

HP Email Archiving software for IBM Lotus Domino Version 2.1

Installation and Administration Guide

Covers installation, configuration, and administration of HP EAs Domino through version 2.1.2.



Legal and notice information

© Copyright 2007, 2012 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

- 1 HP EAs Domino overview 15
 - 1.1 Introduction 17
 - Prerequisites for installation 17
 - HP Integrated Archive Platform and archiving software 17
 - HP EAs Domino terminology 18
 - 1.2 Lotus Domino architecture and supported configurations 21
 - Lotus Domino network architecture 21
 - The HP Gateway server 21
 - HP EAs Domino configurations 23
 - How HP EAs Domino works with an organization's current system and configuration 23
 - Mining configurations 24
 - Active Gateway configuration 25
 - Dedicated journal server configuration 26
 - Replicated journal configuration 27
 - Scalable multi-Gateway deployment 28
 - Other HP EAs Domino configurations 29
 - Advanced Filtering 29
 - DWA Extension configuration 30
 - Export Search configuration 31
 - Bulk Upload configuration 32
 - 1.3 System requirements 35
 - IAP requirements 35
 - Customer Domino server requirements 35
 - Supported operating systems and Lotus Domino versions 35
 - HP Gateway servers 35
 - Customer servers 36
 - Supported Lotus Notes clients 38
 - IAP Web Interface 38
 - Export Search Web Interface 39
 - Supported character sets 40- 2 Installation 41
 - 2.1 Preparing the HP Gateway environment 43
 - Installing the Windows software on the HP Gateway server 43
 - Synchronizing the date and time 44
 - Installing Lotus Domino server software on the HP Gateway server 44
 - Creating an organizational unit certifier 44
 - Installing the Lotus Domino server software 44

Installing the update (version 8.5.2 only)	45
Running the Lotus Domino server setup program on the master server	45
Running the Domino server	47
Installing the Lotus Notes client software	48
Installing Java Runtime Environment	48
Installing additional HP Gateway servers	49
Registering additional HP Gateway servers	49
Running the Lotus Domino server setup program on additional HP Gateway servers	51
Creating Server Connection documents	52
Backing up Notes IDs and the Domino Directory	53
2.2 Configuring the HP Gateway servers	55
Adding the HP Gateway domain to the Domino Administrator client	55
Setting up security on the HP Gateway server	56
Editing the Agent Manager parameter values	57
Creating connection documents to the customer mail servers	57
Creating and configuring the foreign SMTP domain document	58
Creating and configuring the SMTP connection document	59
Creating a configuration document for the HP Gateway server	59
Limiting the log file size	60
Adding the EAsD_Domain parameter	61
2.3 Configuring the customer's Domino mail domain	63
Granting access for the HP Gateway servers	63
Configure trusted servers	63
2.4 Introducing the HP EAs Domino software	65
HP EAs Domino databases	65
HP EAs Domino database templates	66
HP EAs Domino database access	67
HP Gateway servers	67
Customer servers	70
HP EAs Domino notes.ini entries	73
Entries on HP Gateway servers	73
Entries on customer servers	74
HP EAs Domino binaries	74
2.5 Installing the HP EAs Domino software on the master HP Gateway server	77
Before installing the software	77
Installing the HP EAs Domino software	77
Setting access control (ACL)	80
2.6 Preparing the HP Gateway server for DAS	81
Introduction	81
Changes to the DAS process	81
Building a consolidated directory	83
Scheduling the Directory Cataloger task	86
Creating and configuring the Directory Assistance database	86
Configuring the pointer	88
Verifying the LDAP configuration	88
Editing the DAS Names Configuration document	89

Directory Information	89
Directory Fields	90
Directory Entry Settings	91
Group Cache settings	95
Logging settings	95
Configuring the HP EAs-D DAS Names database	95
Setting the ACL for DAS Names	95
Enabling the Populate DAS Names agent	96
Restarting the server	96
Rebuilding views in the DAS-related databases	97
Configuring the DAS backup servers	97

2.7 Configuring additional HP Gateway servers 99

Configuration steps	99
Deploying the archiving installation to additional HP Gateway servers	100

2.8 Installing HP EAs Domino components in the customer environment 103

2.9 Upgrading or migrating an HP EAs Domino installation 105

Upgrading to remote mining from a local mining installation	106
Overview	106
Upgrade instructions	106
Upgrading to a remote mining installation	106
Shutting down local mining	109
Upgrading an existing remote mining installation	110
Upgrading from EAs Domino 2.0.x to version 2.1.2	110
Introduction	110
Upgrade instructions	110
Upgrading from EAs Domino 2.1 or 2.1.1 to version 2.1.2	117
Introduction	117
Upgrade instructions	118
Upgrading HP EAs Domino components on customer servers	123
Introduction	123
Upgrade instructions	124
Replacing existing HP Gateway hardware	127
Overview	127
Migration instructions	127

2.10 Uninstalling the HP EAs Domino software 131

Uninstalling the HP EAs Domino software	131
Windows servers	131
Linux, Solaris, and AIX	132
Removing Domino configuration files	134
End user client systems	134
IAP	134

3 Configuring the HP EAs Domino environment 135

3.1 HP EAs-D API main view 137

3.2 Editing the Global Configuration document 139

Introduction	139
Configuring the settings	140
General Settings tab	140
Additional Modules tab	141
Address Conversion Settings tab (global)	141
SMTP Alias tab	141
Multiple Domino Domain and Multiple Domino Domain (Group) tabs	142
Agent Settings tab	142
Profile Agent	142
Archive Agent	142
Message Reprocessing	142
DWA Index Settings tab	144
Error Messages tab	145
Administration Alert tab	145

3.3 Configuring the Server Definition document 147

Introduction	147
Configuring the settings	148
Server Settings tab	148
Archiving Options tab	149
Address Conversion Settings tab	151
Profile Agent Settings tab	151
Execution Settings tab	151
Session Settings	151
Program Control	152
DWA Settings tab	153
Gateway Server tab	154
Logging tab	155
Administration Alert tab	156

4 Archiving email to the IAP 157

4.1 Configuring selective archiving 159

The selective archiving process	159
Configuring mining rules	160
Time Conditions tab	161
Folders Settings tab	162
Exceptions Settings	163
Special Fields	163
Attachments & Doc size tab	164
Other Macro Formula tab	165
User Membership tab	165
Defining wildcard patterns	167
Reference Database tab	167
Tombstone Settings tab	168
Session Settings tab	170
Reference Limits	171
Session Limits	171
Archive Strategy	171
User Notification tab	172
Administration Alert tab	173

4.2 Preprocessing messages	175
Preprocessing overview	175
Types of encapsulation	175
Retrieving encapsulated messages	176
Preprocessing steps	176
Configuring the Preprocessing Control document	177
Databases Location tab	178
Encapsulation Settings tab	179
Agent Log Settings tab	180
Execution Settings tab	181
Logging tab	182
Scheduling and enabling the preprocessing agents	182
4.3 Configuring the archiving agents	185
Working with the Profile Agent	185
Viewing Mail Detail documents	185
Scheduling the Profile Agent	187
Enabling other HP EAs-D User agents	187
Statistics User Activity Alert agent	187
Scheduling the agent	187
Editing agent values	188
Purge Not Synchronized person document agent	188
Purge Stats Selective Archive Log agent	189
When to activate the activity log	189
Reducing the amount of text in the log	189
Enabling the preprocessing agents	190
Configuring Get Held Messages	190
Scheduling and enabling the archiving agents	191
4.4 Running an archiving job	193
Scheduling the archiving job	193
Additional program documents	195
Running an archiving job manually	195
Viewing reference documents	198
4.5 Configuring compliance (journal) archiving	201
Configuring the mail server for compliance archiving	201
Advanced Filtering installation	202
Installing the Advanced Filtering module	202
Creating the mail-in journal database	204
Setting the permissions for other Advanced Filtering databases	205
Creating the Mail-In Database document	205
Creating journaling rules (Advanced Filtering)	206
Traffic Definition tab	207
Sender/Receiver Exceptions tab	208
Content Exceptions tab	208
Journal Database tab	209
Rules Status tab	209
Editing journal rules (Advanced Filtering)	210
Lotus Domino native journaling	211
Creating the mail-in journal database	211
Configuring the Advanced Inbound Message Options	213
Enabling journaling	214

Removing Mail-To-Me messages from the journal	215
Configuring Advanced Filtering and Domino native journaling on the same server	217
Archiving journaled messages	217
Configuring the journal mining rule	218
Adding a journal user	220
Editing the Preprocessing Control document	221
Enabling the preprocessing and archiving agents	221
Scheduling the compliance archiving job	221

4.6 Using Bulk Upload 223

Installing the Bulk Upload software	223
Installing the local Bulk Upload files	223
Setting the ACL for the local files	224
Installing the Bulk Upload files on the HP Gateway server	225
The Bulk Upload process	226
Editing the Bulk Upload mining rule	226
Editing the Preprocessing Control document	226
Enabling the agents	227
Scanning the mail files	227
Discovering a mail file owner	228
Reviewing the Mail Detail records	228
Replicating the Bulk Upload database	229
Archiving the mail files	229

4.7 Working with log files 231

HP EAs-D Log database	231
Viewing log files	231
Purging log entries	236

4.8 Event monitoring and alerts 239

Monitoring events	239
Monitoring Event document	240
Event actions	241
Default monitoring events: Configuration issues	241
Configuration issues: Alerts are generated and processing stops	242
Configuration issues: Alerts are not generated but processing stops	242
Configuration issues: Alerts are generated but processing continues	242
Configuration issues: Alerts are not generated and processing continues	243
Default monitoring events: Archiving issues	243
Archiving: Alerts are generated and processing stops	243
Archiving: Alerts are generated but processing continues	243
Archiving: Alerts are not generated and processing continues	244
Alerts	245
The HP EAs-D Alert database	245
Removing documents from the HP EAs-D Alert database	247

4.9 Archiving statistics 249

Configuring and enabling statistics collection	249
Viewing statistics in the HP EAs-D Stats database	249
Removing documents from the HP EAs-D Stats database	251

5 Retrieving email from the IAP 253

5.1 Configuring DWA Extension	255
Introduction	255
Installing DWA Extension	256
Installation on the DWA/proxy server	256
Installation on the HP Gateway server	257
Setting ACL for DWA Extension	258
Setting up IAP SSO with DWA	258
DWA Extension configuration steps	259
Configuration steps on the DWA/proxy server	259
Configuration steps on the HP Gateway server	259
Configuring the Proxy Gateway document (optional)	260
Configuring the Tombstone Prototype document	261
Editing the Tombstone Settings tab	266
Removing conversion requests from the HP EAs-D SC Request database	267
Adding the Agent\Parameters document	268
5.2 Using Export Search	269
Introduction	269
Using the Export Search Desktop tool to export messages	269
Saving query results	271
Using the server to export messages	272
Installing server-side Export Search	272
Setting ACL for Export Search	273
Using the Lotus Notes client to export messages	275
Exporting the messages	275
Extracting the messages	275
Editing or rerunning an export request	279
Using the Export Search Web Interface to export messages	279
Configuring the Export Search documents	280
Creating the Export Search request	280
Running the Export Search agents	285
Export Search agent	285
PopulateFolderFiles agent	285
Removing requests from the Export Search log	285
Scheduling the Export Search agents	286
5.3 Configuring IAP single sign-on	289
Creating the HP EAs-D SSO database	289
Configuring the HP EAs-D SSO database and the Generate SSO Tokens agent	290
Configuring the Search The IAP Archive agent	294
The implementation process	295
Copying design elements from the template	295
Modifying the Search The IAP Archive agent	296
Configuring SSO on the IAP	297
Installing the secret key	297
Modifying the username mapping	298
Configuring the client computers	298
5.4 Working with HP EAs Domino client applications	299
Using the IAP Web Interface	299
Creating a link in the Notes navigation pane	300
Creating a link to the Web Interface	300
Setting up single sign-on	301

Using Local Cache	301
Installing Local Cache	302
Configuring Local Cache	303
Deleting messages from the cache	307
Uninstalling Local Cache	307
Using the Windows Notes Client Plug-In	308
Configuring the plug-in installer	308
Installing the plug-in	311
Uninstalling the plug-in	311
Using the Windows Notes Client Plug-In with Local Cache	311
Adding the tombstone icon	312
Retrieving and viewing encapsulated messages	313
Retrieving and opening encapsulated messages in Lotus Notes and DWA	313
Opening and viewing encapsulated messages in the IAP Web Interface	314
Opening encapsulated messages in Lotus Notes	314

6 Troubleshooting and performance improvement 315

6.1 Troubleshooting 317

Capturing data for HP support	317
Information to collect	317
Processing held messages	317
Message reprocessing rules	318
Collecting held messages for HP support	319
Reference database troubleshooting tools	320
Preventing server instability	320
Mail routing issues	320
Checking mail backup	320
Messages in Hold or Dead state	320
Consolidating mail.box files	321
No route found from HP Gateway server to mail server	321
HP Gateway server not allowed to access Domino mail server	321
HP Gateway server not allowed to access mail file	321
No route found from HP Gateway server to IAP	321
Low priority messages remain in router on HP Gateway	321
Domino debug parameters	322
Dynamic Account Synchronization (DAS) issues	322
Problems copying data from customer Domino Directories to HP Gateway consolidated directory	322
DAS does not load users	322
User already exists in the IAP	325
Users deleted from the Domino Directory are not deleted in the IAP	325
User cannot log on to the IAP Web Interface	325
Archiving issues	326
Archiving tasks not executing	326
Email is not correct	327
“Unable to open index table of Mail Details records” error	327
Replication/save conflicts in HP EAs-D Users database	327
Message attachments named ATTxxxxx	327
Incorrect content-type	328
Message retrieval issues	328
Message retrieval error in DWA	328
NullPointerException error in DWA	328
The recipient's Internet Address is not displayed in the IAP Web Interface	329

SendTo address is incorrect when replying to a Mail-To-Me message	330
Troubleshooting the Notes client plug-in	330
Content appears twice in phone messages	331
Error opening meeting request in Lotus Notes	331
Troubleshooting Export Search (desktop tool)	331
Verifying the file type	331
Creating a file type association	331
Changing the file type association	332
6.2 Performance improvement	335
Compacting databases	335
Editing the HP Gateway server configuration	335
Monitoring the HP Gateway server	336
7 Appendices	337
A Pre-installation worksheets	339
Customer information	339
IAP information	340
HP Gateway environment	341
Domino servers to be mined	343
HP EAs Domino features (Domino servers)	344
HP EAs Domino features (client systems)	345
B Post-installation checklists	347
Installation: Master HP Gateway server	347
Installation: Additional HP Gateway servers	348
Configuration: Email archiving	348
C Software upgrade checklist	351
D Creating and updating HP EAs Domino applications	353
Creating reference and preprocessing applications	353
Creating new EAs Domino applications	353
Refreshing the design of EAs Domino applications	354
Replacing the design of EAs Domino applications	355
E HP EAs Domino scheduled agents	357
F HP EAs Domino settings for Japanese data	361
Email storage formats	361
ISO-2022-JP and Hankaku-Kana characters	361
Changing the HP Gateway server configuration document	362
G IAP configuration	365
Setting LNM	365
Disabling folder support	365
Creating a repository for Clean Envelop encapsulated messages	365
Default LDAP attribute mapping	365
Directory Integration	366

Enabling the Integrated Directory features on the IAP	366
Confirming success	367
Disabling the Integrated Directory features	369
Troubleshooting	370
Account security	370
Creating and running DAS jobs	371
Creating LDAP server connections	371
Creating DAS jobs	372
Assigning HTTP portals	374
Assigning a portal	374
Unassigning and reassigning a portal	376
Starting, scheduling, and stopping DAS jobs	376
Editing or deleting jobs	377
Managing available HTTP portals	378
Editing or deleting available LDAP connections	378
Viewing DAS history logs	378

H Indexed file types and MIME types 381

I Support and other resources 383

Related documentation	383
Additional information	383
Support	383
Subscription service	384
Document conventions and symbols	384

Index 385

Figures

- 1 HP Gateway Domino domain 22
- 2 Remote mining with Active Gateway 25
- 3 Remote mining with dedicated journal server 26
- 4 Remote mining with replicated journal 27
- 5 Scalable Active Gateway deployment 28
- 6 Advanced Filtering configuration 30
- 7 DWA Extension configuration 31
- 8 Export Search on a client system 31
- 9 Export Search on a Lotus Domino server 32
- 10 Bulk Upload configuration 33

Tables

1 IAP and EAs Domino applications for administrators	18
2 IAP and EAs Domino applications for users	18
3 Supported platforms and Domino versions on customer servers: Archiving	36
4 Supported platforms and Domino versions on customer servers: Other EAs Domino applications	37
5 Browser support	38
6 IAP character set support	40
7 ACL for EAs Domino databases on HP Gateway servers	67
8 ACL for EAs Domino databases on customer servers	70
9 HP EAs Domino binaries	74
10 EAs Domino upgrade and migration scenarios	105
11 EAs Domino scheduled agents	357
12 IAP indexed file types and MIME types	381
13 Document conventions	384

Part 1. HP EAs Domino overview

- [Introduction](#), page 17
- [Lotus Domino architecture and supported configurations](#), page 21
- [System requirements](#), page 35

1.1 Introduction

- [Prerequisites for installation](#), page 17
- [HP Integrated Archive Platform and archiving software](#), page 17
- [HP EAs Domino terminology](#), page 18

HP Email Archiving software for IBM Lotus Domino (EAs Domino) is a scalable and flexible archiving solution for Lotus Notes email messages. This guide helps you to complete an EAs Domino installation and configure and administer the archiving software. This guide should be used in conjunction with the *HP Integrated Archive Platform Installation Guide* and the *HP Integrated Archive Platform Administrator Guide*.

Prerequisites for installation

Prerequisites for installing this product include:

- Knowledge of IBM Lotus Domino and Lotus Notes
- Completing the IAP/EAs Domino training
- Reading through this guide, the IAP installation guide, and the IAP administrator guide
- Ensuring that the customer site meets the minimum installation requirements
See "[System requirements](#)" on page 35.
- Completing the EAs Domino installation checklists
See "[Installation worksheets](#)" on page 339.
- Referring to the release notes or readme for any last minute announcements

HP Integrated Archive Platform and archiving software

The HP Integrated Archive Platform (IAP) is a fault-tolerant, secure system of hardware and software that archives email messages and attachments for an organization, and gives users access to their archived messages. The IAP provides the following major functions:

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

HP Email Archiving software for IBM Lotus Domino (EAs Domino) is management and configuration software that is supplied with the IAP.

The following tools allow HP service representatives and Domino administrators to configure, administer, and troubleshoot the system.

Table 1 IAP and EAs Domino applications for administrators

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

Administrators, compliance officers, and users can access the following applications to interact with the system.

Table 2 IAP and EAs Domino applications for users

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

HP EAs Domino terminology

The following HP EAs Domino terms are used in this manual:

Integrated Archive Platform (IAP)

The archiving system. It combines HP server and grid storage technology, native content indexing, and search and policy management software into a single, factory-assembled rack system.

HP EAs Domino

Email archiving software for IBM Lotus Domino that integrates with the IAP.

Repositories

Email and email attachments are archived in repositories. A repository is a virtual collection of documents that are associated with a given user by routing rules (for storing documents) and access control lists (for retrieving documents). Users can search for archived messages only in the repositories to which they have access.

HP Gateway server

The central component between the Domino mail domain and the IAP. It mines messages from the Lotus Domino mail databases and journals, converts them to RFC 822 MIME format, and then routes them to user repositories on the IAP.

HP Gateway domain

HP Gateway servers are part of the HP Gateway Domino domain, which is separate from the customer's Domino mail domain.

Remote mining

The mining of mail databases on Lotus Domino mail or journal servers is performed remotely from the HP Gateway servers.

Compliance archiving

Compliance archiving, also known as journal mining, is the archiving of journal databases for legal or regulatory purposes.

Advanced Filtering

In EAs Domino, messages can be journaled in one of two ways: using native Domino journaling rules or using rules defined in the EAs Domino software. The EAs Domino journaling process is known as Advanced Filtering.

Selective archiving

Selective archiving, also known as email mining, is the archiving of mail files to reduce the amount of primary storage on mail servers. In the EAs Domino software, you can customize the rules that define which messages are archived; for example, messages older than a given number of days or mailboxes larger than a given size.

tombstone

Messages go through a *tombstoning* process after they have been archived to the IAP. In this process, one of several actions can occur after archiving: retain the message in the mail file; delete the message from the mail file; or replace the message with a link, or *tombstone*, to the archived message on the IAP. In compliance archiving, the tombstoning process deletes a message from the journal after it has been successfully archived. In selective archiving, an archived message is usually replaced with a tombstone.

Bulk Upload

The software that identifies mail file ownership for uploading messages to the IAP. Used primarily for the inactive mail files of former employees.

DWA Extension

The software that supports the retrieval of archived messages within Domino Web Access (iNotes).

rissminer

The EAs Domino mining executable program.

hprim

The folder in the Domino data directory that contains the HP EAs Domino databases.

HP EAs-D API

The main configuration database, which contains configuration documents, mining rules, journaling rules (if Advanced Filtering is used), and other configuration options.

HP EAs-D Users

The database containing the mail records of users whose mail files are being mined.

reference databases

Reference databases contain the EAs Domino mining agents and references to the messages that have been mined. There are separate reference databases for selective archiving, compliance archiving, and Bulk Upload.

preprocessing databases

Several types of messages, including signed and encrypted messages, must be encapsulated so they can be archived in a format that preserves all message data intact. This process is performed by an agent in the preprocessing database. There are separate preprocessing databases for selective archiving, compliance archiving, and Bulk Upload.

Dynamic Account Synchronization (DAS)

DAS is the IAP process that creates and updates IAP user or group accounts with information from the Domino Directory Person and Mail-In documents.

HP EAs-D DAS Names database

The EAs Domino database with the data used by DAS to create and update user accounts on the IAP.

1.2 Lotus Domino architecture and supported configurations

- [Lotus Domino network architecture](#), page 21
- [The HP Gateway server](#), page 21
- [HP EAs Domino configurations](#), page 23

Lotus Domino network architecture

Figure 1 on the following page depicts a typical Domino hub and spoke network configuration without clustered mail servers. The HP Gateway servers are deployed in their own Domino domain.

The HP Gateway server

The HP Gateway server is the central component between an organization's mail environment and the IAP. One or more HP Gateway servers can be installed. These servers reside in their own Domino domain, the HP Gateway domain, which is separate from the Domino mail domain.

When there are multiple HP Gateway servers, one Gateway acts as the “master” for the other Gateway servers. The master is the Gateway server used for DAS. At least one other Gateway server should be designated as a DAS backup server.

The main configuration database (HP EAs-D API) and user database (HP EAs-D Users) are replicated from the master to the other Gateway servers. Several EAs Domino databases, including the reference databases that contain the archiving agents, are unique (non-replicating) on each HP Gateway server.

HP Gateway servers perform three major functions:

1. Synchronization: Allow for synchronization of Domino Directory data with user repositories on the IAP.
2. Archiving:
 - Run the EAs Domino mining program and agents to evaluate and execute mining rules.
 - Mine mail files and journals in the Domino mail domain.
3. Message conversion and delivery:
 - Convert Notes native data and Rich Text format to RFC 822 MIME format.
 - Route the converted email to the IAP via Lotus Domino SMTP.

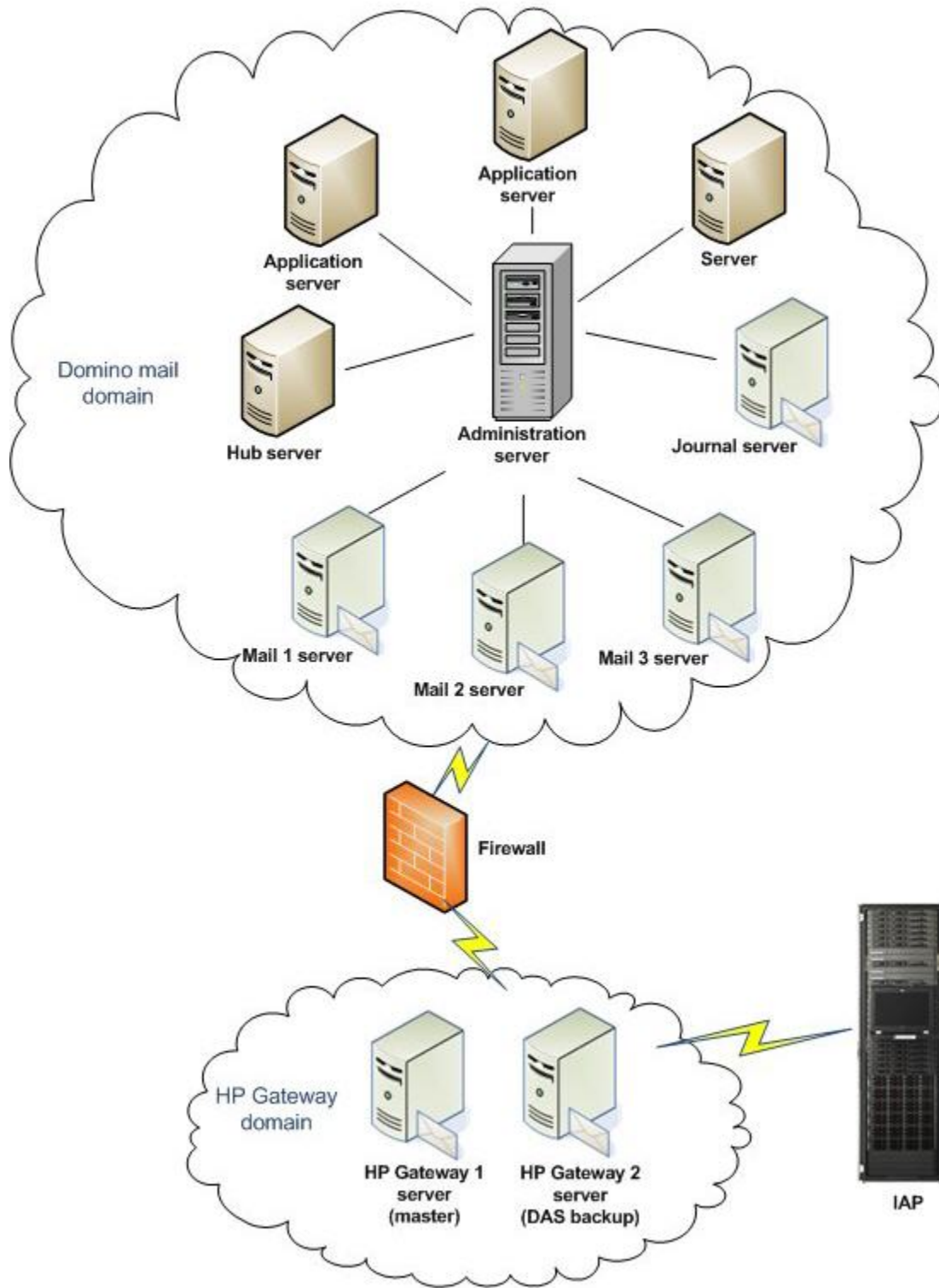


Figure 1 HP Gateway Domino domain

HP EAs Domino configurations

In EAs Domino 2.1, the mining of an organization's journals and mail files is performed from an HP Gateway server. The archiving software is installed on the Gateway server. Supported mining configurations are described in "[Mining configurations](#)" on page 24.

Several optional EAs Domino features require some EAs Domino software to be installed on servers in the organization's Domino mail domain. These configurations are described in "[Other HP EAs Domino configurations](#)" on page 29.

How HP EAs Domino works with an organization's current system and configuration

- In a clustered environment, when the home server for a mail file or journal is not available, mining continues on an alternate server in the cluster.
- Partitioning has no effect on EAs Domino.
- Shared mail has no effect on EAs Domino.
- The HP Gateway servers are in a separate Domino domain from the customer's mail domain, and have their own separate consolidated Domino Directory.
- A database is installed on the HP Gateway server(s) that contains copies of information pulled from the organization's Domino Directories. This database is read during the DAS process (synchronization with the IAP user accounts). It is only used by the HP Gateway servers and is completely separate from any Domino Directories in the customer's mail domain. EAs Domino does not update the Domino Directories in a customer's mail domain.
- Any mail template that is supplied by Lotus is functional with EAs Domino. Customized mail templates that add functionality to the standard Lotus Notes mail template can interfere with EAs Domino operations. 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.

EAs Domino does provide some optional customizations of the standard mail template to improve the end user experience.

Mining configurations

HP EAs Domino supports several deployment options to mine mail files and journals. Each of the options described in this section use *remote mining*, in which the mining functions are executed from the HP Gateway servers rather than the Domino mail servers.

The choice of mining deployment depends on many factors, including:

- The volume of messages
- The physical location of the organization's Domino mail or journal servers
- Bandwidth between the HP Gateway servers and the Domino mail or journal servers
- Domino server clustering

The following configurations can be used for remote mining:

- [Active Gateway configuration](#), page 25
- [Dedicated journal server configuration](#), page 26
- [Replicated journal configuration](#), page 27
- [Scalable multi-Gateway deployment](#), page 28

Software installation and configuration

The archiving executable (rissminer) is installed in the Domino program directory on the HP Gateway server.

EAs Domino databases are installed into an `hprim` folder in the Domino data directory on the HP Gateway server.

The procedure to install the EAs Domino archiving software on HP Gateway servers is described in “[Installing the HP EAs Domino software on the master HP Gateway server](#)” on page 77 and “[Deploying the archiving installation to additional HP Gateway servers](#)” on page 100.

The procedures to configure and administer the archiving software are described in “[Configuring the HP EAs Domino environment](#)” on page 135 and “[Archiving email to the IAP](#)” on page 157.

Active Gateway configuration

In an Active Gateway configuration, an HP Gateway server performs both the mining and the message conversion and routing functions. Messages are mined from journal and/or mail files on the customer's Domino mail servers.

Active Gateway servers require trusted server access to the customer's Domino servers, so the EAs Domino software can access mail journals and user mail files with standard Notes API calls via the Notes Remote Procedure Call protocol (standard NRPC traffic over port 1352).

Active Gateway servers must be granted permission to access the Domino user mail files and journals.

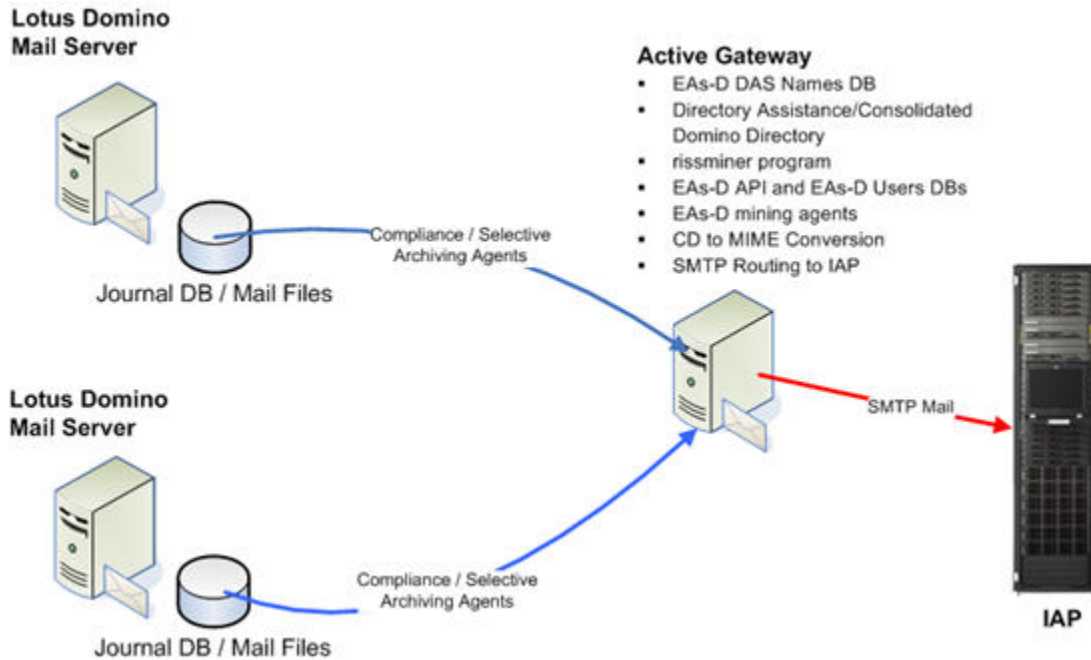


Figure 2 Remote mining with Active Gateway

Dedicated journal server configuration

This configuration supports the mining of a journal server—a dedicated server in the organization's Domino mail domain on which multiple journal databases reside.

An Active Gateway server archives the messages that are journaled and routes the messages to the IAP. (The Gateway server can also selectively archive mail files on the Domino mail servers, as shown in the scenario below.)

