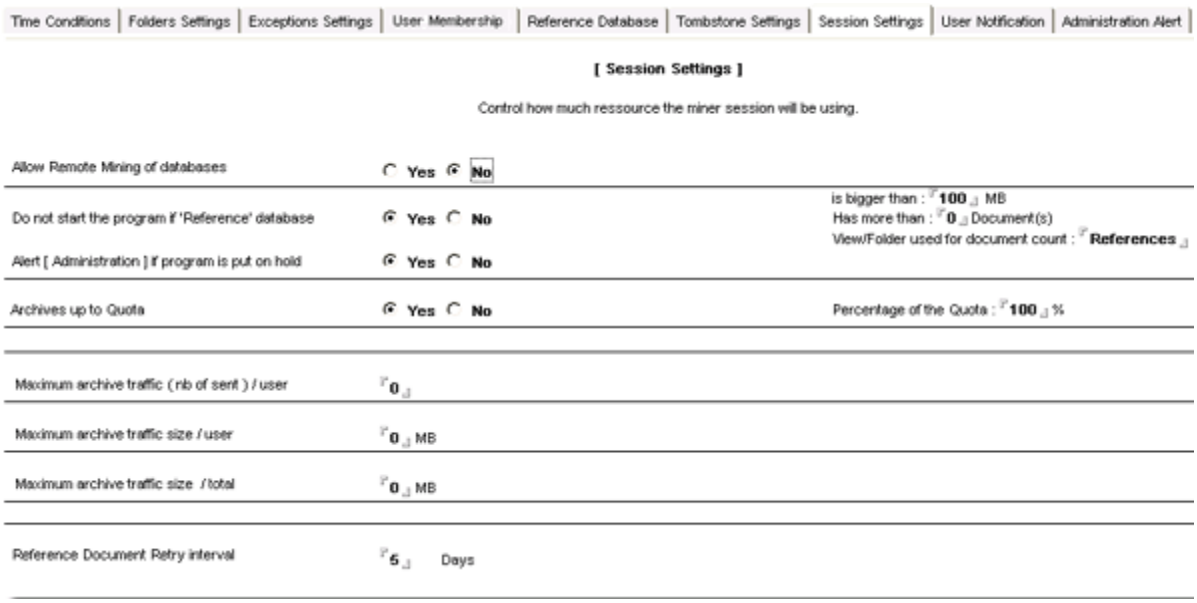
Field	Description
Operate only if document is greater than x Bytes	If the action specified in the **Actions** area should occur only when messages and their attachments exceed a certain size, enter the size in bytes. If the action should always occur, leave the default of 0.

Actions	Select the action to occur in the mail file when messages are mined:
	• Tombstoning actions:
	  • **Shrink Body and remove attachments**: All attachments are removed from the message and the body of the message is trimmed to approximately the length specified in the Shrink to field.
	  If you select this action, enter the trimmed length in bytes in the **Shrink to** field.
	  • **Remove attachments only**: Message attachments are removed, but the message body is left intact.
	  • **Clear body and remove attachments**: Both the body and attachments are removed from the message.
	• Non-tombstoning actions:
	  • **None**: The full message is retained in the mail file and the message is not tombstoned.
	  • **Delete message**: The message is removed from the mail file. Messages are deleted automatically when journals are mined, even if this option is not selected.

Style	If you selected one of the tombstoning actions, a tombstone replaces the message. Use the Style field to format the tombstone. • **Text**: Select this option if users access tombstoned messages only in Lotus Notes. When this setting is chosen, a field to customize the standard tombstone message is displayed. Change the content if you do not want to use the default, "This message has been archived." If the Notes plug-in is installed on client computers, users only see this message if they are offline or the IAP is down. Otherwise, a copy of an archived message appears automatically when the message is opened in the Notes client. (For more information about the plug-in, see "Using the Windows Notes Client Plug-In" on page 120.) When Text is selected, a tombstoned message can be as small as 800 bytes. • **Rich Text**: Select this option if users access archived messages with DWA, or with DWA and Lotus Notes. A Tombstone Prototype document must be configured before choosing this setting. The content that is created in the prototype replaces or appends the message body, depending on the tombstone action that is specified. The **Prototype** value is the key of the Tombstone Prototype document to be used. See "Configuring the Tombstone Prototype document" on page 51. When Rich Text is selected, each tombstoned message is a minimum of 2–3 KB. • If the Notes plug-in is installed on client computers, Lotus Notes users only see "this message has been archived" if they are offline or the IAP is down. Otherwise, a copy of an archived message appears automatically when the message is opened in Notes. • Users opening a tombstoned message in DWA click a link to retrieve the full message from the IAP. The message opens in a separate window or tab.

Session Settings tab

Session settings control the impact of mining sessions on server resources.



Field	Description
Allow Remote Mining of databases	Click **No** to archive only databases on the local mail server. Click **Yes** if you are archiving databases located on remote mail servers.
Do not start the program if 'Reference' database	When you enable this option, mining does not start if the reference database: • Is bigger than n MB, or • Has more than n messages. Click **Yes** if you want to enable the option, and then enter a value for one or both of the parameters. Leave the view set to **References**.
Alert Administration if program is put on hold	This setting appears when you enable the **Do not start...** option above. Click **Yes** to have an alert sent to the administrator with this information. If you select Yes, complete the fields in the Administration Alert tab. See "Administration Alert tab" on page 68.
Archives up to Quota	If you have set a quota for user mailbox size, mailboxes can be mined so their size falls below a percentage of the quota. If you select **Yes** for this setting, complete the **Percentage of the Quota** field. EAs detects when the quota percentage, or threshold, is exceeded and archives messages until the mailbox size falls below the threshold. The archiving strategy for the rule determines which messages are archived first.

Set the maximum size of archive traffic per session in the three traffic size fields. You can set values for any or all of the fields. If there are no size restrictions for a field, enter **0**.	
Maximum archive traffic size [nb of sent] /user	To set a value using the number of messages per user, enter the number of messages.
Maximum archive traffic size/user	To set a value using mailbox size, enter the user mailbox size in MB.
Maximum archive traffic size/total	To set a global value, enter a maximum size in MB for archive traffic per session.
Reference Document Retry interval	Message pointers in the reference databases and/or linked documents in the preprocessing databases are temporary and are always re-created if they are lost, for example after a server crash. Use this field to set the time until the pointers are re-created. The default is 3 days. Note that a new pointer is created even if one already exists. The duplicates are removed by the Tombstone agent. **Note**: Until references are processed, the corresponding messages remain on the mail server.

User Notification tab

Use this tab to compose a memo that is sent to the users' mailboxes. This message provides feedback about the archive process, for example "Messages have been archived." The message body is appended by the number and total size of messages archived in the user's mail file.

Enable or disable user notification by clicking **Enable** or **Disable**.

Field	Description
Subject	Enter a subject for the notification.
Message body	Enter the notification message.
Comments	Enter any comments about the notification.

Administration Alert tab

Administration email alerts are sent when:

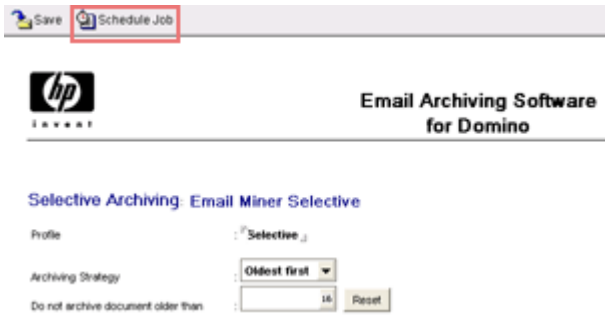
- A reference database cannot be found or opened.
- The mining process cannot start because the reference database is too large. This alert works with the options in session settings. See "Session Settings tab" on page 67.

Field	Description
From	Enter a value, such as the name of the mining rule.
SendTo	Click the arrow and select a name or names from the address book. (Usually this alert is sent to the administrator.) Delete the default entry for the field.
Subject	Enter a subject for the alert. For example, Miner Did Not Start.
Comments	Enter any comments about the alert.

Scheduling the mining job

After configuring the mining rule, schedule the mining job.

1. In the EAs-D API main view, open the rule for editing by double-clicking inside the rule document.
2. Click **Schedule Job** in the upper left corner of the mining rules document created for the profile.

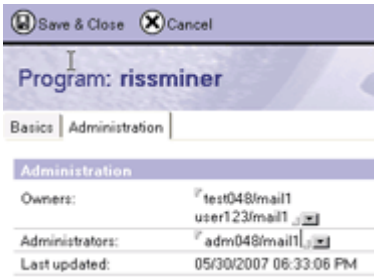


The rissminer program document appears.

3. Complete the fields in the **Basics** tab.

Field	Description
Basics	
Program name	Leave the default value: **rissminer**
Command line	Leave the default value. Note that the -k command line switch and the name of the mining rule is picked up in the command.
Server to run on	The default is the current mail server. If you need to change the server, click the arrow and select another server. This is the only field in the Basics column that you should edit.
Comments	Leave the default value.
Schedule	
Enabled/disabled	Click the arrow and select **Enabled** to enable the program document.
Run at times	Enter a time period to run the program. The time period and repeat interval depend on the type of archive job you are running. • For selective archiving, you might want to run the program once a day, with the time set to a specific hour. When you use a specific hour, the repeat interval must be set to 0. • For journaling, run the program throughout the day. Enter a time period of 12:00 AM–11:59 PM, with a brief repeat interval (not less than 10 minutes).
Repeat interval	Enter the time between mining sessions, in minutes. You will need to experiment to see how long the mining process takes. The time depends on the number of mailboxes, the size of the messages, and the speed of the server. The repeat interval should never be less than 10 minutes. If you entered a specific hour in the Run at times field, set this field to **0**.
Days of week	Click the arrow and select the check box in front of each day the job runs. For journaling, be sure to select each day of the week. Click **OK** when you are finished.

4. (Optional) Click the **Administration** tab and complete the settings.



Field	Description
Owners	Click the arrow and select any additional owners of the mining task.
Administrators	Click the arrow and select any additional administrators of the mining task.
Last updated	Do not edit — information only.

5. Click **Save & Close** to save the program document.
6. Click **Save** to save the mining rule.

A rissminer program document must be created in the Domino Directory of each mail server on which the mining rule is enabled.

1. In the Domino Administrator client, click the **Configuration** tab.
2. Expand **Server** and select **All Server Documents**.
3. Select the server, and then select **Create** > **Server** > **Program**.
4. Complete the program document fields according to steps 2–4 above.

Editing a rule or schedule

To make changes to the mining rules:

1. Open the EAs-D API main view.
2. Double-click inside the mining rule document to open the rule.
3. Double-click inside the relevant field and make the change.
4. Save the revised rule.
5. If you are making changes to the schedule, open the program document from the Configuration tab and make the schedule changes.

Enabling the mining agents

The Archive and Tombstone agents are located in the EAs-D reference databases, and process the messages that have been mined. These agents must be scheduled and enabled in each reference database that is used.

1. In the Designer client, open the reference database:
   a. Click **Open an Existing Database**.
   b. Select the server on which the EAs Domino databases are installed.
   c. Browse to the `hprim` folder, and then scroll down to the relevant reference database:
      - Selective archiving: HP EAs-D Reference (mnr) (`hp_riss_minerreferenc.nsf`)
      - Journaling: HP EAs-D Reference (jrl) (`hp_riss_journalreferenc.nsf`)
      - Bulk upload: HP EAs-D Reference (blk) (`hp_riss_blkupdreferenc.nsf`)
   d. Click **Open**.
2. In the Design pane, select **Shared Code** > **Agents** in the reference database.

   The Archive and Tombstone agents appear.
3. Double-click **Archive**, and then click **OK** to bypass the warning.

   The Properties for Agent dialog box appears.
4. Make sure the Trigger is set to **On schedule** and the Target is set to **All new & modified documents**.

5. Set the schedule:
   a. Click the arrow in the box next to the Schedule button to select a parameter.

      For journaling, the schedule should be set to more than once a day.
   b. Click the **Schedule** button and set the run time.

      The schedule should be set in conjunction with the schedule in the rissminer program document.

      For journaling, the agents should run frequently, all day. The times should be at least 20 minutes apart.
   c. Ensure that the server name appears in the **Where agent runs** box.
   d. Click **OK**.
6. After the changes have been made, close the Properties dialog box. Save and close the agent by pressing the **Esc** key, then clicking **Yes** when prompted to save your changes.
7. Click **Enable**.
8. Repeat this process for the Tombstone agent.
9. To enable the agents on another server, repeat steps 1–8.

   The agents must be scheduled on each server used for archiving.

Enabling the preprocessing agent

The Encapsulate agent processes several types of messages including calendar notices, tasks, and signed and encrypted messages, so they can be archived in a format that preserves all message data intact. This agent must be scheduled and enabled in each preprocessing database that is used for archiving.

See "Preprocessing messages" on page 35 for information on the preprocessing databases.

1. In the Designer client, open the preprocessing database:
   a. Click **Open an Existing Database**.
   b. Select the server on which the EAs Domino databases are installed.
   c. Browse to the `hprim` folder, and then scroll down to the relevant database:
      - Selective archiving: HP EAs-D PreProcess (miner) (`hp_preproc_miner.nsf`)
      - Journaling: HP EAs-D PreProcess (jrnl) (`hp_preproc_journal.nsf`)
      - Bulk upload: HP EAs-D PreProcess (bulk) (`hp_preproc_blk.nsf`)
   d. Click **Open**.
2. In the Design pane, select **Shared Code** > **Agents** in the database.

   The Encapsulate agent appears.
3. Select the agent and double-click to open it. Click **OK** if a warning message appears.

   The Properties for Agent dialog box appears.
4. Make sure the Trigger is set to **On schedule** and the Target is set to **All documents in database**.

5. Set the schedule:
   a. Click the arrow in the box next to the Schedule button to select a parameter.

      For journaling, the schedule should be set to more than once a day.
   b. Click **Schedule** and set the run time to meet your requirements.

      For journaling, the agent should run frequently, all day. The times should be at least 20 minutes apart.
   c. Ensure that the correct server appears in the Where agent runs box.
   d. Click **OK**.
6. Close the Agent Properties dialog box and the agent, and then click **Enable**.
7. To enable the agent on another server, repeat steps 1–6.

   Preprocessing databases are not replicated, so the agent must be scheduled and enabled on each server used for archiving.

HP EAs-D Users database

The HP EAs-D Users database (`hp_rissuser.nsf`) contains the records of users whose mail files are being mined. Users are added to the database when they are associated with a mining rule and the Profile Agent in the database is run.

When the Profile Agent in the EAs-D User database is run, it creates or updates the user records, known as Mail Detail records, and synchronizes the information in the records with the users' Person documents. See "Scheduling and enabling the Profile Agent" on page 73 and "Viewing Mail Detail records" on page 74.

Scheduling and enabling the Profile Agent

The Profile Agent creates Mail Detail records when users are added to a mining rule. It synchronizes values in the Mail Detail records with values in the corresponding Person documents.

To configure the Profile Agent in the Designer client:

1. Open the HP EAs-D Users database in the `hprim` folder on any mail server with a copy of the database.
2. In the Design pane, select **Shared Code** > **Agents** in the database.
3. Double-click **profileAgent**. Click **OK** to bypass the warning.

   The properties dialog box appears.
4. On the Basics tab, make sure the Trigger is set to **On schedule** and the Target is set to **All documents in database**.
5. Set the schedule:
   a. Click the arrow in the box next to the Schedule button to select a parameter.
   b. Click **Schedule** and set the run time.
   c. In the **Where agent runs** box, select **Any server**.
   d. Click **OK**.
6. Close the Agent Properties dialog and the agent, and then click **Enable** to enable the agent.

NOTE:

After the EAs software is configured, you can force the agent to populate the EAs-D Users database by opening the server console and entering:

```
tel amgr run "hprim\hp_rissuser.nsf" 'profileAgent'
```

If Domino 7.0.3 is installed on the server, do not run the agent manually. See "JVM panic gc0 error" on page 130.

Viewing Mail Detail records

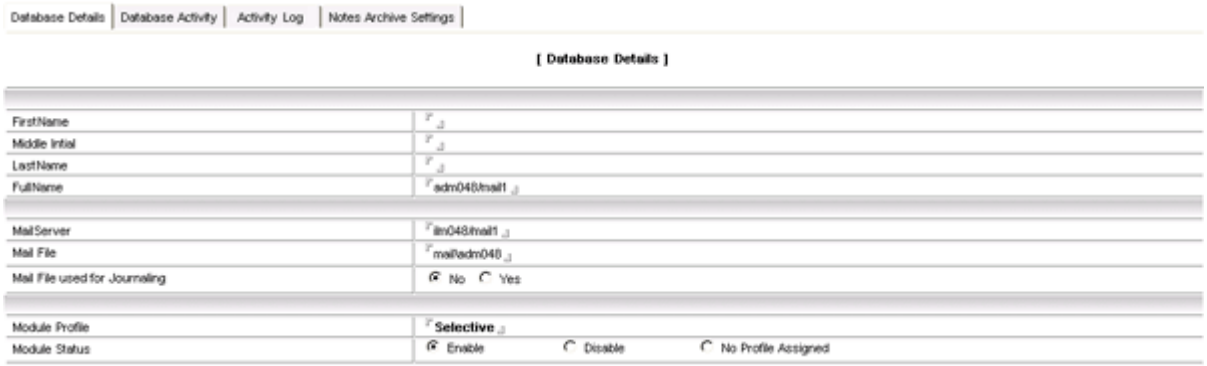
Mail Detail records import values from several fields in the Domino Person or Mail-In documents, so that user mail files and Journal mail-in databases can be associated with one or more mining rules.

During synchronization, the Profile Agent updates the Mail Detail records with any changes from the Domino Person or Mail-In documents. It also refreshes the last synchronization date and other information such as the size of the user's mail database.

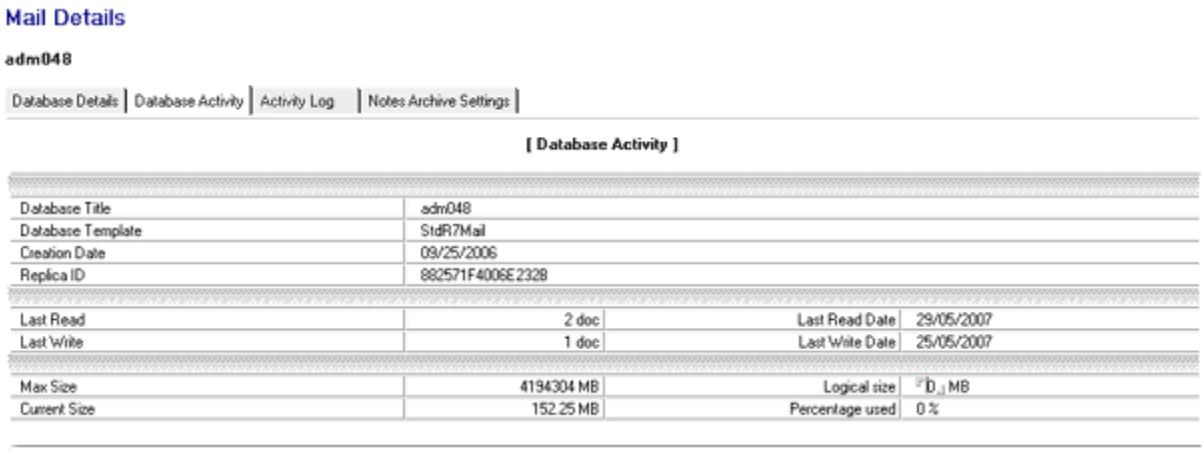
- The **Database Details** tab records the user's name, the mail database name, the mail server where the database resides, and the mining rules that the user or mail-in database is associated with.

NOTE:

When a Mail Detail record is created, the Module Profile field contains the name(s) of one or more mining rules that the user is associated with. If a rule's User Membership configuration is changed, and the user or mail-in database is no longer associated with the rule, the Module Status field is changed to No Profile Assigned.