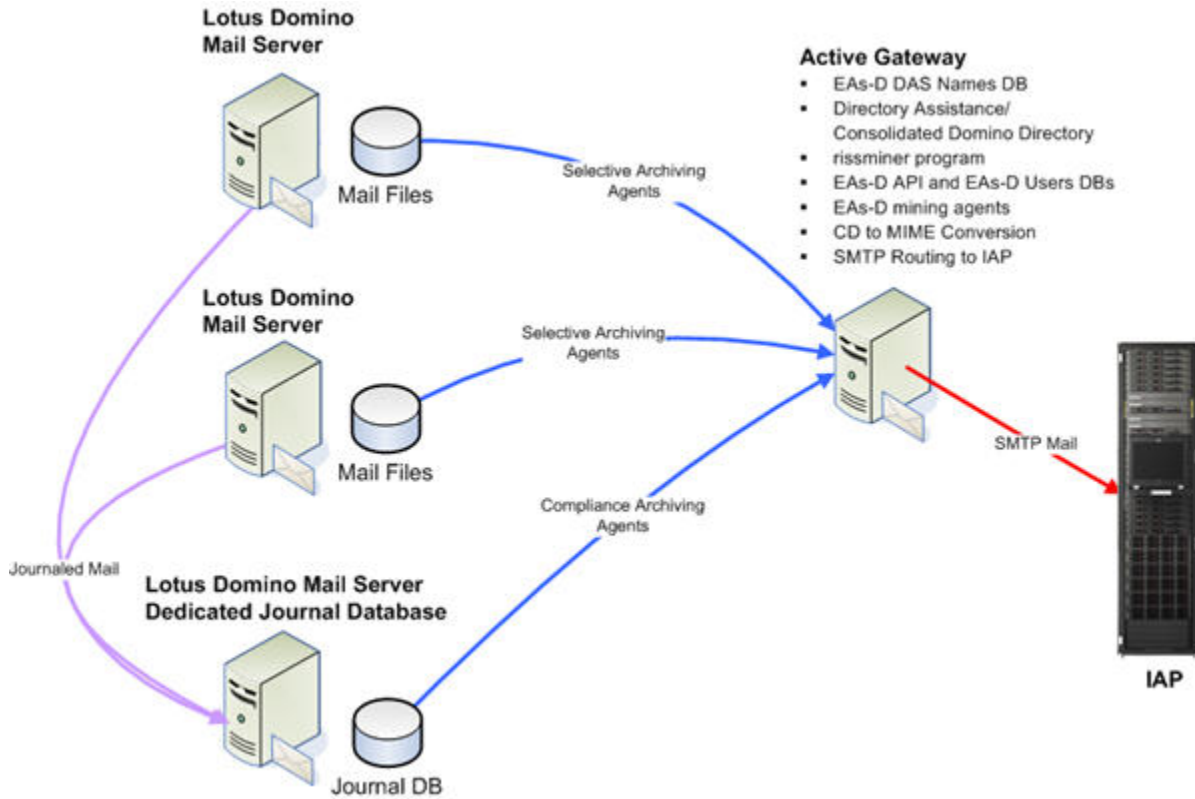


Figure 3 Remote mining with dedicated journal server

Replicated journal configuration

In this configuration, Domino servers that are located outside the data center and have limited bandwidth or other constraints replicate their journal databases to a Domino server inside the data center. Standard Domino connection documents are configured for bi-directional replication. An HP Gateway server archives the messages from these replicated journal databases, while Domino replication transfers the deletion stubs generated by the tombstoning process back to the source server.

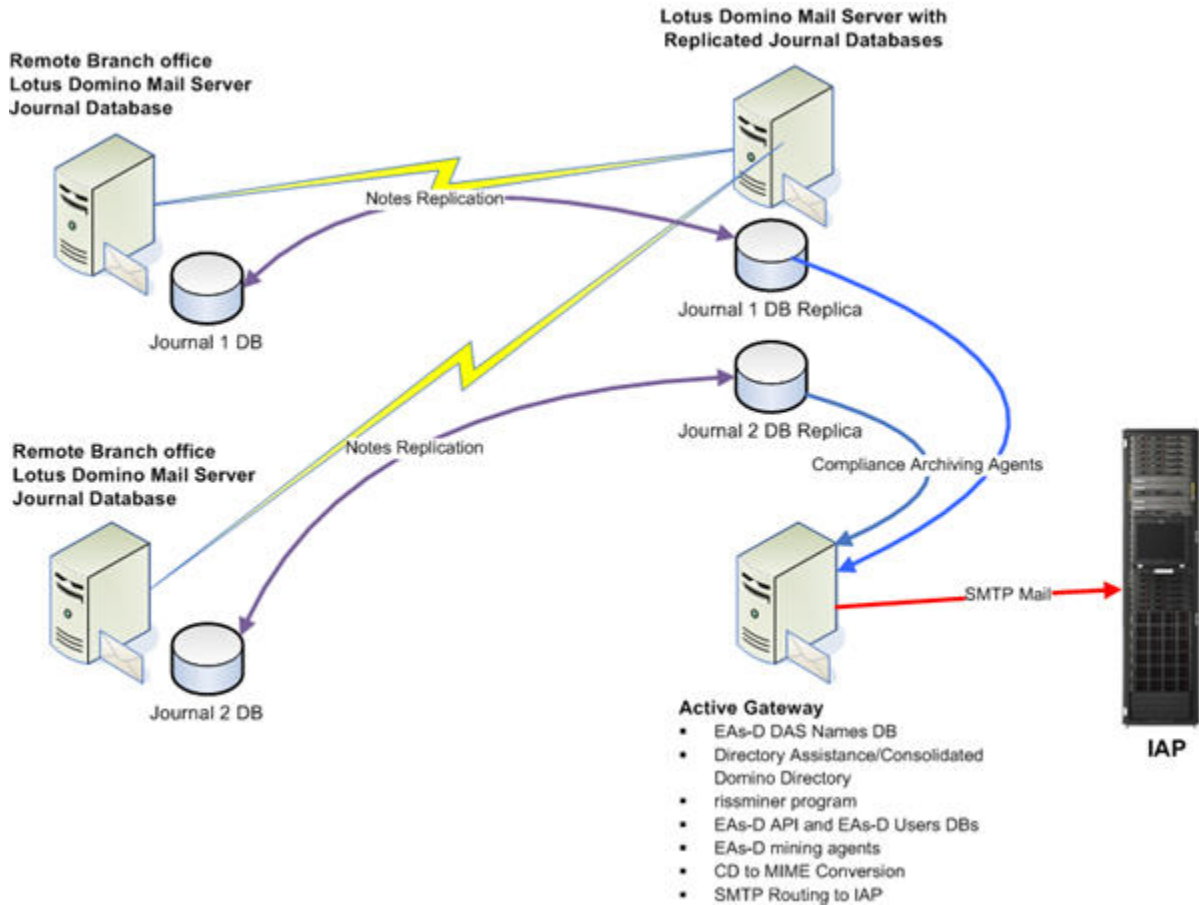


Figure 4 Remote mining with replicated journal

! **IMPORTANT:**

Under no circumstances should a journal database be created directly on an HP Gateway server, unless it is a replica of a database that is maintained on a customer server.

Scalable multi-Gateway deployment

HP Gateway servers can meet the requirements of an enterprise deployment by dedicating servers for specific tasks. In the scenario illustrated below:

- A Domino server is dedicated for journaling. All mail servers journal their email to one or more mail-in journal databases on this server. An Active Gateway mines the messages from the dedicated journal server.
- Two other Active Gateways selectively mine the user mail files on the Domino mail servers.

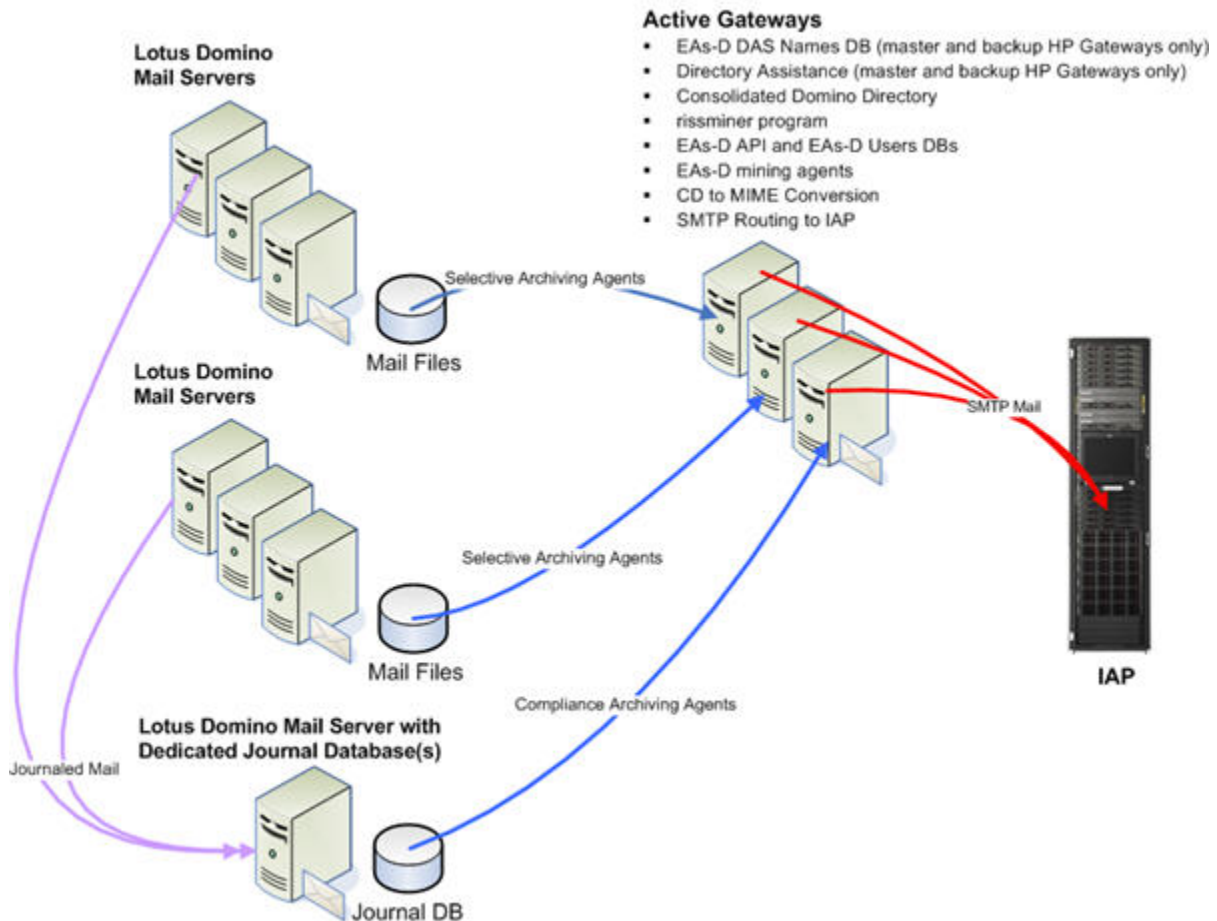


Figure 5 Scalable Active Gateway deployment

Other HP EAs Domino configurations

If any of these optional EAs Domino features are implemented, some EAs Domino software is installed on server(s) in the organization's mail environment:

- [Advanced Filtering](#), page 29
- [DWA Extension configuration](#), page 30
- [Export Search configuration](#), page 31
- [Bulk Upload configuration](#), page 32

① IMPORTANT:

The configuration database (HP EAs-D API) must be installed for all these optional features. This instance of HP EAs-D API is unique to the organization's mail environment, and is totally separate from the HP EAs-D API instance used in the HP Gateway domain. The database should be replicated between the customer servers that run any of these optional EAs Domino configurations.

Advanced Filtering

HP EAs Domino archives messages that are journaled using:

- **Native Domino journaling**
This is the method provided with the Lotus Domino software. When it is enabled, all messages that pass through the Domino router are copied to the journal.
- **Advanced Filtering (HP EAs Domino journaling)**
Advanced Filtering can be used to journal messages instead of native Domino journaling. This method captures only messages that meet the journaling rules defined in EAs Domino. For example, Advanced Filtering is capable of capturing messages that are sent or received by organizational units or specific users.
When Advanced Filtering is used, a journaling rules filter, a listening agent, and the HP EAs-D API database are installed on the Lotus Domino mail server. The Advanced Filtering software should not be installed on a journal server.

Once a message is in the journal database, it is mined by the HP Gateway server and processed in the same way as a message in a user mail file.

The graphic below shows an example of Advanced Filtering.

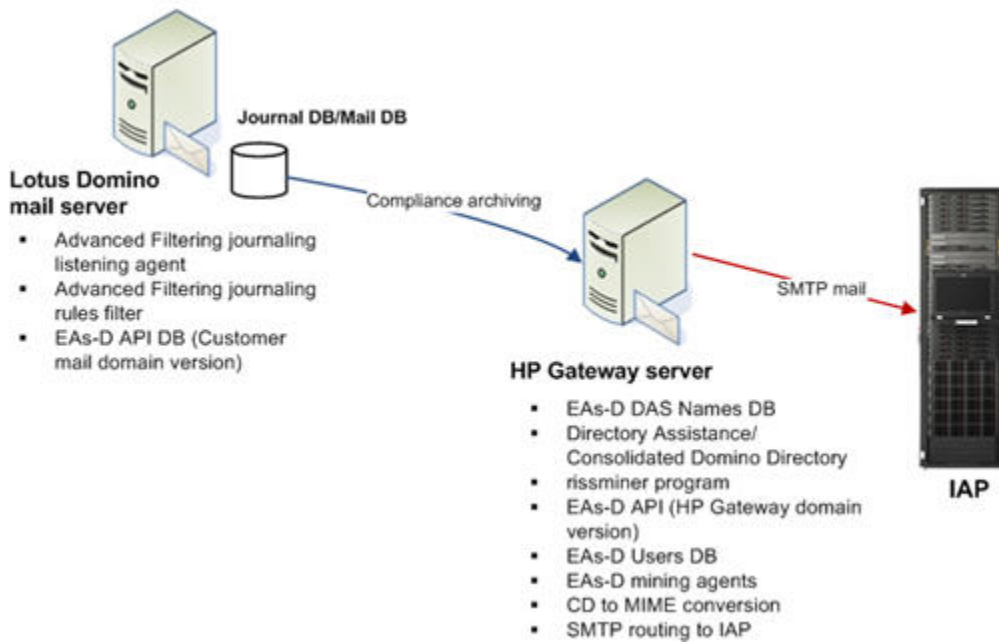


Figure 6 Advanced Filtering configuration

Software installation and configuration

The journaling rules filter and listening agent are installed in the Domino data directory on the mail server. See “[HP EAs Domino binaries](#)” on page 74. The customer version of the configuration database, HP EAs-D API, is installed into an `hprim` folder in the Domino data directory.

For changes that are made to `notes.ini` on the mail server, see “[HP EAs Domino notes.ini entries](#)” on page 73.

The procedures to install and configure the Advanced Filtering software are described in “[Advanced Filtering installation](#)” on page 202.

DWA Extension configuration

DWA Extension allows for retrieval of archived messages via Domino Web Access (iNotes). Messages can be retrieved using a Lotus Domino DWA server or a DWA proxy server. If the organization expects a significant amount of DWA traffic, we recommend that a proxy server be used to reduce the impact of EAs Domino operations.

Several EAs Domino databases must be installed on the DWA server or proxy to execute DWA Extension, including:

- HP EAs-D API, the customer instance of the configuration database. It is used to support the lookup operations that are performed when a user clicks a tombstone URL in DWA.
- HP EAs-D DWA Index, which contains the software to accept and process requests to retrieve archived messages and return them to the request user's browser.
- The EAs Domino log file.

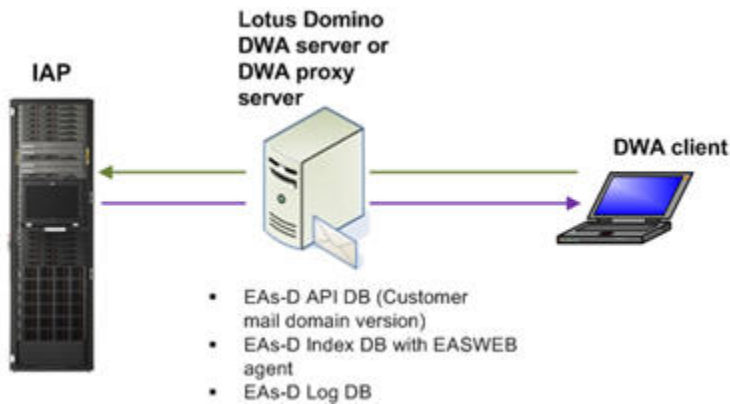


Figure 7 DWA Extension configuration

Software installation and configuration

HP EAs-D API, HP EAs-D DWA Index, and HP EAs-D Log are installed in the `hprim` folder in the Domino data directory on the DWA or proxy server.

The procedures to install and configure the DWA Extension software are described in “[Configuring DWA Extension](#)” on page 255.

Export Search configuration

Export Search allows users (usually compliance officers) to export the results of an IAP search to a Lotus Notes database. Export Search can be run on a Windows client or a customer server.

The client version runs as a standalone Java-based program on a user’s desktop. The following software must be installed on the Windows client machine:

- `ExportSearch.exe`
This executable is included in the Local Cache installation package.
- Java Runtime Environment (JRE) version 1.6 or above.
Must be installed before the Local Cache/Export Search installation.

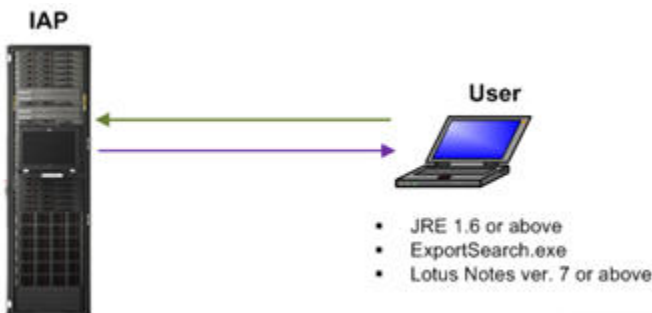


Figure 8 Export Search on a client system

The server version runs as a Java agent in the Export Search database on a Lotus Domino server. Export requests are created on the server via the Notes client or a Web browser on the user's computer. The HP EAs-D API database, the HP EAs-D Locale Configuration database (with localized copies of on-screen messages and forms), and a unique instance of the HP EAs-D Log are also installed on the Domino server.

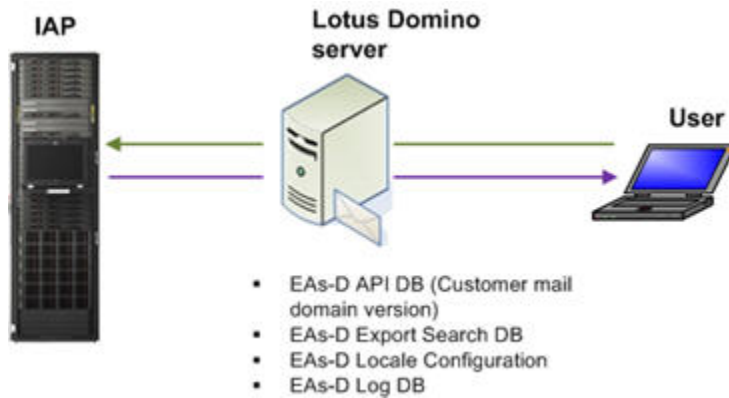


Figure 9 Export Search on a Lotus Domino server

Software installation and configuration (client)

The Export Search executable is installed into a Localcache folder in the client's Notes directory. The procedure to install the Export Search client software is described in [“Installing Local Cache”](#) on page 302.

The procedure to export messages using the Export Search client is described in [“Using the Export Search Desktop tool to export messages”](#) on page 269.

Software installation and configuration (server)

HP EAs-D API, HP EAs-D Export Search, HP EAs-D Locale Configuration, and HP EAs-D Log are installed into an `hprim` folder in the Domino data directory on the server.

The procedures to install the server software and export messages using the Export Search database on the server are described in [“Using the server to export messages”](#) on page 272.

Bulk Upload configuration

Bulk Upload is a utility that is used to scan inactive mail files (for example, of former employees) and prepare those files for archiving.

The scanning process is executed locally on an application server. Inactive mail files must first be copied to the application server from local mail servers. (Bulk Upload should not be installed on a production application server or mail server.)

The scanning process populates the Bulk Upload database with records for the inactive users. The database is then replicated to the HP Gateway server and the mail files are mined from the Gateway.

Lotus Domino application server

- Blkupd executable
- EAs-D API DB (customer mail domain version)

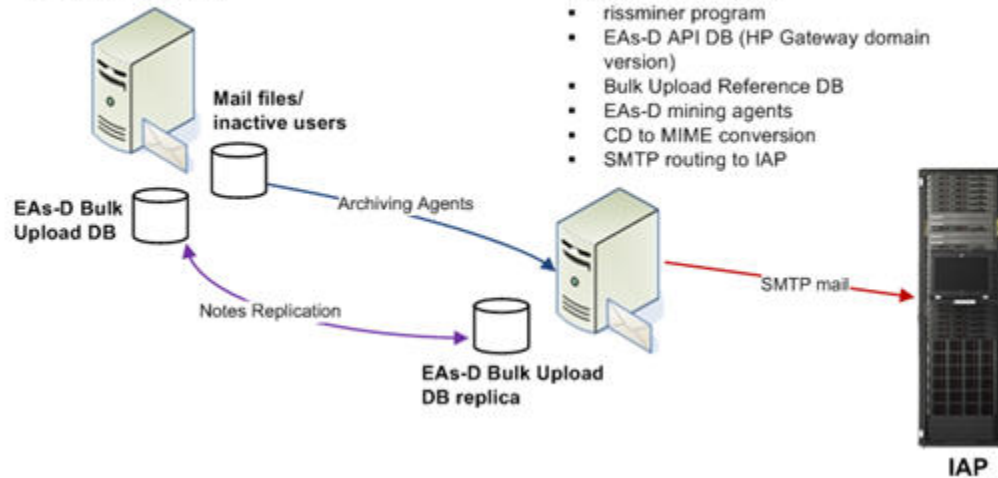


Figure 10 Bulk Upload configuration

Software installation and configuration

The Bulk Upload executable is installed in the Domino data directory on the application server. See “[HP EAs Domino binaries](#)” on page 74. The Bulk Upload database and mail domain version of HP EAs-D API are installed in the `hprim` folder in the Domino data directory.

The Bulk Upload database is replicated to the HP Gateway server.

The procedures to install, configure, and run the Bulk Upload software are described in “[Using Bulk Upload](#)” on page 223.

1.3 System requirements

The system requirements that must be met for the HP EAs Domino installation are listed in the following topics:

- [IAP requirements](#), page 35
- [Customer Domino server requirements](#), page 35
- [Supported operating systems and Lotus Domino versions](#), page 35
- [Supported Lotus Notes clients](#), page 38
- [IAP Web Interface](#), page 38
- [Export Search Web Interface](#), page 39
- [Supported character sets](#), page 40

IAP requirements

IAP is the only compatible archiving platform for HP EAs Domino.

HP EAs Domino 2.1.2 supports version 2.1.x of the IAP software.

Customer Domino server requirements

- For journaling, if the organization is using Advanced Filtering (EAs Domino journaling), the mail server must meet IBM system requirements plus the following:
 - Additional 512 MB RAM per server
 - Additional 200 MB free disk space per server
- If the organization is using Domino native journaling, there are no additional memory requirements.
- Signed and encrypted message validation requires additional free space on Lotus Domino servers used for the optional DWA Extension feature. Space requirements vary, depending on the quantity and size of signed and encrypted messages that are processed. 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 Lotus Domino versions

HP Gateway servers

In the HP Gateway environment, the HP Gateway servers use Windows Server 2008 R2 software (64-bit) and Lotus Domino version 8.5.3 (32-bit).

Customer servers

In the customer's mail environment, support for installed EAs Domino components is listed below.

For existing customers using Lotus Domino 7.x, EAs Domino support may be available if an issue can be reproduced in later (supported) versions of Domino.

Table 3 Supported platforms and Domino versions on customer servers: Archiving

Platform	OS	EAs-D Advanced Journal Filtering	Support via HP Gateway only
		Lotus Domino release	
Intel 32-bit	Windows server 2008	8.5.x	8.5.x
	Windows server 2003	8.0.x, 8.5.x	8.0.x, 8.5.x
	Red Hat Enterprise Linux 5		8.0.x, 8.5.x
	SUSE Linux Enterprise 11		8.5.2
	SUSE Linux Enterprise 10		8.0.x, 8.5.x
Intel 64-bit	Windows server 2008	8.5.x	8.5.x
	Windows server 2003	8.5.x	8.0.x, 8.5.x
	Red Hat Enterprise Linux 5		8.0.x, 8.5.x
	SUSE Linux Enterprise 11		8.5.2
	SUSE Linux Enterprise 10		8.0.x, 8.5.x
Sun SPARC	Sun Solaris 10		8.0.x, 8.5.x
IBM pSeries (RS6000)	AIX 6.1 (64-bit)		8.5.x
	AIX 5.3 (32-bit)		8.0.x
	AIX 5.3 (64-bit)	8.0.x, 8.5.x	8.0.x, 8.5.x
IBM iSeries (AS/400)	I5/OS V7 Release 1		8.5.2
	I5/OS V6 Release 1		8.0.x, 8.5.x
	I5/OS V5 Release 4		8.0.x, 8.5.x
IBM zSeries	Any	Contact HP	Contact HP
IBM OS/390	Any	Contact HP	Contact HP

Table 4 Supported platforms and Domino versions on customer servers: Other EAs Domino applications

Platform	OS	DWA Extension/ Export Search	Bulk Upload
		Lotus Domino release	
Intel 32-bit	Windows server 2008	8.5.x	8.5.x
	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
	SUSE Linux Enterprise 10		8.0.x
Intel 64-bit	Windows server 2008	8.5.x	8.5.x
	Windows server 2003	8.0.x, 8.5.x	8.0.x, 8.5.x
	Red Hat Enterprise Linux 5		8.0.x
	SUSE Linux Enterprise 10	8.0.x	8.0.x
Sun SPARC	Sun Solaris 10	8.0.x	8.0.x
IBM pSeries (RS6000)	AIX 5.3 (32-bit)	8.0.x	8.0.x
	AIX 5.3 (64-bit)	8.0.x, 8.5.x	8.0.x, 8.5.x
IBM iSeries (AS/400)	I5/OS V6 Release 1	8.0.x	8.0.x
	I5/OS V5 Release 4		8.0.x
IBM zSeries	Any	Contact HP	Contact HP
IBM OS/390	Any	Contact HP	Contact HP

Supported Lotus Notes clients

The operating systems and Lotus Notes (32-bit) versions listed below are supported by HP EAs Domino 2.1.x.

For existing customers using Lotus Notes 7.x, EAs Domino support may be available if an issue can be reproduced in later (supported) versions of Lotus Notes.

- Windows 7 Ultimate/Professional/Enterprise (32- and 64-bit): Lotus Notes 8.5.1 Fix Pack 1 (and above)
- Windows Vista: Lotus Notes 8.0.x, 8.5.x (Standard and Basic)
- Windows XP (SP2 only): Lotus Notes 8.0.x, 8.5.x (Standard and Basic)
- Red Hat Linux and Macintosh OS: 8.0.x (Standard) by request to HP

Lotus Notes Standard version 8.5.3 (32-bit) is used in the HP Gateway environment.

NOTE:

The Notes license is not officially supported on the Windows 2008 Server by IBM; however, you may want to install Notes on those Gateways to make administration easier.

IAP Web Interface

The following table shows tested browser support for the IAP Web Interface.

Table 5 Browser support

Browser/Version	Supported client OS	Browser requirements	Display requirement
Microsoft Internet Explorer (IE) 7.0	Microsoft Windows XP Professional - SP 2	Cipher strength 128-bit Internet option: JavaScript v 1.0 or v 1.1 enabled	Minimum requirement: 1024 x 768 @ 16 bit color
Microsoft Internet Explorer (IE) 7.0	Microsoft Windows XP Professional - SP 3	Cipher strength 128-bit Internet option: JavaScript v 1.0 or v 1.1 enabled	Minimum requirement: 1024 x 768 @ 16 bit color
Microsoft Internet Explorer (IE) 8.0	Microsoft Windows XP Professional - SP 2	Cipher strength 128-bit Internet option: JavaScript v 1.0 or v 1.1 enabled	Minimum requirement: 1024 x 768 @ 16 bit color
Mozilla Firefox 3.58	Microsoft Windows XP Professional - SP 2	Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.8) Gecko/20100202 Firefox/3.5.8 (.NET CLR 2.0.50727) Internet option: JavaScript v 1.0 or v 1.1 enabled	Minimum requirement: 1024 x 768 @ 16 bit color

Export Search Web Interface

The Export Search Web Interface can be accessed with the following supported browsers:

- Microsoft Internet Explorer for Windows versions 6.x, 7.x, and 8.x
- Mozilla Firefox versions 2.x and 3.x

Supported character sets

The character sets in the table below are supported by EAs Domino 2.1.x and IAP 2.1.x.

The IAP does not perform automatic character set detection. If the character set is not provided in the email message, the system uses a default of ISO-8859-1 (Latin1).

See “[HP EAs Domino settings for Japanese data](#)” on page 361 for information about ingestion of email with Japanese characters into the IAP.

Table 6 IAP character set support

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

Part 2. Installation

The topics in this section describe how to install the Lotus Domino server files and HP EAs Domino files in the HP Gateway environment.

Installation of the software is performed by the HP service representative and the Domino administrator.

- [Preparing the HP Gateway environment](#), page 43
- [Configuring the master HP Gateway server](#), page 55
- [Configuring the customer's Domino mail domain](#), page 63
- [Introducing the HP EAs Domino software](#), page 65
- [Installing the HP EAs Domino software on the master HP Gateway server](#), page 77
- [Preparing the HP Gateway server for DAS](#), page 81
- [Configuring additional HP Gateway servers](#), page 99
- [Installing HP EAs Domino components in the customer environment](#), page 103
- [Upgrading or migrating an HP EAs Domino installation](#), page 105
- [Uninstalling the HP EAs Domino software](#), page 131

❗ **IMPORTANT:**

If the software is being installed on an HP ProLiant DL360 G6 or G7 server, bring an external USB CD/DVD drive to the installation. These servers are not equipped with an internal CD/DVD drive.

❗ **IMPORTANT:**

BCC information is revealed to non-compliance users during IAP requests when the IAP MBean `ExternalAPIMBean` attribute `RemoveBCCHeader` is set to `true`. To keep the BCC information from being revealed, set the attribute to `false`:

1. Locate the file `/install/L3/build/properties/iapversion build tag/HTTP-Portal.xml` on the IAP kickstart server, and open it with the vi text editor.
 2. Add the following into the XML in that file:

```
<mbean name="Application:name=ExternalAPIMBean"><attribute name="RemoveBCCHeader">False</attribute></mbean>
```
 3. Rekick all the HTTP portals to automatically apply the setting.
-

2.1 Preparing the HP Gateway environment

This chapter describes how to install the Lotus Domino software on HP Gateway servers. The HP service representative performs the following tasks:

- [Installing the Windows software on the HP Gateway server](#), page 43
- [Synchronizing the date and time](#), page 44
- [Installing Lotus Domino server software on the HP Gateway server](#), page 44
- [Installing the Lotus Notes client software](#), page 48
- [Installing Java Runtime Environment](#), page 48
- [Installing additional HP Gateway servers](#), page 49
- [Creating Server Connection documents](#), page 52
- [Backing up Notes IDs and the Domino Directory](#), page 53

Installing the Windows software on the HP Gateway server

The HP Gateway server requires an installation of Windows 2008 R2 server software with a single network interface and a fixed IP address on the customer network.

1. Update the ProLiant firmware using the HP SmartStart CD (version 7.7 or above) or the HP Firmware Maintenance CD.
2. Install the Windows server software that ships with the HP Gateway server.
 - For HP ProLiant DL360 G6 and G7 Gateway servers, install 64-bit Windows Server 2008 R2 software.
 - If you are upgrading an older Gateway running Windows Server 2003 R2 software, install 32-bit Windows 2008 R2 server software.
3. After installing the software, perform the following steps:
 - Configure TCP/IP and assign the static IP address and host name that are defined in the customer's DNS.
 - Open the firewall ports listed below. (Firewall ports are closed by default in Windows server 2008.)
 - On all HP Gateway servers, open ports 80, 443, 1352, and 2050.
 - On the master HP Gateway and the Gateway server(s) used for DAS backup, open ports 389 and 636 for the LDAP service.
 - Optionally, configure the HP Gateway server to join the customer's Windows domain. This is not a requirement for EAs Domino.
4. Apply Microsoft security updates.
5. Update the ProLiant drivers using the HP SmartStart CD.

Synchronizing the date and time

Verify that the HP Gateway server's date and time are synchronized with a designated server in the customer environment.

From the HP Gateway, double-click the date in the lower right corner of the screen and set the date, time zone, and time to match the server in the customer environment.

 **NOTE:**

If the HP Gateway server has joined the customer's Windows domain, the time on the Gateway is synchronized automatically with the domain controller.

Installing Lotus Domino server software on the HP Gateway server

After installing the Windows server software, install the Lotus Domino server software on the HP Gateway server and run the server setup program.

Creating an organizational unit certifier

Before the implementation is begun, the Domino administrator must create a special organizational unit certifier, which will be used by HP to generate server and user IDs.

The certifier must be in the same organization as the mail servers that are being mined. This allows the HP Gateway servers and the mail servers to authenticate each other's identity – the first step in establishing a working connection between the servers.

For example: `/ou=hparchive/o=acme` where *hparchive* is the organizational unit within the organization *acme*.

The recommended file name for the certifier is **HPCert.id**. Copy the certifier to `C:\lotus\ids\` on the HP Gateway server.

Cross certification is not required when the certifier is used.

Installing the Lotus Domino server software

Follow these steps to install Lotus Domino version 8.5.3 server software on the HP Gateway server.

 **NOTE:**

Always install the 32-bit version of the Domino software, even if the HP Gateway server is running a 64-bit version of the Windows server software.

1. Double-click the installation executable to begin the installation program.
2. Unless otherwise specified by the Domino administrator, in the Location to Save Files dialog box, click **Next** to accept the default location.
3. Click **Next** in the Welcome dialog box.

4. Click **I accept the terms in the license agreement**, and then click **Next**.
5. Specify the Program Files Directory Name by entering **c:\lotus\domino**, and click **Next**.
6. Specify the Data Files Directory Name by entering **c:\lotus\domino\data**, and click **Next**.
7. Click **Domino Enterprise Server**, and then click **Next**.
8. Confirm the installation location and features, and click **Next** to start the Domino server installation process.
9. Click **Finish** in the successful installation dialog box.

Installing the update (version 8.5.2 only)

If you installed Lotus Domino Server 8.5.2, install Lotus Domino Server 8.5.2 Fix Pack 2, which has been posted with the EAs Domino 2.1.2 software.

Running the Lotus Domino server setup program on the master server

Use the following steps to run the Lotus Domino server setup program on the master HP Gateway.

To set up additional Gateway servers, see [“Running the Lotus Domino server setup program on additional HP Gateway servers”](#) on page 51.

1. From the Start menu, launch the Domino server application.
If the server setup program does not begin, use Windows Explorer to navigate to `c:\lotus\domino` and double-click `nserver.exe` to launch the program.
2. From the Service window:
 - a. Click **Start Domino as a Windows service**.
 - b. Select the check box for **Always start Domino as a service at system startup**.
 - c. Click **Next**.
3. In the Fonts dialog box, click **Next** to continue.
4. Click **Setup the first server or a stand-alone server**, click **Next**, and then follow these steps:
 - a. Provide a server name and title:
 - Server Name: Enter the server name. For example, `HPGateway1`.
 - Server Title: Enter a title. For example, `HP Gateway Server 1`.
 - b. Click **Next**.
 - c. Select **I want to use an existing certifier ID file** and click **Browse** to select the certifier created in [“Creating an organizational unit certifier”](#) on page 44.
 - d. Click **Next**.
 - e. When prompted, enter the password for the certifier ID.
 - f. Specify the Domino domain name that will be used for the HP Gateway servers. Normally, this is **HPGateway**.
 - g. Click **Next**.

5. Specify an administrator name and password:
 - a. Last Name: Enter the administrator name. Normally, this is **HPadmin**. (This will be used as a generic account name).
 - b. Password: The Domino administrator must provide and confirm the HP administrator password.

 **NOTE:**

Be sure to note the administrator password.

- c. Select the **Also save a local copy of the ID file** check box. Browse to the C:\lotus\ids\ directory and name the file **HPAdmin.id**.
 - d. Click **Next**.
6. Click **Customize** in the Internet services that the Domino Server should provide.
7. In Advanced Domino Services:
 - a. Make sure that only these Domino tasks are selected:
 - Database Replicator
 - Mail Router
 - Agent Manager
 - Administration Process
 - LDAP ServerThe LDAP Server task should only be selected for the master server (and the HP Gateways used for DAS backup).
 - SMTP ServerAll other tasks should be deselected.
 - b. Click **OK**, and then click **Next**.
8. In the Network settings dialog box, click **Customize**.
9. In Advanced Network Settings:
 - a. Deselect **NetBios over TCP/IP port driver**.
 - b. Ensure that **TCP/IP** is selected.
 - c. Ensure that the HP Gateway server's fully qualified DNS name is defined.

The DNS name must be fully formed for Internet use. The "." and extension are required for the Domino router to route mail properly to the IAP. For example: HPGateway1.acme.com.
 - d. Click **OK**, and then click **Next**.
10. Ensure that both security check boxes are selected, and then click **Next**.
11. Review the setup selections and, if correct, click **Setup**.

If incorrect, click **Back** until you reach the relevant section, make your changes, then continue back to this screen.
12. In the Congratulations dialog box, click **Finish** to complete the setup process.

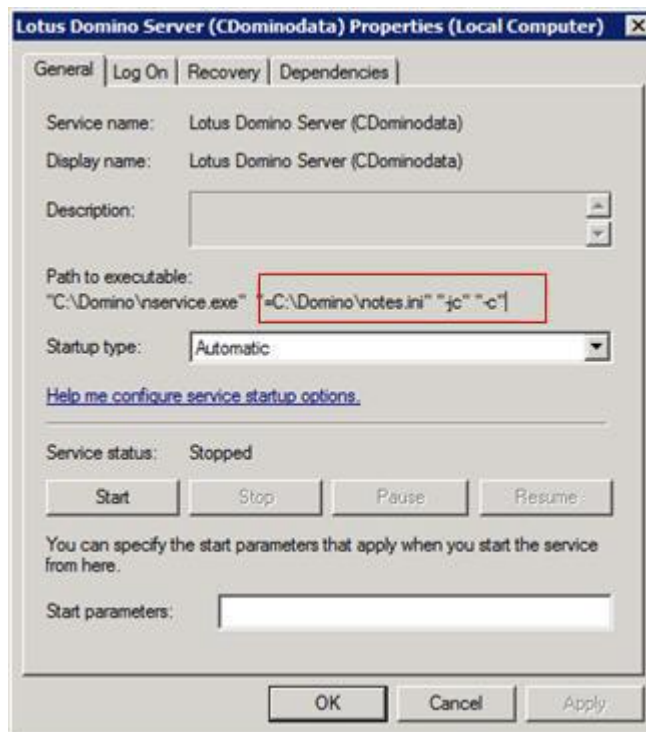
Running the Domino server

Windows Server 2008 does not allow services, including the Domino server, to display a console. For the Domino server console window to appear, the server must be run under the Server Controller.

The Java-based Server Controller is automatically installed when the Domino server software is installed. It is started when the Lotus Domino Server service is started and the relevant options are appended to the executable.

To start the service:

1. On the HP Gateway server, select **Start > Administrative Tools > Services**.
2. Select and right-click **Lotus Domino Server**, and then select **Properties**.
3. Verify that the **jc** and **c** options are appended to the executable. These options should be added by default.



4. Ensure that the Startup type is **Automatic**.
5. Click **Start** and then click **OK** to start the service.

The Domino Console does not appear when the service is started. Double-click the console to open it. The console automatically connects to the Domino server and the Server Controller.

Installing the Lotus Notes client software

Use the HP administrator ID to install the Lotus Notes 8.5.2 (Standard) Administrator, Designer, and Notes clients on the HP Gateway server. Installing the client software is required for support and HP CPE needs. If there is more than one HP Gateway, it is a good idea to install the clients on each Gateway server.

The Lotus Notes client software is provided with the installation media.

1. Double-click the installation executable to begin the installation program.
2. Unpack the installation files to a temporary location.
3. In the Welcome screen, accept the terms of the license agreement and click **Next**.
4. Enter the customer information and click **Next**.
5. Do not change the default locations for the program and data files. Click **Next**.
6. In the Custom Setup dialog box, select all three program features for installation and click **Next**.
 - Notes Client: Select for installation. Expand the list and keep Client Single Logon Feature and Migration Tools unselected.
 - Domino Designer: Select for installation.
 - Domino Administrator: Select for installation. Expand the list and keep Domino Directory Windows Sync Services unselected.
7. Ensure that the check boxes are selected for making Notes the default email, calendar, and contacts programs.
8. Click **Install**.
9. Click **Finish** when the Install Wizard Completed dialog box appears.
10. Open the system environment variables. In the Path variable, ensure that the Notes program folder is listed in the Path variable.

For example:

```
%PATH%;C:\lotus\notes
```

Installing Java Runtime Environment

Install Java Runtime Environment (JRE) version 1.6 or later (32-bit) on the HP Gateway server. The software can be downloaded from:

<http://www.java.com/en/download/manual.jsp>

After installation, perform the following steps:

1. Open the system environment variables.
2. In the Path variable, ensure that the path to the Java bin folder is listed.

For example:

```
%PATH%;C:\Java\jdk1.6.0_018\bin
```

If you make a change to the Path variable, restart the HP Gateway server to ensure that JRE is in effect before the EAs Domino software is installed.

Installing additional HP Gateway servers

When there is more than one server in the HP Gateway Domino domain, follow these steps on each additional Gateway server:

1. Register the server using the instructions in [Registering additional HP Gateway servers](#) below.
2. Install the Lotus Domino server software: “[Installing the Lotus Domino server software](#)” on page 44.
3. Run the Lotus Domino server setup: “[Running the Lotus Domino server setup program on additional HP Gateway servers](#)” on page 51.
4. Start the Domino server service: “[Running the Domino server](#)” on page 47.
5. Install the Lotus Notes, Administrator, and Designer clients: “[Installing the Lotus Notes client software](#)” on page 48.
6. Install the Java Runtime Environment: “[Installing Java Runtime Environment](#)” on page 48.

Registering additional HP Gateway servers

Register the servers in the HP Gateway Domino domain. This process creates a server ID file and a server document in the Domino Directory for each new HP Gateway server.

1. Open the Domino Administrator client using the HP Gateway administrator ID.
2. In the Configuration tab, expand **Server** and select **All Server Documents**.
The server document for the master HP Gateway server is displayed.
3. In the Tools list, expand **Registration** and select **Server**.
4. In the Choose a Certifier dialog box that appears:
 - For Server, specify the master HP Gateway as the registration server. For example, HPGateway1.
 - For the certifier ID, use the organizational unit certifier described in “[Creating an organizational unit certifier](#)” on page 44.
5. Click **OK**.
Details about the certifier ID appear in the Register Servers dialog box.
6. Click **Continue** to launch the Register New Server(s) form.
This form allows you to enter multiple servers for registration.

7. Complete the form.

The screenshot shows the 'Register New Server(s)' dialog box. The 'Advanced' tab is active. The 'Registration Server' is 'HPGateway1' and the 'Certifier' is 'hparchive/acme'. The 'Server name' is 'HPGateway3' and the 'Server title' is 'HP Gateway 3'. The 'Domino domain name' is 'HPGateway' and the 'Server administrator name' is 'HPadmin/acme'. The 'ID file password' field is empty. The 'Location for storing server ID' is set to 'In file' with the path 'C:\Program Files\...\servers\HPGateway3.id'. A table at the bottom shows a list of servers with columns for 'Server Name', 'Registration Status', and 'Date'. The table contains one entry: 'HPGateway2', 'Ready for registration', and '06/24/2009'. Buttons for 'Register All', 'Register', 'Remove', and 'Done' are at the bottom.

For each additional HP Gateway server:

- a. Specify the Server name, Server title, Domino domain name, and the HP Gateway administrator.

ⓘ **IMPORTANT:**

Do **not** enter a password in the ID file password field.

- b. Select the **In file** check box for the location to store the server ID.

ⓘ **IMPORTANT:**

Do **not** select **In Domino Directory** as the location to store the server ID. This option requires a password to be supplied with the server ID. It results in the server prompting for a password during each startup and prevents an automatic restart of the server.

- c. After the form is complete for an HP Gateway server, select the green check mark to add the server to the list of servers at the bottom of the form.
- d. After all the HP Gateway servers are listed, click **Register All**.

Server ID files are created in the file system directory that is specified and server documents are created in the Domino Directory for the HP Gateway domain.

The All Server Documents view in the Domino Directory now lists the additional Domino servers that will become HP Gateway servers. Note that these servers have not yet been installed.

After the HP Gateway servers have been registered, the Lotus Domino server software can be installed on each Gateway server. The servers will be installed as additional Domino servers in the HP Gateway domain. Specify the master HP Gateway server as the server to replicate the Domino Directory (`names.nsf`).

Running the Lotus Domino server setup program on additional HP Gateway servers

Follow these steps to run the Lotus Domino server setup program on additional HP Gateway servers.

1. Install the Lotus Domino server software on the HP Gateway.
See “[Installing the Lotus Domino server software](#)” on page 44.
2. From the Start menu, launch the Domino server application.
If the server setup program does not begin, use Windows Explorer to navigate to `c:\lotus\domino` and double-click `nserver.exe` to launch the program.
3. From the Service window:
 - a. Click **Start Domino as a Windows service**.
 - b. Select the check box for **Always start Domino as a service at system startup**.
 - c. Click **Next**.
4. In the Fonts dialog box, click **Next** to continue.
5. Click **Setup an additional server**, and then click **Next**.
6. Select **The server ID file is stored on a floppy disk, CD or network drive**. Browse to the server ID file you created in “[Registering additional HP Gateway servers](#)” on page 49, and then click **Next**.
The server name associated with the server ID is displayed.
7. Click **Next**.
8. Click **Customize** in the Internet services that the Domino Server should provide.
9. In Advanced Domino Services:
 - a. Make sure that only these Domino tasks are selected:
 - Database Replicator
 - Mail Router
 - Agent Manager
 - Administration Process
 - SMTP Server
 - LDAP Server (only for servers used for DAS backup)All other tasks should be deselected.
 - b. Click **OK**, and then click **Next**.
10. In the Network settings dialog box, click **Customize**.

11. In Advanced Network Settings:
 - a. Deselect **NetBios over TCP/IP port driver**.
 - b. Ensure that **TCP/IP** is selected.
 - c. Ensure that the HP Gateway server's fully qualified DNS name is defined.
For example: HPGateway2.acme.com.
 - d. Click **OK**, and then click **Next**.
12. Ensure that both security check boxes are selected, and then click **Next**.
13. In the provide system databases window, complete the following fields, and then click **Next**:
 - Other Domino server name: Enter the name of the master HP Gateway server. For example, HPGateway1/Acme.
 - Optional network address: Enter the DNS/hostname or IP address of the master Gateway server. For example, HPGateway1.acme.com.
14. Review the setup selections and, if correct, click **Setup**.
If incorrect, click **Back** until you reach the relevant section, make your changes, then continue back to this screen.
15. In the Congratulations dialog box, click **Finish** to complete the setup process.

Creating Server Connection documents

If there is more than one HP Gateway server, create a Server Connection document on the master HP Gateway server to each additional Gateway server.

1. From the Administrator client on the master Gateway server, click the **Configuration** tab, expand **Server**, and then click **Connections**.
2. Click **Add Connection**.
3. Configure the following settings on the Basics tab:
 - Connection type: Select **Local Area Network**.
 - Source server: Enter the name of the master HP Gateway server. By default, this field is populated with the current server name.
 - Source domain: Enter the name of the HP Gateway domain.
 - Use the port(s): **TCPIP**
 - Destination server: Enter the name of the destination HP Gateway server.
 - Destination domain: Enter the name of the HP Gateway domain.
 - Optional network address: Enter the fully-qualified hostname or the IP address of the destination Gateway server.
4. On the Replication/Routing tab, configure the replication type to be **Pull Push**.
5. On the Schedule tab, configure the following fields:
 - Connect at times: **12:00 AM – 11:59 PM each day**
 - Repeat interval of: **60 minutes**
 - Days of week: Ensure all days are selected.
6. Click **Save & Close**.
7. Repeat steps 2–6 to create a connection document to each additional HP Gateway server.

Backing up Notes IDs and the Domino Directory

After installing the Lotus Domino server software on each HP Gateway server, back up the following directories:

- C:\lotus\ids
- C:\lotus\domino\data\names.nsf

2.2 Configuring the HP Gateway servers

Complete the following procedures to configure the Domino server settings on the HP Gateway servers.

- [Adding the HP Gateway domain to the Domino Administrator client](#), page 55
- [Setting up security on the HP Gateway server](#), page 56
- [Editing the Agent Manager parameter values](#), page 57
- [Creating connection documents to the customer mail servers](#), page 57
- [Creating and configuring the foreign SMTP domain document](#), page 58
- [Creating and configuring the SMTP connection document](#), page 59
- [Creating a configuration document for the HP Gateway server](#), page 59
- [Limiting the log file size](#), page 60
- [Adding the EAsD_Domain parameter](#), page 61

Adding the HP Gateway domain to the Domino Administrator client

The Lotus Domino Administrator client is the standard tool used for Domino server administration tasks. To make it easy to work with the HP Gateway servers, add each Gateway server to the list of servers in the Domino Administrator.

1. Start the Domino Administrator client.
2. Switch to the HP Gateway administrator ID (created during installation of the HP Gateway server).
3. Select **File > Preferences > Administration Preferences**, and then click the **Basics** tab in the Administration Preferences dialog box.
4. Click **New**, and configure the following settings:
 - Domain name: Enter the Domino domain name that was assigned to the HP Gateway server during installation.
See [“Running the Lotus Domino server setup program on the master server”](#) on page 45.
 - Domino Directory servers: Enter the fully qualified name of the server ID created for each HP Gateway server.
5. Click **OK**.

A new bookmark is added to the bar on the left side of the Domino Administrator client interface. The domain name is shown when you hold the mouse pointer over the icon.

Setting up security on the HP Gateway server

The HP Gateway servers are in an external Domino domain. Security must be set up to make sure that existing servers and administrators can work with the HP Gateway servers.

Perform the following steps on each HP Gateway server:

1. Select the HP Gateway domain in the Domino Administrator client, select the Gateway server, and then click the **People and Groups** tab.
2. Add the Domino servers that will be mined to OtherDomainServers:
 - a. Expand **Groups**, select **OtherDomainServers** in the Groups list, and then click **Edit Group**.
 - b. In the group's member list, add the names of the customer's Domino servers that the HP Gateway server will mine.

(You might want to simply copy and paste names from a mail server's LocalDomainServers group.)
 - c. Click **Save & Close**.
3. Add the HP Gateway administrator to LocalDomainAdmins:
 - a. In the Groups list, select **LocalDomainAdmins**, and then click **Edit Group**.
 - b. In the group's member list, add the fully qualified Notes ID of the HP Gateway administrator and any other users with rights to perform administration tasks on the Gateway server (such as mail domain administrators).
 - c. Click **Save & Close**.
4. Configure permissions on the HP Gateway server:
 - a. With the Gateway server still selected in the Domino Administrator client, click the **Configuration** tab, and then expand **Server**.
 - b. Click **Current Server Document**, click the **Security** tab, and then click **Edit Server**.
 - c. Add **LocalDomainServers** and **LocalDomainAdmins** to the following fields:
 - Full Access Administrators
 - Administrators
 - Run unrestricted methods and operations
 - Run restricted LotusScript/Java agents
 - Run simple and formula agents
 - Create databases and templates
 - Create new replicas
 - Create master templates
 - d. In the Access server field, add **LocalDomainAdmins**, **LocalDomainServers**, and **OtherDomainServers** to the Access Server list.
 - e. Save the changes. Keep the Server document open so you can edit the Agent Manager values in the next section.



NOTE:

If you intend to use a special signing ID for the security fields listed in steps 4c and 4d above, add the fully qualified name of the signing ID to the relevant security fields.

Editing the Agent Manager parameter values

Set the HP EAs Domino recommended options in the Agent Manager to avoid server instability.

In the Server document for the HP Gateway server:

1. Click the **Server Tasks** tab.
2. Click the **Agent Manager** tab, and then click **Edit Server**.
3. Change the Daytime Parameter values as follows:
(In some circumstances, the HP engineering staff might recommend increasing these values.)
 - Start time: Enter **08:00 AM**.
 - End time: Enter **08:00 PM**.
 - Max concurrent agents: Enter **5**.
 - Max LotusScript/Java execution time: Enter **480 minutes**.
 - Max % busy before delay: Enter **70**.
4. Change the Nighttime Parameter values as follows:
(In some circumstances, the HP engineering staff might recommend increasing these values.)
 - 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**.
5. Click **Save & Close**.
6. Repeat this procedure for each HP Gateway server.

Creating connection documents to the customer mail servers

Connection documents are required for the HP Gateway servers to archive messages from the customer mail or journal servers.

Create a separate Connection document to each Domino server that the Gateway server will mine.

1. From the Administrator client, click the **Configuration** tab, expand **Messaging**, and then click **Connections**.
2. Click **Add Connection**.

3. On the **Basics** tab, configure the following settings:
 - Connection type: Select **Local Area Network**.
 - Source server: Enter the fully-qualified name of the HP Gateway server. By default, this field is populated with the current server name.
 - Source domain: Enter the name of the HP Gateway domain.
 - Use the port(s): **TCPIP**.
 - Destination server: Enter the name of the first Domino mail or journal server that the HP Gateway will communicate with to archive email.
 - (Optional) Destination domain: Enter the name of the mail domain.
4. On the Replication/Routing tab, select **None** in the Routing task drop-down box.
5. On the Schedule tab, configure the following fields:
 - Connect at times: **12:00 AM – 11:59 PM**
 - Repeat interval of: **60 minutes**
 - Days of week: Ensure all days are selected.
6. Click **Save & Close**.
7. Repeat steps 2–6 to create a Connection document to each mail and journal server that the HP Gateway server communicates with for message archiving.

Creating and configuring the foreign SMTP domain document

Perform the following steps on each HP Gateway server to create a foreign SMTP document to the IAP:

1. From the Administrator client, select the HP Gateway server.
2. Click the **Configuration** tab, expand **Messaging**, and then click **Domains**.
3. Click **Add Domain**.
4. Click the **Basics** tab. In the Domain type field, click the arrow and select **Foreign SMTP Domain**.
5. Click the **Routing** tab, and configure the following settings:
 - Internet Domain: Enter a domain name for the IAP. We recommend that you use the value in the Name field in the `Domain.jcml` file.

❗ **IMPORTANT:**

The domain name **must** contain at least one dot ("."). For example:

`iap_domain.com`

Additionally, the domain name must not contain any spaces or non-ASCII characters.

- Internet host: Enter the host name or virtual IP (VIP) address of the IAP. If the VIP address is used, we recommend enclosing it in square brackets.
6. Click **Save & Close**.

Creating and configuring the SMTP connection document

A connection must be created from each HP Gateway server to the IAP system for mail routing.

1. From the Administrator client, select the HP Gateway server.
2. Click the **Configuration** tab, expand **Server**, and then click **Connections**.
3. Click **Add Connection**.
4. Click the **Basics** tab, and configure the following settings:
 - Connection type: Select **SMTP**.
 - Source server: Enter the fully qualified name of the HP Gateway server.
 - Connect via: Select **Direct connection**.
 - SMTP MTA relay host: Enter the hostname or VIP address of the IAP from the `BlackBoxConfig.bct` file. If the VIP address is used, we recommend enclosing it in square brackets.
 - Destination domain: Enter the name of the IAP Internet domain.

 **NOTE:**

This **must** be the same as the Internet domain name you entered above in the foreign SMTP document.

5. Click the **Replication/Routing** tab, and then configure the following settings:
 - Replication task: Click the arrow, and select **Disabled**.
 - Routing task: Click the arrow, and select **SMTP Mail Routing**.
 - Route at once if: Enter **1**.
 - Routing cost: Leave **1** (the default).
6. Click **Save & Close**.
7. Repeat these steps on each HP Gateway server.

Creating a configuration document for the HP Gateway server

Create a Server Configuration document on each HP Gateway server by following these steps:

1. From the Administrator client, select the HP Gateway server.
2. Click the **Configuration** tab, expand **Messaging**, and then click **Configurations**.
3. If a configuration does not exist for the server, click **Add Configuration**. If a dialog box prompts you to create a configuration, click **Yes**.
4. In the configuration document, click the **Basics** tab, then enter the HP Gateway server name into the Group or Server name field.

5. Click the **Router/SMTP** tab.
 - a. Configure the following settings in the **Basics** tab:
 - Number of mailboxes: Change to **3**.
 - SMTP used when sending: Select **Enabled**.
 - Exhaustive lookup: Select **Enabled**.
 - b. Click the **Advanced** tab, and then click the **Controls** tab.
 - c. In the Additional Controls area, change Hold Undeliverable Mail to **Enabled**.
 - d. Click the **Restrictions and Controls** tab, and then click the **Transfer Controls** tab.
 - e. Change the Low Priority mail routing time range to **12:00 AM - 11:59 PM**.
6. Click the **MIME** tab, and then click the **Conversion Options** tab.
7. Click the **Outbound** tab and configure the following settings:
 - Message content: Change to **from Notes to HTML**.
 - Lookup Internet address for: Select **Enabled**.
 - Perform exhaustive lookups: Select **Enabled**.
8. In the **MIME** tab, click the **Advanced** tab, and then click the **Advanced Outbound Message Options** tab.
9. Select **Enabled** in the Internet Mail server sends Notes private items in messages field.
10. Click **Save & Close**.

**NOTE:**

Japanese language customers: See [“HP EAs Domino settings for Japanese data”](#) on page 361 for additional options that can be set in the configuration document.

Limiting the log file size

Limit the size of the Domino server's log file based on the age of log entries. This prevents the Domino log file from growing too large. (The default setting is for Domino to purge the log after seven days.)

1. Open `notes.ini` on the server
2. Scroll to the Log parameter.

The default Log parameter displays `Log=log.nsf, 1, 0, 7, 40000`, where:

- `log.nsf` is the log database file name
 - `1` is the option that logs to the console as well as to the log file
 - `0` is an unused option that is always set to 0
 - `7` is the number of days to save entries in the log file
 - `40000` is the (maximum) size of an entry, in bytes
3. Change the number of days.

We recommend changing the setting to three days.
 4. Save the file.

5. Do one of the following:
 - If you plan to make the changes described in the next section, [Adding the EAsD_Domain parameter](#), keep the `notes.ini` file open.
 - If you do not plan to make the changes in the next section, restart the Domino server.
6. Repeat these steps on each HP Gateway server.

Adding the EAsD_Domain parameter

In remote mining, the standard Lotus *Domain* parameter in `notes.ini` is populated with the HP Gateway domain name.

A separate parameter must be manually added to list the customer's mail domain, if user mail files are selectively archived and Ensure Owner Receipt (EOR) is specified. (EOR allows emails that are sent to a distribution list to be archived in each recipient's IAP repository.)

1. In `notes.ini`, add the following variable:
`EAsD_Domain=<name of customer's mail domain>`

For example:
`EAsD_Domain=Acme`
2. Save the file, and then restart the Domino server.
3. Repeat these steps on each HP Gateway server.

2.3 Configuring the customer's Domino mail domain

The tasks below are performed on the Lotus Domino administration server by the Domino administrator. These tasks establish access for the HP Gateway servers in the customer's Domino domain.

① IMPORTANT:

In a customer environment where mail and journal servers are clustered:

- The HP Gateway servers and agent signer must have access to all mail and/or journal servers in the cluster. The instructions below apply to all servers that are clustered with mail and journal servers used in the archiving process.
 - The HP Gateway servers and agent signer must be listed in the ACL of the mail files and journals to be archived, on all mail and journal servers in the cluster.
-

Granting access for the HP Gateway servers

1. From the Domino Directory on the Administration server, select **View > Groups**.
2. Select and double-click the OtherDomainServers group, or a similar group in the Domino Directory that allows access to user mail files.
3. Click **Edit Group**.
4. Add each HP Gateway server's fully-qualified name to the Members field.
5. Click **Save & Close**.

Configure trusted servers

Configure trust between the HP Gateway servers and the Domino servers that are being mined.

1. On the Administration server, click the **Configuration** tab, expand **Server**, and then click **All Server Documents**.
2. Select the first mail or journal server, and click **Edit Server**.
3. Click the **Security** tab and locate the Server Access area.
4. In the Trusted servers field, enter the name of each HP Gateway server.
5. Click **Save & Close**.
6. Repeat steps 2–5 for each mail or journal server that will be mined.

2.4 Introducing the HP EAs Domino software

The files installed by HP EAs Domino are described in this chapter.

- [HP EAs Domino databases](#), page 65
- [HP EAs Domino database templates](#), page 66
- [HP EAs Domino database access](#), page 67
- [HP EAs Domino notes.ini entries](#), page 73
- [HP EAs Domino binaries](#), page 74`

HP EAs Domino databases

The EAs Domino databases listed below are installed in an `hprim` folder created in the Domino data directory.

- **HP EAs-D API:** `hp_rissapi.nsf`
The main configuration database, which contains configuration documents, mining rules, journaling rules (if EAs Domino Advanced Filtering is used), and other configuration options.
- **HP EAs-D Users:** `hp_rissuser.nsf`
The database that holds records of the EAs Domino users.
- **HP EAs-D DAS Names:** `hp_dasnames.nsf`
The database that holds the records used by DAS to create and update user repositories on the IAP.
- **HP EAs-D Stats:** `hp_easd_stats.nsf`
The database that records statistics collected during execution of the archiving agents.
- **HP EAs-D Alert:** `hp_rissalert.nsf`
The database that records alerts collected during execution of the archiving agents.
- **HP EAs-D CEE Log:** `hp_ceelog.nsf`
The database used to log messages processed by Clean Envelop Encapsulation.
- **HP EAs-D Get Held Messages:** `hp_getheldmsgs.nsf`
The database used to store messages rejected by the IAP.
- **HP EAs-D Log:** `hp_risslog.nsf`
The database that logs the actions of EAs Domino components.
- **HP EAs-D Locale Configurations:** `hp_localecfg.nsf`
A database with configuration tables that can be localized to various languages, so that messages and forms can appear in a user's native language.
- **HP EAs-D Export Search:** `hp_rissexportsearch.nsf`
The database used to support the export of messages from the IAP.
- **HP EAs-D Bulk Upload:** `hp_rissblkupd.nsf`

The database used to archive email of inactive users.

- HP EAs-D DWA Index: `hp_dwaindex.nsf`

The database used in retrieving archived messages in Domino Web Access (DWA).

- HP EAs-D SC Request: `hp_rissreq.nsf`

A database used in DWA retrieval of messages.

- Reference databases:

Databases containing the archiving agents as well as pointers, or references, to the messages being processed.

- HP EAs-D Reference (miner): `hp_riss_minerreferenc.nsf`
- HP EAs-D Reference (jrnl): `hp_riss_journalreferenc.nsf`
- HP EAs-D Reference (blk): `hp_riss_blkupreferenc.nsf`

- Preprocessing databases:

Databases containing the agents to process signed and encrypted messages and Clean Envelope messages.

- HP EAs-D PreProcess (miner): `hp_preproc_miner.nsf`
- HP EAs-D PreProcess (jrnl): `hp_preproc_journal.nsf`
- HP EAs-D PreProcess (blk): `hp_preproc_blk.nsf`

HP EAs Domino database templates

The `Templates` directory on the installation media contains NTF files with the design elements for HP EAs Domino databases.

The templates are provided for the following purposes:

- Creation of additional EAs Domino databases, for example, additional reference and preprocessing databases
- Creation of journal databases
- Source of several EAs Domino design elements
- Emergency repair, in case of design corruption in the databases

❗ IMPORTANT:

Do **not** copy EAs Domino templates into the Domino data directory on the HP Gateway servers. The overnight Design process might use the templates to refresh agents, causing the agents to lose schedule information. The templates can be placed in the data directory of the Notes client.

The EAs Domino database templates are listed below.