- The **Database Activity** tab shows the title of the user mailbox, the mail template it is based on, the date the user database was created, the database replica ID, the last date the Mail Detail record was synchronized with the Person or Mail-In document, the maximum size set for the database, and its current size.



- The **Activity Log** provides a brief summary of the archiving activity in the user database, showing the date and time of archiving, the number of messages archived, and their total size.
- The **Notes Archive Settings** tab shows any native Notes archive databases that have been sent to the IAP. Information includes the name of the archive file, the server it resides on, the mail template it is based on, the date the file was created, and the current size of the file in MB.

Enabling other HP EAs-D Users agents

In addition to enabling the Profile Agent, schedule and enable the agents listed below. You can also change some field values for these agents.

Statistics User Activity Alert agent

If a user's mail file has not been mined for more than a certain number of days, the user's Mail Detail record is flagged to appear in the Mail File\By User Activity – Alert view.

Editing agent values

By default, the mail file is flagged after 15 days. You can change the number of days by following these steps:

1. In the Administrator client, open the HP EAs-D API database.
2. Click **User Configuration** in the left menu of the EAs-D API main view.
3. Click **Global Settings** in the left menu of the User Configuration view.
4. In the Agent\Parameters view, double-click the **Statistics User Activity Alert** entry.

   The Agent's Parameters document appears.
5. In **Argt1: How many days > "inactive" mailfile**, double-click the **Value** field and change the number of days.

   The user's Mail Details record will be flagged if the mail file has not been mined for this number of days.

   Do not change the value in Argt2.
6. Select **File** > **Save**, and then close the document.

Scheduling the agent

To schedule and enable the agent using the Designer client:

1. Open the HP EAs-D Users database in the `hprim` folder on any server with a copy of the database.
2. In the Design pane, select **Shared Code** > **Agents**.
3. Double-click **Stats\User Activity Alert – Agent**, and then click **OK** to bypass the warning.

   The Properties for Agent dialog box appears.
4. Make sure the Trigger is set to **On schedule** and the Target is set to **All documents in database**.
5. Set the schedule, selecting **Any server** in the **Where agent runs** box.
6. Click **OK**.
7. Close the Agent Properties dialog and the agent, and then click **Enable** to enable the agent.

Purge Not Synchronized person document agent

This agent removes the Mail Detail records of users whose Person documents have been removed from the Domino Directory.

By default, Mail Details records are kept for 20 days after the last synchronization with the Domino Directory. You can change the number of days by following these steps:

1. In the Administrator client, open the HP EAs-D API database.
2. Click **User Configuration** in the left menu of the EAs-D API main view.
3. Click **Global Settings** in the left menu of the User Configuration view.
4. In the Agent\Parameters view, double-click the **Purge Not Synchronized 'person' document** entry.

   The Agent's Parameters document appears.
5. In **Argt1: How many days to be kept** double-click the **Value** field and change the number of days.

   The user's Mail Details record is deleted if the mail file is not synchronized for this number of days.
6. Select **File** > **Save**, and then close the document.
7. Schedule and enable the agent.

   Follow the procedure in "Statistics User Activity Alert agent" on page 75.

Purge Selective Archive Log agent

EAs selective archiving saves an activity log in each user's Mail Detail record. The maximum amount of text that can be stored in the log is set in the Purge Selective Archive Log agent. The default value is 20 lines of text.

You can edit this value downward, but it should **not** be increased. An error occurs when Lotus Notes records store more than 64 KB of text, and the following message is displayed:

```
Notes error:  Field is too large or View's column selection formulas are
too large.
```

The agent must also be scheduled and enabled to avoid the Notes error condition.

If you want to decrease the amount of text stored in the activity log, follow these steps:

1. Click **User Configuration** in the left menu of the EAs-D API main view.
2. Click **Global Settings** in the left menu of the User Configuration view.
3. In the Agent\Parameters view, double-click the **Purge Stats Selective Archive Log** entry.

   The Agent's Parameters document appears.

4. In **Argt1: Number of lines max**, edit the **Value** field to reduce the number of lines.

   Legal values are 0–20. If the value is set to 0, the agent purges all log entries when it is run.
5. Select **File** > **Save** from the top menu, and then close the document.
6. Schedule and enable the agent.

   Follow the procedure in "Statistics User Activity Alert agent" on page 75.

Running the mining job

The mining job runs automatically after:

- Creating the mining rule
- Scheduling the job in the rissminer program document
- Scheduling and enabling the preprocessing and mining agents
- Scheduling and enabling the Profile Agent

You can force the mining program and agents to run immediately by entering the commands below in the server console.

NOTE:

Do not run Profile Agent, the Archive agent, or the Tombstone agent manually if Domino 7.0.3 is installed on the server. See "JVM panic gc0 error" on page 130 for more information.

- `load rissminer –k<profile>`
  where <profile> is the name of the mining rule. This runs the mining program.
- `tel amgr run "hprim\hp_preproc_miner.nsf" 'encapsulate'`
  This runs the Encapsulate agent in the preprocessing database. The filename should be changed to reflect the preprocessing database that is used.
- `tel amgr run "hprim\hp_riss_minerreferenc.nsf" 'archive'`
  This runs the Archive agent. The filename should be changed to reflect the reference database that is used.
- `tel amgr run "hprim\hp_riss_minerreferenc.nsf" 'tombstone'`
  This runs the Tombstone agent. The filename should be changed to reflect the reference database that is used.

The syntax for the commands must be exactly as shown, with double quotes around the database name, and single quotes around the agent name.

IMPORTANT:

Do not shut down a Domino server while the rissminer process is running. Check the list of running processes on the server and kill the rissminer process before issuing the quit command to Domino.

If the server is stopped while the rissminer process is running, or if the server crashes, a rissminer `<mining_rule_name_date_time_stamp>.lock` file is left behind. When the server is restarted, the presence of this lock file causes rissminer to shut down immediately. You can create a task to automatically delete the lock file when the server is restarted. See "Mining program shuts down" on page 129.

6 Configuring compliance (journal) archiving

- Overview, page 79
- Journaling recommendations, page 80
- The journaling process, page 82
- Creating HP EAs Domino journaling rules, page 85
- Mail.box issue, page 89

Overview

HP EAs Domino can archive journaled messages using one of two methods:

- Advanced Filtering, also known as EAs Domino journaling
- Domino native journaling

For both methods, message copies are captured and put in a mail-in journal database that is mined by the rissminer program. Pointers to the messages are placed in the HP EAs-D Journal Reference database (`hp_riss_journalreferenc.nsf`) and acted on by agents in the journal reference database and the journal preprocessing database, HP EAs-D PreProcess.

The mail-in database can be mined remotely by an HP gateway server or journal server, or can be mined locally when it is on the same mail server as the EAs Domino databases.

NOTE:

The maximum supported size for messages to be archived is 100 MB. This includes any attachments to the message.

Encrypted messages

Any mail-in database document that is used for journaling must not specify the encryption option. This is necessary to prevent standard journaled messages from being encrypted when they are sent to the IAP. It also prevents an extra layer of encryption from being added to previously-encrypted messages. Encrypted messages cannot be indexed by the IAP.

Calendar notices

Notes calendar notices and other non-Memo, Reply messages that are journaled are automatically encapsulated before they are archived. See "Preprocessing messages" on page 35.

Encapsulated messages can be exported from the IAP to a Notes database, where they can be opened like any other message. See "Using Export Search" on page 107.

NOTE:

Notes calendar notices are converted to iCal format (.ics) before they are archived.

Mail-To-Me messages

If you use Domino native journaling, HP EAs-D Tools must be configured and the cleanup agent enabled.

Domino native journaling cannot filter out messages that users send to themselves from the IAP Web Interface. Since these messages are already archived, the mining agents skip them and leave them in the journal. EAs-D Tools provides an automated process for removing Mail-to-Me messages from the journal mail-in database.

HP EAs-D Tools and the mail-in database must be on the same server. For the steps to create and configure EAs-D Tools, see "Configuring the HP EAs–D Tools database" on page 141.

NOTE:

If you use EAs Domino journaling, Mail-To-Me messages are handled in the journaling rules content exceptions. See "Creating HP EAs Domino journaling rules" on page 85.

Journaling recommendations

Advanced Filtering (HP EAs Domino journaling)

- Use HP EAs-D Mail Journal (`hprim/hp_riss_journal.nsf`) as the mail-in database. In this database, HP has removed the $Inbox folder and several other folders that are found in the standard Domino journal template. $Inbox is known to cause journaling problems when too many messages accumulate inside the folder.
- Do not use a customized journal template for the mail-in database. Customized templates can cause rissminer to report an incorrect number of message processes, along with other potential problems.
- Make sure the encryption option in the Mail-In Database document is **not** specified.
- Create journaling rules using the instructions in "Creating HP EAs Domino journaling rules" on page 85.
- Do not edit an EAs Domino journaling rules document while the Advanced Filtering server task (mwadvt) is loaded. Journaling rules information is stored in a memory cache. If rules are modified while the mwadvt task is loaded, messages might not be captured properly in the journal database.
  If a journaling rule requires modification, stop the mwadvt task by using the Domino server console command `tell mwadvt quit`. After the task is stopped, all incoming and outbound messages are held in the server's mail.box until the task is reloaded. Make the necessary changes to the journaling rules document(s) and ensure that all updated documents are saved and closed. Then, from the Domino Administrator or server console, issue the command `load updall hprim\hp_rissapi.nsf`. Restart the mwadvt task by using the Domino server console command `load mwadvt`. After the mwadvt task has completed initialization and restarted, all held messages are journaled using the updated rules and are released for routing by the Domino router.
  If more than one Domino server shares the API database, the mwadvt task must be stopped on all servers while the journaling rule update(s) are performed. After the journaling rules document is updated and saved, the database must be replicated to all appropriate servers. When replication is complete, reload the mwadvt task on all servers.
  For more information, see "Editing journal rules" on page 89.

Domino native journaling

- Only the mail-in style of Domino native journaling is supported with EAs Domino archiving.
- HP recommends that you use HP EAs-D Mail Journal (6) (`hp_mailjrn65.ntf`) as the template for the mail-in database. This template is located in the `Templates` folder on the EAs installation CD.
  HP has removed the $Inbox folder and several other folders that are found in the standard Domino journal template. $Inbox is known to cause journaling problems when too many messages accumulate inside the folder.
- Always use `hp_mailjrn65.ntf` or the standard journal template that ships with Domino. Do not use another, customized, journal template for the mail-in database. Customized templates can cause rissminer to report an incorrect number of message processes, along with other potential problems.
- Make sure the encryption option in the Mail-In Database document is **not** specified.
- Follow the instructions in the Domino documentation to create the journaling rules. Be sure to define an exception so that messages sent to the IAP are not journaled again. See Defining an IAP exception in the native journaling rules below.
- EAs Domino requires Editor with Delete access to the mail-in journal databases.

Defining an IAP exception in the native journaling rules

When you define the journaling rules in the Domino server configuration document, be sure to create a journaling exception so that messages sent to the IAP are not journaled again.

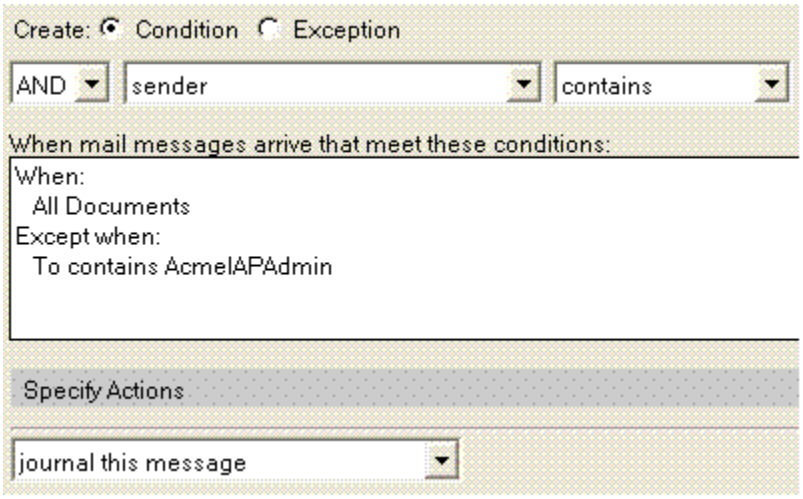
Locate the IAP email address by following these instructions:

1. In the `hprim` folder, open the HP EAs-D API database.
2. Click **Server Definition** in the left menu.
3. In the Server Definition view, locate the Server Definition document.
4. Note the address in the IAP Email address field.

In the journaling rule exception, enter the value as everything before @ in the IAP email address field.

For example, if the IAP email address is AcmeIAP01Admin@acme.com, the rule would specify:

- When: All Documents
- Except when: To contains AcmeIAP01Admin



Configuring HP EAs Domino journaling and native journaling on the same server

Running both EAs Domino journaling and Domino native journaling on the same server is not common. However, there are situations where it might be used. For example, an organization might require that all messages are journaled for an existing business process, but only a subset of users' messages are archived to the IAP.

To run both EAs Domino and native journaling simultaneously, it is important that each journaling configuration takes the other configuration into account.

- EAs Domino journaling rules: Add an exception to prevent messages that are routed to the native journaling mail-in database from being journaled by the EAs mwadvt task. Add the entry in the Except to field in the Sender/Receiver Exceptions tab.

NOTE:

The Except to field will already contain one entry, to exclude messages sent to the IAP. To support multiple entries in this field, create a group in the Domino Directory with all the addresses as members.

- Native Domino journaling rules: Add an exception to prevent messages addressed to the EAs Domino mail-in database from being journaled. See "Defining an IAP exception in the native journaling rules" on page 81.

The journaling process

Follow these steps to enable journals to be mined:

1. Create journaling rules to capture messages.
   - If you are using EAs Domino journaling, follow the instructions in "Creating HP EAs Domino journaling rules" on page 85.
   - If you are using Domino native journaling, follow the instructions in the Domino documentation.
     - Be sure to define an exception so that messages sent to the IAP are not journaled again. See "Defining an IAP exception in the native journaling rules" on page 81.
     - Be sure to filter out messages that users send to themselves from the IAP Web Interface. See "Mail-To-Me messages" on page 80.
2. Configure the mining rule so the mail-in database can be selectively archived.

   This rule must be configured whether you are using EAs Domino journaling, or Domino native journaling.

   a. Open the HP EAs-D API database.

   b. In the main view, under Mining Rules, double-click **Email Miner Journaling**.

   c. Complete the following fields at the top of the mining rules document:

Field	Description
Policy Status	Select **Enable** when you are ready to activate the rule and begin mining the journal mail-in database.
Profile	The descriptive name for the mining rule.
Archiving Strategy	Leave the default: Oldest first.
Do not archive document older than	Leave this field blank.

d. Make sure the following options are set in the mining rules document:

Field	Description
Time Conditions/Memo Reply	Do not edit.
Folders Settings	• No Time Condition – "on demand": Do not list folders in this field. • Configure the remaining fields according to your company's legal policies.
Exceptions Settings	Do not edit.
User Membership	• Ensure that the **Active for servers** setting is accurate, especially if the journal mail-in database is on a remote server. For more information, see "User Membership tab" on page 62 • In Person entry, select the mail-in database(s) to be mined. **Note**: If `rim_journaling_*` appears in the String pattern matching field, it can be deleted. This value is simply an example.
Reference Database	• Select **Regular** if the reference database is used for local mining. Select **Extended** if the reference database is used in remote mining. • Do not edit the Reference Database path and name. • Enter the Reference Database Server name if the reference database is not on the local server.
Tombstone Settings	Do not edit.
Session Settings	If the mail-in database is being mined remotely, select **Yes** for Allow Remote Mining of databases. Do not edit the remaining settings.
User Notification	Do not edit.
Administration Alert	Do not edit.

3. Schedule the journal mining job.

   Be sure to follow any specific instructions for journaling listed in "Scheduling the mining job" on page 69.

4. Schedule and enable the Encapsulate agent in `hprim/hp_preproc_journal.nsf`.

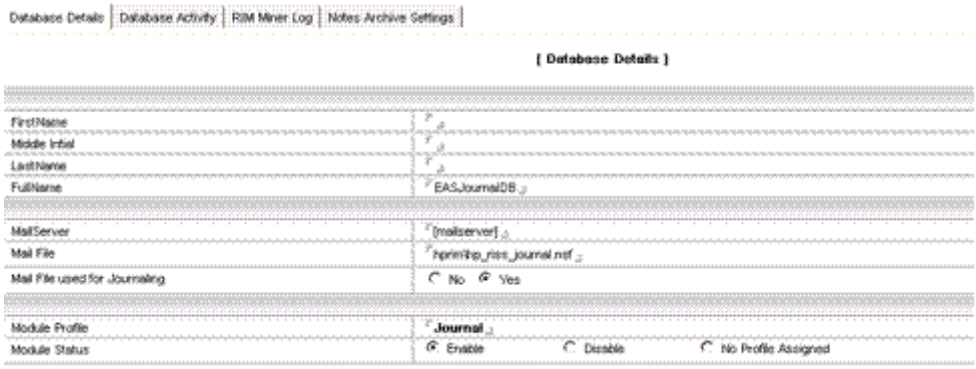
   Be sure to follow any specific instructions for journaling listed in "Enabling the preprocessing agent" on page 72.

5. Schedule and enable the Archive and Tombstone agents in `hrpim/hp_riss_journalrefer-enc.nsf`.

   Be sure to follow any specific instructions for journaling listed in "Enabling the mining agents" on page 71.

6. Add a journal "user" to the HP EAs-D Users database by creating a Mail Detail mail-in record.
   a. In the Domino Administrator client, open the HP EAs-D Users database in the `hprim` folder.
   b. In the **Create** menu, select **Mail Details** > **Database Details**.

      A new Mail Detail record appears.
   c. On the **Database Details** tab, set the following values:



Field	Description
FullName	Enter the mail-in database name; for example EASJournalDB.
MailServer	Enter the name of the server on which the mail-in database is located.
Mail File	Enter the path to the mail-in database, either for EAs journaling or for native Domino journaling. If you are using EAs journaling, enter the path and name of the journal file as `hprim/hp_riss_journal.nsf`.
Mail File used for Journaling	Click **Yes**.
Module Profile	Enter the name of the mining rule for journaling (Email Miner Journaling).
Module Status	Click **Enable**.

   d. Save the record.

   The journal user is added to the EAs-D Users database the next time the Profile Agent is scheduled to run. You can force the Profile Agent to add the journal user to the database by opening the server console and entering:

```
tel amgr run "hprim\hp_rissuser.nsf" 'profileAgent'
```

NOTE:

If Domino 7.0.3 is installed on the mail server, do not run Profile Agent manually. For more information, see "JVM panic gc0 error" on page 130.

The messages are journaled and the mail-in journal database is mined automatically, according to the journaling rules and the mining agents and schedule.

To force mining to occur, issue the commands shown in "Running the mining job" on page 77. Use `hprim\hp_riss_journalreferenc.nsf` for the reference database name. Do not run the mining agents manually if Domino 7.0.3 is installed on the server.

Creating HP EAs Domino journaling rules

Messages are captured using one or more journaling rules that determine which messages are copied to the journal.

The method for creating EAs Domino journaling rules is described in this section. If you are using native Domino journaling, follow the instructions in the Domino documentation and the recommendations in "Domino native journaling" on page 81.

Messages can be scanned by an anti-virus program before they are captured, if the option is configured during installation of the EAs software.

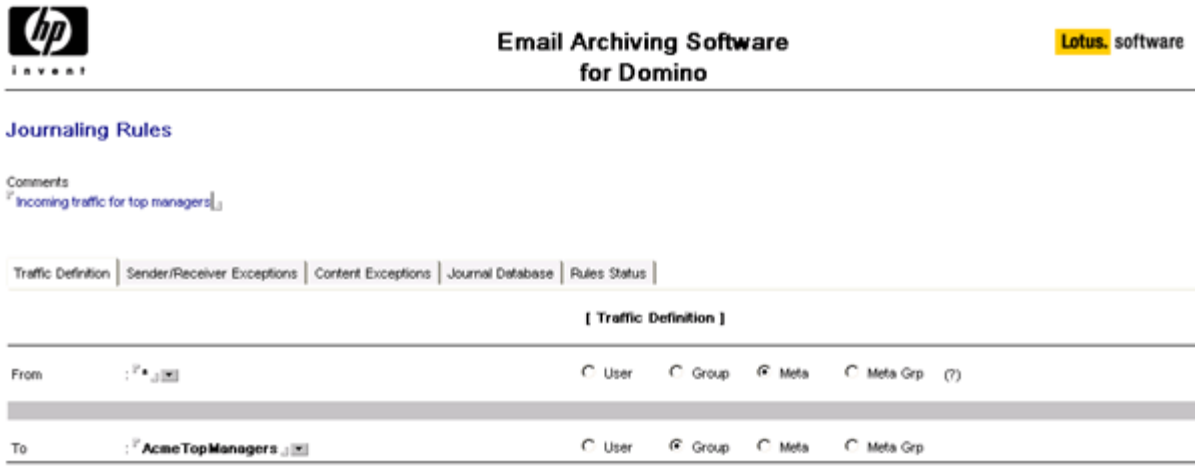
IMPORTANT:

If you are deleting or disabling an existing rule to replace it with a new journal rule, or if you are editing a journal rule, stop the Advanced Filtering (mwadvt) task before continuing. See the instructions in "Editing journal rules" on page 89. For more information on the mwadvt task see "HP EAs Domino journaling" on page 80.

A default EAs journaling rule has been created by following these steps:

1. In the Domino Admin client, open the HP EAs-D API database.
2. In the main view, double-click **Journaling Rules**.

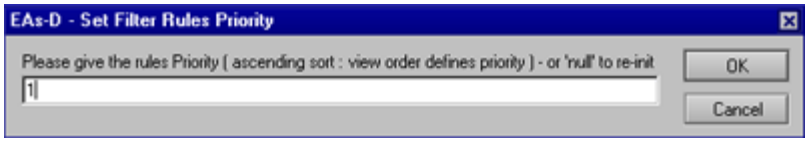
   The Journaling Rules document appears.



3. Configure the rule by completing the settings in the Journaling Rules document.
   - "Traffic Definition tab" on page 86
   - "Sender/Receiver Exceptions tab" on page 87
   - "Content Exceptions tab" on page 87
   - "Journal Database tab" on page 88
   - "Rules Status tab" on page 88
4. Select **File** > **Save** to save the rule.
5. Create other journaling rules, if necessary, by selecting **Create** > **Archiving** > **2. Journaling Rule**.

   For example, if the first rule is for incoming messages, you could create a second rule for outgoing messages.

6. (Optional) If there are two or more journaling rules, prioritize execution of the rules:
   a. In the main view, select the rule with the top priority.
   b. Select **Actions** > **Filter rules** > **1. Set 'Priority'**.
   c. Enter **1** in the dialog box that appears, and then click **OK**.



   d. Click **OK** to confirm the priority.
   e. Repeat steps a–d, creating a priority for each journaling rule.

Traffic Definition tab

Complete the traffic definitions settings, which describe who is sending or receiving the journaled messages.

If messages are sent to or from a group, note that groups are defined according to the time journaling is executed, not at the time the rule is created.

From	The From field defines who is sending the journaled messages. For example, if the rule governs outgoing messages, this field would define the user or group who is sending mail. 1. Click the arrow and select a user or group from the list, or enter a wildcard to define a group or to cover all outgoing messages. 2. Click the radio button to define the sender. The Meta and Meta group categories use wildcards. For more information, see "Defining wildcard patterns" on page 63.
To	The To field defines who the journaled messages are sent to. For example, if the rule governs incoming messages, this field would define the user or group who receives the mail. 1. Click the arrow and select a user or group from the list, or enter a wildcard to define a group or to cover all incoming messages. 2. Click the radio button to define the recipient. The Meta and Meta group categories use wildcards. For more information, see "Defining wildcard patterns" on page 63.
Comments	Enter any comments about the traffic definition.

Sender/Receiver Exceptions tab

Define any exceptions to the traffic definition. Be sure to define the **Except to** field so that messages sent to the IAP are not journaled again.

Field	Description
Except From	Messages from this user or group should not be journaled. 1. Click the arrow and select a user or group from the list, or enter a wildcard to define a group. 2. Click the radio button to define the sender. The Meta and Meta group categories use wildcards. For more information, see "Defining wildcard patterns" on page 63.
Except To	Define this field so that messages sent to the IAP are not journaled again. The name in this field works with the IAP email address your HP service representative entered in the server definition document when the software was installed. For example, if the IAP email address is AcmeIAP01Admin@iap01.acme.com, the value in this field would be AcmeIAP01Admin (everything before @). The IAP email address is listed in the Server Definition document. **Note**: If you need additional entries in this field, create a group in the Domino Directory with all the addresses (including the IAP) as members.
Comments	Enter any comments about the traffic exceptions.

Content Exceptions tab

Enter the following exceptions on this tab:

- An exception for Mail-to-Me messages (messages that users send to themselves from the IAP Web Interface). These messages must be excluded from journaling because they are already archived. Enter the following Notes formula to exclude Mail-to-Me messages:
  `@IsUnAvailable(x_pt_mailtome)`
- Any other exceptions for messages sent to or from a user or group (for example, exceptions to the Black and Red rules).
  Exceptions can be made to the message size, the maximum size of attachments, the attachment name, the number of attached files, the number of recipients, the subject, and recipient names.

The Notes formula you define for this setting must return a value of True. The simplest way to define exceptions is to use the formula wizard. Click **Wizard**, build the formula, and then click **OK** when it is complete.

Journal Database tab

Complete this tab to select the mail-in database used for journaling.

Field	Description
Journal this email in mail-in	Click the arrow and select the mail-in account name. You are responsible for creating the Mail-In Database document. See the Domino Administrator help for instructions on creating the document. The Mail-In Database document must specify the following settings: • Encrypt incoming mail: **No** For more information, see "Encrypted messages" on page 79. • File name: Enter the file name of the mail-in database. For example, `hprim/hp_riss_journal.nsf`. • Allow foreign directory synchronization: **Yes**.
Comments	Enter any comments about the configuration.

Rules Status tab

Complete the following settings:

Field	Description
Reference	Enter a name for this rule. For example, if the rule governs incoming messages for top managers, you could name it TOP_IN.
Expiration Date	Enter any expiration date for the journaling rule.
Start Date	Enter the start date for applying the journaling rule.
Status	Click the arrow and select **Enable** or **Disable** to enable or disable the journaling rule.
Sever(s)	Enter the servers on which this journaling rule is active.
Comments	Enter any comments about the rule.

Editing journal rules

IMPORTANT:

Before editing journaling rules, stop the mwadvt task on the server.

To make changes to a journal rule:

1. From the Domino Administrator or server console, stop the mwadvt task by issuing the command `tell mwadvt quit`.

   If more than one Domino server shares the HP EAs-D API database, stop the mwadvt task on all relevant servers.
2. Open the HP EAs-D API database, and double-click the Journaling Rules document in the main view.
3. Double-click the relevant settings and make the changes.
4. Click **File** > **Save** to save the changes.
5. From the Domino Administrator or server console, issue the command `load updall hprim\hp_rissapi.nsf`.
6. In a multi-server environment, wait for the HP EAs-D API to replicate to all message processing servers.
7. Restart the mwadvt task by issuing the command `load mwadvt` on all relevant servers.

Mail.box issue

If you are using more than one mail.box file on a mail server, and want to consolidate to a single mail.box, delete the other mail.box files first.

1. Stop the mail server.
2. Make sure there are no entries in the mail.box files.
3. Delete the multiple mail.box files (mail1.box, mail2.box, etc.) before adding the new, single mail.box file.
4. Restart the server.

7 Using bulk upload

Bulk upload is a utility that can be used for one-off archiving. For example, it can be used to discover the mail files of former employees or inactive users and archive the messages in their mail files. It can also be used to locate and archive messages in the old mail files of existing users.

When EAs Domino is first installed, you might use bulk upload quite a lot. After the initial uploads, it's likely you would use the process only when employees leave the organization or when you need to perform a one-off upload to the IAP.

Running bulk upload involves five steps:

1. Editing the bulk upload mining rule, page 91.
2. Editing the Preprocessing Control document, page 92
3. "Enabling the agents" on page 92.
4. "Discovering the databases" on page 92.
5. "Mining the databases" on page 93.

You can also use bulk upload to find the owner of a mail database. See "Forcing a database owner" on page 93.

Editing the bulk upload mining rule

The mining rule for bulk upload is similar to the mining rules created for active users. The fields in the Mail Detail records that are created are similar to those in the HP EAs-D Users Mail Detail records.

A default bulk upload mining rule has been created in the HP EAs-D API database.

To use the default rule:

1. In the Domino Administrator client, open the HP EAs-D API database.
2. In the Mining Rules area of the EAs-D API main view, double-click **Email Miner Bulk**.
3. On the User Membership tab, select the server(s) with the mail databases to be discovered and mined.
4. Configure the Reference Database tab:
   - Reference document:
     - Click **Regular** for local mining.
     - Click **Extended** for remote mining.
   - Reference Database Server name:
     If the reference database is not on the local server, enter the name of the server on which it is located. Otherwise, leave the field blank.
5. Do not edit the settings on the remaining tabs.
6. Enable and save the mining rule.

Editing the Preprocessing Control document

To edit the document:

1. In the Domino Administrator client, open the HP EAs-D API database.
2. In the PreProcessing Controls area of the EAs-D API main view, double-click **PreProcessing Controls Default for Bulk Upload**.
3. In the **Databases Location** tab, select the server(s) running the Encapsulate agent.
4. In the **Encapsulation Settings** tab, edit the temporary work directory if necessary.

   For more information on the temporary work area, see "Encapsulation Settings" on page 37.
5. Enable and save the document.

Enabling the agents

After editing the bulk upload mining rule and configuring the Preprocessing Control document, enable the preprocessing and mining agents.

- For preprocessing, enable the Encapsulate agent in HP EAs-D Bulk Upload Preprocessing database (`hprim\hp_preproc_blk.nsf`).
- For mining, enable the Archive and Tombstone agents in the HP EAs-D Bulk Upload Reference database (`hprim\hp_riss_blkupdreferenc.nsf`).

Discovering the databases

Discover the user databases containing the messages to be archived. The discovery is run from the command line.

1. In the Domino Administrator client, open the server console by selecting **Server** > **Status** > **Server Console**.
2. Issue the following command:

   ```
   load hpblkupd –d<db/dir> –kbulk
   ```

   For example, to locate the database files in the terminated sub-directory in the Domino data directory, load the files into the default bulk upload database, and associate them with the bulk upload rule, enter:

   ```
   load hpblkupd -dterminated -kbulk
   ```

The following arguments can be used for database discovery:

Argument	Description
`-d<db/dir>`	The database or directory to search. You can run the process on a single database or a directory. If you do not specify a value for –d, the tool searches every database in the Domino data directory.
`-r<db>`	The database to store Mail Detail records created for each database that is discovered. The default discovery database (no –r argument) is `hp_rissblkupd.nsf`.
`-k[profile]`	The name of the mining rule. If you use the default bulk upload rule, this value is `bulk`.
`-v`	Verbose mode, which also displays the discovered databases.

Forcing a database owner

Every mail database should have an owner that can be associated with a user in the IAP.

To force a particular database owner, you can use the argument –o{x@xx.xx], where {x@xx.xx] is the Internet address of the owner.

For example, if you want to force Joe Smith as owner of a database, you might enter:

```
load hpblkupd –d<db> –ojoesmith@company.com
```

If you do not specify a value for the owner, bulk upload tries to find the owner using the following steps. The process ends when the owner is found and the owner value is saved.

1. Get Owner from DelegationProfile. (For example, if Joe Smith was a company manager and delegated his email to his assistant.)
2. Get Owner from CalendarProfile.
3. Get Owner from the SENT view. The process looks for the most frequent FROM field.
4. Get Owner from the database access control list (ACL). The process looks for a user with at least READER access.

Reviewing the Mail Detail records

To review the Mail Detail records that are created during database discovery:

1. In the Domino Administrator client, open the HP EAs-D API database.
2. In the left menu of the main view, click **Bulk Upload Config**.
3. In the document views, review the list of mail files.
   a. Double-click an entry to open the Mail Detail record.

      The Database Details tab in the record lists the database owner, the mail server, the path in the data directory, and the mining rules profile.

   b. Delete any mail files that should not be archived by right-clicking the file in the document view and selecting **Delete**.

      Approve the deletions when you close the bulk upload database.

Mining the databases

To mine the messages in the databases, follow these instructions:

1. Navigate to **Server** > **Status** > **Server Console** in the Domino Administrator client.
2. Issue one of the following commands to run the mining program:
   - `load rissminer –r –v –kbulk`
     This mines the documents stored in `hp_rissblkupd.nsf`, the default bulk upload database.
   - `load rissminer –r<db> –v –kbulk`
     This mines documents stored in a database other than the default bulk upload database. Enter the relevant database value in <db>.
3. Open the bulk upload reference database (`hprim\hp_riss_blkupdreferenc.nsf`) to view the references that were created.

   See "Viewing references" on page 40 for more information.
4. If any reference documents are in the preprocessing state, issue the following command:

   ```
   tel amgr run "hprim\preproc_blk.nsf" 'encapsulate'
   ```

5. Run the Archive and Tombstone agents:

```
tel amgr run “hprim\hp_riss_blkupdreferenc.nsf” ‘archive’
tel amgr run “hprim\hp_riss_blkupdreferenc.nsf” ‘tombstone’
```

NOTE:

If Domino version 7.0.3 is installed on the server, do not complete step 5. The Archive and Tombstone agents must be scheduled. Do not run these agents from the command line.

8 Configuring IAP single sign-on

With IAP single sign-on (SSO), users are automatically authenticated for access to the IAP Web Interface when they log into their Lotus Notes account. Authentication with the IAP is performed using Domino credentials.

To use IAP SSO, follow the procedures in this chapter.

SSO involves configuration on the mail servers, changes to the mail template, and configuration on the IAP.

NOTE:

SSO can only be used with IAP version 1.6.1 or later. If you are using IAP version 1.6.1, make sure the 1.6.1 Hotfix software is installed.

- Copying the SSO templates, page 95
- Configuring the HP EAs–D SSO database and the Generate SSO Tokens agent, page 96
- Configuring The Search the IAP Archive agent, page 99
- Configuring The Search the IAP Archive agent, page 99
- Configuring the client computers, page 103

Copying the SSO templates

Two templates must be copied from the Templates directory on the installation media to a Notes client:

- HP EAs-D SSO (`hp_EAsDSSO.ntf`)
  Used to configure the HP EAs-D SSO database on Domino mail servers, generate a secret key for authentication, and configure the Generate SSO Tokens agent.
- HP EAs-D Mail (R6) with SSO (`mail6RIM16-SSOx.ntf`)
  Used to provide customized design elements that can be added to mail templates, adding a link to the IAP from users' Notes mail files.

1. Copy HP EAs-D SSO (`hp_EAsDSSO.ntf`) and HP EAs-D StdR6Mail (`mail6RIM16–SSOx.ntf`) from the `Templates` directory on the installation media into the root data directory of the Notes client (for example, `C:\lotus\notes\data`).
2. In the Notes client, select **File** > **Database** > **New**.

   The New Database window appears.
3. Specify the new HP EAs-D SSO database:
   a. In the **Server** box, specify the name of the server you selected.
   b. In the **Title** box, enter **HP EAs-D SSO**.
   c. In the **File name** box, enter **hprim\rimsso.nsf**.

NOTE:

The `rimsso.nsf` file name is hard-coded in the Search the IAP Archive agent used in IAP SSO. If you change the file name, be sure to change the file name in the agent. See "Configuring The Search the IAP Archive agent" on page 99.

4. Specify the template for the HP EAs-D SSO database:
   a. In the **Server** box, leave **Local**.
   b. In the **Template** box, select **HP EAs-D SSO**, and then click **OK**.
5. Close the database.

Configuring the HP EAs-D SSO database and the Generate SSO Tokens agent

Before configuring the HP EAs-D SSO database and the Generate SSO Token agent, select a primary server for the EAs-D SSO application. The server does not have to be a mail server. However, it does need to have replicas of the primary Domino Directories for all mail domains participating in the SSO configuration.

1. Start the Domino Administrator client, and switch to an ID file that has rights to create databases and run unrestricted agents on the mail servers.
2. In the Administrator client, open the server that you selected. Click the **Server** tab, select **Server Console**, and enter the following command:

   ```
   set config hprim_sso_append_notesdomain=1
   ```

NOTE:

This step is required if multiple Notes domains share one IAP. Otherwise, it is optional.

Note that this step improves SSO response time.

3. In the Administrator client, perform the following steps to sign the HP EAs-D SSO database:
   a. In the **File** menu, select **Open Server** and then select the server.
   b. In the **Show me** box, select **Databases only**.
   c. Select the HP EAs-D SSO file.
   d. With the file selected, right-click and select **Sign** from the context menu.
   e. Leave the default settings, and click **OK**.
4. In the Designer client, open HP EAs-D SSO.
5. In the **File** menu, select **Database** > **Access Control**, and then configure access for the user. Click **OK** when you have finished.
   - User type: **Person**
   - Access: **Manager**
   - Select the **Replicate or copy documents** check box.
   - In Roles, select the **RIM SSO Admin** check box.

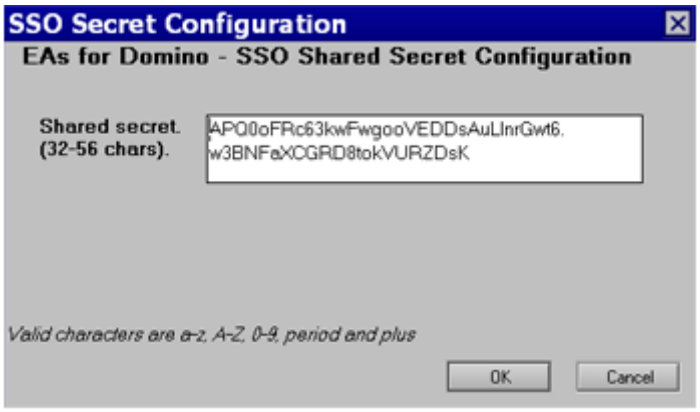
6. In the Notes client, open HP EAs-D SSO.

   The EAs-D SSO database opens to the following window.

7. In the Notes **File** menu, select **Database** > **Access Control**.
8. Perform the following steps in the ACL window:
   a. Check that the ID has Manager access and the RIM SSO Admin role.
   b. Set the Default access level to **Reader**.
   c. If all members of the LocalDomainAdmins group are trusted with SSO information, enter that group into the ACL and give it Manager rights with the RIM SSO Admin role.

      As an alternative, identify a group with a smaller list of members who are trusted with SSO information and enter that group instead.
   d. Click **OK** when all changes to the ACL are complete.
9. Configure the SSO Shared Secret:
   a. In the HP EAs-D SSO database window, click **Configure SSO Shared Secret**.

      A default secret is displayed. You can change this secret to any text string between 32 and 56 characters long using the characters A-Z, a-z, 0-9,. (period), and/or +.



      The secret is shared by all Domino servers and the IAP. It is the basis for the cryptographic authentication that allows the IAP to accept Domino credentials for sign-on. This secret should be known only to a small set of administrators.

      Users with the RIM SSO Admin role in the EAs-D SSO database ACL can view and change the secret. Note that if you change the secret in Domino, you must also change it on the IAP. (See "Configuring SSO on the IAP" on page 102.)
   b. Click **OK** to save the secret.