Template for new reference databases:

- HP EAs-D Reference NTF: `hp_referenc.ntf`

Template for new preprocessing databases:

- HP EAs-D PreProcess NTF: `hp_preproc.ntf`

Template for Mail-to-Me administration, tombstone auditing, and message analysis:

- HP EAs-D Tools NTF: `hp_tools.ntf`

Template for mail journals:

- HP EAs-D Journal NTF: `hp_mailjrn.ntf`

Templates for IAP single sign-on support:

- HP EAs-D SSO Mail Sample: `hp_ssomail_sample.ntf`
- HP EAs-D SSO NTF: `hp_sso.ntf`

Template with design components:

- HP EAs-D Shared Objects NTF: `hp_sharedobjects.ntf`

All other database templates:

- HP EAs-D Alert Rep: `hp_alert.ntf`
- HP EAs-D API NTF: `hp_api.ntf`
- HP EAs-D Bulk Upload NTF: `hp_blkupd.ntf`
- HP EAs-D Clean Envelope Log: `hp_ceelog.ntf`
- HP EAs-D DAS Names NTF: `hp_dasnames.ntf`
- HP EAs-D DWA Index NTF: `hp_dwaindex.ntf`
- HP EAs-D Export Search NTF: `hp_exportsearch.ntf`
- HP EAs-D GHM NTF: `hp_getheldmsgs.ntf`
- HP EAs-D Locale Configurations NTF: `hp_localecfg.ntf`
- HP EAs-D Log NTF: `hp_log.ntf`
- HP EAs-D Server Requests NTF: `hp_req.ntf`
- HP EAs-D Stats: `hp_stats.ntf`
- HP EAs-D Users NTF: `hp_user.ntf`

HP EAs Domino database access

HP Gateway servers

Ensure the ACL is set correctly for the databases listed below.

Table 7 ACL for EAs Domino databases on HP Gateway servers

Database	Users	User type	Access	Permissions	Roles
HP EAs-D Alert	LocalDomain Admins (or substitute)	Server group	Manager	Replicate or copy documents	

Database	Users	User type	Access	Permissions	Roles
	LocalDomain Servers	Server group	Manager	Delete documents, replicate or copy documents	
	OtherDomain Servers	Server group	No access		
	Default		Manager	Delete documents, replicate or copy documents	
HP EAs-D API, HP EAs-D Reference databases, HP EAs-D SC Request, HP EAs-D Users* (*See HP EAs-D Users entry in ACL for EAs Domino databases on customer servers below)	LocalDomain Admins (or substitute)	Person group	Manager	Delete documents, replicate or copy documents	Admin
	LocalDomain Servers	Server group	Manager	Delete documents, replicate or copy documents	Admin
	OtherDomain Servers	Server group	No access*	Read public documents, write public documents, replicate or copy documents	
	Default		Manager	Delete documents, replicate or copy documents	Admin
HP EAs-D CEE Log	LocalDomain Admins (or substitute)	Person group	Manager	Delete documents, replicate or copy documents	Admin
	LocalDomain Servers	Server group	Manager	Delete documents, replicate or copy documents	Admin
	OtherDomain Servers	Server group	No access		Admin
	Default		Manager	Delete documents, replicate or copy documents	Admin
HP EAs-D DAS Names, HP EAs-D Get Held Messages, HP EAs-D Stats	LocalDomain Admins (or substitute)	Person group	Manager	Delete documents, replicate or copy documents	
	LocalDomain Servers	Server group	Manager	Delete documents, replicate or copy documents	
	OtherDomain Servers	Server group	No access		
	Default		Manager	Delete documents, replicate or copy documents	

Database	Users	User type	Access	Permissions	Roles
HP EAs-D Log, HP EAs-D PreProcess databases	LocalDomain Admins (or substitute)	Person group	Manager	Delete documents, replicate or copy docu- ments	
	LocalDomain Servers	Server group	Manager	Delete documents, replicate or copy docu- ments	
	OtherDomain Servers	Server group	No access	Read public documents, write public documents, replicate or copy docu- ments	
	Default		Manager	Delete documents, replicate or copy docu- ments	
HP EAs-D API, HP EAs-D Reference databases, HP EAs-D SC Request	LocalDomain Admins (or substitute)	Person group	Manager	Delete documents, replicate or copy docu- ments	Admin
	LocalDomain Servers	Server group	Manager	Delete documents, replicate or copy docu- ments	Admin
	OtherDomain Servers	Server group	No access	Read public documents, write public documents, replicate or copy docu- ments	
	Default		Manager	Delete documents, replicate or copy docu- ments	Admin

Customer servers

EAs Domino databases are installed or created on customer servers when the Advanced Filtering, Export Search (server side), DWA Extension, Bulk Upload, and Single Sign On features are used.

Access must be set for the databases listed in the table below.

! IMPORTANT:

The databases used for Advanced Filtering, DWA Extension, and Export Search require additional access configuration. Refer to the following topics: [“Creating the mail-in journal database”](#) on page 204, [“Setting ACL for DWA Extension”](#) on page 258, and [“Setting ACL for Export Search”](#) on page 273.

Table 8 ACL for EAs Domino databases on customer servers

Database	Users	User type	Access	Permissions	Roles
HP EAs-D API (required whenever EAs Domino features are installed on customer servers) This is separate from the database on the HP Gateway servers	LocalDomain Admins (or substitute)	Person group	Manager	Delete documents, replicate or copy documents	Admin
	LocalDomain Servers	Server group	Manager	Delete documents, replicate or copy documents	Admin
	OtherDomain Servers	Server group	No access	Read public documents, write public documents, replicate or copy documents	
	DWA users, Export Search users	Person group	Reader		
	Notes ID used in DWA Index EASWEB agent security		Reader		
	Default		Manager	Delete documents, replicate or copy documents	Admin

Database	Users	User type	Access	Permissions	Roles
HP EAs-D Bulk Upload (required for Bulk Upload) <i>This database is replicated to the HP Gateway server when Bulk Upload is used. Ensure that the HP EAs-D Bulk Upload database on the HP Gateway specifies Editor access for OtherDomainServers.</i>	LocalDomain Admins (or substitute)	Person group	Manager	Delete documents, replicate or copy documents	Admin
	LocalDomain Servers	Server group	Manager	Delete documents, replicate or copy documents	Admin
	OtherDomain Servers	Server group	Editor	Read public documents, write public documents, replicate or copy documents	
	Default		Manager	Delete documents, replicate or copy documents	Admin
HP EAs-D DWA Index (required for DWA Extension)	LocalDomain Admins (or substitute)	Person group	Manager	Delete documents, replicate or copy documents	Admin
	LocalDomain Servers	Server group	Manager	Delete documents, replicate or copy documents	Admin
	OtherDomain Servers	Server group	No access	Read public documents, write public documents, replicate or copy documents	
	DWA users	Person group	Depositor		
	Notes ID used in EASWEB agent security		Editor		
	Default		Manager	Delete documents, replicate or copy documents	Admin
HP EAs-D Export Search (required for Export Search)	LocalDomain Admins (or substitute)	Person group	Manager	Delete documents, replicate or copy documents	Admin
	LocalDomain Servers	Server group	Manager	Delete documents, replicate or copy documents	Admin
	OtherDomain Servers	Server group	No access	Read public documents, write public documents, replicate or copy documents	
	Export Search users	Person group	Author	Create documents	

Database	Users	User type	Access	Permissions	Roles
	Default		Manager	Delete documents, replicate or copy documents	Admin
HP EAs-D Journal (required for Advanced Filtering) Must be created from hp_mailjrn template	Administrators, listed individually (not group)	Person	Manager	Replicate or copy documents	Admin
	LocalDomain Servers	Server group	Depositor	Replicate or copy documents	Admin
	HP Gateway servers, listed individually	Server	Editor	Replicate or copy documents	Admin
	ID that signed agents (if agents were signed with user ID)	Person	Editor	Delete documents, replicate or copy documents	Admin
	Anonymous		No access		
	Default		No access		
HP EAs-D Locale Configuration (required for Export Search)	LocalDomain Admins (or substitute)	Person group	Manager	Delete documents, replicate or copy documents	Admin
	LocalDomain Servers	Server group	Manager	Delete documents, replicate or copy documents	Admin
	OtherDomain Servers	Server group	No access	Read public documents, write public documents, replicate or copy documents	
	Export Search users		Reader		
	Default		Manager	Delete documents, replicate or copy documents	Admin
HP EAs-D Log (required for Bulk Upload)	LocalDomain Admins (or substitute)	Person group	Manager	Delete documents, replicate or copy documents	
	LocalDomain Servers	Server group	Manager	Delete documents, replicate or copy documents	
	OtherDomain Servers	Server group	No access	Read public documents, write public documents, replicate or copy documents	

Database	Users	User type	Access	Permissions	Roles
	Default		Manager	Delete documents, replicate or copy documents	
HP EAs-D SSO (rimssso.nsf) (required for IAP single sign-on) Must be created from hp_sso template	LocalDomain Admins (or sub-group of admins)	Person group	Manager	Replicate or copy documents	RIM SSO Admin
	LocalDomain Servers	Server group	Manager	Replicate or copy documents	RIM SSO Admin
	OtherDomain Servers	Server group	No access		
	Anonymous		No access		
	Default		Reader		
HP EAs-D Users (required for Advanced Filtering) <i>This database is replicated from the HP Gateway server when Advanced Filtering is used. Ensure that the HP EAs-D Users database on the HP Gateway specifies Editor access for OtherDomainServers.</i>	LocalDomain Admins (or substitute)	Person group	Manager	Delete documents, replicate or copy documents	Admin
	LocalDomain Servers	Server group	Manager	Delete documents, replicate or copy documents	Admin
	OtherDomain Servers	Server group	Editor	Read public documents, write public documents, replicate or copy documents	
	Default		Manager	Delete documents, replicate or copy documents	Admin

HP EAs Domino notes.ini entries

The EAs Domino entries added to `notes.ini` are listed below.

ⓘ IMPORTANT:

On both the HP Gateway servers and the customer mail servers, the `hprim_api=hprim\hp_rissapi.nsf` entry must always exist in the `notes.ini` file for EAs Domino to function properly.

Entries on HP Gateway servers

On the HP Gateway servers, the `notes.ini` file is updated with the following entries upon installation of the HP EAs Domino software:

- `hprim_api=hprim\hp_rissapi.nsf`

This entry must exist in the file for EAs Domino to work.

- `HP_EAS-D_CONTROL_IAP_HASHES_COLLISION=1`

When set to "1", this parameter enables the cache of message hashes that is maintained in the Archive agent. The cache allows the Archive agent to detect references to duplicate messages and avoid performing an extra query to the IAP.

- The standard Lotus *Domain* parameter in `notes.ini` is populated with the HP Gateway domain name.

If user mail files are selectively archived and Ensure Owner Receipt is specified, a separate parameter must be added manually to list the customer's mail domain:

```
EAsD_Domain=<name of customer's mail domain>
```

Entries on customer servers

- `hprim_api=hprim\hp_rissapi.nsf`

This entry is automatically added to `notes.ini` on customer servers when the EAs Domino installer is used to install Advanced Filtering, DWA Extension, Export Search, or Bulk Upload components. If these components are added manually, the `hprim_api=hprim\hp_rissapi.nsf` entry **must** be added manually to `notes.ini` on the servers.

- The EAs Domino installer adds the following entries to `notes.ini` on customer servers that run Advanced Filtering (HP EAs Domino journaling):

- `EXTMGR_ADDINS = advsrv`
- `servertasks = mwadv`
- `$MailWatcherServerName=CN=[server name]/O=[organization]`
- `MWADVSRVOTHERSERVICES=[anti-virus-real-time-task-name]`

Allows anti-virus scanning to be executed before the journaling capture

- If Norton anti-virus software is used (for example, `rtvscan.exe` from the Symantec Internet Security Suite), manually add this entry:

```
MWADVSRVOTHERSERVICESAO=[anti-virus-real-time-task-name]
```

HP EAs Domino binaries

The HP EAs Domino software includes the following binary files:

Table 9 HP EAs Domino binaries

Description	Operating system	Filename	Installation directory
The mailbox mining executable, <code>rissminer</code> . Handles message identification and selection for archiving by creating EAs Domino reference documents. Rissminer is installed and run on HP Gateway servers.	Windows (32 and 64 bit)	<code>nrissminer.exe</code>	<code>Domino\data</code>
The journaling rules filter. It is installed on a customer mail server when Advanced Filtering (HP EAs Domino journaling) is used to journal messages.	Windows (32 and 64 bit)	<code>nmwadv</code>	<code>Domino\data</code>
	Linux, Solaris, AIX (32 and 64 bit)	<code>mwadv</code>	<code>/notesdata</code>

Description	Operating system	Filename	Installation directory
<p>The journaling listening agent.</p> <p>It is installed on a customer mail server when Advanced Filtering (HP EAs Domino journaling) is used to journal messages.</p>	Windows (32 and 64 bit)	nadvsvr.dll	Domino\data
	Linux, Solaris (32 and 64 bit)	libadvsvr.so	/notesdata
	AIX (32 and 64 bit)	libadvsvr.a	/notesdata
<p>Bulk upload for inactive mail files.</p> <p>It is installed on a customer application server and executes mail file ownership identification so that messages can be archived to the IAP.</p>	Windows (32 and 64 bit)	nhpblkupd.exe	Domino\data
	Linux, Solaris, AIX (32 and 64 bit)	hpblkupd	/notesdata
<p>The uninstaller.</p> <p>Uninstalls previous version of the EAs Domino software on Windows systems. (Java Runtime Environment version 1.6 or later must be installed on the server for this executable to run.)</p>	Windows (32 and 64 bit)	Uninstaller.exe	Domino\data\HPRIMUninstaller

2.5 Installing the HP EAs Domino software on the master HP Gateway server

- [Before installing the software](#), page 77
- [Installing the HP EAs Domino software](#), page 77
- [Setting access control \(ACL\)](#), page 80

Before installing the software

Before installing the EAs Domino software, ensure that:

- The contents of the installation media have been extracted to a temporary folder.
- Java Runtime Environment version 1.6 or later (32-bit) is installed on the HP Gateway server.
- The Agent Manager, Router, and Replicator tasks are running on the HP Gateway server.
- All non-Lotus Notes applications are closed.
- Folder capture is disabled on the IAP. HP EAs Domino does not support folder capture.
Open `Domain.jcml` on the IAP kickstart server at `/install/configs/primary/` and ensure that the `FolderSupportEnabled` parameter is set to the default value of `false` for the domain.

NOTE:

These instructions cover a new installation of the EAs Domino software. If you are upgrading from an earlier version of the software, see [“Upgrading or migrating an HP EAs Domino installation”](#) on page 105.

Installing the HP EAs Domino software

Follow the instructions in this section to install the EAs Domino 2.1.2 software on the HP Gateway server.

If there are multiple HP Gateway servers, use these instructions to install the software on the server that acts as the master Gateway server. The configuration will be deployed by the installer to other Gateway servers. See [“Deploying the archiving installation to additional HP Gateway servers”](#) on page 100.

The installation should be performed from a Windows client workstation.

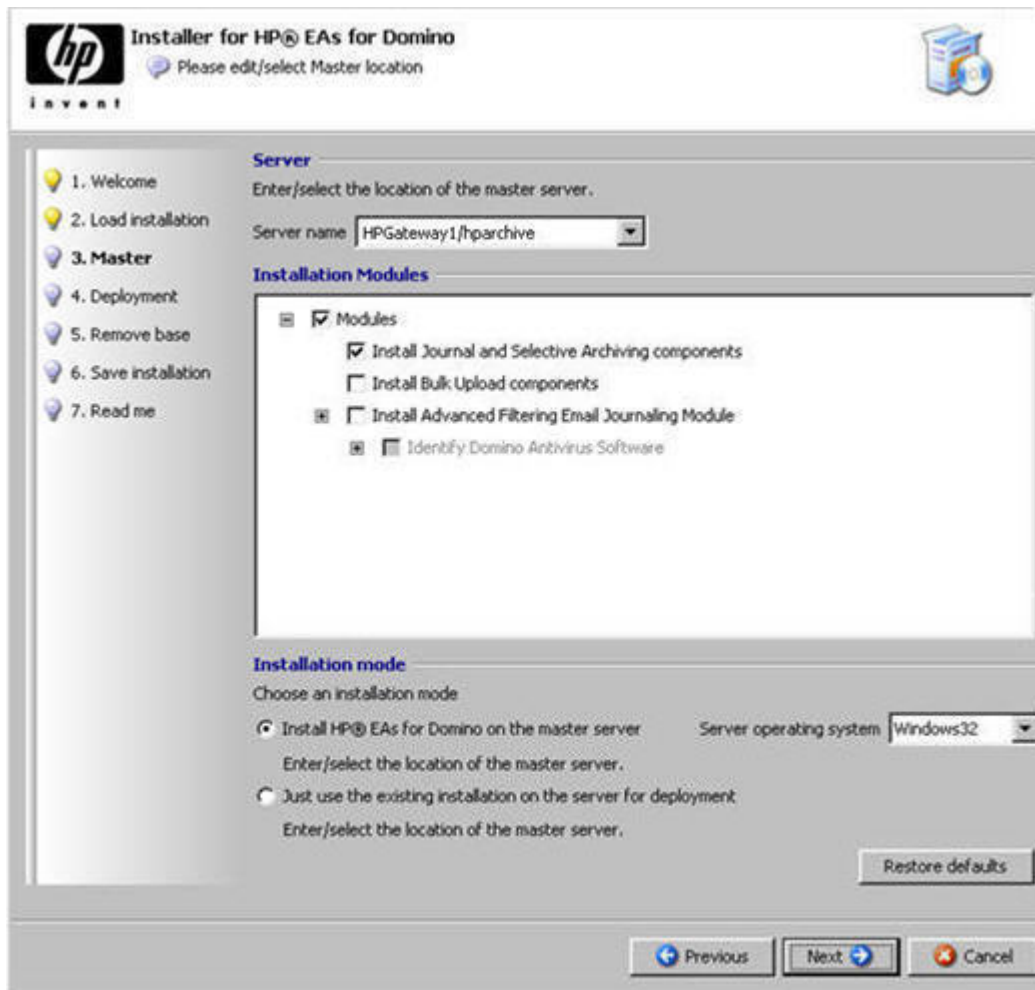
1. Open the Domino Administrator client using the HP Gateway administrator ID.
 - a. If the organization prefers to use another ID to create and sign databases and agents, switch to that ID by selecting **File > Security > Switch ID**.
 - b. Open the server that is used as the master HP Gateway server.
2. Open Windows Explorer, and navigate to the folder where the EAs Domino installation files were extracted. Locate the `server` directory and double-click the `Setup.exe` file.
3. Click **Next** at the 1. Welcome window.



NOTE:

An incorrect operating system might appear for the client used in the software installation. This value is obtained by the Java Virtual Machine and EAs Domino cannot override it. This issue does not affect the software installation.

4. Click **Next** at the 2. Load installation window.
5. In the 3. Master window, perform the following actions:
 - a. In the Server name drop-down list, select the HP Gateway server on which to install the software.
 - b. Select the **Modules** check box, and then select **Install Journal and Selective Archiving components**.
 - c. Under Choose an installation mode, select **Install HP EAs Domino on the master server**.
Verify that the correct server operating system is shown.
 - d. Click **Next**.



6. If a password dialog box appears, enter the password for the ID.
7. In the 4. Deployment window, click **Next**.
8. In the 5. Remove Base window, select whether to delete the temporary installation base (hp_riss_install.nsf) on the server, and then click **Next**.
 - If you want to save the installation base, click **No**.
Selecting No leaves the install base so you can review status messages recorded during the installation.
 - If you do not want to save the installation base, click **Yes**.
9. In the 6. Save Installation window, select the **Save this installation** check box if you want to save the installation (for example, to deploy the installation to other HP Gateway servers). Browse for a location in which to save the installation.
The installation configuration is saved as an XML file.
10. In the 7. Readme window:
 - Verify that the View readme check box at the top of the window is selected.
 - Verify that the installation information is correct.
Make sure that Install on master server has been set to **Yes**.

11. Click **Install**.

An installation progress bar is displayed.

After the software is successfully installed, the Readme appears on screen.

12. Click **Finish**.

13. Complete the master HP Gateway server installation:

- Set the ACL for the EAs Domino databases using the instructions in the next section.
- Edit the Global Configuration and Server Definition documents in the HP EAs-D API database. See [“Editing the Global Configuration document”](#) on page 139 and [“Configuring the Server Definition document”](#) on page 147.
- Configure the HP Gateway server for DAS. See [“Preparing the HP Gateway server for DAS”](#) on page 81.

Setting access control (ACL)

Configure the access control settings for the EAs Domino databases that are used on the HP Gateway servers.

1. In the Domino Administrator client, click the **Files** tab and select the `hprim` folder in the Domino data directory.
2. Right-click HP EAs-D API, and select **Access Control > Manage**.
3. Ensure the correct access is set for the databases listed in [“EAs Domino ACL for HP Gateway databases”](#) on page 67.

For tighter security, you can adjust the default level in the databases to No access. This might be required if, for example, a group with access to the HP Gateway is not authorized to work with EAs Domino data.

4. Ensure that the ID used to sign the EAs Domino databases is added to the appropriate group (usually LocalDomainAdmins or LocalDomainServers).
5. Configure any other settings that the organization uses to set access to its databases.
6. Click **OK**, and close the window.

2.6 Preparing the HP Gateway server for DAS

The topics in this chapter describe how to configure the master HP Gateway server and backup Gateway servers for DAS, the synchronization of user accounts with the IAP.

These procedures are performed by the HP service representative.

- [Introduction](#), page 81
- [Building a consolidated directory](#), page 83
- [Scheduling the Directory Cataloger task](#), page 86
- [Creating and configuring the Directory Assistance database](#), page 86
- [Configuring the pointer](#), page 88
- [Verifying the LDAP configuration](#), page 88
- [Editing the DAS Names Configuration document](#), page 89
- [Configuring the HP EAs-D DAS Names database](#), page 95
- [Restarting the server](#), page 96
- [Rebuilding views in the DAS-related databases](#), page 97
- [Configuring the DAS backup servers](#), page 97

For the procedures required on the IAP, see [“Directory Integration”](#) on page 366.

Introduction

To prepare for DAS, entries from the customer's Domino Directories are copied and aggregated into a single consolidated directory on the master HP Gateway. Selected data in the consolidated directory is then copied to the HP EAs-D DAS Names database (`hprim\hp_dasnames.nsf`). This database is used by DAS to create and update user and group accounts on the IAP.

Changes to the DAS process

HP EAs Domino 2.1 includes support for three new features:

- IAP repositories for shared mailboxes, which are represented as mail-in databases in the Domino Directory. Access control is provided via mappings from directory groups.
- An IAP repository retention period that is set via an attribute in the Domino Directory for each user or shared mailbox.
- Support for legacy email addresses, which allows users to access messages archived under an old email address.

The DAS process has been changed to support this functionality. [“Directory Integration”](#) on page 366 describes the configuration changes that must be made on the IAP side.

On the EAs Domino side, the new DAS Names database is used as the data source for DAS. The Populate DAS Names agent in the database copies selected information from the consolidated Domino Directory and adds custom values, using the settings in the DAS Names Configuration document.

Shared mailbox support

Shared mailboxes are stored as Mail-In Database documents in the consolidated Domino Directory and are imported into the IAP as groups via the DAS Names database.

The DAS process:

- Creates a group repository for the shared mailbox.
- Imports attributes from the Mail-In Database document including the email addresses of associated users.
- Creates a simple routing rule for each email address that is associated with the shared mailbox.
- Finds the users in the IAP that correspond to users in the Mail-In Database document, and gives those users access to the shared mailbox repository.

Access control is provided via mappings from Domino Directory groups. (If the groups are managed in another directory, such as an LDAP directory, the customer is responsible for synchronization between that directory and the Domino Directory.)

Retention attribute support

An optional `iapRepositoryRetention` attribute can be used to set the retention period in user and shared mailbox repositories.

This attribute is located in the Domino Directory Person and Mail-In Database documents. (If the attribute is created in another directory, such as an LDAP directory, the customer is responsible for synchronization between the directory and the Domino Directory.)

When a user or group mailbox is imported into the IAP:

- DAS sets the repository retention period to be the value of the `iapRepositoryRetention` attribute associated with the user or group.
- The `iapRepositoryRetention` period is not respected if it is less than the IAP domain retention period set in the `Domain.jcml` file. In that case, DAS sets the repository retention period to be the same as the domain retention period.
- The default unregulated repository retention period in `Domain.jcml` is used if the `iapRepositoryRetention` attribute is missing or has not been set.

Legacy email address support

Users with new email addresses can now successfully search for messages in their IAP repository that were archived under their old email address. When this optional feature is set in the DAS Names Configuration document and the DAS job is run, legacy email addresses are added as alias/proxy addresses in the IAP user repositories.

No changes are required on the IAP. However, a DAS job does take longer to run when this feature is implemented.

Previously-ingested messages that ended up in the IAP's Catchall repository before this feature was introduced can be re-routed using the IAP's reprocessing function.

Building a consolidated directory

EAs Domino uses a consolidated Domino Directory to aggregate Person, Mail-In, and Group documents from the customer Domino Directories that are employed in the archiving process. The customer's Domino Directories are not affected in any way.

The steps below describe how to create the consolidated directory on the master HP Gateway server.

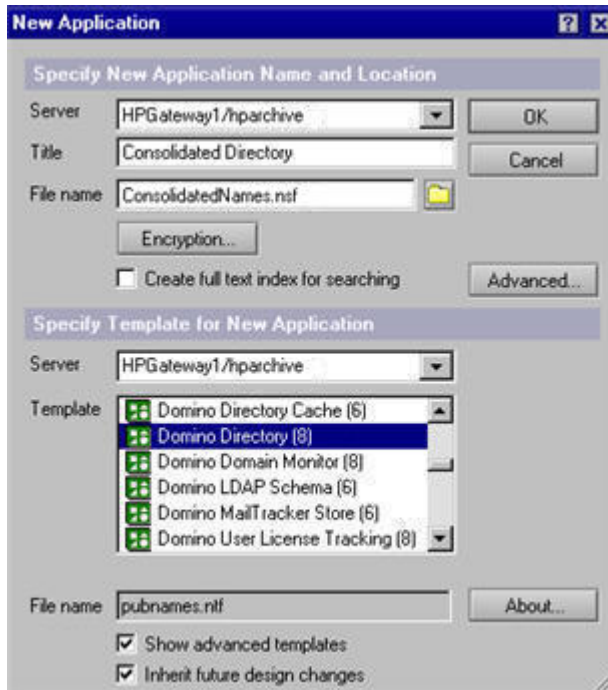
(For users upgrading from a previous version of EAs Domino: The customer's Domino Directories are copied directly into the consolidated directory when the Dircat task is run. Replicas of the customer's Domino Directories are no longer created on the HP Gateway.)

 **NOTE:**

The master HP Gateway and the Gateway server(s) used for DAS backup must be granted Reader access to each applicable Domino Directory in the customer mail domain.

1. From the Administrator client, select **File > Application > New**.
The New Application window appears.
2. In the Specify New Application Name and Location area:
 - a. Specify the master HP Gateway server in the **Server** box.
 - b. In the **Title** box, enter **Consolidated Directory**.
 - c. In the **Filename** box, name the database **ConsolidatedNames.nsf** and place it in the Domino data directory on the HP Gateway server.

3. In the Template for New Application area:
 - a. Select the HP Gateway server in the **Server** box.
 - b. Select the **Show advanced templates** check box.
 - c. Select **Domino Directory**.



4. Click **OK** and close the About document.
5. Click **Save & Close** in the Directory Profile form that appears.
6. Click **File > Application > Access Control** and ensure that:
 - The HP Gateway server, and the Gateways used for DAS backup, have Manager access with all roles.
 - The signer of the agents (if not the server ID) has Reader access.
7. Create the configuration document:
 - a. Under **Configuration**, expand **Directory** and select **Extended Directory Catalog**.
 - b. Click **Add Extended Directory Catalog**.

8. Configure the Extended Directory Catalog settings:

- Directories to include: Enter each customer Domino Directory used in the archiving process, in the format:
`CustomerServerName/CustomerOrg!!names.nsf`
These Directories will be copied directly into the consolidated directory when Dircat is run. Be sure to include any Domino Directories that contain only Group, Person, or Mail-In database entries.
- Additional fields to include: Add **MailServer**, **MailFile**, **HttpPassword**, and **ShowPassword** to the bottom of the list.
If support for legacy email addresses is required, and an additional field is used to configure this support, add the field to the list. This setting ("Additional field to scan for aliases") is configured in the Directory Entry Settings tab of the [DAS Names Configuration document](#).
- Remove duplicate users: Leave the default: **Yes**.
- Group types: Leave the default: **Mail and Multi-purpose**.
- Include Mail-In Databases: Leave the default: **Yes**.
- Include Servers: **No**.
- Restrict aggregation to server: Enter the name of the master HP Gateway server.

The screenshot shows the 'Extended Directory Catalog' configuration window with the 'Basic' tab selected. The window has three tabs: 'Basics', 'Advanced', and 'Administration'. The 'Basics' tab contains the following settings:

Directories to include:	ServerName/Org2!!names.nsf ServerName/Org5!!names.nsf
Additional fields to include:	FirstName MiddleInitial LastName Location MailAddress Shortname MailDomain InternetAddress MessageStorage Members AltFullName AltFullNameLanguage GroupType HttpPassword ShowPassword MailFile MailServer
Note: No fields means ALL	
Remove duplicate users:	Yes
Group types:	Mail and Multi-purpose
Include Mail-In Databases:	Yes
Include Servers:	No
Restrict aggregation to server:	HPGateway1/hparchive

9. Save and close the configuration document, and then close the consolidated Domino Directory.
10. If there is more than one HP Gateway server, replicate the consolidated directory to the other Gateway servers.

Scheduling the Directory Cataloger task

Schedule the days and times to run the Directory Cataloger (Dircat). Initially, this task builds the consolidated directory by copying data from the customer Domino Directories that are listed in the Extended Directory Catalog. After that, Dircat is run to keep the contents of the consolidated directory synchronized with the source Directories.

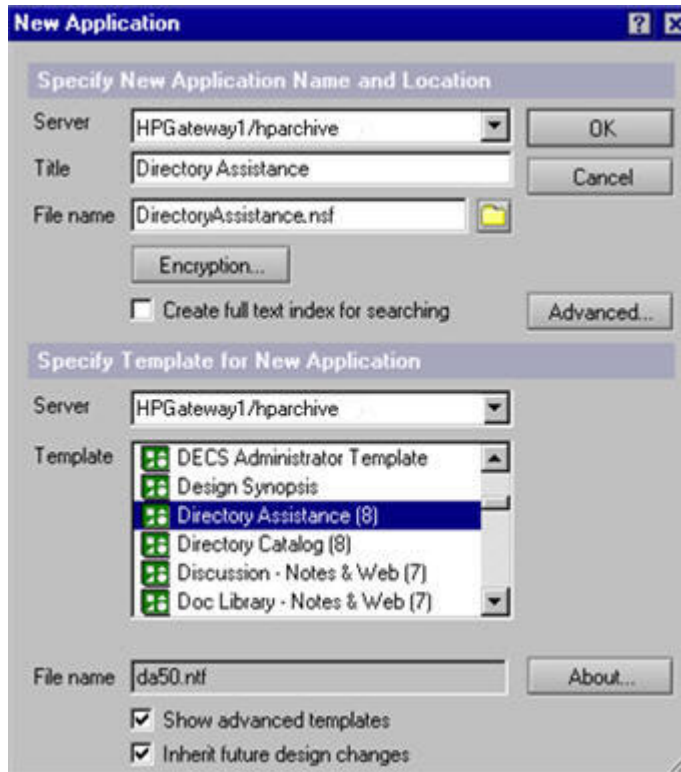
1. In the Administration client, click the **Configuration** tab, expand **Server**, and select **All Server Documents**.
2. Select the Server document for the master HP Gateway server, and click **Edit Server**.
3. Click the **Server Tasks** tab, and then click the **Directory Cataloger** tab.
4. Configure the following settings:
 - Directory catalog filenames: Add the filename of the consolidated Domino Directory you just created: **ConsolidatedNames.nsf**
 - Schedule: Select **Enabled**
 - Run Directory Cataloger task at: Enter **00:00 - 23:59**
 - Repeat interval of: Enter **30** minutes
 - Days of week: Ensure all days are selected
5. Save the Server document.
6. Complete steps 2–5 for the Gateway servers used for DAS backup. In step 4, ensure the Schedule is set to **Disabled**.

Creating and configuring the Directory Assistance database

The HP Gateway servers use Directory Assistance to look up entries in the consolidated directory. This section explains how to create the Directory Assistance database and document.

1. In the Administrator client, select **File > Application > New**.
The New Application window appears.
2. In the Specify New Application Name and Location area:
 - a. Specify the master HP Gateway server in the **Server** box.
 - b. In the **Title** box, enter **Directory Assistance**.
 - c. In the **Filename** box, name the database **DirectoryAssistance.nsf** and place it in the Domino data directory on the HP Gateway server.

3. In the Template for New Application area of the window:
 - a. Select the HP Gateway server in the **Server** box.
 - b. Select the **Show advanced templates** check box.
 - c. Select **Directory Assistance**.