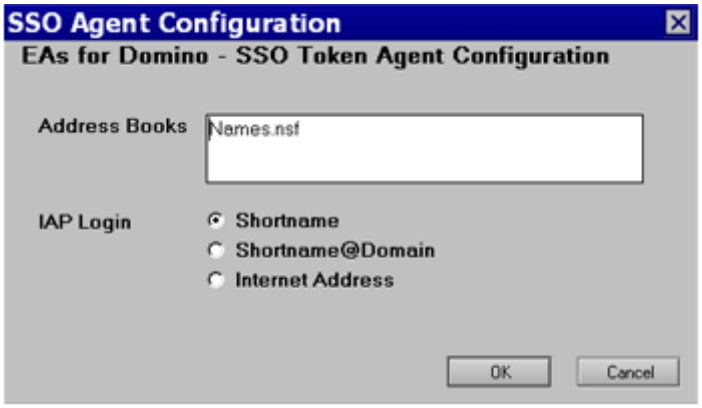
10. Export the SSO Shared Secret:
    a. In the HP EAs-D SSO database window, click **Export the Shared Secret**.
    b. Select a location to save the secret in an XML file, and then click **Save**.

       You will use the XML file as a reference when performing the IAP configuration for SSO (see step 2 in "Configuring SSO on the IAP" on page 102.

       IMPORTANT:
       The XML file is not encrypted. It should not be left exposed, where unauthorized users might be able to find and read it.

11. In the HP EAs-D SSO database window, click **Configure SSO Token Agent**.

    The SSO Agent Configuration box appears.



    a. In the **Address Books** box, enter the filenames of all Domino Directories on the server that contain Person documents for users participating in EAs Domino SSO.

       The filenames should be separated by commas.
    b. In **IAP Login**, select the type of login to be used to access the IAP.
    c. If you select Internet Address as the IAP Login type, be sure to complete the steps in the following sections:
       - "Modifying the Search The IAP Archive agent" on page 102
       - "Modifying the UID" on page 103
    d. Click **OK**.

    Note: The `notes.ini` variable `HPRIM_SSO_APPEND_NOTESDOMAIN` used in previous versions of EAs Domino is obsolete. That functionality now corresponds to the second choice in IAP Login: shortname@domain.

12. Return to the Designer client and open HP EAs-D SSO.
13. In the Shared Code pane, click **Agents** and then double-click the **Generate User Tokens** agent.

    The Agent properties dialog box appears.

14. In the properties dialog box:
    a. Select **On schedule** for the trigger, and then select **Daily** in the drop-down list.
    b. Click the **Schedule** button and verify that the correct server name appears in the **Run on** drop-down list.
    c. Set the execution time close to 12:00 AM (for example, 12:15 AM).
    d. Click **OK**, and then close the dialog box.
15. Enable the agent.

To force an initial run of the agent, go to the Domino server console and issue the command:

```
tell amgr run "hprim\rimsso.nsf" 'Generate User Tokens'
```

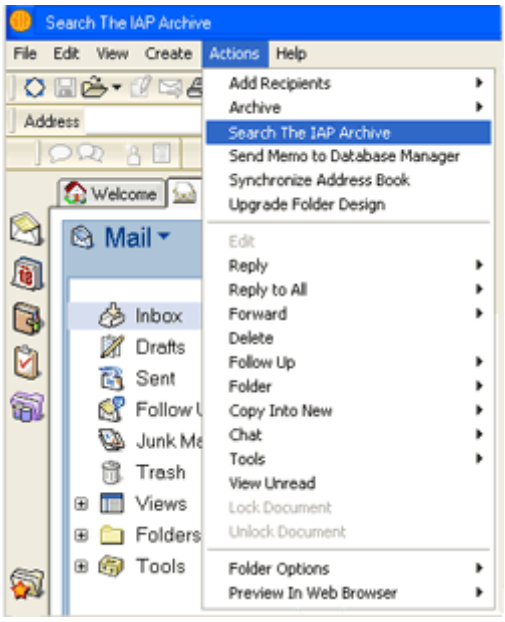
NOTE:

Create replica copies of `hprim\rimsso.nsf` on all additional mail servers in the Domino domain to ensure all users can authenticate via IAP SSO. Deployment of the database to one or more hub servers and modifications to connection documents might be necessary to enable scheduled replication across the domain.

Configuring the Search The IAP Archive agent

The HP EAs-D Mail (R6) with SSO template file (`mail6RIM16-SSOx.ntf`) is a modified version of the Domino 6 mail database template. The EAs-D SSO code in this template works on Domino 6, 7, and 8 servers.

The template contains a Domino agent called Search the IAP Archive that can be accessed from the Actions menu in a user's Notes client. It launches a browser window with a URL that connects to the IAP and authenticates the user.



The template also contains a sample modification of the action bar in the $Inbox folder, adding a Search the IAP button. This sample shows an easy way for users to log into the IAP.

Instructions for using the template's design elements to modify a production template are given below.

IMPORTANT:

The HP EAs-D Mail (R6) with SSO template can be used as-is to create mail files for test and demonstration purposes. However, it is not intended to be a direct replacement for any of the mail templates on your Domino systems.

You should continue to use the production templates that are shipped by IBM and supported for the versions of Notes and Domino that are installed.

The implementation process

Follow the process below to implement changes in user mail files:

1. Copy individual design elements from HP EAs-D Mail (R6) with SSO into individual user mail files for test purposes.
2. (Optional) Translate and develop alternative customizations (e.g., modified framesets, outlines, smarticons, etc.) that use the same technique as the Search The IAP button to launch the Search The IAP Archive agent from the Notes client.
3. Develop one or more templates by creating design-only copies of the mail modified file(s), using **File** > **Database** > **New Copy** from the Notes client menu. Deploy those template databases on the Domino servers, and use Domino Designer to insert the customized design elements into user mail files.

Only the first step of this process is documented below in "Copying design elements from the template" on page 101. Standard Notes development and administration techniques should be used for steps 2 and 3.

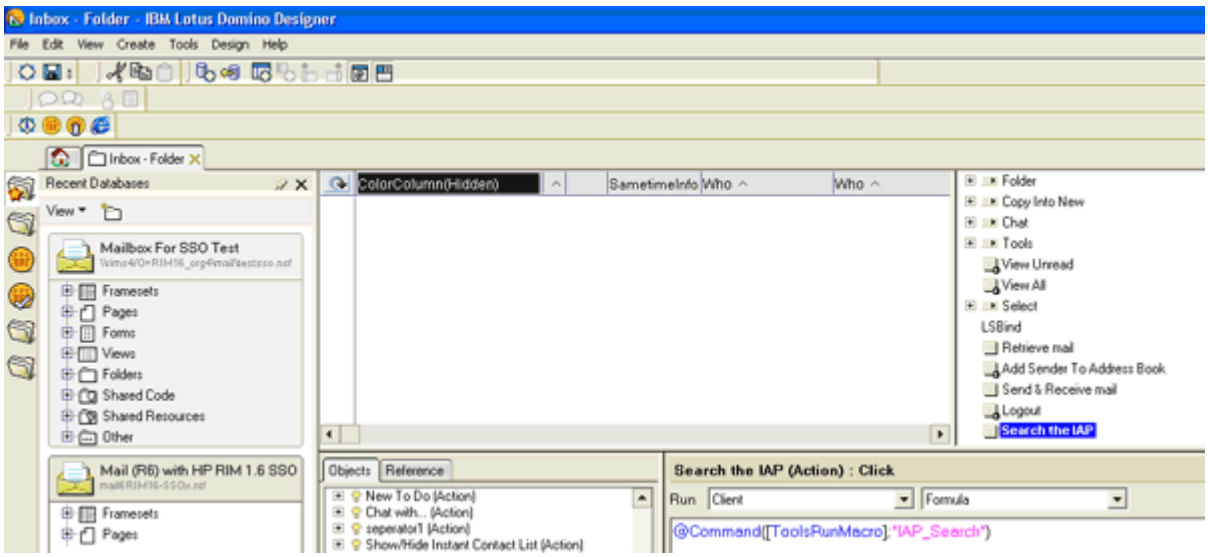
Copying design elements from the template

1. In the Designer client, open the following files:
   - HP EAs-D Mail (R6) with SSO (`mail6RIM16-SSOx.ntf`)
   - A user mail file
2. In the Shared Code section of `mail6RIM16-SSOx.ntf`, open the Agents list and copy the Search The IAP Archive agent to the clipboard.
3. In the Shared Code section of the user mail file, open the Agents list and paste the Search The IAP Archive agent into the list.

NOTE:

If you changed the `rimsso.nsf` file name in "Copying the SSO templates" on page 95 be sure to change the file name in the agent. Open the Search the IAP Archive agent, select **Main**, and change the file name in **open rimsso.nsf database on server**.

4. Open the Folders section of `mail6RIM16-SSOx.ntf`, and then open the $Inbox folder.
5. Slide out the actions pane from the right side of the Designer window.



6. Select the **Search The IAP** action, and copy the action button to the clipboard.
7. Open the Folders section of the user's mail file, and then open the $Inbox folder.
8. Slide out the actions pane.
9. Place your cursor inside the actions pane, and paste the Search The IAP action button.
10. If you want, drag and drop the action to reorder within the sequence.

    Note that the code for this action is a simple Notes @Formula, which can be used in other contexts in addition to or instead of the $Inbox action bar.

NOTE:

If you customize any design elements other than the ones in the template, be sure to take careful notes on each element that is modified.

Modifying the Search The IAP Archive agent

If you selected Internet Address in step 11 of Configuring the HP EAs–D SSO database and the Generate SSO Tokens agent, perform the following steps in the user's mail file:

1. In the Shared Code section of the user's mail file, open the Agents list and select the Search The IAP Archive agent.
2. Open the agent.
3. In the Initialize section of the agent:
   a. Remove the "'" character from `'gConfigLoginItem = ITEM_INET_ADDR`.
   b. Add the "'" character to `gConfigLoginItem = ITEM_SHORT_NAME`.

      The item is changed to `'gConfigLoginItem = ITEM_SHORT_NAME`.
   c. Save the change and close the agent.

Configuring SSO on the IAP

Installing the secret key

For the IAP to accept Domino SSO authentication, you must install the secret SSO key into the L3 Registry running on the IAP kickstart server.

NOTE:

SSO can only be used with IAP version 1.6.1 or later. If you are using IAP version 1.6.1, make sure the 1.6.1 Hotfix software is installed.

To install the SSO secret, SSH into the IAP kickstart machine, and then perform the following steps:

1. Navigate to the `/install/tools/registry/loader` directory and issue the following command:

   ```
   vi SSO_DOMINO.archive
   ```
2. In line 4 of the `SSO_DOMINO.archive` file, enter the secret SSO key after `key:`.

   For example, `key:[`*`secret SSO key`*`]`

   Use the secret key as it appears in the XML file that you exported earlier. (See step 10 in "Configuring the HP EAs–D SSO database and the Generate SSO Tokens agent" on page 96). Be sure to include all text between the `<RIMSSO version="1.6">` and `</RIMSSO>` tags in the XML file, including the date stamp that appears at the end.
3. Navigate to the `/install/tools/registry/bin` directory and run the RegistryLoader using the following command:

   ```
   regloader.pl -l
   ```

   Domino SSO is enabled on the IAP after the RegistryLoader is run.

IMPORTANT:

Whenever the IAP is kickstarted, the SSO secret key is lost and these steps must be repeated.

Modifying the UID

Perform the following steps on the IAP if you selected Internet Address as the IAP Login in the SSO Token Agent Configuration (step 11 in Configuring the HP EAs–D SSO database and the Generate SSO Tokens agent).

Stop the current DAS job:

1. Log into the IAP PCC and navigate to Account Synchronization.
2. On the DAS Available Jobs page, select the job, and click **Stop**.

Make the following modification:

1. SSH into the HTTP portal and navigate to the DAS runtime directory:

   ```
   cd /opt/DAS/runtime
   ```

   NOTE:

   If there is more than one HTTP portal on the IAP, be sure to select the HTTP portal on which the DAS job is running.

2. From the runtime directory, issue the following command:

   ```
   vi LoadChangesDomino.dse
   ```

3. Search for `BLOB,0,UID`.
4. Change the UID to `mail` so that the UID looks like `BLOB,0,mail`.
5. Save the `LoadChangesDomino.dse` file.
6. Issue the following command:

   ```
   cp LoadChangesDomino.dse LoadChanges.dse
   ```

7. On the DAS Available Jobs page in the PCC, select the job, and click **Start** to restart the DAS job.

Configuring the client computers

For SSO to work, a functioning browser must be installed on the client computer and the browser must be configured correctly in the Location Document in the Notes client.

To check whether a user's Location Document is set up correctly:

1. Click the **Location** pop-up in the lower right corner of the Notes client window.
2. Select **Edit Current**.

   The location document is displayed.

3. Click the **Internet Browser** tab, and check that an appropriate value is entered in the **Internet Browser** field.

   The recommended setting is either Microsoft Internet Explorer, which launches the browser in its own window, or Notes with Internet Explorer, which launches the browser in a tab in the Notes client.

4. Click **Save & Close**.

9 Working with HP EAs Domino client applications

Copies of archived messages can be viewed and retrieved from the IAP in several ways, depending on the EAs 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 send message copies to their mailboxes. These functions do not require software to be installed on client systems. A link to the Web Interface can be added in users' Notes databases.
- **Export Search**: Messages can also be exported from the IAP Web Interface as standard Notes NSF files. One benefit of this feature is that messages can be read using standard Notes software for legal and other purposes. Another benefit is that the NSF files can be transported anywhere.
- **Local Cache**: A local cache can be installed on Windows clients (normally on laptop or notebook computers) so that users can access archived messages offline while they are traveling.
- **Windows Notes Client Plug-In**: A plug-in can be installed on Windows clients to give users instant access to archived messages when they are online. The plug-in can also be used with Local Cache.

These methods are explained in the following sections:

- Using the IAP Web Interface, page 105
- "Creating an IAP Web Interface link in Lotus Notes" on page 106
- Using Export Search, page 107
- Using Local Cache, page 113
- Using the Windows Notes Client Plug-In, page 120
- Using the Windows Notes Client Plug-In with Local Cache, page 123
- Adding the tombstone icon (optional), page 123

For information on working with signed and encrypted messages, see "Retrieving and viewing encapsulated messages" on page 124.

For information on adding new MS Office 2007 MIME types to the File Description table, see "Adding MS Office 2007 MIME type support to HP EAs Domino" on page 125.

For information on the client operating systems that EAs Domino supports, see "System requirements" on page 14.

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. They can save and reuse their search-query definitions and results, and send copies of archived email to their Lotus Notes mailbox.

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 "System requirements" on page 14.)

The following list shows the basic information required to use the Web Interface. More detailed information is located in the HP EAs Domino user guide and the IAP user guide.

- IAP Web Interface URL: IP address of the IAP foreign domain (the HP gateway server)
- Username for login: User's email address or Notes Short Name
- Password: Password for accessing email, normally the user's Lotus Notes Internet password

- Content Type for search: email
- Send (All Items or Checked Items) sends email copies to the user's Inbox.
  Export (All Items or Checked Items) is a function that requires software to be installed on the client system. For information on exporting email, see "Using Export Search" on page 107.

Creating an IAP Web Interface link in Lotus Notes

A link can be created in Lotus Notes that takes users directly to the IAP Web Interface when the link is clicked.

There are two methods for creating the link:

- The first method simply creates a link to the Web Interface in the Notes navigation pane. After users click the link icon, they must log in to the IAP Web Interface before viewing their archived messages. This method involves some small changes to the mail template.
- The second method sets up a single sign-on for Notes and the IAP Web Interface. When users log into their Notes account, they are automatically authenticated for Web Interface access. Authentication with the IAP is performed using Domino credentials. This method involves more extensive changes to the mail template, generation of a secret key, and configuration on the IAP.

Creating a link to the Web Interface

Use these instructions to create a link from Notes to the IAP Web Interface. This link must be created using a Windows client.

When users click the link, they are taken to the login screen for the Web Interface, where they must enter their user name and their Notes Internet password.

To set up the link:

1. Using the Domino Designer client, open the mail template on the server.
2. In the Design pane, click **Shared Resources**, and then click **Images**.
3. Click **New Image Resource**.
4. In the **Open** dialog box, select a graphic to use as an icon for the link, and then click **Open**.
5. Save and close the Image Resource.
6. In the Design pane, click **Shared Code** and then click **Outlines**.
7. Open **NotesMailOutline**.
8. Click **New Entry**.
9. In the **Label** field, enter a name for the link.
10. From the **Type** list, select **URL**.
11. In the **Value** field, enter the URL or IP address of the IAP Web Interface (the IAP foreign domain).
12. Click **Folder** in the **Image** area.

    The Insert Image Resource dialog box is displayed.
13. Select the Image Resource you created in step 4, and then click **OK**.
14. Press **Esc** to exit out of Domino Designer, and then click **Yes** when prompted to save changes.

When users access Lotus Notes, an icon for the link to the IAP Web Interface is displayed in the navigation pane.

Using Export Search

Export Search is a tool that you will typically use to retrieve messages that have been requested by compliance officers for litigation-related review. With Export Search, message links are exported from the IAP Web Interface to a DLD file. The linked messages are then downloaded into a standard Notes NSF file, usually one created for this purpose. The original messages remain on the IAP.

The email search itself is performed in the IAP Web Interface. When the time comes to extract the message links from the DLD file, you can choose whether to use a local client, or use the Export Search database on the message processing server. If you are extracting a large number of messages, the server-side option is the better choice.

Employees can also use the Export Search tool to export message copies from the IAP. However, they must have the Local Cache software package installed on their machines to use the feature.

IMPORTANT:

Java Runtime Environment (JRE) version 1.6 or later must be installed on the client machine before the Local Cache software can be installed and before Export Search can be run.

Using the client to extract messages

To export email from the IAP Web Interface, Local Cache must be installed on the client machine, with the IAP domain and address configured in the Local Cache settings. The Local Cache installation includes the Export tool that is required for this operation.

After installing the Local Cache package, link the DLD file extension to `ExportSearch.exe`, which is located in the newly-created Localcache folder: `\Program Files\lotus\notes\Localcache`.

See "Installing Local Cache" on page 113 and "Configuring Local Cache" on page 115 for more information.

To export email copies from the IAP using a local client:

1. Create a folder in the local mailbox to hold the exported messages.

   If the messages are being exported to another mailbox to which you have access, create a folder in that mailbox.

2. Search for the relevant messages in the IAP Web Interface.

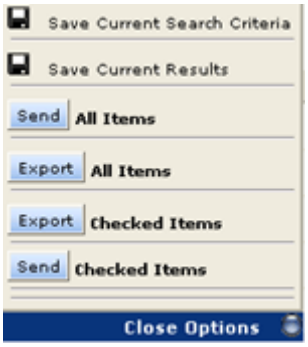
   If your search is a complicated one, use the Advanced Search instructions in the *HP Integrated Archive Platform User Guide*.

   NOTE:

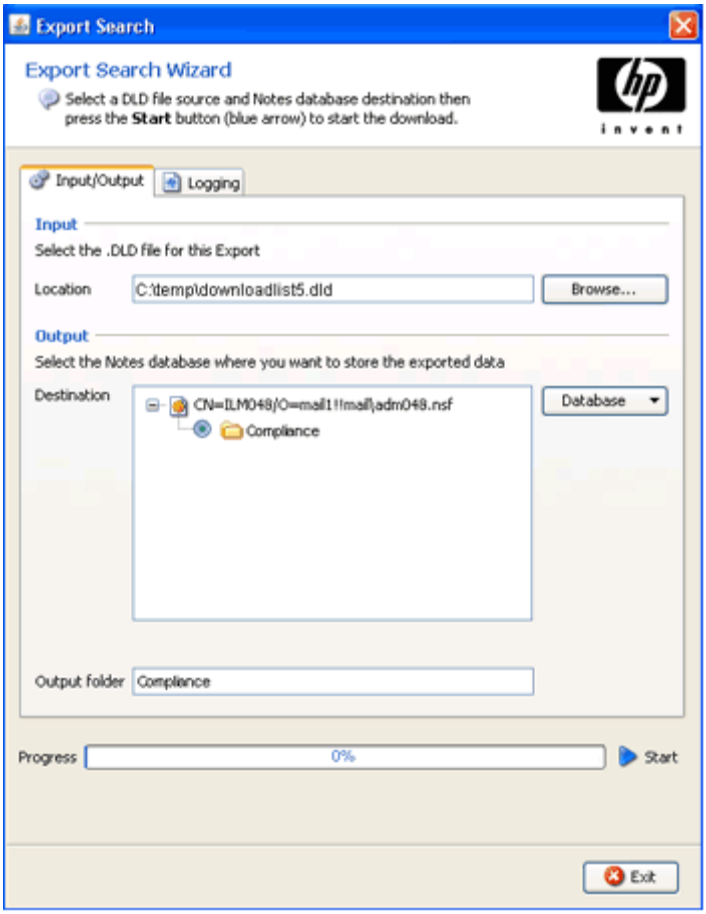
   If IAP 2.x is installed, you cannot use the Folder Name field in Advanced Search. HP EAs Domino 2.0 does not capture folder names when messages are archived.

3. 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.

4. Click **More Options** to open the options menu.



5. To export all results, click **Export All Items**. To export the selected items, click **Export Checked Items**.
   The file download dialog box appears.
6. Click **Open** to open the DLD file.
   The DLD file extension must be associated with `ExportSearch.exe` to open the file.
7. Enter the Notes password in the dialog box that appears, and then click **OK**.
   The Export Search wizard appears.
8. In the **Output** area, select a Notes database to contain the downloaded messages.
   The default database is the local mail file on the client machine.
9. Expand the mailbox and select the folder you created in step 1.



10. Click the **Start** arrow next to the progress bar to start the download.

    A log appears displaying the download results.

11. Review the log for any errors that might have occurred during the download process.
12. If the log shows a successful download, click **Exit** to close the Export Search wizard.
13. Use Notes to open the destination database and view the downloaded messages.

Using the server to extract messages

Follow these instructions when there are a large number of messages to export.

NOTE:

A large amount of memory might need to be allocated to the Domino Java memory pool if you export 10,000 or more messages or messages with large file attachments (20 MB or larger). For Export Search to have the necessary memory to export messages, change the `notes.ini` JavaMaxHeapSize setting to a value of 512 MB:

```
set config JavaMaxHeapSize=536870912
```

After changing the JavaMaxHeapSize value, restart the server.

Modifying files for server-side Export Search

If you implement server-side Export Search, several files must be modified. Instructions are shown in the steps below. These instructions apply to each Domino server where the `hprim` files are installed.

NOTE:

Your HP service representative might have performed these steps during EAs Domino software installation. If so, an entry has been added to the server's `\Domino\jvm\lib\security\java.policy` file (as referred to in step 4).

1. Locate and remove the existing `retriever`*`n.n.n.n`*`.jar` file from the Domino server's `\Domino\jvm\lib\ext` folder.
2. In the extracted installation files, open the `jvm.lib.ext` folder and copy the following files to the server's `\Domino\jvm\lib\ext` folder:
   - `retriever`*`n.n.n.n`*`.jar`
   - `dns.jar`
   - `activation` *`n.n.n`*`.jar`
3. (Domino 6.x servers only) Copy the following files from the `jvm.lib.ext` folder in the installation files to the server's `\Domino\jvm\lib\ext` folder:
   - `saxAPI.jar`
   - `securityAPI.jar`
4. Modify the `\Domino\jvm\lib\security\java.policy` file by adding the following entry to the top of the "standard" properties list:

   ```
   permission java.security.AllPermission;
   ```

   Security settings on the Domino server must be modified so that Export Search has permission to perform HTTPS operations when interacting with the IAP.
5. If you plan to export 10,000 or more messages or messages with large file attachments (20 MB or larger), allocate sufficient memory to the Domino Java memory pool.

   Ensure the JavaMaxHeapSize in `notes.ini` is set to a value of 512 MB or greater: `set config JavaMaxHeapSize=536870912`.

6. Restart the Domino server.

Exporting the messages

To export email copies from the IAP Web Interface:

1. Search for the relevant email.

   If the search is a complicated one, use the Advanced Search instructions in the *HP Integrated Archive Platform User Guide*.

> **NOTE:**
> If IAP 2.x is installed, you cannot use the Folder Name field in Advanced Search. HP EAs Domino 2.0 does not capture folder names when messages are archived.

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

   The file download dialog box appears.
5. Click **Save** to save the DLD file.

   Save the file in a folder that the server can locate; for example, a folder on a client system's hard drive. You might want to create a folder especially for these downloads.

Extracting the messages

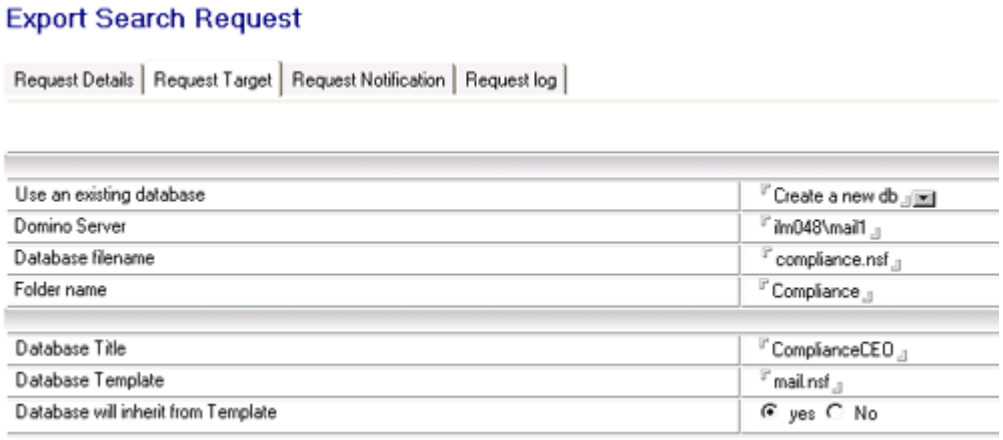
To extract the messages from the DLD file to a mail database:

1. In the Notes client, open the HP EAs-D Export Search database in the `hprim` folder.
2. In the **Create** menu, select **Configuration** > **IAP Host**.
3. Enter the IP address of the IAP Web Interface (the IAP foreign domain created during system installation), and select **File** > **Save**.
4. In the **Create** menu, select **IAP Search Export to NSF**.

   The Export Search Request appears, opened to the Request Details tab. The Request ID, date, and author fields are already populated.
5. Complete each remaining **Request Details** tab field as shown below.

Field	Description
IAP host name or IP	Click the arrow, select the IAP Host IP, and then click **OK**.
DLD file(s)	Drag and drop the DLD file from the client into this field.

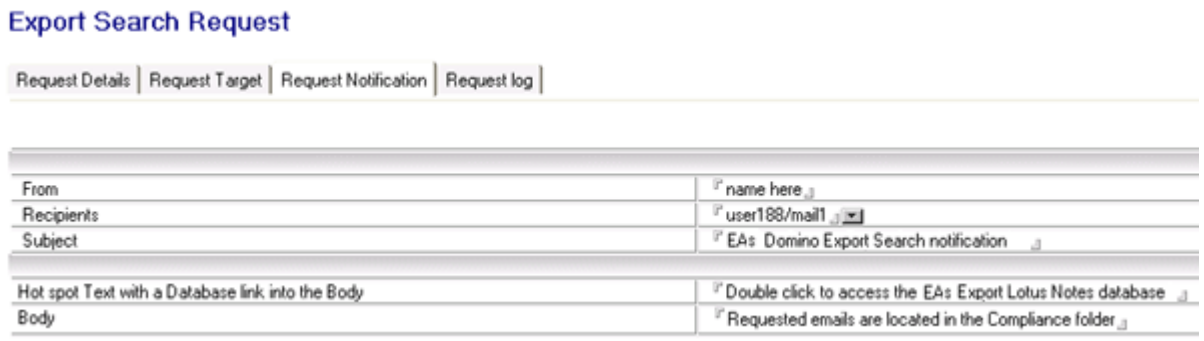
6. Click the **Request Target** tab and complete the fields as shown below. All fields must be completed.



Field	Description
Use an existing database	Click the arrow and choose whether to add the messages to an existing database or create a new database, and then click **OK**.
Domino server	Enter the name of the server where the database is located. **Note**: Make sure that the compliance officer has access to this server and database.
Database filename	Enter the name of the new or previously-created database.
Folder name	Enter the name of the folder in which the messages will be extracted.
Database Title, Database Template	If you are creating a new database, enter a database title, and name of the mail database template.
Database will inherit from Template	Click **Yes**.

7. Click the **Request Notification** tab and complete the fields. All fields must be completed.

   This tab configures an email that is sent to compliance officers telling them the retrieved messages are ready to be viewed. The email includes a link to the database containing the messages.



Field	Description
From	Enter a name.
Recipients	Click the arrow, select the recipients, and then click **OK**.
Subject	You can change the subject line from the default.
Hot Spot text	You can change the text from the default.
Body	Add any comments for the body of the message. For example, if the messages are downloaded into a new folder in the database, you can mention that the link will open the database to the Inbox and users must open another folder.

8. Select **File** > **Save** to save the request.

The **Request log** tab shows the start and end time of the export, the number of URLs (DLD links to archived messages that were downloaded), and the total size of the export. Do not edit this tab.

You can limit the time that export requests are kept. See "Removing requests from the log" on page 112 for more information.

Removing requests from the log

The Purge_Document agent is used by the Export Search database to remove requests that are older than a certain number of days. The default removes requests that are more than 90 days old.

The agent can be scheduled to run as needed, but is usually run once daily (the default is set to run daily at 1:00 a.m.).

You can change the number of days that export requests are kept by editing the Agent Parameters document.

1. Using the Domino Administrator client, open the EAs-D Export Search database in the `hprim` folder on the mail server.
2. In the **View** menu, select **Go To**, and then select **Agent**.
3. Expand **Agent**, select **Parameters**, and then click **OK**.

   The Agent\Parameters view appears.
4. Double-click the document listed in PURGE_DOCUMENT.
5. Double-click the value in **Argt1: Number of Days** and change the number of days.

   Do not change the Form Name value in Argt2.
6. Click **File** > **Save**, and then close the document.
7. In the Designer client, schedule and enable the Purge_Document agent.

   Use the scheduling instructions in "Purging log entries" on page 44.

Using Local Cache

Local Cache is a client application that gives Windows-based Notes users offline access to their archived messages. It is most useful for employees traveling with a laptop or notebook computer.

When client machines are online, users can pull copies of archived messages 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.

Whether clients are online or offline, users have one-click access to messages stored in the cache. When they open a tombstoned message and click a pointer to retrieve the message, the cached copy of the content is displayed.

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.

NOTE:

Local Cache can be combined with a plug-in for no-click retrieval of messages. See "Using the Windows Notes Client Plug-In with Local Cache" on page 123.

During installation, Local Cache creates a database, `DefaultLCDestination.nsf`, in the client machine's `notes\data\mail` directory. The cache can be configured to set the message retention period, cache size, and other parameters.

Users might not have access to the most recent messages that have been archived, depending on how often you set the rissminer program and mining agents to run.

Installing Local Cache

The EAs Local Cache installer installs both the Local Cache (`LocalCache.exe`) and the Export Search (`ExportSearch.exe`) applications in a new Localcache folder that is created in the client's Notes directory.

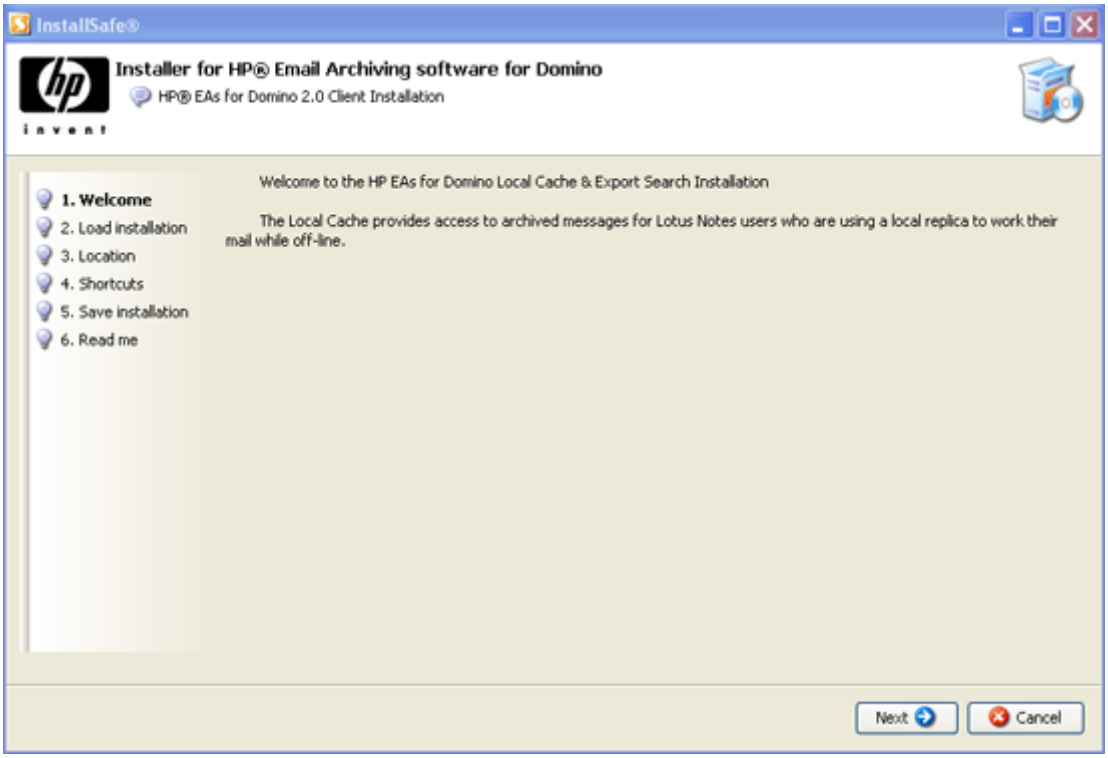
IMPORTANT:

Before you install the Local Cache software, ensure that Java Runtime Environment (version 1.6 or later) is installed on the machine. You might need to manually add the program to the system variables path.

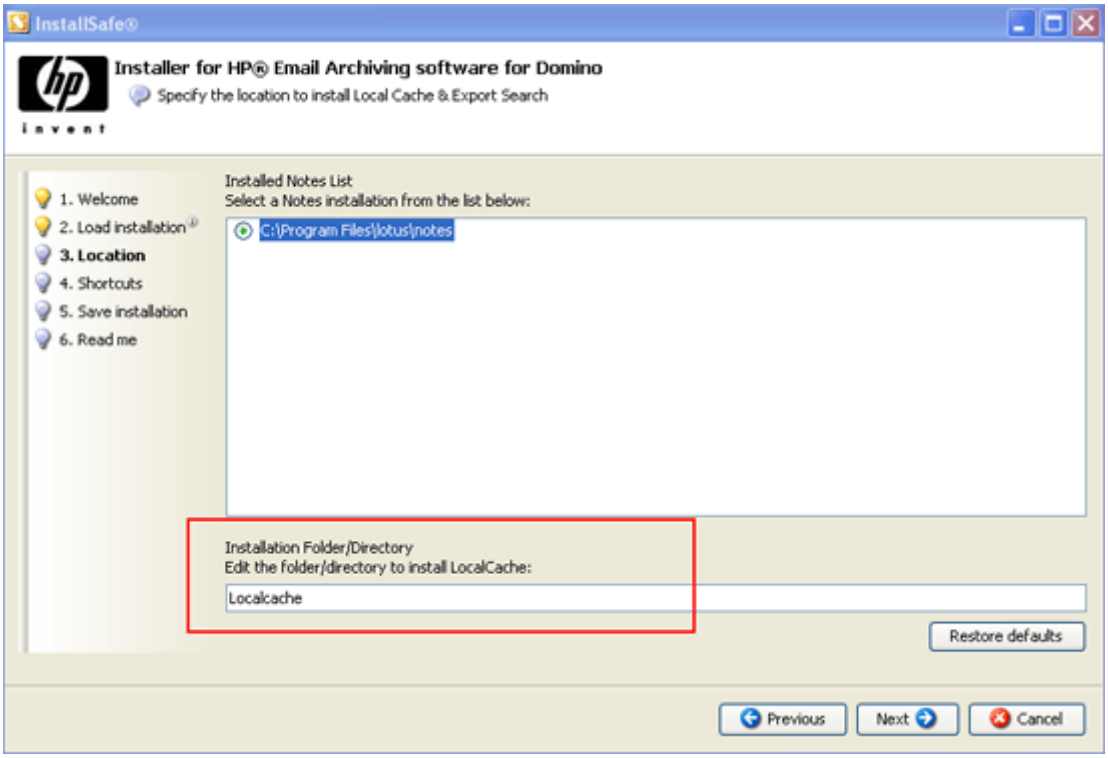
To install Local Cache on the client system:

1. Navigate to the `client\Local Cache & Export` directory on the installation CD and click **Install.exe**.
2. Click **Next** at the 1. Welcome window.
3. Click **Next** at the 2. Load installation window.

   The 3. Location window appears, showing the location of the Notes client.



4. In the Installation folder box, enter a name for the Local Cache folder.



5. Click **Next**.
6. In the 4. Shortcuts window, select a location (desktop or Start menu) if you want to create shortcuts to the Local Cache and Export Search applications.

7. In the 5. Save installation window, select whether to save the installation on the client.
   - If you choose to save the installation, select the **Save this installation** check box, and browse for a location in which to save the installation.
   - If you do not save the installation base, click **Next**.
8. Confirm the installation parameters in the install preview screen.

   If you need to make adjustments, use the Previous button or the sequence menu on the left side of the screen.
9. Click **Install**.

   The installation actions are displayed on screen.
10. Click **Finish** to close the installation window.

Configuring Local Cache

To configure Local Cache on the client system:

1. Double-click the HP EAs Local Cache shortcut on the client desktop or Start Menu, or `LocalCache.exe` in the `Lotus\Notes\[local cache]` folder.

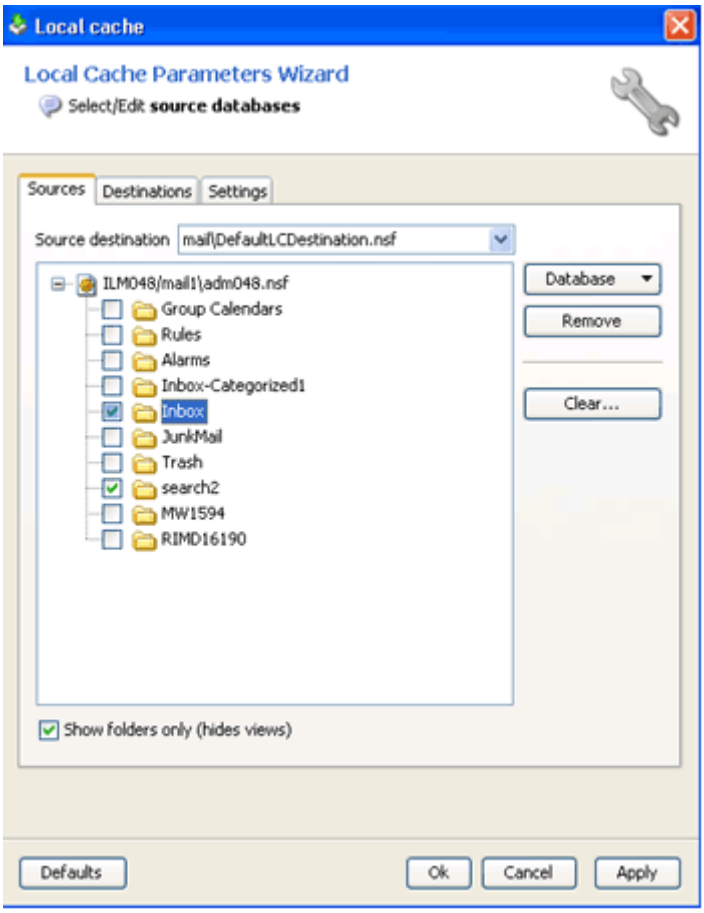
   The Local Cache Parameters Wizard appears.
2. On the **Sources** tab, click **Database**, select **Open**, and then select the source database (the user's live mail file on the server).