4. Click **OK** and close the About document.
5. Click **File > Application > Access Control** and ensure that the master HP Gateway server, the Gateway servers used for DAS backup, and the HP administrator ID have Manager access with all roles.
6. In the Directory Assistance database, click **Add Directory Assistance**.
7. Configure the settings in the Basics tab:
 - Domain type: **Notes**
 - Domain name: Enter a name that is not a real, existing domain name. (This name is simply an internal handle that Domino uses.)
 - Company name: Enter a name that is not an existing company name.
 - Search Order: **1**
 - Make this domain available to: Select both options:
 - **Notes Clients Internet Authentication/Authorization**
 - **LDAP Clients**
 - Group Authorization: **Yes**
 - Use exclusively for Group Authorization or Credential Authentication: **No**
 - Enabled: **Yes**

8. Click the **Naming Context (Rules)** tab, and in the **N.C. 1** row configure the following settings:
 - OrgUnit and Organization: *
 - Enabled: **Yes**
 - Trusted for Credentials: **Yes**
9. Click the **Domino** tab:
 - a. In the **Replica 1** row configure the following settings:
 - Server Name: Enter the name of the master HP Gateway server.
 - Domino Directory Filename: Add the name of the HP EAs-D DAS Names database (hprim\hp_dasnames.nsf).
 - Enabled: **Yes**
 - b. In the **Replica 2** row, configure the settings used in step a, substituting the first DAS backup server in Server Name.
 - c. In the Replica 3–5 rows, repeat step b for any additional DAS backup servers.
10. Click **Save & Close**.
11. Replicate the Directory Assistance database to the DAS backup servers.

Configuring the pointer

Configure the pointer to the Directory Assistance database.

1. In the Domino Administrator client, click the **Configuration** tab, expand **Server**, and select **All Server Documents**.
2. Select the Server document for the master HP Gateway server, and click **Edit Server**.
3. On the Basics tab, locate the **Directory assistance database name** field in Directory Information, and enter the filename of the Directory Assistance database: **DirectoryAssistance.nsf**.
4. Click **Save & Close**.
5. Repeat steps 2–4 for each HP Gateway server used for DAS backup.

Verifying the LDAP configuration

Verify that the LDAP configuration in the Server Configuration document exists within the HP Gateway directory.

1. In the Domino Administrator client, click the **Configuration** tab.
2. Expand **Directory**, expand **LDAP**, and then click **Settings**.

If a message prompts you to create a Server Configuration document, click **Yes**, and then click **Save & Close**. Press **F9** to refresh.
3. Click **Edit LDAP Settings**.
4. Scroll to Automatically Full Text Index, and click **Yes** if it is not already selected.
5. Scroll to DN Required on bind, and click **Yes**.
6. Click **Save & Close**.

Editing the DAS Names Configuration document

Complete the DAS Names Configuration document to specify the information that is used to populate the DAS Names database.

1. In the Domino Administrator client, click the **Files** tab and open the `hprim` folder.
2. Open the **HP EAs-D API** database.
3. Open the document under **DAS Names Configuration** in the main view.
4. Configure the settings in each tab:
 - “[Directory Information](#)” on page 89
 - “[Directory Fields](#)” on page 90
 - “[Directory Entry Settings](#)” on page 91
 - “[Group Cache settings](#)” on page 95
 - “[Logging settings](#)” on page 95
5. Select **File > Save** to save the DAS Names Configuration document.

Directory Information

The settings in this tab define the type of consolidated directory entries that are copied to the DAS Names database.

DAS Names Configuration

Directory Information	Directory Fields	Directory Entry Settings	Group Cache Settings	Logging
[Directory Information]				
Consolidated Directory file name:	ConsolidatedNames.nsf			
Directory entries types to copy:	<input type="radio"/> Person	<input checked="" type="radio"/> Person & Mail-In Dbs		
	<input type="radio"/> Mail-In Database	<input type="radio"/> Other		
Require valid Internet address:	<input checked="" type="radio"/> Yes <input type="radio"/> No			
Require Internet password:	<input type="radio"/> Yes <input checked="" type="radio"/> No			

Field	Description
Consolidated Directory file name	The Domino Directories are compiled into a single consolidated directory: <code>ConsolidatedNames.nsf</code> (This directory was created in " Building a consolidated directory " on page 83.)
Directory entries types to copy	Select the type of consolidated directory entries to be copied to the DAS Names database: <ul style="list-style-type: none"> Person: Select if only creating/updating personal user accounts in the IAP. Mail-In Database: Select if only creating/updating group accounts (for shared mailboxes) in the IAP. Person & Mail-In Dbs: Select if both user and group accounts will be created and updated in the IAP. Other: Select if you prefer to create a Notes formula to define the entries that are copied. Enter the formula using a Notes @function. Include <code>Type="Person"</code> and/or <code>Type="Database"</code> along with other conditions as needed.
Require valid Internet address	Leave the default: Yes . (Required by DAS to create the user or group account on the IAP.)
Require Internet password	If you select Yes , only users who have Internet passwords assigned in the Domino Directory can log into the IAP.

Directory Fields

This tab lists the fields to be copied from the consolidated directory's Extended Directory Catalog to the DAS Names database. These fields are used in creating and updating accounts on the IAP and should not be edited.

Directory Information Directory Fields Directory Entry Settings Group Cache Settings Logging	
[Directory Fields]	
Standard Directory fields to copy:	Form; Type; FullName; MailDomain; MailServer; MailFile; InternetAddress; iapRepositoryRetention
Additional Directory fields to copy:	
Type	Fields
Person	FirstName; MiddleInitial; LastName; MailAddress; Shortname; HttpPassword
Database	Description

Field	Description
Standard Directory fields to copy	The fields in the directory catalog that are always copied to DAS Names and imported into the IAP accounts.
Person	Additional fields in the Person documents that are imported into DAS Names and IAP user accounts.
Database	Additional fields in the Mail-In Database documents that are imported into DAS Names and IAP group accounts.



NOTE:

Do not edit these fields unless you are specifically instructed to do so by HP support.

Directory Entry Settings

The settings in this tab can do four things:

- Define the rules for building an access list for IAP group repositories. Access is determined by the Member field, which is added to Mail-In Database documents when they are imported into DAS Names. The Member field contains a list of email addresses that correspond to users with group repository access.
- Define access control for the IAP group repositories.
- Define a Person document field to be scanned for legacy email addresses. The legacy addresses are added to the dominoProxyAddresses attribute that is sent to DAS, so that both old and new email addresses are listed in a user's IAP repository.
- Define a formula using one or more fields from the consolidated directory to set the IAP username (uid).

If you do not require support for any of these features, do not complete this tab.

[Directory Entry Settings]

Mail-In Database Distinguished Names

Org Unit and Org appended to Mail-In DB names: (Example: /OU=Mailbox/O=Acme Corp)

Repository Access Control

Manage repository access control for:

Enter a Notes @Function. The formula is applied to each Directory entry and must evaluate to "Yes" or "No" to determine whether access control is computed for that entry.

Match entries to access names/groups using: Fullname with prefix/suffix Notes @Formula None

Access Group prefix:

Access Group suffix:

Override access settings using field: Yes No

Alias Address Management

Scan FullName field for valid SMTP Aliases: Yes No

Additional field to scan for aliases:

IAP UID Mapping

Notes Formula for short name:

You can optionally provide a Formula to compute the short name to be used as a key for each user by entering that formula in this field. Leave it blank to use the default formula for this key. (Most customers will not want to change this value.)

Field	Description
Mail-In Database Distinguished Names	
Org Unit and Org appended to Mail-In Database names	Leave this field blank unless you want the organization and organizational unit appended to Mail-In Database names.
Repository Access Control: Determine the members of a group repository.	
Manage repository access control for	Enter any valid Notes @function formula that resolves to Yes or No for a Mail-In Database document. This formula is applied to each database entry to determine whether access control is computed for the entry.

Field	Description
Match entries to access names/groups using	<p>Determine how to find users who can access the group repository. These users are added to the Member field.</p> <ul style="list-style-type: none"> Fullname with prefix/suffix This option uses the Fullname from each selected document and combines it with a prefix and/or suffix to locate a matching group name and associated email addresses. The group name should follow a standard format, such as: GroupMailbox <unique ID><department or division> For example: GroupMailbox 123 CommercialDivision In this example, "GroupMailbox" is the prefix, "123" is the unique ID, and "CommercialDivision" is the suffix. Notes @Formula If you select this option, enter a Notes formula that calculates a list of user email addresses and/or group names associated with a shared mailbox. This formula runs in the context of a Mail-In Database document and has access to all the document's field information. All Notes formula features, including loop-ups, can be used to create the result list. None Select this option if a specific field in the Mail-In Database document is used to determine Member values. Then complete "Override access settings..." below.
Override access settings using field	<p>If the access list names and/or groups are stored in a specific field, select Yes and then enter the field name. (Make sure that the option in "Match entries..." above is set to None.)</p> <p>The field should hold either a multi-valued list of groups or a list of email addresses. Groups are expanded to find the Internet email addresses of their members.</p>
<p>Alias Address Management: If support for legacy email addresses is required, configure one of these settings.</p>	
Scan FullName field for valid SMTP Aliases	<p>When set to Yes, all Internet-style addresses from the User Name field in Person documents are synchronized with IAP user accounts. Addresses must be in valid RFC-821 address syntax.</p>
Additional field to scan for aliases	<p>If the legacy email addresses are in another, dedicated field in the Person documents, enter the name of the field.</p> <p>Addresses must be in valid RFC-821 address syntax.</p> <p>Note: If you use this option, add the field to the consolidated directory's Extended Directory Catalog, in "Additional fields to include." See step 8 in Building a consolidated directory.</p>
<p>IAP UID Mapping</p>	

Field	Description
Notes Formula for short name	<p>By default, the Notes ShortName is used to set the IAP username (uid) for logging in to the IAP. If you want to substitute a different field or combination of fields for the ShortName, complete a Notes formula to define them. The formula can use any field in the consolidated directory and do anything that the Notes formula language allows.</p> <p>The default formula is:</p> <pre data-bbox="609 359 1349 443"> @If (Type={Person}; ShortName; Type={Database}; @ReplaceSubstring (@Name ([Abbreviate];@Subset (FullName;1)); { }:{/};{_}:{.}); { }) </pre> <p>As an example, if you wanted to use the EmployeeID field instead of ShortName, the formula would be:</p> <pre data-bbox="609 516 1349 600"> @If (Type={Person}; EmployeeID; Type={Database}; @ReplaceSubstring (@Name ([Abbreviate];@Subset (FullName;1)); { }:{/};{_}:{.}); { }) </pre> <p>Note: If you complete this entry and also use IAP single sign-on, change the login type to Formula for the SSO Generate User Tokens agent. See step 6 in Configuring the HP EAs-D SSO database and the Generate SSO Tokens agent.</p>

Group Cache settings

Keep the default of **Yes** to ensure better performance when email addresses in the Member field are calculated.

Logging settings

The EAs Domino log file records the actions of the Populate DAS Names agent in the DAS Names database.

Field	Description
Agent log database	The location of the EAs Domino log file in the Domino data directory: hprim/hp_risslog.nsf
Log stream name	Populate DAS Names
Log level	Keep the default of None , unless General or Verbose are required for troubleshooting. Change this setting only when asked to do so by HP support.

Configuring the HP EAs-D DAS Names database

Follow the steps in the sections below to configure the DAS Names database.

Setting the ACL for DAS Names

Set access to the database.

1. In the Domino Administrator client, click the **Files** tab and select the `hprim` folder in the Domino data directory.
2. Right-click HP EAs-D DAS Names, and select **Access Control > Manage**.
3. Set the access for the following users:
 - LocalDomainAdmins (or substitute): **Manager**
Must have rights to delete documents and replicate or copy documents.
 - LocalDomainServers: **Manager**
Must have rights to delete documents and replicate or copy documents.
 - OtherDomainServers: **No access**
 - Notes ID that signed the databases and agents during installation of the EAs Domino databases: **Manager**
Must have rights to delete documents and replicate or copy documents.
4. Set Default to **Manager**.
Must have rights to delete documents and replicate or copy documents.
5. Configure any other settings that the organization uses to set access to its databases.
6. Click **OK**, and close the window.

Enabling the Populate DAS Names agent

The Populate DAS Names agent in the HP EAs-D DAS Names database reads the consolidated directory and the DAS Names Configuration document and populates the DAS Names database.

Schedule and enable the agent by following these instructions:

1. Open HP EAs-D DAS Names (`hprim\hp_dasnames.nsf`) in the Domino Designer client.
2. Expand **Codes** and then expand **Agents**.
3. Open the **Populate DAS Names** agent.
4. Change the agent's schedule if necessary.

The default is for the agent to run every two hours.

Do not change any of the other default settings.

5. Click **Enable**. In the dialog box that appears, select the master HP Gateway server as the server the agent runs on, and then click **OK**.

 **NOTE:**

Do not enable the Directory Catalog Status Report agent in DAS Names.

Running the agent manually

The Populate DAS Names agent can be run manually from the HP Gateway server console. (Wait until the initial setup of the HP Gateway server is complete, and the Domino server has been restarted. You should rebuild the views in the consolidated directory before running the agent for the first time.)

 **IMPORTANT:**

Do not run this agent manually while it is scheduled in the Agent Manager. This will create duplicate entries in DAS Names.

1. Pause the agent's schedule on the master Gateway:
`tell amgr pause`
2. Make sure the Agent Manager is paused by checking the running tasks:
`show tasks`
3. Run the Populate DAS Names agent:
`tell amgr run "hprim\hp_dasnames.nsf" 'Populate DAS Names'`

Restarting the server

Restart the Domino server on the HP Gateway after configuring the server for DAS.

If you are completing the initial set up of the Gateway server and a `mail.box` file exists, remove the file during the Domino server restart.

Rebuilding views in the DAS-related databases

After Dircat has completed its first run and before running the Populate DAS Names agent for the first time, rebuild the views in the consolidated directory, `ConsolidatedNames.nsf`, by pressing CTRL+SHIFT+F9.

Before running a DAS job for the first time on the IAP, rebuild the views in the DAS Names database, `hp_dasnames.nsf`, by pressing CTRL+SHIFT+F9. This will ensure that IAP user accounts are successfully created or updated.

Configuring the DAS backup servers

If multiple HP Gateway servers are deployed, one or more Gateways should be configured as a backup for the DAS process.

To configure each DAS backup server:

1. Ensure that firewall ports 389 and 636 are open for the LDAP service and the LDAP task is running on the backup server.
2. Install the HP EAs-D DAS Names database on the server.

This database is deployed to the backup server during installation of the EAs Domino software. (See [“Deploying the archiving installation to additional HP Gateway servers”](#) on page 100.) If DAS Names is not deployed during the software installation, you can manually replicate it from the master to the backup server.

3. Ensure that the consolidated directory and the Directory Assistance database are replicated from the master Gateway server to the backup server.
4. Ensure that the pointer to the Directory Assistance database has been configured on the backup server.

See [“Configuring the pointer”](#) on page 88.

5. Verify the LDAP configuration on the backup Gateway server.

See [“Verifying the LDAP configuration”](#) on page 88.

To switch the DAS process from the master HP Gateway server to a backup server, follow these instructions:

1. Stop the Dircat task and disable the Populate DAS Names agent on the master HP Gateway.
2. In the Domino Administrator client:
 - a. Open the Server document for the master HP Gateway server.
 - b. Click the Server Tasks tab and the Directory Cataloger tab, and then disable the schedule.
 - c. Open the Server document for the backup server.
 - d. Click the Server Tasks tab and the Directory Cataloger tab, and enable the schedule.
 - e. Open the consolidated directory. In the “Restrict aggregation to server” field, change the name to the DAS backup server.

- 3.** In the Domino Designer client:
 - a.** Open the HP EAs-D DAS Names database.
 - b.** Open the Populate DAS Names agent and select the DAS backup server as the server the agent runs on.
 - c.** Enable the agent.
- 4.** In PCC Web Administration on the IAP:
 - a.** Navigate to the Account Synchronization page.
 - b.** Click the LDAP connection and open it for editing.
 - c.** Change the Host Name value to the IP address of the backup Gateway server, then save the change.

2.7 Configuring additional HP Gateway servers

If more than one HP Gateway server is deployed, use the instructions in this chapter to configure each additional server for EAs Domino.

- [Configuration steps](#), page 99
- [Deploying the archiving installation to additional HP Gateway servers](#), page 100

Configuration steps

Follow these steps for the additional HP Gateway servers:

1. Ensure that a Server Connection document has been created on the master Gateway server to each additional Gateway server.
See [“Creating Server Connection documents”](#) on page 52.
2. Configure the Domino server settings on each additional Gateway server:
 - [“Setting up security on the HP Gateway server”](#) on page 56
 - [“Editing the Agent Manager parameter values”](#) on page 57
 - [“Creating connection documents to the customer mail servers”](#) on page 57
 - [“Creating and configuring the foreign SMTP domain document”](#) on page 58
 - [“Creating and configuring the SMTP connection document”](#) on page 59
 - [“Creating a configuration document for the HP Gateway server”](#) on page 59
3. Limit the size of the Domino log file on the server.
See [“Limiting the log file size”](#) on page 60.
4. Add a parameter in `notes.ini` to list the customer’s mail domain, if selective archiving and End Owner Receipt are used.
See [“Adding the EAsD_Domain parameter”](#) on page 61.
5. Ensure the consolidated directory has been replicated from the master Gateway server.
6. Install the EAs Domino software.
See [“Deploying the archiving installation to additional HP Gateway servers”](#) on page 100.
7. Ensure the additional HP Gateway servers are covered by a Server Definition document.
See [“Configuring the Server Definition document”](#) on page 147.

Deploying the archiving installation to additional HP Gateway servers

When there is more than one HP Gateway server, deploy the archiving installation from the master HP Gateway server to the other Gateway servers by following the instructions below.

Before installing the software, ensure that:

- The Agent Manager, Router, and Replicator tasks are running on the HP Gateway servers.
- All non-Lotus Notes applications are closed.

The installation must be performed from a Windows client workstation.

1. In the Domino Administrator client, switch to the ID that was used to install the EAs Domino files on the master HP Gateway server.
2. Open Windows Explorer, and navigate to the folder where the EAs Domino installation files were extracted. Locate the `server` directory and double-click the `Setup.exe` file.
3. Click **Next** at the 1. Welcome window.



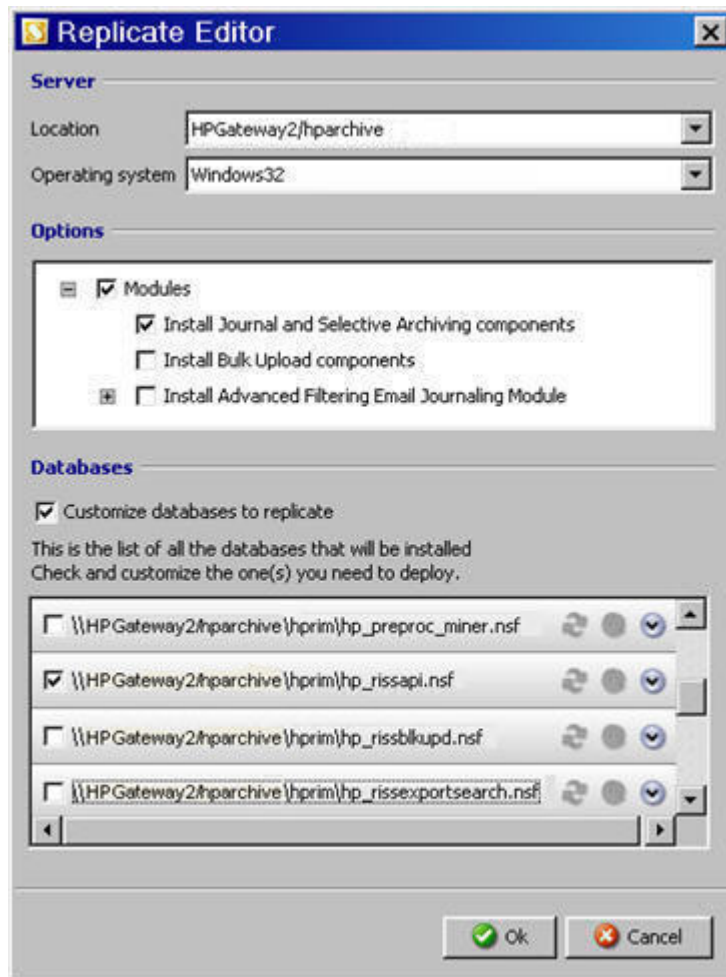
NOTE:

An incorrect operating system might appear for the client used in the software installation. This value is obtained by the Java Virtual Machine and EAs Domino cannot override it. This issue does not affect the software installation.

4. In the 2. Load installation window, select **Load an existing installation** and browse for the location of the installation database.
The 3. Master window appears.
5. In the 3. Master window:
 - a. Select the master HP Gateway server from the drop-down list at the top of the window.
 - b. Under Installation mode, select **Just use the existing installation on the server for deployment**.
 - c. Click **Next** to open the 4. Deployment window.
6. In 4. Deployment, select the **Deploy HP EAs for Domino on other servers** check box.

7. Click **Add**.

The Replicate Editor appears.



8. In the Replicate Editor:

- a. Select the location of the first HP Gateway server where the installation will be deployed.
- b. Confirm the Gateway server's operating system.
- c. Select the **Modules** check box, and then select **Install Journal and Selective Archiving components**.
- d. Select the **Customize databases to replicate** check box, and then select the following databases for replication:
 - HP EAs-D API (hp_rissapi.nsf)
 - HP EAs-D Users (hp_rissuser.nsf)
 - HP EAs-D Stats (hp_easd_stats.nsf)
 - HP EAs-D Alert (hp_rissalert.nsf)

This subset of EAs Domino databases should be replicated to all additional HP Gateways.

In addition, replicate HP EAs-D DAS Names (hp_dasnames.nsf) to the Gateway server(s) designated as backup for the DAS process.

- e. Click **OK**, and then click **Next**.

9. To add another HP Gateway server, click **Add** and repeat the procedure in step 9.
10. After configuring the deployment, confirm the deployment locations and the number of databases that will be replicated.

If you need to make adjustments, select the relevant server using the up/down arrows, and then click **Edit** or **Remove**.



11. Click **Next** when you are finished adding the servers.
12. In the 5. Remove Base window, select whether to delete the temporary installation base (hp_riss_install.nsf) on the server, and then click **Next**.
 - If you want to save the installation base, click **No**.
 - If you do not want to save the installation base, click **Yes**.
13. In the 6. Save Installation window, select the **Save this installation** check box if you want to save the installation. Browse for a location in which to save the installation.
14. In the 7. Readme window:
 - Verify that the View readme check box at the top of the window is selected.
 - Verify that the installation information is correct.
 - Ensure that Install on master server has been set to **No**.
15. Click **Install**.

After the software is installed, the Readme appears on screen.
16. Click **Finish**.
17. Set the ACL for the EAs Domino databases.

See "[Setting access control \(ACL\)](#)" on page 80.
18. Restart the Domino server on the HP Gateway.
19. After the server is restarted, use the Administrator client to delete mail.box, if it exists.

2.8 Installing HP EAs Domino components in the customer environment

The procedures in the previous chapters covered EAs Domino software installation on the HP Gateway servers.

EAs Domino files are installed on the customer's Domino servers in the following cases:

- For compliance archiving, some EAs Domino files are installed on the organization's mail servers. For the installation procedures, see “[Configuring compliance \(journal\) archiving](#)” on page 201. Archiving of the journals is performed from the HP Gateway servers.
- Bulk Upload can be executed on an application server in the customer environment. Archiving of the mail files discovered by Bulk Upload is performed from the HP Gateway server, after the Bulk Upload database is replicated to the Gateway server. To install this application, follow the procedures in [Using Bulk Upload](#), page 223.
- When DWA Extension or Export Search are implemented, the software to retrieve messages in DWA or to export archived messages is installed on Domino server(s) in the mail environment. The installation procedures are described in the following chapters:
 - [Configuring DWA Extension](#), page 255
 - [Using Export Search](#), page 269
- For single sign-on to the IAP (SSO), an HP EAs-D SSO database must be installed on the organization's mail servers. For the procedure to follow, see “[Configuring IAP single sign-on](#)” on page 289.

To upgrade an EAs Domino installation on a customer server, see “[Upgrading HP EAs Domino components on customer servers](#)” on page 123.

HP EAs-D API database in the mail environment

The EAs Domino configuration database (HP EAs-D API) must be installed and replicated among all servers in the customer's mail environment that execute EAs Domino applications (Advanced Filtering, DWA Extension, Export Search, or Bulk Upload).

The HP EAs-D API database used in the mail domain is distinct from the HP EAs-D API database in the HP Gateway domain. This allows separation of the HP Gateway/remote mining configuration requirements from the customer's mail environment.

❗ IMPORTANT:

If EAs Domino databases are installed manually on customer servers, add the following entry to the `notes.ini` file:

```
hprim_api=hprim\hp_rissapi.nsf
```

(This entry is added automatically when the EAs Domino installer is used to install Advanced Filtering, DWA Extension, Export Search, or Bulk Upload components.)

2.9 Upgrading or migrating an HP EAs Domino installation

This chapter describes four upgrade/migration scenarios:

- [Upgrading to remote mining from a local mining installation](#), page 106
- [Upgrading an existing remote mining installation](#), page 110
- [Upgrading HP EAs Domino components on customer servers](#), page 123
- [Replacing existing HP Gateway hardware](#), page 127

Consult this table to decide which scenario to use.

Table 10 EAs Domino upgrade and migration scenarios

Current EAs Domino installation	Upgrade/migration scenario
<p>Local mining</p> <p>Local mining on mail servers is no longer supported as of the EAs Domino 2.1 release. EAs Domino archiving software that is installed and archiving on customer mail servers must be disabled on the mail servers and upgraded for remote mining on the HP Gateway.</p> <p>An EAs Domino 2.1.x installation requires more powerful, and sometimes additional, HP Gateway servers than have been used with earlier versions of EAs Domino.</p>	<p>Upgrading to remote mining from a local mining installation, page 106</p>
<p>RIM for Domino version 1.6</p> <p>Support for RIM for Domino 1.6 ended in November, 2010. For continued support, customers must upgrade to EAs Domino 2.1.x and install new HP Gateway hardware. Older Gateway servers (for example, HP ProLiant G4 servers) are not supported for EAs Domino 2.1.x due to their limited CPU, memory, disk speed, and disk space.</p>	<p>Upgrading to remote mining from a local mining installation, page 106</p>
<p>Remote mining: EAs Domino version 2.0.x</p> <p>If the existing HP Gateway servers are already configured for remote mining and are not experiencing performance problems, they might be sufficiently powerful for the software to be upgradeable in place.</p>	<p>Upgrading from EAs Domino 2.0.x to version 2.1.2, page 110</p>
<p>Remote mining: EAs Domino version 2.1</p> <p>If you are upgrading a remote mining installation from EAs Domino 2.1 or 2.1.1 to EAs Domino 2.1.2, follow this procedure.</p>	<p>Upgrading from EAs Domino 2.1 or 2.1.1 to version 2.1.2, page 117</p>
<p>EAs Domino journaling or other components in the customer environment</p> <p>If Advanced Filtering, DWA Extension, Export Search, and/or IAP single sign-on software components are currently installed on customer servers, they must be upgraded on those servers.</p>	<p>Upgrading HP EAs Domino components on customer servers, page 123</p>

Current EAs Domino installation	Upgrade/migration scenario
<p>HP Gateway hardware</p> <p>If only the HP Gateway servers are being replaced and the EAs Domino software is not being upgraded, follow this procedure.</p>	<p>Replacing existing HP Gateway hardware, page 127</p>

Before starting an upgrade:

- Complete the upgrade worksheet: “[Software upgrade checklist](#)” on page 351.
- We recommend that you make backup copies of all currently-installed EAs Domino database files.

Upgrading to remote mining from a local mining installation

Overview

In this scenario, new HP Gateway hardware is installed with EAs Domino 2.1.2 software and the existing EAs Domino archiving installation is shut down.

This scenario is required when the HP Gateway server does not meet EAs Domino 2.1.2 hardware requirements (listed in the support matrix) and/or the EAs Domino archiving software is installed on the customer’s mail servers.

The scenario entails:

- Installing EAs Domino 2.1.2 on one or more new HP Gateway servers.
- Copying configuration information from the existing EAs Domino archiving installation.
- Completing the new configuration.
- Putting the new HP Gateway servers into production.
- Shutting down the old installation and removing the archiving software from the customer’s mail servers.

Upgrade instructions

Before upgrading the EAs Domino software, ensure that:

- The contents of the installation media have been extracted to a temporary folder.
- Java Runtime Environment (32-bit) version 1.6 or later is installed on the HP Gateway server.
- All non-Lotus Notes applications are closed.

Upgrading to a remote mining installation

1. Configure the environment on the new HP Gateway servers:
 - a. Install the Windows 2008 R2 server software and the Lotus Domino software on the new HP Gateway servers.

Follow the instructions in each section of “[Preparing the HP Gateway environment](#)” on page 43.

❗ **IMPORTANT:**

If the software is being installed on an HP ProLiant DL360 G6 or G7 server, bring an external USB CD/DVD drive to the installation. These servers are not equipped with an internal CD/DVD drive.

- b.** Configure the Domino server settings on the new HP Gateway servers.

For the Gateway server acting as the master server, follow the instructions in each section of [“Configuring the master HP Gateway server”](#) on page 55.

For additional Gateway servers, follow the instructions in [“Configuring additional HP Gateway servers”](#) on page 99.
- c.** Install the EAs Domino 2.1.2 software on the new HP Gateway servers.

For the master Gateway server, follow the instructions in [“Installing the HP EAs Domino software on the master HP Gateway server”](#) on page 77.

For additional Gateway servers, follow the instructions in [“Deploying the archiving installation to additional HP Gateway servers”](#) on page 100.
- 2.** Copy configuration information from the existing installation by following the directions in step 3 or step 4, depending on the software version of the existing installation.
- 3.** Follow these instructions if the existing software is RIM for Domino 1.6.x:

 - a.** Open the HP EAs-D API database on the new HP Gateway.
 - b.** Open the API database on the existing installation, and then copy the mining rule documents from the existing database into the API database on the new Gateway server.
 - c.** From the menu on the new API database, select **Actions > Migrate Configurations**.

A page of instructions opens, which includes buttons for additional actions.
 - d.** Follow the instructions on the page to pull configuration information from the existing RIM for Domino 1.6.x installation into the EAs Domino 2.1.2 configuration on the new Gateway server.
- 4.** Follow these instructions if the existing software is EAs Domino 2.0.x:

 - a.** Open the HP EAs-D API database on the new HP Gateway and delete the Global Configuration document.
 - b.** Open the API database in the existing installation and select and copy the following documents:

 - Global Configuration document
 - Server Definition documents
 - Preprocessing Control documents
 - Mining rule documents

Do not copy Tombstone Prototype documents, unless there are custom Prototype documents that need to be used in the new installation.
 - c.** Paste the copied documents into the EAs-D API database on the new Gateway server.

 **NOTE:**

It is possible that the names (keys) of some existing configuration documents will conflict with the default set created by the EAs Domino installer. If this is the case, rename or delete the default configuration documents to avoid possible confusion. (Open the document to check the document version in the upper right corner.) Ensure that pasting documents into the new configuration does not result in more than one default for any configuration type.

5. Steps 3 and 4 copied over as much of the existing installation's configuration as possible to the new installation. Refresh the configuration documents so that new default rules are applied:
 - a. In the new HP EAs-D API database, select all the documents by pressing **CTRL + A**.
 - b. On the menu, select **Actions > Tools > View Refresh Fields** to run the agent that refreshes the selected documents.
6. Open and edit the following tabs in each mining rule:
 - **User Membership** tab: Make sure the **Include Users on selected Mail server(s)** field is set appropriately. If **Local server** is selected, change the value to **All servers**. If **Only Selected server(s)** is selected, the values can usually be left as is.
 - **Tombstone Settings** tab: Ensure that the settings are correct, as there are new options in EAs Domino 2.1. If DWA Extension is implemented, this tab must be edited so that a new 2.1 tombstone prototype key can be used. See "[Tombstone Settings tab](#)" on page 168 for configuration information.
 - **Session Settings\Session Limits** tab: Select **Yes** to Allow Remote Mining of databases.
7. Check the settings in the configuration documents and edit where necessary:
 - Ensure that all fields in each Server Definition document are completed correctly, including the IAP Login and IAP Password fields. See "[Configuring the Server Definition document](#)" on page 147 for information.
 - Ensure that all HP Gateway servers are covered by a Server Definition document.
 - Edit the Global Configuration document. See "[Editing the Global Configuration document](#)" on page 139.
 - Edit the PreProcessing Control documents. See "[Configuring the Preprocessing Control document](#)" on page 177.
 - If DWA Extension is implemented, edit the Tombstone Prototype document for one of the 2.1 TSKeys. See "[Configuring the Tombstone Prototype document](#)" on page 261.
8. Configure the master HP Gateway server and backup Gateway servers for DAS. See "[Preparing the HP Gateway server for DAS](#)" on page 81.

9. Schedule and enable the agents:
 - a. Schedule and enable the preprocessing agents on each new HP Gateway server.
For the steps to follow, see [“Scheduling and enabling the preprocessing agents”](#) on page 182.
 - b. Configure the archiving agents and the Get Held Messages agent on the new Gateway servers.
The procedures to configure and schedule these agents are described in [“Configuring the archiving agents”](#) on page 185.
 - c. Schedule and enable the Purge_Document agent in the HP EAs-D Stats, HP EAs-D Alert, and HP EAs-D Log databases.
 - d. If selective archiving is used, schedule and enable the agents in the HP EAs-D Users database.
See [“Scheduling the Profile Agent”](#) on page 187 and [“Enabling other HP EAs-D User agents”](#) on page 187.
 - e. If DWA Extension is implemented, schedule and enable the Purge_Document agent to remove tombstone conversion requests in the HP EAs-D SC Request database on the new Gateway servers.
See [“Removing conversion requests from the HP EAs-D SC Request database”](#) on page 267.
10. Ensure that a rissminer program document for each mining rule is scheduled on the new HP Gateway servers, so that archiving can begin.
See [“Running an archiving job”](#) on page 193.

Shutting down local mining

When archiving is running properly on the new HP Gateway servers, follow these steps on the mail servers:

1. Shut down local mining by disabling the rissminer program documents on each mail server.



NOTE:

Any messages that were tagged for processing by rissminer will be retagged by rissminer in the new EAs Domino installation. This occurs after the Reference Document Retry interval (configured in the mining rule) has elapsed.

2. Do one of the following:
 - If Advanced Filtering, DWA Extension, IAP single sign-on, and/or Export Search are deployed on a customer server, upgrade those components on the relevant servers.
Follow the directions in [“Upgrading HP EAs Domino components on customer servers”](#) on page 123.
 - If none of the above components is installed on a customer server, remove the software using the procedure in [“Uninstalling the HP EAs Domino software”](#) on page 131.
3. Remove the IAP foreign domain document and the connection documents to the old HP Gateway servers from the Domino mail domain servers.
See [“Removing Domino configuration files”](#) on page 134.
4. Shut down the old HP Gateway servers.

Upgrading an existing remote mining installation

- [Upgrading from EAs Domino 2.0.x to version 2.1.2, page 110](#)
- [Upgrading from EAs Domino 2.1 or 2.1.1 to version 2.1.2, page 117](#)

Upgrading from EAs Domino 2.0.x to version 2.1.2

Introduction

In this scenario, the EAs Domino software on existing HP Gateway servers is upgraded to EAs Domino 2.1.2. The existing Gateway servers must meet EAs Domino 2.1 hardware requirements.

The scenario entails:

- Backing up the current EAs Domino installation.
- Stopping all archiving processes.
- Replacing system level executables, including EXE, DLL, and JAR files with EAs Domino 2.1.x archiving components.
- Upgrading the design of existing EAs Domino databases and templates.
- Adding new EAs Domino 2.1.x databases and templates.
- Adding new EAs Domino 2.1.x documents to the HP EAs-D API database.
- Restarting archiving.

Upgrade instructions

Before upgrading the EAs Domino software, ensure that:

- The contents of the installation media have been extracted to a temporary folder.
- A Remote Desktop connection has been created on the client to each HP Gateway server.
- Java Runtime Environment (32-bit) version 1.6 or later is installed on the HP Gateway server.
- All non-Lotus Notes applications are closed.

Preparing the HP Gateway servers for the upgrade

1. Back up the following items:
 - EAs Domino databases
 - Consolidated Domino Directory used for DAS
 - Directory Assistance database

2. Stop rissminer, the mining executable, from running on all HP Gateway servers:
 - a. Choose one of the HP Gateway servers to be the “master” for purposes of this installation.
 - b. Start the Domino Administrator client.
 - c. Select **File > Open Server** and open the master Gateway server.
 - d. Click the **Configuration** tab, expand **Servers** and select **Programs**.
 - e. Disable each rissminer program document so that rissminer stops running on schedule.
 - f. On the master Gateway server, click the **Server** tab, then the **Status** tab, and open the Domino server console.
 - g. Click **Live** in the upper right part of the view to start live console. This allows you to see what is happening on the server in real time.
 - h. Force the master HP Gateway server to replicate to all the other Gateway servers so that the changes to the program documents propagate to all the Gateway servers:
 - In the server console, enter the following command in the Domino Command field at the bottom of the window:


```
rep <Gateway server name> names.nsf
```

 (where <Gateway server name> is the name of a target Gateway server)

For example:

```
rep Gate2/mydomain names.nsf
```
 - Click **Send**.
 - Repeat these steps for each target Gateway server.

You will see the replications occur in the server console.

3. In the Designer client, disable the Archive and Tombstone agents and the Profile Agent.

4. Locate the Domino server executable folder.

You can enter the following command in the Domino server console to find the locations of the Domino executables and data folders:

```
Show Stat Server.Path.*
```

The output will look something like this:

```
Server.Path.Configfile = C:\Domino\notes.ini
Server.Path.Data = C:\Domino\data
Server.Path.Executable = C:\Domino\
```

Remember the locations for later use.

5. Using the Domino Administrator client, open the Domino server on each HP Gateway and enter the following command in the server console:

```
quit
```

Wait until the server is completely shut down. (This process can take several minutes.) The Domino server console will close automatically.

6. Using Remote Desktop connections, follow these steps on each HP Gateway server:
 - a. Make a backup copy of the `notes.ini` file in the Domino executable directory.
 - b. In a text editor, open the `notes.ini` file for editing.
 - c. Find the entry that begins with:
`ServerTasks=`
 For example: `ServerTasks=Update, Replica, Router, AMgr, AdminP, LDAP`
 - d. Remove **,AMgr** from the server tasks.
 This prevents the Agent Manager from loading when the Domino server is restarted. The Agent Manager cannot be running while EAs Domino database designs are being replaced.
 - e. Save the `notes.ini` file.
 You can keep the file open, since it will be edited again in later steps.

Upgrading the EAs Domino installation

1. Replace the EAs Domino system level executables via Remote Desktop.
 Confirm file replacements if prompted by Windows.
 - a. Replace `rissminer`.
 The mining executable file, `nrissminer.exe`, is located in the Domino server executable folder on the HP Gateway.
 In Windows File Explorer, replace the current file on each HP Gateway server with the `nrissminer.exe` file from the installation package. In the installation package, the file is located in:
`RELEASE\server\resources\applications\hpRimServerInstall_<version>\data\container.zip\Windows32\{BIN}\`
 - b. Replace the JAR files.
 There are four JAR files that must be replaced on each HP Gateway server:
`activation*.jar, dsn.jar, easdNet.jar, retriever*.jar`
 On the server, they are located in the `<Domino executable folder>\jvm\lib\ext` folder.
 Two of the JAR files (shown with a * above) include a version number; for example:
`activation 1.1.1.jar`
 You must remove any existing JAR file with the `activation` or `retriever` root name and add the JAR file from installer package.
 The JAR files are located in the installer package in:
`RELEASE\server\resources\applications\hpRimServerInstall_<version>\data\container.zip\Windows32\{BIN}\jvm\lib\ext\`
2. In the Domino administrator client, restart the Domino server on each Gateway by entering the following command in the Domino server console:
`restart server`

3. Upgrade the design of the EAs Domino databases in the <Domino data>\hprim folder:
 - a. Replace the design of the HP EAs-D SC Request database (hp_rissreq.nsf), using the instructions in [“Replacing the design of EAs Domino applications”](#) on page 355.
The template to use is HP EAs-D Server Requests.
 - b. For all other databases in the hprim folder, perform a design refresh using the instructions in [“Refreshing the design of EAs Domino applications”](#) on page 354.

You have now upgraded the design of all existing EAs Domino databases.

4. In the Notes client, open the HP EAs-D API database and ensure that it includes at least one of the following document types listed below. Create any missing documents using the Create menu in the database.

Document type	Configuration instructions
Global Configuration	Editing the Global Configuration document , page 139
DAS Names Configuration	Editing the DAS Names Configuration document , page 89
Mining Rules	Configuring selective archiving , page 159 Configuring the journal mining rule , page 218
Server Definition	Configuring the Server Definition document , page 147
PreProcessing Controls	Configuring the Preprocessing Control document , page 177

Instructions for adding the Message Reprocessing, Tombstone Prototype, and Monitoring Event documents are detailed in the steps below.

The Proxy Gateway document (optionally used in DWA Extension), the Export Search documents, and the Journaling Rules document are configured in the mail domain version of the HP EAs-D API database.

5. Add Message Reprocessing documents to the HP EAs-D API database by following steps a-f below. Go to step 6 if you are updating previously-installed documents.

Message Reprocessing documents contain rules defining the actions that should be performed when an archiving error occurs. (These actions can only be modified by HP support.) The Message Reprocessing documents are not attached to the HP EAs-D API database when the database is refreshed. You need to add or update them manually.

To add the documents HP EAs-D API database:

- a. In the Notes client, open the HP EAs-D API template (`hp_api.ntf`).
- b. Select **View > Go to > Message Reprocessing Codes**.

The Message Reprocessing documents are displayed in the view. "[Message reprocessing rules](#)" on page 318 explains how these documents are used.

Weight	Error Message	Action
0	3A:F2	REPROCESS_CBC
1	Cannot convert Notes Rich Text message to MIME message	REPROCESS_CMF
2	HTMLAPI Problem converting to HTML	REPROCESS_CMF
3	Invalid or missing RFC822 header name	REPROCESS_CEE
4	Note item not found	REPROCESS_CFA
5	Remote system no longer responding	RETRY_GHM
6	Specified database is not currently open	RETRY_GHM
7	SMTP Protocol Returned a Permanent Error 551 Error during archive process due to Internal Error in the Server	RETRY_GHM
8	SMTP Protocol Returned a Permanent Error 551 Permanent Error.	REPROCESS_CEE
9	SMTP Protocol Returned a Permanent Error 551	RETRY_GHM
10	SMTP Protocol Returned a Permanent Error	RETRY_GHM

- c. Select **CTRL + A** to select all the documents, then select **Edit > Copy**.
- d. Open the HP EAs-D API database (`hprim\hp_rissapi.nsf`).
- e. Select **View > Go to > Message Reprocessing Codes**.
- f. Select **Edit > Paste**.

The documents now appear in the view.

6. If you are updating previously-installed Message Reprocessing documents, and the documents have not been customized, follow steps a-h below.

(In most cases, Message Reprocessing documents are not customized. Contact HP support if you need to update customized Message Reprocessing documents. HP support will assist you in recording the customized information, deleting and replacing the documents, and reapplying the customizations. Do not make these changes yourself.)

- a. In the Notes client, open the HP EAs-D API database (`hprim\hp_rissapi.nsf`).
- b. Select **View > Go to > Message Reprocessing Codes**.
- c. Select **CTRL + A** to select all the documents, then select **Edit > Delete** to delete the currently-installed documents.
- d. Open the HP EAs-D API template (`hp_api.ntf`) in the Notes client.
- e. Select **View > Go to > Message Reprocessing Codes**.
- f. Select **CTRL + A** to select all the documents, then select **Edit > Copy**.
- g. In the HP EAs-D API database, select **View > Go to > Message Reprocessing Codes**.
- h. Select **Edit > Paste**.

The updated documents now appear in the view.

7. Add the Monitoring Event documents to the HP EAs-D API database.

These documents define the actions that should be performed when certain archiving events occur (and can only be modified by HP support). They are not attached to the HP EAs-D API database when the database is refreshed, and must be installed manually.

- a. In the Notes client, open the HP EAs-D API template (`hp_api.ntf`).
- b. Select **View > Go to > Monitoring > Event**.

The Monitoring Event documents are displayed in the view.

Name
Default
hp.archive.iap.credentials.requiresAP2OrAbove
hp.archive.serverdefinition.notfound
hp.archive.iap.credentials.empty
hp.archive.statistics.init.failure
hp.archive.iap.credentials.invalid
hp.iap.http.invalid
hp.iap.smtp.invalid
hp.archive.reference.invalid
hp.archive.reference.view.invalid
hp.archive.fieldremapper.initconfig.failure
hp.archive.reference.document.invalid
hp.archive.templateVersion.print
hp.archive.serverdefinition.print
hp.fieldremapper.nameslookup.secondarydirectory
hp.archive.reference.print
hp.archive.reference.settings.print
hp.archive.exception.breakexception
hp.archive.selective.originaldocument.invalid
hp.archive.originaldocument.alreadyarchived
hp.archive.exception

- c. Select **CTRL + A** to select all the documents, then select **Edit > Copy**.
- d. Open the HP EAs-D API database (`hprim\hp_rissapi.nsf`).
- e. In the main view, select **Edit > Paste**.

The documents now appear in the view.

[“Monitoring events”](#) on page 239 explains how these documents are used.

8. If DWA Extension is used, add the new TSKey 2.1 Tombstone Prototype documents to the HP EAs-D API database.

These documents must be installed manually.

- a. In the Notes client, open the HP EAs-D API template (`hp_api.ntf`).
- b. In the main view, select the three TSKey 2.1 Tombstone Prototype documents, and then select **Edit > Copy**.
- c. Open the HP EAs-D API database (`hprim\hp_rissapi.nsf`).
- d. In the main view, select **Edit > Paste**.

The documents now appear in the view.

To configure the document, see [Configuring the Tombstone Prototype document](#), page 261.

9. Ensure that the databases listed below are added to the `hprim` folder on each Gateway server.
 - HP EAs-D DAS Names (`hp_dasnames.nsf`)
 - HP EAs-D Stats (`hp_easd_stats.nsf`)
 - HP EAs-D Alert (`hp_rissalert.nsf`)
 - HP EAs-D CEE Log (`hp_ceelog.nsf`)

These databases add new EAs Domino functionality.

- a. Create the databases by following the instructions in [“Creating new EAs Domino applications”](#) on page 353 or by extracting the databases from the following folder:
`RELEASE\server\resources\applications\hpRimServerInstall_<version>\data\container.zip\{DATA}\hprim\`
- b. Set the ACL for the HP EAs-D Stats, HP EAs-D Alert, and HP EAs-D CEE Log databases using the instructions in [“Setting access control \(ACL\)”](#) on page 80. The ACL for HP EAs-D DAS Names is set in the next procedure.
- c. Replicate the HP EAs-D Stats and HP EAs-D Alert databases to all HP Gateway servers.

Upgrading the databases used for DAS and restarting the archiving processes

1. Reconfigure the consolidated Domino Directory used for DAS:
 - a. In the Designer client, open the consolidated directory.
 - b. Expand **Shared Elements** and then expand **Subforms**.
 - c. Right-click each subform listed below, select **Delete**, and click **Yes** to confirm the deletion.
 - `dominoDN`
 - `dominoUID`
 - `dominoProxyAddresses`
 - d. Scroll to the `$PersonExtensibleSchema` subform and double-click to open.
 - e. Double-click the `dominoDN` entry to open it for editing. Right-click the entry, select **Cut** and click **Yes** to save the changes to `$PersonExtensibleSchema` subform. Repeat this process for `dominoUID` and `dominoProxyAddresses`.
 - f. In the Administrator client, open the consolidated directory.
 - g. Expand **Directory**, select **Extended Directory**, and open the Extended Directory for editing.
 - h. In Additional fields to include, delete **dominoDN**, **dominoUID**, and **dominoProxyAddresses**, and then click **Save & Close**.
2. In the Administrator client, open the Directory Assistance database.
 - a. Click the **Replicas** tab.
 - b. For each replica listed, change the database name in the Domino Directory Filename field to HP EAs-D DAS Names (`hprim\hp_dasnames.nsf`).

3. Upgrade the DAS functions:
 - a. Complete the DAS Names Configuration document.
See [“Editing the DAS Names Configuration document”](#) on page 89.
 - b. On the master HP Gateway server, set the ACL for the DAS Names database and schedule the Populate DAS Names agent.
See [“Configuring the HP EAs-D DAS Names database”](#) on page 95.
 - c. Ensure that HP EAs-D DAS Names (`hp_dasnames.nsf`) is replicated from the master Gateway to the Gateway server(s) designated as backup for the DAS process.
4. Restart the Agent Manager:
 - a. In the Remote Desktop connections, open `notes.ini` on each HP Gateway server (if the file is not already open).
 - b. Find the entry that begins with `ServerTasks=` and add **,AMgr** to the list. Be sure to enter the comma separator.
 - c. Save and close the file.
5. In the Domino Administrator client, restart the Domino server on each Gateway by entering the following command in the Domino server console:


```
restart server
```
6. Re-enable rissminer:
 - a. In the Domino Administrator client, select **File > Open Server** and open the master Gateway server.
 - b. Click the **Configuration** tab, expand **Servers** and select **Programs**.
 - c. Enable each rissminer program document so that rissminer starts running on schedule.
7. Rebuild the views in the consolidated Domino Directory and HP EAs-D DAS Names database.
This action should be performed after the Directory Cataloger has completed its first run and before the Populate DAS Names agent is run for the first time. See [“Rebuilding views in the DAS-related databases”](#) on page 97.

Upgrading from EAs Domino 2.1 or 2.1.1 to version 2.1.2

Introduction

In this scenario, the EAs Domino software on existing HP Gateway servers is upgraded to EAs Domino 2.1.2.

The scenario entails:

- Backing up the current EAs Domino installation.
- Stopping all archiving processes.
- Running the HP EAs-D Updater, which:
 - Upgrades the design of existing EAs Domino databases.
 - Adds or updates the HP EAs-D Alert database for system and archiving alerts, and HP EAs-D CEE Log database for logging messages processed through Clean Envelop Encapsulation.
 - Creates, modifies, or removes `notes.ini` entries.
 - Creates, modifies, or removes files on the HP Gateway servers.

- Adding or updating Monitoring Event documents to the HP EAs-D API database, and updating existing Tombstone Prototype and Message Processing documents.
- Restarting archiving.

Upgrade instructions

Before upgrading the EAs Domino software, ensure that:

- The contents of the installation media have been extracted to a temporary folder.
- Java Runtime Environment (32-bit) version 1.6 or later is installed on the HP Gateway server.
- All non-Lotus Notes applications are closed.

Preparing the HP Gateway servers for the upgrade

1. Back up the following databases:
 - EAs Domino databases
 - Consolidated Domino Directory used for DAS
 - Directory Assistance database
2. Record the schedules of the following EAs Domino agents:
 - All scheduled agents in the HP EAs-D Users database, including the Profile Agent
 - Purge_Documents agent in HP EAs-D Log and HP EAs-D SC Request databases
 - On the master Gateway server and DAS backup servers: Populate DAS Names agent
 - On each HP Gateway server:
 - Archive, Tombstone, and Reference Cleanup agents in the HP EAs-D reference databases
 - Encapsulate and Remove Obsolete PreProcess Documents agents in the HP EAs-D preprocessing databases
 - Get Held Messages agent in HP EAs-D Get Held Messages
3. Stop rissminer, the mining executable, from running on all HP Gateway servers:
 - a. Start the Domino Administrator client.
 - b. Select **File > Open Server** and open the first Gateway server.
 - c. Click the **Configuration** tab, expand **Servers** and select **Programs**.
 - d. Disable each rissminer program document so that rissminer stops running on schedule.
 - e. Repeat these steps on each Gateway server.
4. In the Designer client, disable the Archive and Tombstone agents and the Profile Agent.
5. Make a backup copy of the `notes.ini` file in the Domino executable directory.

Running the EAs Domino Updater

Ensure that the Domino server on each HP Gateway server to be upgraded is running and then follow these steps:

1. Open Windows Explorer, and navigate to the folder where the EAs Domino installation files were extracted. Locate the `Updater` directory and double-click the `Setup.exe` file.
The Upgrader Login window appears, with the Notes ID from the previous session.
2. If the organization prefers to use another ID to create and sign databases and agents, click **Switch ID** and select the ID.

3. Enter the password for the Notes ID, and then click **OK**.

4. Click **Next** in the Welcome window.

5. Click **New** to add an HP Gateway server.

The Domino & Update selection wizard appears.

6. Configure the update:

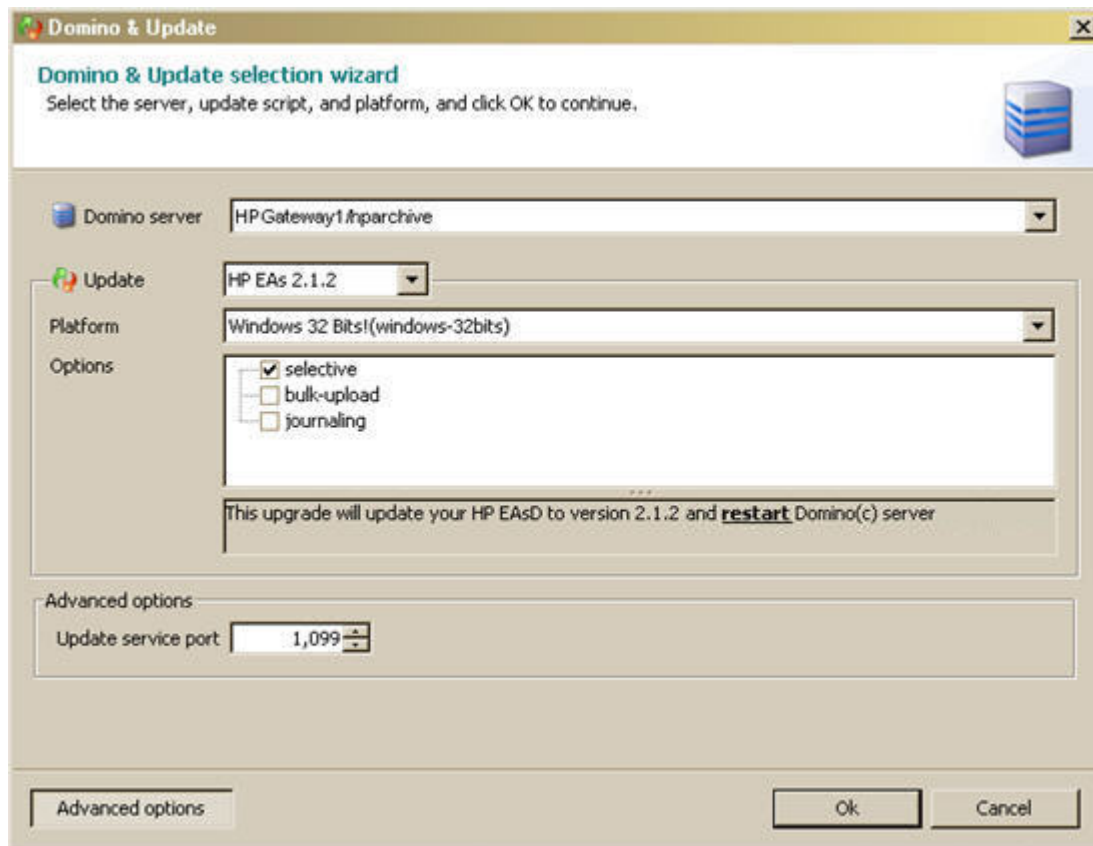
a. In the Domino server field, select the HP Gateway server to update.

b. Ensure the Update version is **HP EAs 2.1.2** and the Platform is **Windows 32 bits**.

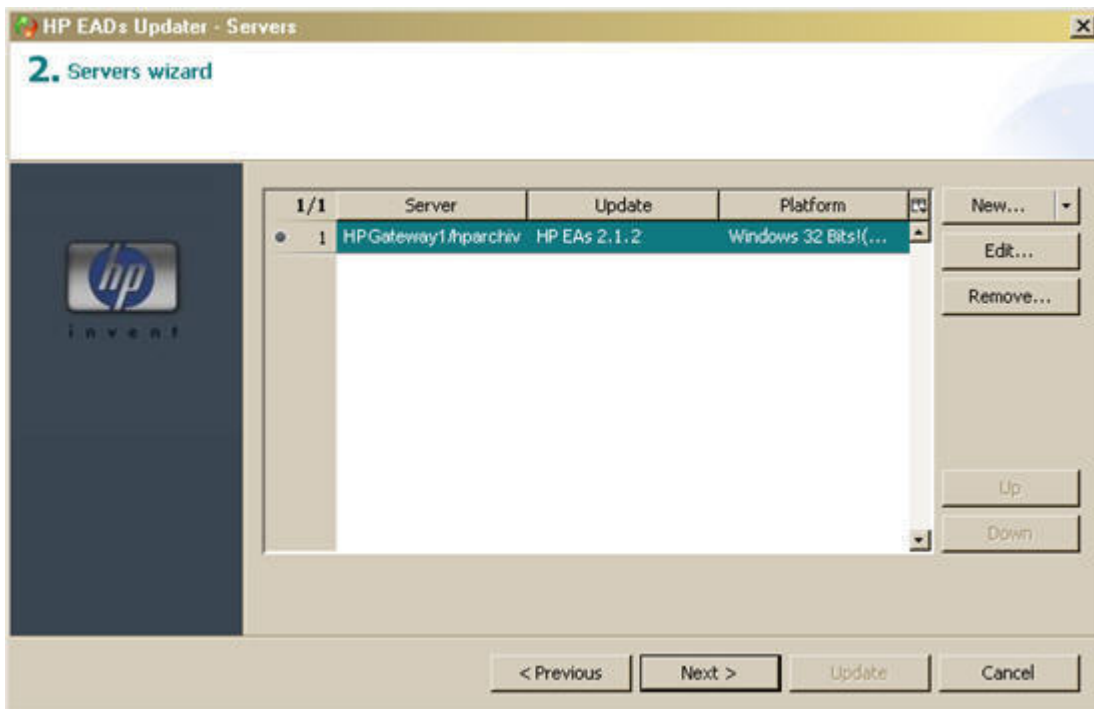
c. In Options, select the **selective** check box.

d. Do not update the service port in Advanced options.

e. Click **OK** to continue.



The Gateway server is added to the update list.



7. To add another HP Gateway server, click **New** and then follow the procedure in step 6. Repeat for each additional HP Gateway server.
8. Click **Next**.
A summary appears with the selected upgrades.
9. Click **Update**.
The servers will be updated one by one, in the order set in the update list.
During the upgrade process, a log appears in the installation window describing the changes that are taking place.
10. After the upgrade is complete, check all template versions and file versions to make sure the upgrade was successful.

The Upgrader does not restart the Domino server after the upgrade is complete. You will restart the server later in the upgrade process.

Adding or updating documents in the HP EAs-D API database

1. Update the Message Reprocessing documents.

Message Reprocessing documents contain rules defining the actions that should be performed when an archiving error occurs. They are not attached to the HP EAs-D API database when the database is refreshed and need to be updated manually.

(In most cases, Message Reprocessing documents are not customized. Contact HP support if you need to update customized Message Reprocessing documents. HP support will assist you in recording the customized information, deleting and replacing the documents, and reapplying the customizations. Do not update customized documents yourself.)

- a. In the Notes client, open the HP EAs-D API database (`hprim\hp_rissapi.nsf`).
- b. Select **View > Go to > Message Reprocessing Codes**.
- c. Select **CTRL + A** to select all the documents, then select **Edit > Delete** to delete the currently-installed documents.
- d. Open the HP EAs-D API template (`hp_api.ntf`) in the Notes client.
- e. Select **View > Go to > Message Reprocessing Codes**.
- f. Select **CTRL + A** to select all the documents, then select **Edit > Copy**.
- g. In the HP EAs-D API database, select **View > Go to > Message Reprocessing Codes**.
- h. Select **Edit > Paste**.

The updated documents now appear in the view.

Weight	Error Message	Action
0	3A:F2	REPROCESS_CBC
1	Cannot convert Notes Rich Text message to MIME message	REPROCESS_CMF
2	HTMLAPI Problem converting to HTML	REPROCESS_CMF
3	Invalid or missing RFC822 header name	REPROCESS_CEE
4	Note item not found	REPROCESS_CFA
5	Remote system no longer responding	RETRY_GHM
6	Specified database is not currently open	RETRY_GHM
7	SMTP Protocol Returned a Permanent Error 551 Error during archive process due to Internal Error in the Server	RETRY_GHM
8	SMTP Protocol Returned a Permanent Error 551 Permanent Error.	REPROCESS_CEE
9	SMTP Protocol Returned a Permanent Error 551	RETRY_GHM
10	SMTP Protocol Returned a Permanent Error	RETRY_GHM

2. Add or update the Monitoring Event documents.

These documents define the actions that should be performed when certain archiving events occur, and can only be changed by HP support. They are not attached to the HP EAs-D API database when the database is refreshed, and must be installed manually.

- a. In the Notes client, open the HP EAs-D API template (`hp_api.ntf`).
- b. Select **View > Go to > Monitoring > Event**.
The Monitoring Event documents are displayed in the view.
- c. Select **CTRL + A** to select all the documents, then select **Edit > Copy**.
- d. Open the HP EAs-D API database (`hprim\hp_rissapi.nsf`).
- e. In the main view, select **Edit > Paste**.

Name
Default
hp.archive.iap.credentials.requiresAP2OrAbove
hp.archive.serverdefinition.notfound
hp.archive.iap.credentials.empty
hp.archive.statistics.init.failure
hp.archive.iap.credentials.invalid
hp.iap.http.invalid
hp.iap.smtp.invalid
hp.archive.reference.invalid
hp.archive.reference.view.invalid
hp.archive.fieldremapper.initconfig.failure
hp.archive.reference.document.invalid
hp.archive.templateVersion.print
hp.archive.serverdefinition.print
hp.fieldremapper.nameslookup.secondarydirectory
hp.archive.reference.print
hp.archive.reference.settings.print
hp.archive.exception.breakexception
hp.archive.selective.originaldocument.invalid
hp.archive.originaldocument.alreadyarchived
hp.archive.exception

3. (If upgrading from version 2.1) If DWA Extension is used and the “shrink body and remove attachments” tombstone option is specified in the mining rule, update the TSKey 2.1 Tombstone Prototype documents.

This allows the preserved body text to be visible in DWA.

Replace the existing TSKey 2.1 Tombstone Prototype document by following these steps:

- a. In the Notes client, open the HP EAs-D API database (`hprim\hp_rissapi.nsf`).
- b. Remove the current TSKey 2.1 Tombstone Prototype document that you are using.
Do not remove a customized tombstone prototype.
- c. Open the HP EAs-D API template (`hp_api.ntf`).
- d. In the main view, select the TSKey 2.1 Tombstone Prototype documents, and then select **Edit > Copy**.
- e. In the main view of the HP EAs-D API database, select **Edit > Paste**.
The revised document now appears in the view.
- f. For customized tombstone prototypes, copy the hotspot and the relevant text from the old prototype document to the new prototype document, and then save the new document.
Remove the old prototype document by selecting **Edit > Delete**.

Restarting the archiving processes

1. Open the Designer client and sign, schedule and enable the scheduled EAs Domino agents, including the following EAs Domino agents if you are upgrading from version 2.1:
 - Purge_Document agent in HP EAs-D Alert
 - Purge_Document agent in HP EAs-D Stats

For more information, see “[Removing documents from the HP EAs-D Alert database](#)” on page 247 and “[Removing documents from the HP EAs-D Stats database](#)” on page 251.

2. In the Domino Administrator client, restart the Domino server on each Gateway by entering the following command in the Domino server console:

```
restart server
```
3. Re-enable rissminer:
 - a. In the Domino Administrator client, select **File > Open Server** and open the master Gateway server.
 - b. Click the **Configuration** tab, expand **Servers** and select **Programs**.
 - c. Enable each rissminer program document so that rissminer starts running on schedule.

Upgrading HP EAs Domino components on customer servers

Introduction

If Advanced Filtering (EAs Domino journaling), IAP single sign-on, DWA Extension, and/or Export Search components are currently deployed on customer servers, they can either be upgraded in place or removed and reinstalled as a clean install. The instructions below explain how to upgrade in place.

All EAs Domino software that is installed on customer servers must be upgraded to version 2.1.2.

Upgrade instructions

To upgrade EAs Domino components on a customer server:

1. In the Domino Administrator client, open the server on which the EAs Domino software is installed.
2. Open the Domino server console, and stop the router by entering the command:
`tell router quit`
3. If Advanced Filtering is installed on the server, stop the journaling rules executable by entering this command in the server console:
`tell mwadvrt quit`
4. Replace the design of any database in the following table that exists on the customer's server. These databases are located in the `<Domino data directory>\hprim` folder.

For the procedure to replace a database design, see [“Replacing the design of EAs Domino applications”](#) on page 355.