   A confirmation dialog appears.
3. In the Confirmation dialog box, click **Yes** to create a default cache database (the destination database) on the user's machine.
4. Enter the Notes password for the client.

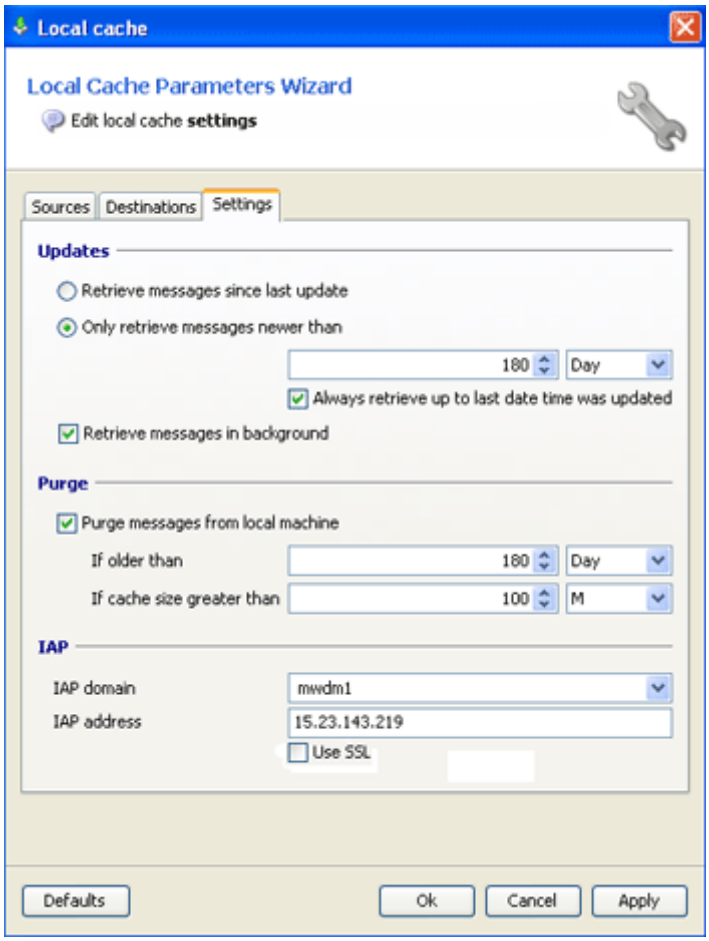
   The Local Cache database (`mail\DefaultLCDestination.nsf`) appears in the Source destination field on the Sources tab. This database also appears on the Destinations tab.

   This is the database used for caching archived messages that are retrieved from the IAP.
5. Expand the user's mail file.

6. Select the mail folder(s) where cached messages are stored, and then click **Apply**.



7. Click the **Settings** tab and configure the cache.



a. In the **Updates** area, select the age of the messages to be retrieved. The Local Cache retrieves and caches any archived message where the received date is more recent than the number of days specified.

To ensure a continuous flow of messages, select the **Always retrieve up to last date** check box.

b. In the **Purge** area, limit the scope and size of the cache. Select the **Purge messages from local machine** check box and enter a cutoff time and maximum cache size. Both options must be set.

The value in the **If older than** field is the maximum number of days that archived messages are kept in the cache. You can enter **0** to keep all archived messages that fall within the "older than" date range. You can enter **0** to keep all archived messages that fall within the maximum cache size.

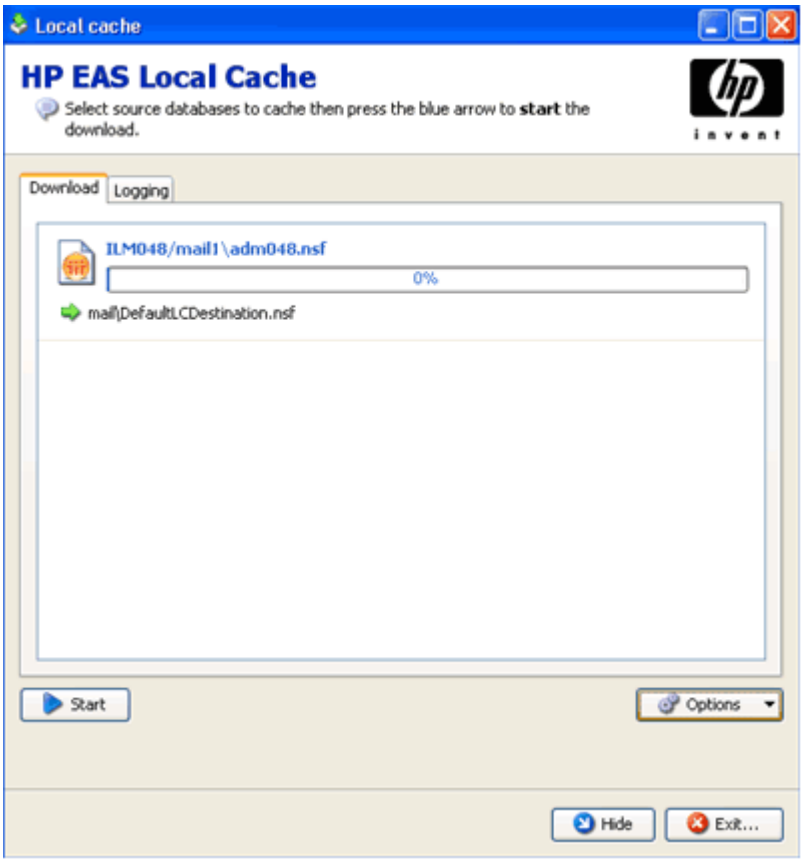
The cache size takes priority over the cutoff time. For example, if the age of the messages causes the cache to exceed the maximum size, messages are deleted in reverse chronological order until the size of the cache falls below the specified limit.

c. The IAP domain name and IAP IP address are automatically entered in the **IAP** area.

d. Make sure the **Use SSL** check box is not selected.

8. Click **OK**.

   The source and the destination databases appear on the Download tab.



9. To use Local Cache:

   a. Click **Start** to import the archived message copies into the cache.

   A log of the download results appears on the Logging tab. The log is stored in the `Localcache` directory that was created during installation.

   Log entries can be cleared or copied by using the icons at the top of the tab:

   - Clear specific types of log entries (summary, warning, error, etc.).
   - Clear a specific entry or entries.
   - Copy an entry or entries.
   - Clear all entries in the log.

   b. When the download is complete, click **Exit** to close Local Cache, or click **Hide** to keep Local Cache running in the background.

   If users choose to hide Local Cache, the icon remains in the system tray. Local Cache is closed automatically when you log out of Windows.

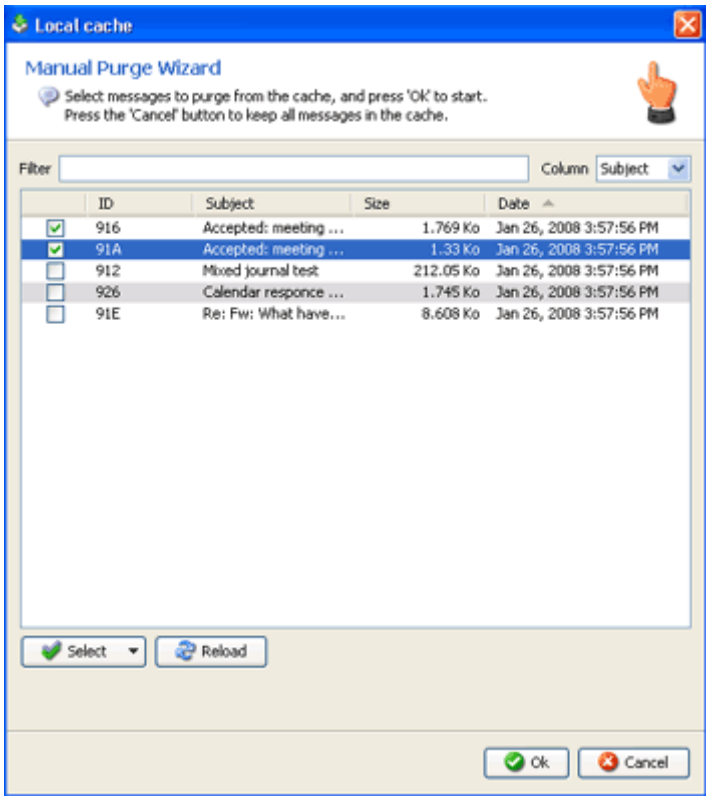
Deleting messages from the cache

When the cache size or time limit is exceeded, messages are automatically deleted from the cache in reverse chronological order.

Messages can be manually deleted from the cache by following these steps:

1. Double-click the Local Cache icon on the desktop or in the Start menu.
2. In the Local Cache window, click **Options** and then select **Manual Purge**.

   The Manual Purge wizard appears with the list of messages in the cache.



3. Use the Column drop-down list to filter the messages by date, size, subject, or ID, and then click **Reload** to refresh the message list.
4. Select the messages to delete, and then click **OK**.

   To delete all cached messages, click the **Select** drop-down list, select **All**, and then click **OK**.
5. Click **Exit** to exit the Local Cache window.

Uninstalling Local Cache

The `LocalCache.exe` and `ExportSearch.exe` files can be manually removed from a client system. However, after Local Cache is activated, tombstoned messages are marked with pointers to full messages copies held in the cache. Therefore, the Local Cache database (`mail\DefaultLCDestination.nsf`) and any other cache database that was created should not be removed.

Using the Windows Notes Client Plug-In

A plug-in can be installed on Windows clients to automatically retrieve tombstoned messages. The plug-in can be installed on its own or, for users traveling with a laptop, installed with Local Cache.

Users have instant access to their archived messages when the computer is online. When they select a message, its content appears automatically.

The process works in a somewhat different way when the plug-in is installed together with Local Cache. For more information, see "Using the Windows Notes Client Plug-In with Local Cache" on page 123.

NOTE:

Messages that are sent using the Phone Message form in Notes can be archived and tombstoned. When users view a tombstoned phone message via the plug-in, the message content appears twice. This is due to the way the plug-in merges data retrieved from the IAP with data stored in the tombstone. The message does not consume twice the storage space in IAP.

Configuring the plug-in installer

The plug-in is a DLL file that plugs into Windows Lotus Notes clients via standard API interfaces. It examines requests that the client makes to retrieve messages from the Domino server and redirects those requests to the IAP if the message has been archived.

The plug-in installer is an MSI file that installs the DLL on Windows client systems. It must be configured for your company's EAs Domino environment.

NOTE:

Building the MSI installer with the EAs configuration tool requires that the Microsoft .NET 2.0 (or later) framework is installed on your system. The .NET framework is not required on clients using the MSI to install the plug-in.

To configure the installer:

1. Copy the `MakeHpClientMSI` directory from the installation CD to your local hard drive.

   The directory contains the following items:

   - `BinMakeMsi` (folder)
   - `NhpClientMSI` (folder)
   - `NhpClientSourceMSI` (folder)
   - `MakenHpClientMSI.bat` (batch file)
2. Navigate to the `NhpClientSourceMSI` folder in the installation directory you created.
3. Open `variableInstallation.ini`.
4. Modify the following variables in the `variableInstallation.ini` file.

   These changes are incorporated into the client's `notes.ini` file when the installer is run.

Variable	Value
RISS_HOST_ADDRESS=	Change the sample IP address to the IP address of your IAP HTTP portal, or the DNS name that resolves to that IP address. Be sure to keep **=0** after the address so this variable is added to `notes.ini`.
HPCLIENT_FROM_DOMAINTOREMOVE=	This variable removes the extraneous FromDomain added to a message during archiving, so it does not appear when users create a reply to the message. Change the sample name to one or more Domino domain name(s). Separate multiple values with commas. Example of a single domain:`HP-CLIENT_FROM_DOMAINTOREMOVE=EASCPE@usa.hp.com` Example of multiple domains: `HP-CLIENT_FROM_DOMAINTOREMOVE=big-corp.com,AJG,EASCPE@usa.hp.com`, which removes any one of these three FromDomain values if they exist. Be sure to keep **=0** after the name(s).
HPCLIENT_HTTP_MAX_PLUGIN_FAIL-URE=	Message retrieval can fail if network connectivity is interrupted or if a message cannot be found on the IAP. This variable determines the number of failures before the plug-in is disabled. You can edit the default of 10 failures. The counter is reset when a message is retrieved successfully. Be sure to keep **=0** after the number of failures.
RISS_USE_HTTPS=	This variable determines whether the plug-in uses HTTPS (SSL) or HTTP to communicate with the RISS. Do not edit this entry. The value must be **0** to use regular HTTP to communicate with the IAP.
RISS_DOMAIN_NAME=	The name of the storage domain on the IAP. Change the sample name to your IAP domain name. Be sure to keep **=0** after the name.
HPRIMCLIENTVERSION=	Do not change this entry.
HPRIM_KEEP_ENCAP_FILE_DAYS=	Encapsulated, or encap, files are temporary files that process signed or encrypted messages. If you want to keep the encap files for a period of time, enter the number of days they should be kept. The default setting is 2 days.
HPRIM_KEEP_ALL_ENCAP_FILES=	• **0** keeps encap files for the amount of time specified in the `HPRIM_KEEP_ENCAP_FILE_DAYS=` variable. • **1** keeps all encap files indefinitely. (Not recommended.) Be sure to keep **=0** after the number of days.
HPRIM_REMOVE_ALL_ENCAP_FILES=	• **0** removes encap files after the number of days specified in the `HPRIM_KEEP_ENCAP_FILE_DAYS=` variable. • **1** forces the removal of all encap files at Notes shutdown or at the next startup. Be sure to keep **=0** after the entry.

Variable	Value
EXTMGR_ADDINS	This variable registers the plug-in with the Notes Extension Manager. Do not change this entry.
NOTES_PATH	Do not change this entry.
HPCLIENTEXCLUDE=localcache, taskldr=0	Do not change this entry. It appears when Local Cache is installed in addition to the plug-in.

A completed variableInstallation.ini file would look like this sample:

```
RISS_HOST_ADDRESS=15.1.1.1=0
HPCLIENT_FROM_DOMAINTOREMOVE=EASCPE@usa.hp.com=0
HPCLIENT_HTTP_MAX_PLUGIN_FAILURE=10=0
RISS_USE_HTTPS=0=0
RISS_DOMAIN_NAME=iapdomain=0
HPRIMCLIENTVERSION=1.6.2=0
HPRIM_KEEP_ENCAP_FILE_DAYS=2=0
HPRIM_KEEP_ALL_ENCAP_FILES=0=0
HPRIM_REMOVE_ALL_ENCAP_FILES=0=0
EXTMGR_ADDINS=nhpclient.dll=1
NOTES_PATH=D:\Lotus\Domino
HPCLIENTEXCLUDE=localcache, taskldr=0
```

5. Open languageInstallation.ini in the NhpClientSourceMSI folder.

   You can change or translate the text of any entry in this file, but **do not** delete any of the entries.

   The text appears in message prompts that are displayed when the installer is run.

6. Execute MakenHpClientMSI.bat to create the installer.

   The installer (NhpClient.msi) is placed in the NhpClientMsi folder in the MakeHpClientMSI directory. The file is now ready to be distributed.

Installing the plug-in

It is your responsibility to distribute or install the file on each client system.

When the plug-in is installed on the client:

- The plug-in file (nhpclient.dll) is placed in the client's Lotus Notes Program File directory.
- The HP EAs Domino – Notes Client Plug-in program is placed in the Control Panel program list (where it can also be uninstalled).
- The notes.ini file is updated with the values set in variableInstallation.ini.
- The installer is placed in the client's Windows\Installer directory.
- Users must restart their computers after the plug-in is installed.

The plug-in communicates with the IAP using the client's Microsoft Internet Explorer LAN settings.

Users can have another browser as the default. However, if a proxy or other special configuration is required for LAN connectivity to the IAP, the LAN settings must be configured in Internet Explorer.

Using the Windows Notes Client Plug-In with Local Cache

Windows clients can use the plug-in together with Local Cache for no-click access to archived messages.

The plug-in interacts with the cache in three ways:

- **Message is in the cache**: When users open a tombstoned message, the plug-in looks for a pointer to the message in the cache. If it is found, the plug-in it retrieves the message from the cache and automatically displays it for the user. This improves performance and reduces the load on the IAP.
- **Message is not in the cache and user is online**: When users open a tombstoned message that is not in Local Cache, the plug-in retrieves the message from the IAP and displays it for the user.
- **Message is not in the cache and user is offline**: When users open a tombstoned message that is not in the cache, they see text stating that the message has been archived. The message cannot be retrieved until the user is online.

NOTE:

Make sure that the `HPCLIENTEXCLUDE=localcache, taskldr=0` variable is listed in `notes.ini`. This variable is required for proper functionality when the plug-in and Local Cache are used together. It is added in `variableInstallation.ini` and executed when the plug-in installer is run. See "Configuring the plug-in installer" on page 120 for more information.

Adding the tombstone icon (optional)

Follow these optional steps to add the tombstone icon to the mail template(s). The tombstone icon signifies to users that messages have been archived.

The icon must be created using a Windows client.

1. Copy `ldapcomp.nsf` from the `Templates` folder on the EAs installation CD to the Notes data directory on the Notes client.
2. In the Designer client, open the Mail template and then open `ldapcomp.nsf`.
3. In the left-hand navigation pane of `ldapcomp.nsf`, expand **Shared Resources**, and then expand **Images**.
4. Copy `Tombstone.GIF` and paste it into the Mail template in **Shared Resources** > **Images**.
5. In the Mail template, select **Folders** from the left-hand navigation pane.
6. Double-click **($Inbox)** in the right-hand folder list.
7. Select the first **Who** column.
8. From the top menu bar, select **Create** > **Insert New Column**.
9. Below the Column Value heading, click the **Formula** radio button.
10. In the **Column Value** field, enter the following formula:

    ```
    @If(@Contains(HPTombstoned; "1" :  "2" :  "3"); "tombstone.gif"; 0)
    ```

    This makes the icon appear for any tombstoned message that is (1) archived, (2) in Local Cache without the Notes Client Plug-in, (3) in Local Cache with the Notes Client Plug-in).
11. Display the Properties dialog box for the column by selecting **File** > **Database** > **Properties**.
12. Change the column width to **1**, clear the **Resizable** check box, and select the **Display values as icons** check box.
13. Close the Properties dialog box. Press **Esc** and then click **Yes** to save.

Because columns are not shared across folders and views, every inherent folder and view within the Mail template must also be changed. Personal folders that are created prior to this change do not display the icon.

Retrieving and viewing encapsulated messages

Retrieving and opening encapsulated messages in Lotus Notes and DWA

Encrypted messages can be decrypted when users retrieve them in DWA or Notes. Signatures in signed messages can be validated if the original sender's certified public key is available in the Domino Directory or the recipient's Personal Address Book.

When users open a retrieved message in their Notes mailbox or DWA, the message is automatically unpacked from its encapsulated format and restored with 100% fidelity. Users can open and view the message as they would with any other message.

Opening encapsulated messages in the IAP Web Interface

- Users can view signed messages in the IAP Web Interface, provided they have the sender's public key.
- Users cannot view encrypted files in the Web Interface. They can, however, open encrypted messages if they export a copy of the message to their Notes mailbox.