Database title	Database file name	Feature implemented	Template name
HP EAs-D API	<code>hp_rissapi.nsf</code>	EAs Domino configuration (mail domain version)	HP EAs-D API NTF
HP EAs-D Bulk Upload	<code>hp_rissblkupd.nsf</code>	Database of inactive users	HP EAs-D Bulk Upload
HP EAs-D DWA Index	<code>hp_dwaindex.nsf</code>	DWA (iNotes) Extension	HP EAs-D DWA Index NTF
HP EAs-D Export Search	<code>hp_rissexport-search.nsf</code>	(Server-side and Web based) Export Search	HP EAs-D Export Search NTF
HP EAs-D Locale Configuration	<code>hp_localecfg.nsf</code>	Localized user interface for Web-based Export Search	HP EAs-D Locale Configurations NTF
HP EAs-D Log	<code>hp_risslog.nsf</code>	Logging	HP EAs-D Log NTF
HP EAs-D SSO	<code>rimsso.nsf</code> or <code>hp_sso.nsf</code>	IAP single sign-on	HP EAs-D SSO NTF
HP EAsD Users	<code>hp_rissuser.nsf</code>	Required for Advanced Filtering	HP EAs-D Users NTF

5. If any of the above databases does not already exist on the mail server and is needed for a feature, create the database using the procedure in [“Creating new EAs Domino applications”](#) on page 353.

The features that are implemented are shown in the table above.

6. Upgrade the executable and JAR files:

a. Stop the Domino server by entering `quit` in the server console.

b. After the Domino server has quit, replace or remove the files in the table below.

- **Location of files to be removed or replaced:** You can enter the following command in the server console to find the locations of the Domino server executable folder and data folder:

```
Show Stat Server.Path.*
```

The output will look something like this:

```
Server.Path.Configfile = C:\Domino\notes.ini
```

```
Server.Path.Data = C:\Domino\data
```

```
Server.Path.Executable = C:\Domino\
```

- **Location of files to be used for replacement:** These files are located in the following folders in the EAs Domino 2.1.2 installer package:

Journaling files (Windows 32- or 64-bit): `RELEASE\server\resources\applications\hpRimServerInstall_<version>\data\container.zip\Windows<version>\{BIN}\`

Journaling files (Linux, AIX 64-bit): `RELEASE\server\resources\applications\hpRimServerInstall_<version>\data\container.zip\<operating system>\{DATA}\`

Bulk Upload files (Windows 32-bit): `RELEASE\server\resources\applications\hpRimServerInstall_<version>\data\container.zip\Windows32\{BIN}\`

Bulk Upload files (Linux, AIX 64-bit): `RELEASE\server\resources\applications\hpRimServerInstall_<version>\data\container.zip\<operating system>\{DATA}\`

JAR files (Windows 32-bit): `RELEASE\server\resources\applications\hpRimServerInstall_<version>\data\container.zip\Windows32\{BIN}\jvm\lib\ext\`

File name	Installed location on server	Action
nrisminer.exe (Windows) rissminer (Linux, AIX) (mining executable)	Domino executable folder	Remove this file. (No longer used on customer servers.)
mwadv.t.exe (Windows) mwadv.t (Linux, AIX) (journaling rules filter)	Domino executable folder	Add or replace.
nhpblkup.d.exe (Windows) hpblkup.d (Linux, AIX)	Domino executable folder	Add or replace.
nadv.srv.dll (Windows) libadv.srv.so (Linux) libadv.srv.a (AIX) (journaling listening agent)	Domino executable folder	Add or replace.
activation*.jar	<Domino executable folder>\jvm\lib\ext	Add or replace. Note: Be sure to remove any current JAR file starting with "activation."
dsn.jar	<Domino executable folder>\jvm\lib\ext	Add or replace.
easdNet.jar	<Domino executable folder>\jvm\lib\ext	Add or replace.
retriever*.jar	<Domino executable folder>\jvm\lib\ext	Add or replace. Note: Be sure to remove any current JAR file starting with "retriever."

7. Remove the following databases if they have been installed in the <Domino data directory>\hprim folder:

- hp_dasnames.nsf
- hp_easd_stats.nsf
- hp_rissalert.nsf
- hp_preproc_blk.nsf
- hp_preproc_journal.nsf
- hp_preproc_miner.nsf
- hp_riss_blkupreferenc.nsf
- hp_riss_journalreferenc.nsf
- hp_riss_minerreferenc.nsf
- hp_rissreq.nsf
- hp_rissuser.nsf

8. Start the Domino server.

9. Configure any new components, or check and adjust the configurations in existing components.

For information, go to the following sections:

- Advanced Filtering: [Advanced Filtering installation](#), page 202
- DWA Extension: [Configuring DWA Extension](#), page 255
- Export Search: [Using the server to export messages](#), page 272
- IAP single sign-on: [Configuring IAP single sign-on](#), page 289

 **NOTE:**

The mail domain version of HP EAs-D API can be replicated to all servers in the mail domain that have EAs Domino software installed.

Replacing existing HP Gateway hardware

Overview

In this scenario, the existing installation is cloned to new HP Gateway hardware. The EAs Domino software version remains the same.

This scenario entails:

- Installing EAs Domino 2.1.2 on the new HP Gateway servers using an existing Gateway server's installation as the source of the new installation.
- Enabling the archiving agents on the new HP Gateway servers.
- Ensuring that the new Gateway servers have picked up the archiving load.
- Retiring the old Gateway servers.

Migration instructions

To replace HP Gateway servers:

1. Install the Windows 2008 R2 server software and the Lotus Domino software on the new HP Gateway servers.

Follow the instructions in each section of "[Preparing the HP Gateway environment](#)" on page 43.

 **IMPORTANT:**

If the software is being installed on an HP ProLiant DL360 G6 or G7 server, bring an external USB CD/DVD drive to the installation. These servers are not equipped with an internal CD/DVD drive.

2. Configure the Domino server settings on the new HP Gateway servers.
Follow the instructions in each section of "[Configuring the master HP Gateway server](#)" on page 55.
3. Install EAs Domino 2.1.2 on the new Gateway servers.
 - a. Select an existing HP Gateway to be used as the master server for the installation.
 - b. Follow the directions in "[Deploying the archiving installation to additional HP Gateway servers](#)" on page 100.

4. Update the DAS configuration:
 - a. Create and configure a new consolidated directory on one of the new HP Gateway servers using the directions in [“Building a consolidated directory”](#) on page 83. Replicate the directory to all new HP Gateway servers.
 - b. Schedule the Dircat task.
See [“Scheduling the Directory Cataloger task”](#) on page 86.
 - c. Configure a new Directory Assistance database using the instructions in [“Creating and configuring the Directory Assistance database”](#) on page 86. Replicate the database to the servers used for DAS backup.
 - d. Verify that the LDAP configuration exists on the server.
See [“Verifying the LDAP configuration”](#) on page 88.
 - e. Ensure the Populate DAS Names agent is scheduled and enabled.
See [“Enabling the Populate DAS Names agent”](#) on page 96.
5. Restart the Domino server on the Gateway.
6. Rebuild the views in the consolidated directory and HP EAs-D DAS Names database.
Perform this action after the Directory Cataloger has completed its first run and before the Populate DAS Names agent is run for the first time. See [“Rebuilding views in the DAS-related databases”](#) on page 97.
7. Adjust the archiving configuration:
 - a. Add a Server Definition document to cover the new HP Gateway servers **or** edit the Server Settings tab in the existing Server Definition document(s), replacing the old Gateway server names with the new Gateway server names.
Each new server must be covered by a Server Definition document.
For more information, see [“Configuring the Server Definition document”](#) on page 147.
 - b. Ensure that the mining rules are enabled.
 - c. Add the new Gateway servers to the Databases Location tab in the Preprocessing Control documents.
 - d. Schedule and enable the preprocessing agents on each new Gateway server.
See [“Scheduling and enabling the preprocessing agents”](#) on page 182.
 - e. Configure the archiving agents and the Get Held Messages database on the new Gateway servers.
See [“Configuring the archiving agents”](#) on page 185.
8. Create and schedule a rissminer program document on each new HP Gateway server.
See [“Running an archiving job”](#) on page 193.
9. Ensure that the new HP Gateway servers are archiving data.

10. After you observe that archiving is running properly on the new Gateway servers:
 - a. Disable the rissminer program documents on the old Gateway servers.

 **NOTE:**

Any messages that were tagged for processing by rissminer will be retagged by rissminer in the migrated EAs Domino installation. This occurs after the Reference Document Retry interval (configured in the mining rule) has elapsed.

- b. Shut down the existing HP Gateway servers.

2.10 Uninstalling the HP EAs Domino software

This chapter describes the steps required to uninstall HP EAs Domino software and related files.

If you are upgrading from earlier versions of the EAs Domino software, see [“Upgrading or migrating an HP EAs Domino installation”](#) on page 105.

 **NOTE:**

We recommend that you make backup copies of all EAs Domino database files before uninstalling them.

- [Uninstalling the HP EAs Domino software](#), page 131
- [Removing Domino configuration files](#), page 134
- [End user client systems](#), page 134
- [IAP](#), page 134

Uninstalling the HP EAs Domino software

Windows servers

Follow these steps to remove EAs Domino software from each Windows server where it is installed.

1. To remove a compliance archiving configuration, follow these steps:
 - a. In the Administrator client, open the server and then open the server console.
 - b. Stop the journaling agents, so that new messages cannot be journaled.
If Advanced Filtering is installed, these are the journaling listening agent (nadvsrv) and the journaling rules filter (nmwadvt).
 - c. Run the mining program (rissminer) and the Archive, Preprocessing, and Tombstone agents until the journal and the preprocessing and journal reference databases are empty.
See [“Running an archiving job manually”](#) on page 195.

2. To remove a selective archiving configuration, follow these steps:
 - a. In the Administrator client, open the server.
 - b. Click the **Configuration** tab, expand **Server** and select **Programs**.
 - c. Select the rissminer program document for the archiving profile and click **Edit Program**.
 - d. Disable the schedule and click **OK**.
 - e. Open the server console and run the Archive, Preprocessing, and Tombstone agents until the selective archive preprocessing and reference databases are empty.
See [“Running an archiving job manually”](#) on page 195.
3. Stop the Domino server.
4. Navigate to the `HPRIMUninstaller` folder in the Domino program directory.
5. Double-click `Uninstaller.exe` to uninstall the EAs Domino files.



NOTE:

Java Runtime Environment (32-bit) version 1.6 or later must be installed on the server before the uninstaller is run.

6. Manually remove the following items from the servers:
 - Any databases that were created after installation
 - Any databases that were replicated from other servers
 - Any directories that were created, such as the preprocessing working directories
7. Restart the Domino server.

Linux, Solaris, and AIX

Follow these steps to remove EAs Domino software from each server where it is installed.

1. To remove a journaling configuration, follow these steps:
 - a. In the Administrator client, open the server and then open the server console.
 - b. Stop the journaling agents, so that new messages are not being journaled.
If Advanced Filtering is installed, these are the journaling listening agent (`libadvsvr`) and the journaling rules filter (`mwadvf`).
 - c. Run the mining program (`rissminer`) and the Archive, Preprocessing, and Tombstone agents until the journal and the preprocessing and journal reference databases are empty.
See [“Running an archiving job manually”](#) on page 195.

2. To remove an archiving configuration, follow these steps:
 - a. In the Administrator client, open the server.
 - b. Click the **Configuration** tab, expand **Server** and select **Programs**.
 - c. Select the rissminer program document for the archiving profile and click **Edit Program**.
 - d. Disable the schedule and click **OK**.
 - e. Open the server console and run the Archive, Preprocessing, and Tombstone agents until the selective archive preprocessing and reference databases are empty.

See [“Running an archiving job manually”](#) on page 195.

3. Stop the Domino server.
4. In the server console, navigate to the `lotus/notes/data` directory and enter the following commands:

```
rm -r hprim
rm mwadvr
rm libadvsvr.a or rm libadvsvr.so
rm rissminer
rm blkupd
```

5. Open `notes.ini` and remove the following:

- `$MailWatcherServerName`
- On all servers that run rissminer or archiving agents:
`HPRISSMINER_MAX_REF_SESSION` and `HP_EAS-D_CONTROL_IAP_HASHES_COLLISION`
 if these entries are listed

- All variables matching `HPRIM_*`

- If Advanced Filtering is installed:

```
MWADVSRVOTHERSERVICES=[anti-virus-real-time-task-name] and MWADVSR-
VOTHERSERVICESAO=[anti-virus-real-time-task-name]
```

HP EAs-added values from the following entries:

```
extmgr_addins=...,advsvr
servertasks=.,mwadvr
```

6. Manually remove the following items from the servers:
 - Any databases that were created after installation
 - Any databases that were replicated from other servers
 - Any directories that were created, such as the preprocessing working directories
7. Restart the Domino server.

Removing Domino configuration files

(Local mining configurations)

Remove the IAP foreign domain document and the connection documents to the HP Gateway servers from the servers in the Domino mail domain.

From the Domino Directory on the Administration server:

1. Click the **Configuration** tab and expand **Messaging**.
2. Select **Connections**.
3. Delete the Connection document to each HP Gateway server.
4. Select **Domains**.
5. Select the IAP foreign domain and delete the domain.

End user client systems

Remove the following items if they were installed on client systems:

- (Windows only) Notes client plug-in
You can use Add or Remove Programs in the Control Panel to remove the plug-in.
- (Windows only) LocalCache.exe and ExportSearch.exe
These files are located in the \lotus\notes\Localcache directory on the client and must be manually removed.
Do **not** remove the default Local Cache database (DefaultLCDestination.nsf) or any other Local Cache database that was created. Tombstoned messages are marked with pointers to full message copies held in the cache.
- EAs Domino agents or other alterations to the mail template(s)
- EAs Domino entries in notes.ini

IAP

If IAP single sign-on is used, remove the secret key. See “[Configuring IAP single sign-on](#)” on page 289.

Part 3. Configuring the HP EAs Domino environment

- [HP EAs-D API main view](#), page 137
- [Editing the Global Configuration document](#), page 139
- [Configuring the Server Definition document](#), page 147

3.1 HP EAs-D API main view

HP EAs Domino databases are installed in the `hprim` folder of the Domino data directory.

The 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 configuring and administering EAs Domino.

To open the HP EAs-D API database:

1. In the Domino Administrator client, open the Domino server.
 - In the HP Gateway domain, open any HP Gateway server.
 - In the customer mail domain, open any Domino server on which the EAs Domino software is installed. (The mail domain instance of the HP EAs-D API database should be replicated to the relevant servers.)
2. Click the **Files** tab and open the `hprim` folder.
3. Double-click the **HP EAs-D API** database file.

The main view appears. The Global Configuration document is listed in the view along with the Server Definition document, the mining rules, the Advanced Filtering journaling rules, and other documents needed to configure EAs Domino applications.

Program	Comments
<ul style="list-style-type: none"> ▼ Global Configuration Global Configuration EAs for Domino 	EAs for Domino IAP main mod
<ul style="list-style-type: none"> ▼ Audit Profile Audit Profile: Example Audit Configuration for HP EAsD (Runs on server: <Export Search Server> for 0 reference databases) 	Example Audit Configuration d
<ul style="list-style-type: none"> ▼ DAS Names Configuration DAS Names Configuration 	
<ul style="list-style-type: none"> ▼ Journaling Rules Rule: Server = * Journal Mail-In Db = FROM = * TO = * EXCEPT FROM = EXCEPT TO = iap 	Default rule to capture all ema
<ul style="list-style-type: none"> ▼ Mining Rules Mining Rule: Bulk Mining Rule: DWA Sample Mining Rule: Journaling Mining Rule: Selective 	Sample Bulk Upload rule - min Sample Selective Archiving ru Archive all messages in the Jo Sample Selective Archiving ru
<ul style="list-style-type: none"> ▼ Server Definition Server Definition for Default Server Definition <Disable> 	Default Server Definition docu
<ul style="list-style-type: none"> ▼ Export Search Export Search Destination for <Export Search Server> Export Search Templates for Mail[R8]mail8.ntf 	Allowed Serve(s) and Destina Allowed Templates for Export!
<ul style="list-style-type: none"> ▼ PreProcessing Controls PreProcessing Controls for Default for Bulk Upload for hprim\hprim_preproc_blk.nsf PreProcessing Controls for Default for Journaling for hprim\hprim_preproc_journal.nsf PreProcessing Controls for Default for Selective for hprim\hprim_preproc_miner.nsf 	Default PreProcessing Config Default PreProcessing Config Default PreProcessing Config
<ul style="list-style-type: none"> ▼ Proxy Gateway Proxy Gateway DEFAULT Proxy Gateway sample2/Company 	Default Proxy Gateway for DW Example Proxy Gateway docu
<ul style="list-style-type: none"> ▼ Tombstone Prototype Tombstone Prototype TSKey 2.1-1 - US English Tombstone Prototype TSKey 2.1-2 - US English Tombstone Prototype TSKey 2.1-3 - US English Tombstone Prototype TSKey1 - US English Tombstone Prototype TSKey2 - US English Tombstone Prototype TSKey3 - US English 	Example - 8.51 & LC Compatib Example - 8.51 & LC Compatib Example - 8.51 & LC Compatib Example - fully argumented for Example - small formula with P Example - small formula with U

3.2 Editing the Global Configuration document

- [Introduction](#), page 139
- [Configuring the settings](#), page 140

Introduction

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

To view 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.



The screenshot shows the HP logo and the title "Email Archiving Software for Domino". Below the title is a navigation bar with tabs: "General Settings", "Additional Modules", "Address Conversion Settings", "Agent Settings", "DWA Index Settings", "Error Messages", and "Administration Alert". The "General Settings" tab is selected, and the content area displays a table of configuration settings.

[General Settings]	
Domino Directory for Journaling and Mining Rules	ConsolidatedNames.nsf
Journaling & Mining Rules database	hprim/hp_rissapi.nsf
Users Mail Details database	hprim/hp_rissuser.nsf
Log database	hprim/hp_risslog.nsf
Archiving Servers	LocalDomainServers

3. View and edit the settings on the Global Configuration tabs:
 - “[General Settings tab](#)” on page 140
 - “[Additional Modules tab](#)” on page 141
 - “[Address Conversion Settings tab \(global\)](#)” on page 141
 - “[Agent Settings tab](#)” on page 142
 - “[DWA Index Settings tab](#)” on page 144 (Customer environment only)
 - “[Error Messages tab](#)” on page 145
 - “[Administration Alert tab](#)” on page 145
4. To save changes to the Global Configuration document, select **File > Save**.

Configuring the settings

HP EAs-D API on HP Gateway servers: Edit all tabs in the Global Configuration document except DWA Index Settings.

HP EAs-D API in mail environment: Edit the DWA Index Settings if implementing DWA Extension.

General Settings tab

This tab lists the HP Gateway servers and EAs Domino databases used in selective and compliance archiving.

The filepath is the path from the Domino data directory.

Field	Description
Domino Directory for Journaling and Mining Rules	The Names and Address database to be used in the archiving process. Enter the name of the consolidated directory set up in “ Building a consolidated directory ” on page 83.
Journaling & Mining Rules database	The configuration database, HP EAs-D API (<code>hprim/hp_rissapi.nsf</code>), which stores the mining rules, Advanced Filtering journaling rules, and the EAs Domino configuration documents.
User's Mail Details database	The database containing records of the mail and journal databases that are mined (<code>hprim/hp_rissuser.nsf</code>).
Log database	The EAs Domino log file (<code>hprim/hp_risslog.nsf</code>).
Archiving Servers	The servers from which archiving is implemented. Leave the default: <code>LocalDomainServers</code> .

Additional Modules tab

The databases that are listed in this tab implement optional EAs Domino functions. You do not need to make changes to these fields.

Bulk Upload database	The database (hprim/hp_rissblkupd.nsf) used in archiving inactive mail files to the IAP.
Server request database	The database (hprim/hp_rissreq.nsf) used in retrieving older tombstoned messages in Domino Web Access.
Export Search request database	The database (hprim/hp_rissexportsearch.nsf) used in exporting messages from the IAP.
Audit database	Not available in HP EAs Domino 2.1.x.
Locale (I18N) Configuration database	The localization database (hprim/hp_localecfg.nsf) used to return messages in a user's native language.

Address Conversion Settings tab (global)

The address conversion settings are used in the archiving process to resolve SMTP aliases.

SMTP Alias tab

[Address Conversion Settings]

SMTP Alias | Multiple Domino Domain | Multiple Domino Domain (Group)

[Alias Support]

Resolve SMTP aliases of Notes names

Alias lookup view in Domino Directory:

DNS domains/hostnames accepted for SMTP messages:
(Comma or newline separated list)

Field	Description
Resolve SMTP aliases of Notes names	Keep the check box selected to resolve SMTP aliases.
Alias lookup view in Domino Directory	Leave \$Users (the default).

Field	Description
DNS domains/hostnames accepted for SMTP messages	<p>Enter a comma- or newline-separated list of DNS domains and hostnames that are accepted for SMTP messages.</p> <p>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</p> <p>You can also add the Domino mail domain name in this field. See “The recipient’s Internet Address is not displayed in the IAP Web Interface” on page 329, which explains why you might want to do this.</p>

Multiple Domino Domain and Multiple Domino Domain (Group) tabs

Do not complete these settings. They are not used in EAs Domino 2.1.x.

Agent Settings tab

The fields in this tab are used in the archiving process.

Profile Agent

Leave the default (with the check box selected) for the Use 'Address Conversion Settings' field. This allows users to be identified via Directory Assistance.

Archive Agent

This tab is used by HP support and must not be edited. Remapping preserves data in fields as messages move through the Domino router and into the IAP.

Message Reprocessing

Messages that are rejected by the IAP are placed in a Hold state in the Domino router mail.box and given a failure reason. When the scheduled Get Held Messages agent is run, rejected messages are pulled into EAs Domino's Get Held Messages database and resubmitted to the router for a specified number of times.

After the maximum number of retries, messages that remain in Get Held Messages are reprocessed by the Reference Cleanup agent in the reference database. The actions taken during reprocessing depend on the reason for IAP rejection. A complete list of failure reasons and reprocessing actions is described in [“Message reprocessing rules”](#) on page 318.

Clean Envelop Encapsulation

Messages that cannot be archived because of an RFC-822 or MIME header parsing error are reprocessed using a method known as Clean Envelop Encapsulation. These messages are returned from the IAP with one of the following failure reasons:

- Invalid or missing RFC-822 header name. (The message header was badly formatted.)
- SMTP Protocol Returned a Permanent Error 551 Permanent Error. (There was a syntax error in the RFC-822 data.)

A message identified for Clean Envelop Encapsulation is sent for preprocessing, where it is *encapsulated* — encased in its own database to keep the original message intact. The database with the encapsulated message is attached to a “clean envelope” message and sent to the IAP for ingestion. Clean envelope messages must reside in their own IAP repository, which you will need to create.

❗ **IMPORTANT:**

At this time, Clean Envelop Encapsulation can only be enabled in consultation with HP support.

Clean Envelop header: The header of a clean envelope message is not a copy of the header from the original message. (Although date headers are preserved if possible.) The information that is placed in the header is configured in the Clean Envelop Subject, Clean Envelop To, and Clean Envelop From fields in this tab.

Clean Envelop body: The headers and body of the original message are rendered, as accurately as possible, in the body of the clean envelope message. The body includes:

- Plain text copies of the original headers
- A list of attachment names and sizes from the original message
- Plain text copy of the original body

Because information in the original message might be damaged, perfect fidelity is not guaranteed in the clean envelope body. However, the database that is attached to the clean envelope preserves the original message and any attachments intact.

Completing the Message Reprocessing tab fields

The field values in the Message Reprocessing tab are used in reprocessing messages using Clean Envelop Encapsulation.

Profile Agent	Archive Agent	Message Reprocessing
[Message Reprocessing Settings]		
Emergency Brake:		50
Clean Envelop Subject:		Clean Envelope Message
Clean Envelop To:		CEE_repository@company.com
Clean Envelop From:		EAsD_CEE@company.com
Clean Envelop Body Description:		This is a rendering of the headers and body of the original message.
Clean Envelop Log Database:		hprimhp_ceelog.nsf

Field	Description
Emergency Brake	<p>Use this field to set the threshold for messages that fail to ingest due to RFC-822 or MIME parsing errors.</p> <p>Automated processing of these messages by the Reference Cleanup agent will stop when the number of messages in the Get Held Messages database is greater than the Emergency Brake value.</p> <p>Note: A large number of message rejections by the IAP in a short period of time indicates an IAP problem that requires manual intervention.</p>

Field	Description
Clean Envelop Subject	Enter a subject for clean envelope messages. A date/time stamp and unique sequence string will be added automatically to whatever you enter in this field.
Clean Envelop To	Enter the email address for the special repository in the IAP that contains the clean envelope messages. Note: You will need to create this repository in the IAP. Only compliance officers (and the IAP administrator, if required) should have access to this repository.
Clean Envelop From	Enter an email address defining the sender of the clean envelope message. The sender's domain can be the real company domain, or a fictional domain. The only requirement is that the sender's address must be a valid-looking SMTP address.
Clean Envelop Body Description	Enter a description to be inserted in the body of a clean envelope message. This description will be added to the rendering of the original message in the clean envelope body.
Clean Envelop Log Database	Enter: hprim\hp_ceelog.nsf This field defines the database containing a log of all messages ingested using Clean Envelop Encapsulation. The hp_ceelog.nsf file is created in the hprim folder during EAs Domino installation. The log (and clean envelope body) record as much header data as possible from the original message, including: <ul style="list-style-type: none"> • From • DeliveredDate • PostedDate • SendTo • CopyTo • Subject • MessageID

 **NOTE:**

Searching is limited on messages ingested via Clean Envelope Encapsulation. Searches on message text may work, but are not guaranteed. Searches on specific headers will fail.

DWA Index Settings tab

The settings in this tab are used in the mail domain instance of the HP EAs-D API database when DWA Extension is implemented.

EAs Domino's DWA Extension feature allows users to access archived messages in Domino Web Access. If you plan to use DWA Extension, edit the Retention field in this tab and configure DWA Extension. See [“Configuring DWA Extension”](#) on page 255.

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 automatically purged after this time.

Error Messages tab

The settings in this tab determine where messages are sent if the system encounters errors while processing mail files.

You do not need to complete the settings in this tab. It is not used in EAs Domino 2.1.x.

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.

Administration Alert tab

Alerts can be sent if mining fails to start. This tab lets you configure the alert that is sent and who it is sent to. Alternatively, alerts can be configured in each mining rule.

Alerts can only be enabled in a mining rule. See "[Administration Alert tab](#)" on page 173 for more information.

Field	Description
From	Enter a value such as IAP system.
SendTo	You can change the default value (LotusNotesAdministrator) by: <ul style="list-style-type: none"> Clicking the arrow. Removing the default value. Adding a name from the address list. Clicking OK.
Subject	Enter a subject for the alert. For example, "Mining did not start."

Field	Description
Alert Relay Server	<p>The relay server can be set here, or it can be set in the Server Definition document or the mining rule. (The system checks the mining rule first, then the server definition, then this field.)</p> <p>To configure this setting, click the arrow and select the server through which alerts should be sent. In most cases, this will be a server in the customer's mail domain.</p> <p>If you select Local, alerts will be sent to the local HP Gateway server. In most cases, Local should not be selected.</p> <p>If you leave this field blank, define the relay server in the Server Definition document or the mining rule.</p>

3.3 Configuring the Server Definition document

- [Introduction](#), page 147
- [Configuring the settings](#), page 148

Introduction

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

- In the HP Gateway domain version of the HP EAs-D API database:
Create a Server Definition document for the HP Gateway servers in the domain. (You have the option of creating additional server definitions, if necessary, for specific servers.)
The same Server Definition document can be used for servers handling both compliance and selective archiving.
- In the mail domain version of the HP EAs-D API database:
Create a Server Definition document for the Domino servers on which the HP EAs-D API database is installed. This includes servers used with the DWA Extension, Export Search, Advanced Filtering, and Bulk Upload applications. If a proxy server is used for DWA Extension, include each mail server that redirects user requests to the proxy.
You have the option of creating additional Server Definition documents to cover specific servers. For example, you might want to create a separate server definition for servers that require special options, such as longer query timeout settings.

NOTE:

A server can be listed in only one Server Definition document.

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. For **Is default**, select **Yes** if this will be the default server definition for the Gateway or mail domain. Otherwise, select **No**.

The default server definition will be used by servers that are not explicitly listed in a Server Definition document.

5. If you are configuring a server definition for the HP Gateway servers, complete the following tabs:
 - “Server Settings tab” on page 148
 - “Archiving Options tab” on page 149
 - “Address Conversion Settings tab” on page 151
 - “Profile Agent Settings tab” on page 151
 - “Execution Settings tab” on page 151
 - “Gateway Server tab” on page 154
 - “Logging tab” on page 155
 - “Administration Alert tab” on page 156
6. If you are configuring a server definition for Domino servers in the mail environment, complete the following tabs:
 - “Server Settings tab” on page 148
 - “DWA Settings tab” on page 153 (if using DWA Extension)
7. In Status, click **Enable** to enable the server definition.
8. Select **File > Save** to save the server definition.
9. To create additional Server Definition documents, in the EAs-D API main view select **Create > Archiving > 1. Server Definition** and follow steps 4–8.

Configuring the settings

Server Settings tab

Server Definition :

Comments :

Is default : No Yes Status :

Server Settings | Archiving Options | Address Conversion Settings | Profile Agent Settings | Execution Settings | DWA Settings | Gateway Server | Logging | Administration Alert

[Server Settings]

Domino Server(s)	<input type="text" value="HPGateway1/hparchive"/> <input type="text" value="HPGateway2/hparchive"/>
IAP domain	<input type="text" value="iap_domain"/>
IAP email address	<input type="text" value="iap_admin@iap_domain"/>
IAP host name	<input type="text" value="10.1.0.132:81"/>

Field	Description
Domino Server(s)	Click the arrow and select the servers to be included in the server definition. Groups cannot be used; server names must be explicit.
IAP domain	Enter the IAP store domain name, located in the Name field in Domain.jcml on the IAP.
IAP email address	Enter: <unique administrator name>@<foreign domain> Make sure that the administrator name is unique and not admin or administrator. For <foreign domain>, use the Internet Domain value in "Creating and configuring the foreign SMTP domain document" on page 58. Important! Make sure that the address includes a dot ("."). For example: iap_admin@iap_domain.com
IAP host name	Enter the IAP VIP as defined in the Domain.jcml file. The VIP is defined in the ipToDomainInfo field for the store group assigned for Lotus Domino. Append :81 after the VIP. For example: 15.23.143.221:81

Archiving Options tab

[Archiving Options]	
Ensure Owner Receipt	<input checked="" type="radio"/> Yes <input type="radio"/> No <i>(For Selective Archiving Only)</i>
Allow using IAP 2.0 or Above	<input checked="" type="radio"/> Yes <input type="radio"/> No
IAP Login	<input]<="" td="" type="text" value="iap_login_"/>
IAP Password	<input]<="" td="" type="text" value="iap_password_"/>
Preserve Attachment Icons	<input checked="" type="radio"/> Yes <input type="radio"/> No
Preserve Original Address Headers	<input checked="" type="radio"/> Always copy To, CC, BCC, etc. <input type="radio"/> Only copy each header if larger than 15KB Unicode characters <input type="radio"/> Disable
Truncate Long Headers	<input type="radio"/> Disable <input checked="" type="radio"/> Truncate (Adds "Header truncated by HP EAs for Domino" to end of message)
Allow Address Header Splitting at 32k	<input checked="" type="radio"/> Yes <input type="radio"/> No
Suppress Domain Mismatch Warning	<input checked="" type="radio"/> Yes <input type="radio"/> No
Add Notes "Friendly Address" to all known addresses	<input checked="" type="radio"/> <input type="text" value="Yes"/> <input type="radio"/> No

Field	Description
Ensure Owner Receipt	<p>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 repository.</p> <p>This option is used only for selective archiving. It does not apply to compliance archiving and, if enabled, is ignored.</p>
Allow using IAP 2.0 or above	Select Yes if the IAP software is version 2.0 or above.
IAP Login IAP Password	<p>Enter the credentials that EAs Domino will use to authenticate with the IAP.</p> <p>This IAP user account can be created locally on the IAP or imported via DAS, but it must be defined as an IAP Admin. To do this, open PCC Web Administration, navigate to Account Manager, open the user account form, and select the IAP Admin check box at the bottom of the form.</p> <p>Note: We recommend that you validate these credentials to ensure that EAs Domino has access to the IAP. Select Actions > Tools > 5. Check IAP credentials to run the IAP check wizard.</p>
Preserve Attachment Icons	Select Yes to preserve attachment icons in archived messages.
Preserve Original Address Headers	<p>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.</p> <p>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.</p> <p>Use this field and the other fields on this tab to configure the expansion of message headers during archiving.</p> <ul style="list-style-type: none"> • Always copy To, CC, BCC, etc.: Select to always expand message headers. • Only copy each header if larger than 15 KB Unicode characters: Select if headers should only be expanded if they are larger than 15 KB Unicode characters. • Disable: Select if message headers should not be expanded.
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	<p>Leave the default of Yes.</p> <p>If set to No, a warning prints to the log file if the recipient's domain cannot be found in the Domino Directory. (The log file that is used is defined in the Server Definition's Logging tab.)</p>
Add Notes "Friendly Address" to all known addresses	Select whether to expand message headers to include Notes "friendly" addresses when messages are archived. When enabled, this adds RFC 822 display names to the SMTP email address. For example:544444r "John Doe/HP" <jd@hp.com>.