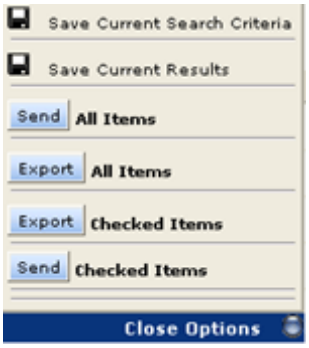
NOTE:

Body and attachment content of encrypted messages is not indexed by the IAP. Searches for these messages in the Web Interface can only be done on header content. Signed messages are fully indexed and their body and any attachments are searchable.

- Users can view calendar notices, tasks, and messages with ATT attachments in the IAP Web Interface.

Opening encapsulated messages

Encapsulated messages can be exported or sent from the IAP Web Interface to the user's mailbox. In the Web Interface, click **More Options** and select one of the Send or Export options in the options menu.



If messages are exported (see "Using Export Search" on page 107), encapsulated messages can be opened and viewed like any other message.

If they are sent (as Mail-To-Me messages), the following steps are required to open them:

1. In the Notes mailbox, double-click the attached file in the message.

   The attachment is the encapsulation database containing a single document, the original message.
2. Without attempting to open the document, copy it to the clipboard.
3. Navigate into an empty folder.

   (You can create a new folder if you want. Do not use the Drafts folder.)
4. Paste the document from the clipboard into the mail folder.

5. If the message is encrypted, switch to the user ID of the message recipient.

   If the message is signed, make sure the Domino Directory or the recipient's Personal Address Book contains a Person document with the certified public key of the sender.

6. Open the message from the folder.

Adding MS Office 2007 MIME type support to HP EAs Domino

Microsoft Office 2007 supports several new file extensions that its applications use on its data files. These file extensions must be mapped to MIME content types, so the IAP can index email file content correctly.

Domino servers ship with a File Identification table that provides mappings between file extensions and MIME types. However, IBM does not support Office 2007 in Domino 6.x and 7.x, and does not provide information about setting up the correct table entries. (See IBM technote 1258670: "Enhancement Request: Support for Microsoft Office 2007 with Lotus Notes.")

To update the File Identification table to support Office 2007 file extensions, follow these steps:

1. Using the Notes client, open the Domino Directory on the HP gateway server.
2. Navigate to the File Identifications view under **Configuration** > **Messaging**.
3. Click **Add File Identification** to open the File Identification document.
4. On the **File Identification** tab, complete the fields as follows:
   - **MIME type**: Enter **application**.
   - **MIME subtype**: Enter the first subtype from the table below.
   - **File extension**: Enter the first file extension from the table below.
   - **Description**: (Optional) Enter text appropriate to the file type.
   - **Outbound**: Select **Send**.
5. Click **Save & Close**.
6. Repeat steps 3–5 for each MIME type listed in the table below.

You might also want to create File Identification documents in the Domino Directory(ies) on your mail servers. This reserves the extension mappings and helps to prevent other software from applying default rules that could result in the mishandling of MS Office 2007 data.

Table 7 New MS Office 2007 MIME types

MIME type	MIME subtype	File extension
Application	vnd.ms-word.document.macroEnabled.12	.docm
Application	vnd.openxmlformats-officedocument.wordprocessingml.document	.docx
Application	vnd.ms-word.template.macroEnabled.12	.dotm
Application	vnd.openxmlformats-officedocument.wordprocessingml.template	.dotx
Application	vnd.ms-powerpoint.template.macroEnabled.12	.potm
Application	vnd.openxmlformats-officedocument.presentationml.template	.potx
Application	vnd.ms-powerpoint.slideshow.macroEnabled.12	.ppsm
Application	vnd.openxmlformats-officedocument.presentationml.slideshow	.ppsx
Application	vnd.ms-powerpoint.presentation.macroEnabled.12	.pptm
Application	vnd.openxmlformats-officedocument.presentationml.presentation	.pptx
Application	vnd.ms-excel.addin.macroEnabled.12	.xlam
Application	vnd.ms-excel.sheet.macroEnabled.12	.xlsm
Application	vnd.openxmlformats-officedocument.spreadsheetml.sheet	.xlsx
Application	vnd.ms-excel.template.macroEnabled.12	.xltm
Application	vnd.openxmlformats-officedocument.spreadsheetml.template	.xltx

10 Collecting held messages for HP technical support

The Get Held Messages Notes application recovers mail.box messages that are in the Hold or Dead state, so they can be used for IAP and EAs diagnostics.

After the application recovers a held message from mail.box, it resubmits the message to the router several times, giving it another chance to be delivered.

The number of retries can be configured. After the maximum number of retries, the message is saved in Get Held Messages and is not returned to mail.box.

During the IAP system installation, you will work with the HP service representative to set up the application. It is installed on the gateway server, which transfers messages from a Domino domain to the IAP system.

Using the application

The following steps should be taken after messages have accumulated:

1. In the Domino Administrator client, open the Get Held Messages database (`hprim\get_held_messages.nsf`) in the Domino data directory.
2. Examine the **Held Mail** views, looking for undeliverable messages that were found in mail.box.
3. In the File menu, select **Database** > **New Copy** to create a complete copy of the database.

   The copy of the Get Held Messages database can be sent to HP for diagnosis of the held messages.

After making a copy of the database, you can remove captured messages that you no longer want.

1. Make sure you are in one of the **Held Mail** views, or you will delete other documents.
2. Select messages for deletion by clicking them in the left margin.

   You can select several messages quickly by dragging the mouse in the left margin.
3. Press the **Delete** key to mark the selected messages for deletion.
4. Press **F9** or **Esc** to delete the messages.

As the mail capture agent runs, it writes various status messages to the server log file. You can view these messages by examining the Domino log (`log.nsf`) and looking for the string `Get Held Messages`.

11 Troubleshooting and performance improvement

This chapter explains how to troubleshoot HP EAs Domino and improve system performance.

- Preventing mail server instability, page 129
- Mining program shuts down, page 129
- JVM panic gc0 error, page 130
- Large Mail Detail log records, page 131
- Message attachments named ATTxxxxx, page 131
- Compacting databases, page 131
- Editing server configuration, page 132
- Monitoring the gateway, page 132
- Limiting the server log file size, page 133

Preventing mail server instability

To avoid problems with mail server instability, make sure the Agent Manager values and the JavaMaxHeap size value in `notes.ini` are set correctly. For more information, see "Editing the Agent Manager parameter values" on page 21 and "Setting the JavaMaxHeapSize" on page 22.

Mining program shuts down

If the Domino server crashes or the server is stopped while the rissminer program is running, a rissminer `<mining_rule_name_date_time_stamp>.lock` file is left behind. When the server is restarted, the presence of this lock file causes rissminer to shut down immediately.

To automatically detect and remove any existing lock files, create a program document in the Domino Directory for all servers running rissminer.

1. In the Domino Administrator client, click the **Configuration** tab.
2. Expand **Server** and select **All Server Documents**.

3. For each server running rissminer:
   a. Select the server in the right pane.
   b. Select **Create** > **Server** > **Program**.
   c. On the Basics tab, complete these fields:

Field	Description
Program name	Enter `cmd`
Command line	Enter `/c erase c:\lotus\domino\rissminer_*.lock` (where `c:\lotus\domino` is the Domino program directory)
Server to run on	The default is the current mail server. To change the server, click the arrow and select another server.
Enabled/disabled	Click the arrow and select **At server startup only**.

   d. Click **Save & Close**.
4. Restart the server.

You can also detect and remove any existing lock files by issuing the following command at the server console:

```
load cmd /c erase c:\lotus\domino\rissminer_*.lock
```

(where `c:\lotus\domino` is the Domino program directory)

JVM panic gc0 error

HP has identified a bug in the Domino 7.0.3 JVM used by Agent Manager that causes server instability and eventual crash with a JVM panic gc0 error message. Domino server 7.0.x versions above 7.0.3 might also have this problem.

The issue occurs when a Domino agent written in Java and containing a JAR file is run manually from the server console or from the Domino Administrator client. It applies to the following agents:

- Archive agent (in HP EAs-D reference databases)
- Tombstone agent (in HP EAs-D reference databases)
- Profile Agent (in HP EAs-D Users database)
- Export Search agent (in HP EAs-D Export Search database)
  Note that only the server-side Export tool is affected.

To avoid the problem, perform one of the following actions:

- Always schedule the EAs agents listed above.
- Apply the IBM Lotus hot fix for this issue by opening an incident report with IBM and requesting the fix for SPR #CJON7BR3CG.
- Upgrade to a more current version of Domino, for example, 8.0.1.

Large Mail Detail log records

An error occurs when Lotus Notes records store more than 64 KB of text, and the following message is displayed on screen:

```
Notes error:  Field is too large or View's column selection formulas are
too large.
```

This error can occur if the Purge Selective Archive Log agent is not scheduled and enabled or if the value for number of lines is set too high in the agent's Parameter document.

To avoid this error, see "Purge Selective Archive Log agent" on page 76.

Message attachments named ATTxxxxx

Lotus Notes and Domino store the name of every file attachment twice in the NSF representation of a message. The visible name, which users see displayed, is stored as part of the composite data (CD) records holding the rich text message body. A second copy of the name is stored in a $File item.

In most cases, these names are identical, but occasionally Domino creates a unique name (beginning with the letters ATT) for use in the $File item. This happens when two files with the same name are attached to the same message; it may also occur in other circumstances. The Domino router on the HP gateway server always uses the filename in the $File item when it converts a message for the IAP but, in cases like this, it results in loss of the original file name.

To prevent this situation from occurring, messages with ATT attachments are submitted to the EAs preprocessing database for encapsulation. This preserves the original filename intact.

To open a message with an ATT attachment, follow the steps in "Opening encapsulated messages" on page 124.

Compacting databases

The HP gateway server should be compacted periodically to save space.

1. In the Administrator client, click **Configuration**.
2. Click the expansion arrow by **Server**, then click **Programs**.
3. Click **Add Program**.
4. In the program name field, enter **ncompact.exe**.
5. In the command line, enter **-B**.
6. Adjust the schedule as needed.
7. Click **Save & Close**.

Editing server configuration

The following settings improve server performance. Add these settings to the `notes.ini` settings.

1. In the Administrator Client, click the **Configuration** tab.
2. Click the Server expansion arrow.
3. Click **Configurations**.
4. Double-click the existing server configuration document.
5. Click the **NOTES.INI Settings** tab.
6. Click **Edit Server Configuration,** click **Set Modify Parameters**, and add the following settings one at a time by selecting the drop-down box from Item.

NOTE:

Some items are not initially provided in the list.

- `log_mailrouting=0`
  Ensures router mail delivery and transfer messages are not logged on the server console.
- `RouterAllowConcurrentXferToAll=1`
  Allows multiple transfer threads between two servers in the same Notes Named Network (NNN), servers in different NNN, and two servers in different domains.
- `MaxMailMessageQueue=20000`
  Limits the number of messages the router queues for transferring, to prevent buffer overflows and out-of-memory errors.
- `MailLogToEventsOnly=1`
  Logs mail routing events in the `log.nsf` file, based on the logging level set in the server configuration document.
- `log_sessions=0`
  Ensures individual sessions are not logged on the server console.
- `no_force_activity_logging=1`
  Prevents automatic activity logging on all databases. Improves the performance of databases, but must be weighed against the need for database activity logging in a production environment.

Monitoring the gateway

The HP gateway server plays a critical role in transferring messages to the IAP archive. Under normal circumstances, transfers occur without incident, but in any complex network there is always the possibility that unanticipated problems can occur.

If undetected, a backup of messages on the gateway server can cause a backup of messages on the production mail servers. Therefore, it is important that you monitor the gateway server for problems.

Domino provides a variety of built-in monitoring tools that work on their own or in combination with network management products like HP OpenView. Domino's internal statistic monitors for Disk.C.Free, Mail.Dead, Mail.Hold. Mail.TotalFailures, and Mail.TotalPending are particularly useful indicators of the state of the gateway server.

Refer to IBM Lotus Software's Domino Administrator help topics "Monitoring the Domino system," "Creating a statistic event generator," and "Platform statistics." Also refer to equivalent documentation for any management products that are used in the network.

In addition, HP supplies the Get Held Messages application, which is useful for monitoring. For more information, see "Collecting held messages for HP technical support" on page 127.

Limiting the server log file size

It is possible to limit the server's log file size based on the age of log entries. This prevents the log file from growing too large.

1. In the Notes client, open the workspace.
2. Click **File** > **Database** > **Open**.
3. Select the gateway server and open the file `log.nsf`.
4. Close the new tab and return to the workspace.
5. Right-click the log icon, then click **Replication** > **Settings**.
6. Click **Space Savers**.
7. Select the **Remove documents not modified in the last __ days** check box.
8. Change the number of days.
9. Click **OK**.

A Indexed document and content types

- Indexed document types, page 135
- Message MIME types, page 135
- Additional indexing detail/limitations for Microsoft Office, page 137

Indexed document types

Users 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.

The following types of messages and 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 can be 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 8 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

File extension	File type	MIME type
.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.msppt
.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
.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

File extension	File type	MIME type
.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 9 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
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

Type	Feature	Office 97–2003	Office 2007
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 10 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

Type	Property	Microsoft Word, PowerPoint, and Excel
Advanced Properties: Summary	Title	Yes
	Subject	Yes
	Author	Yes
	Manager	No
	Company	No
	Category	Yes
	Keywords	Yes
	Comments	Yes
	Hyperlink base	No
	Template	No
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

Type	Property	Microsoft Word, PowerPoint, and Excel
Advanced Properties: Custom (continued)	Group	Yes
	Language	Yes
	Mailstop	Yes
	Office	Yes
	Owner	Yes
	Project	Yes
	Publisher	Yes
	Purpose	Yes
	Received from	Yes
	Recorded by	Yes
	Recorded date	Yes
	Reference	Yes
	Source	Yes
	Status	Yes
	Telephone number	Yes
	Typist	Yes

B Configuring the HP EAs-D Tools database

Domino native journaling cannot filter out messages that users send to themselves from the IAP Web Interface. Since these messages are already archived, the EAs agents skip them and leave them in the journal. EAs-D Tools provides an automated process for removing these Mail-to-Me messages from the journal mail-in database.

This appendix explains how to configure the HP EAs-D Tools database.

- Creating the database, page 141
- Configuring the database, page 142
- Enabling the cleanup agent, page 142

Creating the database

NOTE:

The HP EAs-D Tools database must be placed on the same server as the journal mail-in database, in a folder named `hprim` in the Domino data directory or notesdata directory.

Create the database from the Notes client:

1. Copy the HP EAs-D Tools template (`RIM_tools.ntf`) from the `templates` directory on the CD into the root data directory of your Notes client (for example, `C:\Lotus\Notes\Data`).
2. Start the Domino Administrator client, and switch to an ID file that has rights to create databases and run unrestricted agents on the mail servers.
3. In the **File** menu, select **Open Server**, and then select **Local**.
4. Click the **Files** tab and open the Notes data directory.
5. In the **Show me** box, select **Templates only**.
6. Select HP EAs-D Tools.
7. With the file selected:
   a. Right-click and select **Sign** from the context menu.
   b. Verify that **Active user's ID** and **All design documents** are selected in the dialog.
   c. Click **OK**.
8. Configure the database from the Notes client:
   a. Select **File** > **Database** > **New**.

      The New Database window appears.
   b. In the **Server** box, specify the relevant mail server. Enter the name of the server if it does not appear in the list.
   c. In the **Title** box, enter **HP EAs-D Tools**.
   d. In the **Filename** box, browse to and select the `hprim` folder, then enter the database filename: **RIM_tools.nsf**.

e. In the Template for New Database area of the window, select the server in the **Server** box, and then select the HP EAs-D Tools template in the scroll box.

f. Click **OK** and close the database's About page.

g. Select **File** > **Database** > **Access Control** and adjust the access control settings to make sure that:

- Default has no access to the database.
- LocalDomainAdmins have Manager access, with delete rights and all roles.
- LocalDomainServers have Designer access, with delete rights and all roles.
- The ID file that was used to sign the database (if not already in LocalDomainAdmins) has Designer access, with delete access and all roles.
  If the customer signs databases and agents with a server ID, make sure the server is in LocalDomainServers.

Configuring the database

To configure HP EAs-D Tools:

1. In the Domino Administrator client, open `rim_tools.nsf`.

   The Mail-to-Me Admin view appears.
2. Click the **Mail-to-Me Admin** action button, and select **New** to create a new administration document.
3. Enter or select the mail server to monitor.
4. Specify if the job should be enabled or disabled for scheduled processing.
5. Enter the name of the mail-in journal database on the server.
6. Select the appropriate cleanup action that the agent should perform:
   - Delete the Mail-To-Me messages
   - Move the messages to another database

   If you choose the Move option you must also specify the database to which the Mail-To-Me messages should be moved. This database must already exist and be on the same server as EAs-D Tools. It can be based on the mail template or use a template customized for your company.

Enabling the cleanup agent

Using the Designer client, enable the Email Miner MTM Cleanup agent in HP EAs-D Tools:

1. Open the HP EAs-D Tools database on the mail server.
2. In the Design pane, select **Shared Code** > **Agents** in the database.

   The Email Miner MTM Cleanup agent appears.
3. Double-click the agent name to open the agent. Click **OK** to bypass the warning.

   The Properties for Agent dialog box appears.
4. Click **Schedule** and ensure that **Any server** appears in the Where agent runs box.
5. Adjust the schedule if necessary.

   The default schedule is for the agent to run daily at 1 a.m.
6. Click **OK**.

7. Close the Agent Properties dialog box and the agent, and click **Enable** to enable the agent.

You can run the agent immediately from the server console by issuing the following command:

```
tell amgr run “rim_tools.nsf” ‘Email Miner MTM Cleanup’
```

To enable verbose logging, enter:

```
Set config HPRIM_DebugJournalCleanup=1
```

To disable verbose logging issue, enter:

```
Set config HPRIM_DebugJournalCleanup=0
```

C Creating reference and preprocessing databases

The reference and preprocessing databases should not be replicated during the software installation.

For each message processing server, create a new preprocessing database and corresponding reference database.

Function	Preprocessing database name	Reference database name
Selective archiving	`hp_preproc_miner.nsf`	`hprim/hp_riss_minerreferenc.nsf`
Compliance archiving	`hp_preproc_journal.nsf`	`hprim/hp_riss_journalreferenc.nsf`
Bulk upload	`hp_preproc_blk.nsf`	`hprim/hp_riss_blkupdreferenc.nsf`

- Creating a new preprocessing database , page 145
- Creating a new reference database, page 146

Creating a new preprocessing database

Several types of messages must be preprocessed so they can be archived in a format that preserves all message data intact. Preprocessing is performed in the preprocessing databases.

To create a new preprocessing database:

1. Copy the HP EAs-D PreProcess template (`hp_preproc.ntf`) from the `Templates` directory on the CD into the root data directory of your Notes client (for example, `C:\lotus\notes\data`).
2. Start the Domino Administrator client, and switch to an ID file that has rights to create databases and run unrestricted agents on the mail servers.
3. In the **File** menu, click **Open Server** and select **Local**.
4. Click the **Files** tab and open the Notes data directory.
5. In the Show me box, select **Templates only**.
6. Select HP EAs-D PreProcess (`hp_preproc.ntf`).
7. With the file selected:
   a. Right-click and select **Sign** from the context menu.
   b. Verify that **Active user's ID** and **All design documents** are selected in the dialog.
   c. Click **OK**.

8. Configure the database from the Notes client:
   a. Select **File** > **Database** > **New**.

      The New Database window appears.
   b. In the **Server** box, specify the relevant mail server. Enter the name of the server if it does not appear in the list.
   c. In the **Title** box, enter a name for the database. For example, HP EAs-D PreProcess (miner).
   d. In the **Filename** box, browse to and select the `hprim` folder, then enter the database filename. For example, `hp_preproc_miner.nsf`.
   e. In the Template for New Database area of the window, select the server in the **Server** box, and then select the HP EAs-D PreProcess template in the scroll box.
   f. Click **OK** and close the database's About page.
   g. Select **File** > **Database** > **Access Control** and adjust the access control settings to make sure that:
      - Default has no access to the database.
      - LocalDomainAdmins have Manager access, with delete rights and all roles.
      - LocalDomainServers have Designer access, with delete rights and all roles.
      - The ID file that was used to sign the database (if not in LocalDomainAdmins) has Designer access, with delete access and all roles.
        If the customer signs databases and agents with a server ID, make sure the server is in LocalDomainServers.

Creating a new reference database

The reference databases hold temporary references to the mined messages until the messages are sent to the IAP. Create a new mining, journaling, or bulk upload reference database (as needed) by following these steps:

1. Copy the HP EAs-D Reference template (`hp_riss_referenc.ntf`) from the `Templates` directory on the CD into the root data directory of your Notes client (for example, `C:\lotus\notes\data`).
2. Start the Domino Administrator client, and switch to an ID file that has rights to create databases and run unrestricted agents on the mail servers.
3. In the **File** menu, click **Open Server** and select **Local**.
4. Click the **Files** tab and open the Notes data directory.
5. In the **Show me** box, select **Templates only**.
6. Select HP EAs-D Reference (`hp_riss_referenc.ntf`).
7. With the file selected:
   a. Right-click and select **Sign** from the context menu.
   b. Verify that **Active user's ID** and **All design documents** are selected in the dialog.
   c. Click **OK**.

8. Configure the database from the Notes client:

   a. Select **File** > **Database** > **New**.

      The New Database window appears.

   b. In the **Server** box, specify the relevant mail server. Enter the name of the server if it does not appear in the list.

   c. In the **Title** box, enter a name for the database. For example, HP EAs-D Reference (mnr).

   d. In the **Filename** box, browse to and select the `hprim` folder, then enter the database filename. For example, `hp_riss_minerreferenc.nsf`.

   e. In the Template for New Database area of the window, select the server in the **Server** box, and then select the HP EAs-D Reference template in the scroll box.

   f. Click **OK** and close the database's About page.

   g. Select **File** > **Database** > **Access Control** and adjust the access control settings to make sure that:

      - Default has no access to the database.
      - LocalDomainAdmins have Manager access, with delete rights and all roles.
      - LocalDomainServers have Designer access, with delete rights and all roles.
      - The ID file that was used to sign the database (if not in LocalDomainAdmins) has Designer access, with delete access and all roles.
        If the customer signs databases and agents with a server ID, make sure the server is in LocalDomainServers.

D Account Synchronization

Account Synchronization in the IAP PCC is used to configure dynamic Account Synchronization (DAS), which automatically creates and updates email user accounts on the IAP. You can define multiple configurations that track sets of users from one or more LDAP servers for specific IAP domains.

The following topics are discussed in this appendix:

- Account Synchronization overview, page 149
- Creating and running DAS jobs, page 149
- Viewing DAS history logs, page 153

Account Synchronization overview

To open Account Synchronization, log on to the IAP PCC, and go to **User Management** > **Account Synchronization** in the left menu.

The Account Synchronization view is divided into three sections:

- The DAS Available Jobs section lists all jobs created and assigned to an HTTP portal.
- The LDAP Server Connectors section lists available LDAP connections.
- The Jobs History Logs section shows the history of DAS job runs.

Creating and running DAS jobs

Following are the basic steps for creating and running a DAS job:

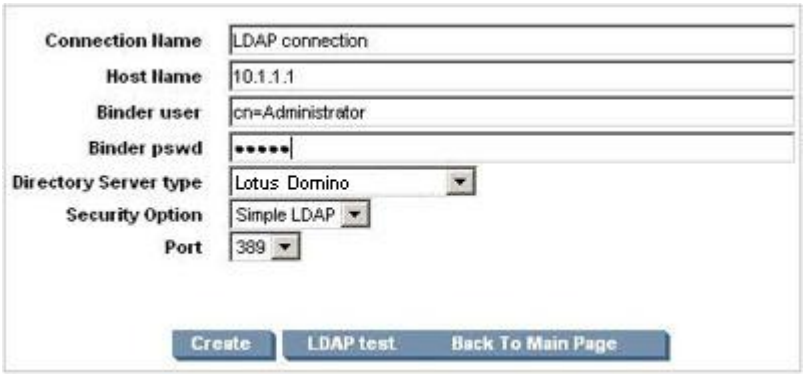
1. Create an LDAP connection. See "Creating LDAP server connections" on page 149.
2. Create the job. When you create a new job, you assign the job a name and an LDAP connection, and set up the job query in the LDAP server. See "Creating jobs" on page 150.
3. Assign the job to an HTTP portal. See "Assigning HTTP portals" on page 152.
4. Run the job. See "Starting, scheduling, and stopping DAS jobs" on page 152.

Creating LDAP server connections

To create an LDAP connection:

1. In the LDAP Server Connectors area, click **New LDAP**.

2. Complete the form to create an LDAP service connection by entering the following information:



Field	Description
Connection Name	Name used to identify the LDAP connection.
Hostname	IP address of the LDAP server.
Binder user	User in the LDAP directory tree that you want to bind to. At a minimum, the user must have read access to all users objects. For example: **cn=Administrator,cn=Users,dc=hostname,dc=com**.
Binder pswd	Password of the Binder user.
Directory Server type	Type of LDAP server to which you are connecting: **Lotus Domino**.
Security Option	Type of LDAP security: **Simple LDAP**.
Port	Opens LDAP port on the LDAP server. Use port **389** for simple authentication.

3. To test the LDAP server connection before creating it, click **LDAP test**.

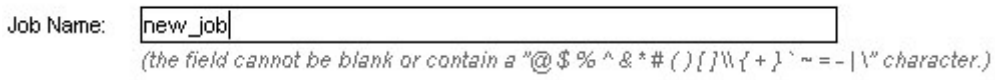
   A content pane displays the status of the LDAP connection. It tells you whether the connection and bind are successful and the authentication types that are supported by the LDAP server. Errors are displayed in red.

4. Click **Create**.
5. Return to the Account Synchronization view and verify that the new LDAP server connection is listed under LDAP Server Connectors.

Creating jobs

To create a DAS job:

1. In the DAS Available Jobs area, click **New JOB**.
2. Name the job you are creating by entering it in the **Job Name** box. Click **Next Step**.



3. From the drop-down list, select the LDAP connection you want to use with the job.

   If you need to create the LDAP connection, click **Create New LDAP Connection** and see "Creating LDAP server connections" on page 149 for further instructions.

4. Click **Next Step**.

5. Complete the form by entering the following information:

Field	Description
LDAP Domain name	Domain to which the users belong. For example: ldaptest.com.
LDAP Starting Point	Root node where the user accounts are stored. For Domino, leave this text box empty to mine all aggregated Domino domains.
IAP DomainID	The IAP domain ID (not the domain name) where users are synchronized with users on the LDAP server. This is the same as the domainID set in `Domain.jcml`.
Deletion Starting Point	The root node where deleted user objects are stored on the LDAP server. For Domino, ignore this box because it is not enabled.

6. To complete the advanced options, see "Mapping advanced options" on page 151.

Mapping advanced options

1. Click the Advanced Options icon ( ) to display the advanced options.
2. Complete the advanced options form by entering the following information:

Field	Description
Group Name	Not used at this time.
USNChanged	Active Directory's unique sequence number (USN). For Domino, ignore this box because it is not enabled.
Delete USNChanged	USN in deleted users directory. For Domino, ignore this box because it is not enabled.
NextRepID	IAP repository ID assigned to new users. DAS retrieves this value from the database, but you can use this feature to specify the repository ID for the first user inserted when DAS runs. For example, if you enter 67, the repository created and assigned for the first imported user is R0000067. You can use this feature if users already exist in the system or to reserve repository IDs for any reason. If you specify a value that is lower than an existing repository ID, DAS automatically changes the value to the next higher number. The default is set to 5.
Audit Repository	Do not change.
Update LDAP filter	Criteria to include or exclude specific users. For Domino, enter at least the minimum filter: **(objectclass=dominoPerson)(mail=*)**.
LDAP Query return attributes	List of return attributes. For Domino, use the following attributes: **uid,sn,modifytimestamp,createtimestamp,cn,givenName,mail,sn,dominouid,dominodn**. The user name is mapped to the Domino UID. The Domino Username attribute can contain multiple user names, but only the primary user name is imported to IAP.
Delete LDAP Filter	Criteria to include or exclude specific users in the LDAP deleted users directory. For Domino, ignore this box because it is not enabled.

3. Click **Next Step** to create the job.

4. To assign this job to an HTTP portal, click **Assign Job**.

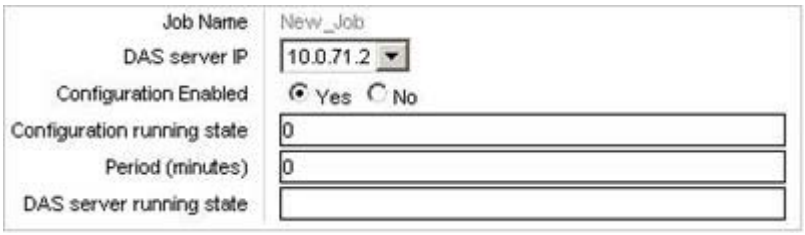
   See "Assigning HTTP portals" on page 152 for further instructions.

Assigning HTTP portals

Before running a DAS job, assign an HTTP portal on which to run the job. Only one job can be assigned to an HTTP portal. If all HTTP portals are being used, reassign the HTTP portal from another job.

To assign an HTTP portal to a job:

1. Click **Assign Job**.



2. Complete the form by entering the following information:

Field	Description
DAS server IP	IP of the DAS HTTP portal where DAS runs the configuration.
Configuration Enabled	Select **Yes** to enable. If not enabled, the job cannot be scheduled or started with this console.
Configuration running state	Do not change.
Period	Number of minutes between job runs. Enter **0** to run the job once.
DAS server running state	Do not change.

3. Click **Save**.

NOTE:

When assigning an HTTP portal to Domino, copy the file `/opt/DAS/runtime/LoadChangesDomino.dse` to `/opt/DAS/runtime/LoadChanges.dse` before running the job.

Starting, scheduling, and stopping DAS jobs

1. In the DAS Available Jobs view, select the job.
2. To start the job without making changes to the schedule, click **Start**.
3. To make a change to the schedule before starting the job:
   a. Click **Schedule**.
   b. Enter the number of minutes between job runs. To run a job once, enter **0**. Otherwise, the DAS schedule should not be set for anything less than 60 minutes, as running DAS jobs too close together can cause problems.
   c. Click **Confirm Schedule** to save your changes.
   d. To launch the selected job, click **Start**.

   A notice appears stating that the job started successfully.
4. Click **Back to Main Page** to return to the DAS view.

To stop a DAS job:

1. In the DAS Available Jobs view, select the job and click **Start/Stop**.

   A notice appears stating that the job has stopped.

2. Click **Back to Main Page** to return to the DAS view.

Viewing DAS history logs

The DAS jobs history log provides a list of job runs for each configured active job. The log includes the job name; the number of IAP users that were added, deleted, and updated; the time between job runs; the job status; and the date and time the job was completed.

To display the history log, scroll down to the **Jobs History Log** area at the bottom of the Account Synchronization view.

To display a history of the previous runs for a specific DAS job, click the job name.

To check the status of a job, view the icon in the **State** column. For example, the icon indicates the job is complete. You can also point to the icon to display the status.

Index

Symbols

.ics notices, 61

A

Account Synchronization
  See DAS
Account Synchronization view, 149
advanced filtering, 79, 85
Agent Manager, recommended options, 21
Archive agent, 71, 83, 92
archive document size limitations, 61
archive references, viewing, 40
archive traffic, 67
archiving instructions, 55
ATT attachments, 131
attachments, message, 61, 124
audience, 9

B

bulk upload
  defined, 91
  discover database, 92
  forcing owner, 93
  mining files, 93
  profile, 91
  running query, 92

C

calendar notices, 79
character set support, 16
clustering, 20
collecting held or dead messages, Lotus Notes, 127
compliance, 79, 109, 109
compliance archiving, 79
  instructions, 82
  mail-in journal, 62
  recommendations, 80
compliance, filtered, 63, 85
  See also advanced filtering
conventions
  text symbols, 10

D

DAS
  assigning HTTP portals, 152
  configuring, 149
  creating and running jobs, 149
  LDAP server connection, 149
  scheduling jobs, 152
databases, compacting, 131
debugging options, 35, 40, 53
distribution lists, expanding, 29
DLD download file
  associating with Export Search, 107
document conventions, 10
Domino
  releases supported, 14
  server configuration, 20, 132
  server requirements, 14
DWA Extension, 34
  cache retention, 26
  configuration steps, 47
  Server Definition document, 49
  server definition settings, 27, 34
  tombstone conversion, 54
  Tombstone Prototype document, 51, 66
  tombstone settings, 53, 66

E

EAs Domino
  Agent Manager values, 21
  compliance archiving, 79
  configuring, 23
  defined, 13
  EAs–D Tools database, 141
  Global Configuration document, 24
  opening, 23
  preprocessing databases, 36, 145
  reference databases, 146
  selective archiving, 55
  server definition document, 27
EAs-D API main view, 23
EAs-D Tools database, 141
EAs-D Users database, 73
EASWEB agent, 47
email distribution lists, expanding, 29
Encapsulate agent, 72, 83, 92
encapsulated files, 72, 121, 124, 131
  temporary work area, 37
  temporary work area for DWA, 34
encapsulated messages, 35
Encapsulation Tools, 41
encrypted messages, 48, 49, 79, 88, 121, 124

EnsureOwnerReceipt, 29
exception settings, 60
Export Search, 105, 107, 107, 109, 109
  using the client to extract messages, 107
  using the server to extract messages, 109, 109
extracting exported messages from DLD file, 110

F

File Identification mapping, 125
filtered compliance, 63
Find Parent tool, 41
folder settings, 59

G

gateway server
  compacting databases, 131
  configuring, 20
  Get Held Messages, 127
  monitoring, 132
Global Configuration document, 24

H

held or dead messages, 127, 132
help, obtaining, 11
HP
  storage Web site, 11
  Subscriber's choice Web site, 11
  technical support, 11
HP_ReferenceInfo, 64
HP_SessionInfo, 64
HTTP portals, assigning, 152

I

IAP
  defined, 13
  requirements, 14
IAP Web Interface, 105
  creating link in Lotus Notes, 106
  defined, 105
  exporting messages, 105, 107
  supported browsers, 16
  viewing signed and encrypted messages, 124
iCal format, 61
improving EAs Domino performance, 129
indexed documents
  Microsoft Office, 135, 137
  types, 135, 137
installation guide, 9
installing
  EAs software, 21
  Local Cache, 113
  software on gateway server, 20
  Windows Notes Client plug-in, 120

J

Java Runtime Environment, 113
JavaMaxHeapSize, 22, 109, 109
journaling, 79
  EAs Domino, 79
  EAs Domino (advanced filtering), 85
  EAs journal database, 79, 88
  enabling mining agents, 71
  enabling preprocessing agent, 72
  exceptions, 87, 87
  incoming messages, 86
  instructions, 82
  mail-in database, 88
  messages, maximum size, 79
  native Domino, 79
  outgoing messages, 86
  preprocessing files, 41
  preprocessing messages, 35
  recommendations, 80
  rules, 25, 25, 85, 88, 89
  schedule, 69, 83
JVM panic gc0 error, 130

L

large distribution lists, 29
LDAP server connection, 149
LDAP servers
  configuring DAS, 149
Local Cache, 105, 107, 107, 120, 123
  configuring, 115
  defined, 113
  installing, 113
  SSL support, 117
local mining, 19
log files, 25, 41
  purging mining entries, 44
Lotus Notes
  archive databases, 75
  collecting held or dead messages, 127
Lotus Notes clients
  adding tombstone icon, 123
  creating link to IAP Web Interface, 106
  EAs Domino applications, 105
  exporting messages from IAP Web Interface, 107, 109, 109
  Local Cache, 113
  retrieving signed and encrypted messages, 124
  supported versions, 16
  Windows Notes Client Plug-in with Local Cache, 123
  Windows plug-in, 120

M

Mail Detail records, 73, 73, 74, 84, 91
mail-in database, 62, 79, 84, 88
Mail-To-Me messages, 80, 87, 141
mail.box, 89

mailboxes, user, 73, 74
memory problems, avoiding, 22, 109
message processing servers, defined, 19
messages, maximum size, 55, 61, 79
MIME Content-Type indexing, 135
mining agents, 71, 83
mining job, 69, 83
  running, 77
mining log, 25, 41
mining rules, editing, 71
MS Office 2007 MIME type support, 125
MTM Cleanup agent, 142
mwadvt task, 89

N

Notes 64 KB error, 76, 131

O

on demand archiving, 59
operating systems supported, 14

P

partitioning, 20
PCC
  Account Synchronization view, 149
  description, 14
pending transactions, 41
performance, improving, 129
  compacting databases, 131
  editing server configuration, 132
  limiting server log size, 133
  monitoring gateway server, 132
permissions, 21
phone message form, 120
PKI encryption, 124
platforms supported, 14
Preprocessing Control document, 36, 92
preprocessing databases, 35, 36, 145
preprocessing temporary directory, 36
Profile Agent, 63, 73, 74
program document, editing, 71
program document, rissminer, 69
Proxy Gateway document, 49
Purge Not Synchronized person document agent, 76
Purge Selective Archive Log agent, 76, 131
purging export requests, 112

R

reference databases, 35, 40, 64, 71, 83, 91, 146
related documentation, 9
remote mining, 19
Reset Status tool, 41
rissminer program, 69, 91

S

S/MIME encryption, 124
selective archiving
  adding users to profile, 73
  archive traffic, 67
  archiving dates, 58, 82
  configuring, 55
  creating profile, 56
  document size limitations, 61
  editing profile, 71
  enabling mining agents, 71, 83
  enabling preprocessing agent, 72
  error alert, 68
  exceptions, 60
  folder settings, 59
  instructions, 55
  log files, 25, 41
  message attachments, 61
  messages, maximum size, 55
  on demand archiving, 59
  preprocessing files, 41
  preprocessing messages, 35
  profile, 62, 82, 91
  Profile Agent, 73
  Purge Not Synchronized person document agent, 76
  Purge Selective Archive Log agent, 76, 131
  reference database, 40, 64, 71
  running job, 77
  scheduling jobs, 69, 83
  synchronizing users, 74
  Time Conditions, 58, 82
  User Activity Alert agent, 75
  user mailboxes, 73
  user notification, 68
  user profile, 62
  viewing archiving references, 40
server configuration, editing, 132
server crashes, avoiding, 21, 22, 129, 130
server definition document, 49
  debugging options, 35
server ID, 20
servers
  DAS, configuring, 149
  Domino, configuring, 20
session settings, 67
session size, 33, 39
signed and encrypted messages, 34, 35
signed messages, 121, 124
single sign-on
  configuring EAs Domino files, 95
  configuring on the IAP, 102
  Generate SSO Tokens agent, 96
  Search the IAP Archive agent, 99
  secret key lost when IAP kickstarted, 102
Subscriber's choice, HP, 11
symbols in text, 10
synchronizing users, 74
system architecture, 18
system prerequisites, 14

system requirements, 14

T

technical support
  HP, 11
text symbols, 10
Tombstone agent, 71
tombstone icon, 123
tombstone settings, 65
traffic, archive, 67
troubleshooting, 129
troubleshooting tools, 35, 41

U

User Activity Alert agent, 75
user database agents, 75
user guide, 9
users
  PCC management, 149
Users database, 73

W

Web sites
  HP documentation, 11
  HP storage, 11
  HP Subscriber's choice, 11
wildcards, 63, 63, 86, 87
Windows Notes Client Plug-in, 105, 120
  configuring, 120
  phone message form, 120
Windows Notes Client Plug-in with Local Cache, 123
Windows users, 113, 123