Address Conversion Settings tab

Do not change the default setting on this tab: **Use Global Config**. The address conversion settings in the Global Configuration document apply to all HP Gateway servers.

Profile Agent Settings tab

Leave the default setting (with the check box selected). This allows users that are selectively archived to be identified via Directory Assistance.

Execution Settings tab

Session Settings

Session Settings	Program Control
Error Notifications	<input type="checkbox"/> LocalDomainAdmins <input type="checkbox"/>
Maximum Session Size for Archive	<input type="checkbox"/> 500M <input type="checkbox"/> (*Size**) <input type="checkbox"/>
Maximum Documents to Archive	<input type="checkbox"/> 10000 <input type="checkbox"/>
Maximum Execution Time for Archive	<input type="checkbox"/> 120 <input type="checkbox"/> Minutes <input type="checkbox"/>
Maximum Documents to Tombstone	<input type="checkbox"/> 10000 <input type="checkbox"/>
Maximum Execution Time for Tombstone	<input type="checkbox"/> 120 <input type="checkbox"/> Minutes <input type="checkbox"/>
Maximum Failed Query Attempts	<input type="checkbox"/> 100 <input type="checkbox"/>
Maximum Query Timeout	<input type="checkbox"/> 4.00 <input type="checkbox"/> seconds <input type="checkbox"/>

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 agents. For example, LocalDomainAdmins.
Maximum Session Size for Archive	Leave the default (500 M). This field lists the maximum amount of data that the Archive agent can process in one session.
Maximum Documents to Archive	Leave the default (10,000). This field lists the maximum number of messages the Archive agent can process in one session.
Maximum Execution Time for Archive	Leave the default (120 minutes). This field lists the maximum amount of time that the Archive agent can run in one session.
Maximum Documents to Tombstone	Leave the default (10,000). This field lists the maximum number of messages that the Tombstone agent can process in one session.
Maximum Execution Time for Tombstone	Leave the default (120 minutes). This field lists the maximum amount of time that the Tombstone agent can run in one session.
Maximum number of Failed Query Attempts	Leave the default (100). This field lists the maximum number of failed queries to the IAP before an EAs Domino Archive or Tombstone agent stops processing.
Maximum Query Timeout	Leave the default (4.00 seconds) unless you find that the timeout is not long enough.

Program Control

These settings provide a quick way to disable the archiving agents or temporarily stop archiving jobs on the HP Gateway servers. (“[Configuring the archiving agents](#)” on page 185 explains the functions performed by the archiving agents.)

Session Settings | Program Control

Check for a Stop signal every 5 seconds

Disable Archive agents
 Stop ALL Running **'Archive'** agents at 07/30/2010 02:26:05 PM for 10 minutes

Disable Tombstone agents
 Stop ALL Running **'Tombstone'** agents at for 10 minutes

Disable Encapsulations
 Stop ALL Running **'Encapsulate'** agents at for 10 minutes

Field	Description
Check for a stop signal	Enter the time (in seconds) between system checks to disable or temporarily stop Archive agents, Tombstone agents, and/or Encapsulate agents on the HP Gateway servers.
Disable Archive agents Stop ALL running 'Archive' agents	Configure these fields to perform one of the following actions: <ul style="list-style-type: none"> To disable scheduled runs of the Archive, Tombstone, and/or Encapsulate agents on the Gateway servers, select the relevant check box. The agent schedule is re-enabled when you clear the check box. Note: Any currently-running jobs will continue until the limits in the Session Settings tab are reached. To stop all currently-running Archive, Tombstone, and/or Encapsulate agents on the Gateway servers, enter the date and time to stop the agents and then set the amount of time that the agents should be stopped. The format for the date and time depend on the locale settings for the Notes client that you are using to edit the document. For example, for the US the date and time might be shown as: 07/27/2010 06:30:11 PM To set the stop time to the current time, click set stop time to now. (You can clear the stop time by clicking clear stop time.)
Disable Tombstone agents Stop ALL running 'Tombstone' agents	
Disable Encapsulations Stop ALL running 'Encapsulate' agents	

DWA Settings tab

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. (Non Memo Reply items such as meeting requests and phone messages are also encapsulated if they are archived.)

When the message is retrieved in DWA, it needs to be unencapsulated for user viewing. 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 the steps to configure DWA Extension, see [“Configuring DWA Extension”](#) on page 255.

[DWA Settings]

DWA Temporary Work Area

C:\RIM_TEMP\DWA\

Note: use OS format for filepath separators - “\” for Windows and “/” for Unix

THIS DIRECTORY MUST EXIST ON THE SERVER.

Field	Description
DWA Temporary Work Area	<p>This field lists the directory that temporarily stores the unencapsulated files. The directory can be on the DWA 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.</p> <p>The size of the directory depends on the environment (how often users send or receive signed or encrypted messages).</p> <p>Important! Always create a new directory for the work area, making sure the following conditions are met:</p> <ul style="list-style-type: none"> • 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 <code>D:\Lotus\Domino\Data\RIM_TEMP</code> if that is the path to your Domino data root. Do not share this directory in your network. <p>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.</p> <p>For example, on a Windows-based Domino server, enter:</p> <pre>C: CD\ MKDIR RIM_TEMP CD RIM_TEMP MKDIR DWA</pre> <p>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:</p> <pre>chown domino:domino RIM_TEMP chmod 755 RIM_TEMP</pre>

Gateway Server tab

The settings on this tab establish the path to the Get Held Messages database, which recovers mail.box messages that are in the Hold or Dead state.

Field	Description
Gateway Server	<p>Leave this field blank if all HP Gateway servers listed in the server definition have their own copy of the Get Held Messages database.</p> <p>Otherwise, click the arrow and select the name of an HP Gateway server with a copy of Get Held Messages. Ensure that the Gateway's Server document lists the other Gateway servers in the Trusted Servers field on the Security tab.</p>

Field	Description
Get Held Messages database file-path	Enter the filepath to the Get Held Messages database from the Domino data directory. For example: hprim\hp_GetHeld Msgs.nsf If the Gateway Server field is left blank, make sure that all HP Gateways controlled by this server definition have the same filepath to the Get Held Messages database.

Logging tab

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

[Debug Options]

Logging Level Basic Information ▼

Write logs to HP Log Database ▼

Print Full Build Number in Log Yes No

Archive | Tombstone | Field Remapper | Body Parser | Statistics |

[Archive Agent Settings]

Enable verbose debug logging Yes No

Enable logging per Nmessages archived Yes No

Field	Description
Debug options	
Logging level	Unless you want to display warnings, errors, or configuration information, keep the default of Basic Information .
Write logs to	To record entries in the EAs Domino log (hprim\risslog.nsf), keep the default, HP Log Database .
Print Full Build Number in Log	Keep the default of Yes .
Logging tabs: Ensure that all options on the tabs listed below are set to No unless you are asked by HP support to enable an option.	
Archive	The Archive tab enables debugging for the Archive agent in the reference database. You can specify logging to be enabled per x number of messages.

Field	Description
Tombstone	The Tombstone tab enables debugging for the Tombstone agent in the reference database. You can specify logging to be enabled per x number of messages.
Field Remapper	The Field Remapper tab enables debugging for message headers.
Body Parser	The Body Parser tab enables debugging for the unique message ID (hash).
HP Gateway statistics collection	
Statistics	<p>When statistics collection is enabled, archiving agent metrics are output to the console and/or to the HP EAs-D Stats database in the <code>hprim</code> folder.</p> <ul style="list-style-type: none"> • Write Metrics Archive Count and Write Metrics Tombstone Count fields: Statistics are written to the HP EAs-D Stats database after <i>n</i> number of references are processed by the Archive or Tombstone agents. • Output Metrics Archive Count and Output Metrics Tombstone Count fields: Statistics are printed to the console after <i>n</i> number of references are processed by the Archive or Tombstone agents.

Administration Alert tab

Alerts can be sent if mining fails to start.



NOTE:

Alerts can only be enabled in a mining rule. See “[Administration Alert tab](#)” on page 173 for more information.

Field	Description
Alert Relay Server	<p>The relay server can be set in this field, or it can be set in the Global Configuration document or the mining rule. (The system checks the mining rule first, then the server definition, then the global configuration.)</p> <p>To configure this setting, click the arrow and select the server through which alerts should be sent. In most cases, this will be a server in the customer's mail domain.</p> <p>If you select Local, alerts will be sent to the local HP Gateway server. In most cases, Local should not be selected.</p> <p>If you leave this field blank, define the relay server in the Global Configuration document or the mining rule.</p>
Comments	Enter any comments about the alert.

Part 4. Archiving email to the IAP

- [Configuring selective archiving](#), page 159
- [Preprocessing messages](#), page 175
- [Configuring the archiving agents](#), page 185
- [Running an archiving job](#), page 193
- [Configuring compliance \(journal\) archiving](#) , page 201
- [Using Bulk Upload](#), page 223
- [Working with log files](#), page 231
- [Event monitoring and alerts](#), page 239
- [Archiving statistics](#), page 249

4.1 Configuring selective archiving

- [The selective archiving process](#), page 159
- [Configuring mining rules](#), page 160

The selective archiving process

Selective archiving, also known as email mining, archives messages on Domino mail servers to the IAP. A tombstone, a link to the original email that is stored in the IAP system, can be created in the user's mail file.

Selective archiving is primarily used to reduce the size of user mail files. A single mining profile can apply to everyone in the organization, or multiple mining profiles can be created. For example, All Managers, All Associates, Temporary Staff, and so forth.

Follow these steps to configure and enable selective archiving:

1. Edit the selective mining profile, which contains the mining rules.
See [“Configuring mining rules”](#) on page 160.
2. Configure the Preprocessing Control document, for handling signed and encrypted messages.
See [“Configuring the Preprocessing Control document”](#) on page 177.
3. Schedule and enable the Encapsulate agent in the preprocessing database.
See [“Scheduling and enabling the preprocessing agents”](#) on page 182.
4. Schedule and enable the Profile Agent.
See [“Working with the Profile Agent”](#) on page 185.
5. Schedule and enable the other HP EAs-D User database agents.
See [“Enabling other HP EAs-D User agents”](#) on page 187.
6. Schedule and enable the Archive, Tombstone, and Reference Cleanup agents.
See [“Scheduling and enabling the archiving agents”](#) on page 191.
7. Ensure that the Get Held Messages agent and the Purge_Document agent in the HP EAs-D Log, HP EAs-D Alert, and HP EAs-D Stats databases have been scheduled and enabled.
8. Schedule and run the archiving job.
See [“Running an archiving job”](#) on page 193.

 **NOTE:**

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

Configuring mining rules

The archiving profile, which contains the mining rules, must be configured in order to archive messages in mail files.

To configure the profile:

1. Double-click the **HP EAs-D API** database file.
2. In the HP EAs-D API main view, double-click **Mining Rule: Selective** under Mining Rules.
The mining rules document appears.
3. Complete the following fields at the top of the document:

Field	Description
Profile	The name of the profile for the mining rule. If you rename the profile, or create a new mining rule, the profile name cannot include spaces or dashes.
Policy Status	Select Enable when you are ready to activate the profile and begin archiving.

4. Continue to configure the mining rule settings.
 - “[Time Conditions tab](#)” on page 161
 - “[Folders Settings tab](#)” on page 162
 - “[Exceptions Settings](#)” on page 163
 - “[User Membership tab](#)” on page 165
 - “[Reference Database tab](#)” on page 167
 - “[Tombstone Settings tab](#)” on page 168
 - “[Session Settings tab](#)” on page 170
 - “[User Notification tab](#)” on page 172
 - “[Administration Alert tab](#)” on page 173
5. When the profile is complete, click **Save**.

Creating additional mining rules

To increase throughput across multiple HP Gateway servers, you can create additional mining rules to distribute the agent processing load.

If you plan to use more than one selective mining rule, copy and paste the current rule. (This can be done before or after editing the rule, depending on how many of the settings are duplicated.)

1. Select the rule in the HP EAs-D API main view.
2. Select **Edit > Copy**, and then select **Edit > Paste**.
3. Change the name of the new rule in the Profile field.
The users covered by the rule are set in the User Membership tab.

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.

[Time Conditions]

Specify how to calculate document age, the time condition is based on TIME/DATE field

Memo, Reply

Memo, Reply, type of document	Last Modified Date	
Specify Form(s) to <u>not</u> archive	Notice Task Appointment	List of Forms to not archive (excludes 'Task' and 'Calendar' Forms)
Archiving Date for not Foldered Document	90 03/02/2010	[- No of Day(s)] Condition also used for all other documents: when Form is not 'Calendar' or 'Task' Example: mail in Inbox only
Archiving Date for Foldered Document	120 01/31/2010	[- No of Day(s)] Mail stored in one or more folders older than xx day(s) will be archived.
Maximum Date for Document Retention	<input type="text" value="16"/>	Documents to be archived will have to be OLDER than the specified date

Field	Description
Memo, Reply type of document	Click the arrow and select the way to define an email's date for archiving purposes: Creation Date, Last Modified Date, or Posted Date.
Specify Form(s) to not archive	List any forms that should not be archived. EAs Domino does not archive appointments (calendar entries), notices (meeting requests), and tasks. All other forms are archived unless they are excluded in this field. Form names can be separated by commas, semicolons, or newlines.
Archiving Date for not Foldered Document *	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 Document *	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.
Maximum Date for Document 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 Documents and non Foldered Documents, leave this field blank.
Comments	Enter any comments about the configuration.

* This date works with the date entered in the Session Settings/Archive Strategy tab to establish a date range for archiving. For example, if the value in this field was one year, and the value in Session Settings was 7 years, messages between 1–7 years old would be archived.

Folders Settings tab

These settings define specific archiving treatment for user mail folders.

[Folders Settings]		
Archive documents stored in specified folders.		
No Time Condition - "on demand"	HPArchivePending	All document stored are candidates for being archived
Remove Doc from folder once archived	\$Inbox	If document passes the archive selection then it is removed from the specified folder
Folders / Views to exclude		All documents found in these folders or views will not be archived.
Include selected Folders / Views only		Process the documents stored in these folders or views only .

Field	Description
No Time Condition — "on demand"	<p>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 configured in the Session Settings tab still applies.) The folder can include nested folders.</p> <p>You can list more than one folder. Folder names can be separated by commas, semicolons, or newlines.</p> <p>Note: HPArchivePending is simply an example and can be removed from this field.</p>
Remove Doc from folder once archived	<p>When you list a folder in this field, messages are removed from the specified folder after they are successfully archived.</p> <p>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.</p> <p>HPArchivePending is simply an example and can be removed from this field.</p> <p>Tip: For mailbox management, you could list the \$Inbox folder.</p>
Folders/Views to exclude	<p>Enter any views or folders containing messages that should not be archived.</p> <p>\$Drafts is automatically excluded during selective archiving.</p> <p>Names can be separated by commas, semicolons, or newlines. The folders listed can include nested folders.</p>
Include selected Folders/Views only	<p>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.</p> <p>If you complete this field, do not complete the Folders/Views to exclude field or the All Document view name field in the Session Settings tab.</p> <p>Names can be separated by commas, semicolons, or newlines. The folders listed can include nested folders.</p>

Exceptions Settings

Use the Exceptions Settings to define exceptions to the overall mining rules.

Special Fields

[Exceptions Settings]

Documents matching exceptions will not be archived.

Special Fields | Attachments & Doc size | Other Macro Formula

Exclude if one or more of the listed fields are found on the document

Document fields: MAILSTATIONERYNAME Excludes the document if any Field exists.
 PROTECTFROMARCHIVE
 RepeatInterval
 \$AttBytesTruncated
 \$DocBytesTruncated
 HpTombstoned

Field	Description
Document fields	<p>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.</p> <p>You can add other fields. Field names can be separated by commas, semicolons, or newlines.</p> <p>Important! Do not delete the HPTombstoned field, or tombstoned messages will be continually re-mined.</p> <p>Note: If you want to exclude a form, complete the "Specify Form(s) to not archive" field on the Time Conditions tab. Appointments (calendar entries), notices (meeting requests), and tasks are automatically excluded from archiving.</p>
Comments	Enter any comments about the configuration.

Attachments & Doc size tab

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

[Exceptions Settings]

Documents matching exceptions will not be archived.

Special Fields
Attachments & Doc size
Other Macro Formula

Exclude if document has unauthorized attachment and/or wrong size (size control is disabled if ZERO)

Unauthorized attachment extensions

Maximum document size MBytes

Minimum document size to be archived KBytes

Attachment control : Enable Disable

Skip the archive if the total document size is **OVER** the allowed limit - the size includes the body and attachments.

Skip the archive if the total document size is **NOT OVER** the allowed limit - the size includes the body and attachments.

Field	Description
Attachment control	Click Enable to enable these settings.
Unauthorized attachment extensions	To exclude message attachments with certain types of extensions, list the extensions. Extensions can be separated by commas, semicolons, or newlines. Note: You can prevent the system from mining attachments that contain notices, such as meeting requests, by entering .ics . This is recommended if the Windows Notes Plug-In is installed on client systems.
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 files 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's email can be archived.

For more information, see [“Working with the Profile Agent”](#) on page 185.

[User Membership]		
Documents matching definition will be selected.		
Is Default Profile: <input type="radio"/> Yes <input checked="" type="radio"/> No		Active for Profile Agent: <input checked="" type="radio"/> Yes <input type="radio"/> No
Include Users on selected Mail server(s): <input type="radio"/> Local server <input checked="" type="radio"/> All servers <input type="radio"/> Only Selected server(s)		Active for database(s): <input checked="" type="checkbox"/> User MailFile <input checked="" type="checkbox"/> Mail in Db
Use Alternate Server: <input type="radio"/> Yes <input checked="" type="radio"/> No		
String pattern matching (Meta)	Groups	Person entry
*/*Sales/Acme	*	*
Parameters	Values	
Default Agent Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Inherited Fields	*	

Field	Description
Is Default Profile	<p>Click Yes if you want to make the profile the default selective archiving rule that is associated with users in the mail domain.</p> <p>Note: One profile must be designated as the default.</p>
Active for Profile Agent	<p>This field determines whether the Profile Agent uses the information in the User Membership tab to find and assign users to the mining rule.</p> <p>For selective archiving, keep the default of Yes to enable the Profile Agent for the rule.</p> <p>The Profile Agent is disabled for compliance archiving (see “Configuring the journal mining rule” on page 218) and for Bulk Upload (see “Editing the bulk upload mining rule” on page 226).</p>
Include Users on selected Mail server(s)	<p>Select the mail servers to be mined with the rule.</p> <p>Either All servers or Only selected servers can be selected.</p> <ul style="list-style-type: none"> • All servers (all mail servers in the domain) Any users who match the value set in the Membership Conditions field are added to the mining rule, regardless of the user's home (mail) server. • Only selected servers Any users who match the value set in Membership Conditions are added to the mining rule when 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	<p>Select User MailFile and/or Mail in Db.</p> <p>Users can be selected from standard Domino mail files (User MailFile) and Mail-in databases (Mail in Db).</p>
Use Alternate Server	<p>Keep the default value of No for selective archiving. This field is only enabled for compliance archiving configurations that use replicated journaling.</p>
Membership conditions	<p>Define the user mail files to be mined using this rule. Select any or all of the following:</p> <ul style="list-style-type: none"> • 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 167. • Groups: A group within the organization. Important! EAs Domino does not support group types that are set to Access Control List. • Person entry: Individual mail files.

Field	Description
Default Agent Status	This field determines whether the users that are assigned to the profile have mining enabled or disabled by default. Click Enable to enable mining for the specified users. If the value is set to Disable, you will need to open the Users database and, in the Mail Detail records, explicitly turn on mining for the specified users. (This is useful for testing purposes to specify the users that Profile Agent assigns to a rule.)
Inherited Fields	EAs Domino Mail Detail records contain several values from Domino Person or Mail-In documents. (See “ Viewing Mail Detail documents ” on page 185.) 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. Note: You can build custom views in the HP EAs-D Users database that display, sort, and/or categorize the Mail Detail records to show the additional fields.
Comment	Enter any comments about the document.

Defining wildcard patterns

Wildcards can be used to define users who are associated with a mining 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 reference documents, pointers to the messages that are eligible for archiving. This tab lists the name and location of the reference database for the mining rule.

[Reference Database]

Reference database is the temporary repository for document before getting formatted and sent to the IAP

Reference Database name: Reference document type: Extended Regular

Reference Database Server name: (leave blank for local) Preserve References for auditing: Yes No

Original field(s) to be added to the Reference record:

Field	Description
Reference Database name	For selective mining, enter <code>hprim/hp_riss_minerreferenc.nsf</code> unless you have created a new mining rule and reference database.
Reference document type	Select Extended . An Extended reference document is used in remote mining and appends the following fields to a message: <ul style="list-style-type: none"> • 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 required for interim processing and troubleshooting. Only one HP Gateway server should ever mine a given database.
Reference Database Server name (leave blank for local)	Leave this field blank.
Preserve References for auditing	Keep the default of No . Auditing is not supported in EAs Domino 2.1.x.
Original fields to be added to the Reference record	This information is used for auditing, which is not supported in EAs Domino 2.1.x.
Comments	Enter any comments about the reference database.

Tombstone Settings tab

Use this tab to specify the action the Tombstone agent takes when a message is archived. 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.

[Tombstone Settings]

Control the creation of tombstones for archived messages, determine size and functionality.

Actions	Style
<input type="radio"/> None <input type="radio"/> Shrink Body and remove attachments <input type="radio"/> Remove attachments only <input checked="" type="radio"/> Clear body and remove attachments <input type="radio"/> Delete message	<input checked="" type="radio"/> Text <input type="radio"/> Rich Text [Text : This message has been archived.]
Operate only if document is greater than	0 Bytes
Reference Document Retry interval	10 Days

Field	Description
Actions	<p>Select the action to occur when a message is mined:</p> <ul style="list-style-type: none"> • Tombstoning actions: <ul style="list-style-type: none"> • Shrink Body and remove attachments: All attachments are removed from the message and the message body is trimmed to approximately the length specified in the Shrink to field. We recommend this option when DWA Extension is implemented. If you select this action, enter the trimmed length in bytes in the Shrink to field. This option offers very good storage savings (typically 80-90% of the savings offered by the clear body and remove attachments option below). Full-text indexing on the Domino server is preserved for the first few sentences or paragraphs of a typical message, depending on the shrink to size that you enter. Users previewing archived messages in DWA or in the Notes client (when Local Cache is installed without the Notes Plug-In) can view part of a message depending on the shrink to size. The full message can be previewed when the Notes Plug-In is installed. • Remove attachments only: Message attachments are removed, but the message body is left intact. This option offers good storage savings (typically 80% of the savings offered by the clear body and remove attachments option below). Full-text indexing and preview are completely preserved. • Clear body and remove attachments: Both the body and attachments are removed from the message. This option offers the best storage savings. However, for messages that are archived, there is a complete loss of full text indexing on the Domino server and message content cannot be previewed in DWA. Notes client users, including those with Local Cache installed, can preview archived messages only if the Notes Plug-In is installed. <p>Note: Customers who use Domino Attached Object Services (DAOS) already benefit from the significant storage gains of attachment single-instancing. If multiple messages contain an attachment, only one copy of the attachment is maintained on the Domino server.</p> <p>HP estimates that EAs Domino tombstoning options provide an additional 15% of storage savings on top of DAOS. However, results can vary dramatically depending on your Domino environment.</p> <p>EAs Domino has no known compatibility problems with DAOS. DAOS occurs at a layer beneath the standard Notes APIs and EAs Domino is unaware that it is in use.</p> <ul style="list-style-type: none"> • Non-tombstoning actions: <ul style="list-style-type: none"> • 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 that are discovered and archived in the Bulk Upload process are deleted during tombstoning. Journalled messages are deleted automatically in compliance archiving, even if this option is not selected.)

Field	Description
Style	<p>If you selected one of the tombstoning actions, a tombstone replaces the message. Use the Style field to format the tombstone.</p> <ul style="list-style-type: none"> 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 308.) 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 261. When Rich Text is selected, each tombstoned message is a minimum of 2–5 KB depending on the Tombstone Prototype key. <ul style="list-style-type: none"> 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.
Operate only if document is greater than x Bytes	<p>If the action specified in the Actions field should occur only when a message and its attachments exceed a certain size, enter the size in bytes.</p> <p>If the action should always occur, leave the default of 0.</p> <p>Note: If users view archived messages in DWA, we recommend that you specify a size of 2000–5000 bytes, depending on the Tombstone Prototype key. Tombstoned items are a minimum of 2–3 KB for TSKeys 1, 2 or 3 and 3.5–5 KB for TSKeys 2.1-x.</p>
Reference Document Retry interval	<p>Documents in the reference databases and any linked documents in the preprocessing databases are temporary and are always re-created if they are lost, for example after a server crash.</p> <p>Use this field to set the time until the documents are re-created. The default is 10 days.</p> <p>Note: Until references are processed, the corresponding messages remain on the mail server.</p>

Session Settings tab

Session settings define archiving strategy and control the impact of mining sessions on server resources.

Reference Limits

Field	Description
Do not start the program if 'Reference' database	<p>When you enable this option, mining does not start if the reference database:</p> <ul style="list-style-type: none"> Is bigger than n MB, or Has more than n messages. <p>Click Yes to enable the option, and then enter a value for one or both of the parameters.</p> <p>Leave the view set to References.</p> <p>Alerts can be sent if mining does not start. See "Administration Alert tab" on page 173.</p>

Session Limits

Field	Description
Allow Remote Mining of databases	Ensure that Yes is selected so that mail files can be mined from the HP Gateway server.
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 (no 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.

Archive Strategy

Field	Description
Archiving Strategy	<ul style="list-style-type: none"> Keep the default of None: <ul style="list-style-type: none"> For compliance archiving and Bulk Upload For selective archiving unless folder options or archiving based on quota are specified in the rule. Folder options are <i>Folders/Views to exclude</i> and <i>Include selected Folders/Views only</i> in the Folders Settings tab. If you have specified archiving to quota or a folder option, select the order in which messages that meet the criteria for archiving are sorted before they are archived: Oldest first or Biggest first.

Field	Description
Do not archive document older than	<p>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.</p> <p>Note: The date in this field must be in the past.</p>
All Document view name	<p>If you want to stipulate a specific view as the primary view that rissminer searches for messages, enter the name of the view.</p> <p>This optional setting lets you use a Notes view selection formula to determine the types of messages to be archived.</p> <p>If you use this setting, do not complete the <i>Include selected Folders/Views only</i> option in the Folders Settings tab.</p>
Archives based on quota	<p>If you have set a quota for user mailbox size, mailboxes can be mined so their size falls below a percentage of the quota.</p> <p>If you select Yes for this setting, complete the Percentage of the Quota field. EAs Domino detects when the quota percentage, or threshold, is exceeded and archives messages until the mailbox size falls below the threshold. The archiving strategy determines which messages are archived first: oldest first or biggest first.</p>

User Notification tab

Use this tab to compose a memo that is sent to user mailboxes. This message provides feedback about the selective archiving 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.

Field	Description
Send notification with Selective Archiving information	Enable or disable user notification by clicking Enable or Disable .
Subject	Enter a subject for the notification.
Message body	Enter the notification message.
Comments	Enter any comments about the notification.

Administration Alert tab

Alerts can be sent to administrators when mining does not start. This can occur if a reference database cannot be opened and checked against the rule's [session settings](#), or if one of the conditions configured in the [reference limits](#) exists.

Alerts can be configured in the Global Configuration document instead of this tab, but they can only be sent if they are enabled in this tab.

Field	Description
From	Enter a value, such as the name of the mining rule.
To	Click the arrow and select a name or names from the address book. (Usually this alert is sent to the Domino administrator.)
Subject	Enter a subject for the alert. For example, "Mining did not start."
Allow Alert to be sent	Click Yes to enable alerts to be sent.
Alert Relay Server	To configure this setting, click the arrow and select the server through which alerts should be sent. In most cases, this will be a server in the customer's mail domain. If you select Local, alerts will be sent to the local HP Gateway server. In most cases, Local should not be selected. This field can be left blank if you have already defined the relay server in the Global Configuration document or the Server Definition document.
Comments	Enter any comments about the alert.

4.2 Preprocessing messages

This chapter explains why some messages must be preprocessed before they can be archived, and describes the steps required to configure the preprocessing settings.

- [Preprocessing overview](#), page 175
- [Configuring the Preprocessing Control document](#), page 177
- [Scheduling and enabling the preprocessing agents](#), page 182

Preprocessing overview

Some Lotus Notes items must be preprocessed so they can be archived in a format that preserves all message data intact. To accomplish this, a copy of the original message is *encapsulated*—encased in its own database.

Encapsulation is performed by the Encapsulate agent in the preprocessing database. Three preprocessing databases are installed on each HP Gateway server, one for selective archiving, one for compliance archiving, and one for Bulk Upload. Each preprocessing database is paired with a corresponding reference database to process messages for archiving.

NOTE:

The original message and the document reference that points to the message must exist in order for encapsulation to work.

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

Types of encapsulation

EAs Domino employs two types of encapsulation:

- **Standard encapsulation:**

In this type of encapsulation, the encapsulation database is attached to a copy of the original message that contains all the headers and unformatted body text of the original message. After processing, the message and database attachment are routed to the user's repository in the IAP. The message is indexable and can also be searched on using header data, since the original message headers are preserved.

Standard encapsulation is used for the following types of messages:

- Lotus Notes PKI and S/MIME signed and encrypted messages
- Non Memo Reply items such as notices (meeting requests) or phone calls
- Older messages with HTML links that are now broken
- Some messages containing custom forms, such as custom forms from workflow applications
- Messages with ATT attachments

See [“Message attachments named ATTxxxxx”](#) on page 327 for a description of these messages.

- **Clean Envelop Encapsulation:**

Clean Envelop Encapsulation is used for messages that are rejected by the IAP's SMTP portal with RFC-822 or MIME parsing errors. An example would be failed ingestion messages with the error message “SMTP Protocol Returned a Permanent Error 551.”

In this type of encapsulation, the encapsulation database is attached to a specially-created “clean envelope” message whose header is configured in the Global Configuration document. The original message header is not preserved in the clean envelope.

An attempt is made to render the original header data and body text in the body of the clean envelope. This makes the data indexable, but the header of the original message cannot be searched on. Attachments are not preserved in the clean envelope.

The encapsulated message that is attached to the clean envelope does preserve, with full fidelity, the original message and any attachments it contains.

After processing, the clean envelope message and its database attachment are routed to a special repository that has been set up in the IAP for clean envelope messages.

For information on configuring the clean envelope, see [“Message Reprocessing”](#) on page 142.

Retrieving encapsulated messages

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 Web Interface to their mail file (Mail-To-Me messages), the message remains inside the encapsulation database. [“Opening encapsulated messages in Lotus Notes”](#) on page 314 explains how to open these messages.

Preprocessing steps

To enable message encapsulation:

1. Configure a Preprocessing Control document for each preprocessing database that is used during archiving.
Follow the steps in the next section to complete these documents.
2. If Clean Envelop Encapsulation is enabled, configure the relevant settings in the Global Configuration document.
See [“Message Reprocessing”](#) on page 142.
3. Schedule and enable the preprocessing agents.
See [“Scheduling and enabling the preprocessing agents”](#) on page 182.

Configuring the Preprocessing Control document

A Preprocessing Control document must be configured for each preprocessing database that is employed during archiving. This document defines the settings that the Encapsulate agent uses to preprocess messages. Three default documents have been created in the HP EAs-D API database: for selective archiving, journaling (compliance archiving), and Bulk Upload.

Follow these steps 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 compliance archiving (journaling), selective archiving, or Bulk Upload to open the document.
3. Determine if this is the default preprocessing configuration for the archiving type.
 - If the document applies only to specific servers, listed in the [Databases Location tab](#), click **No**.
 - If the document applies to any HP Gateway server with the filepath listed on the Databases Location tab, click **Yes**.
4. Configure the settings in each tab:
 - “[Databases Location tab](#)” on page 178
 - “[Encapsulation Settings tab](#)” on page 179
 - “[Agent Log Settings tab](#)” on page 180
 - “[Execution Settings tab](#)” on page 181
 - “[Logging tab](#)” on page 182
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 using **Edit > Copy** and **Edit > Paste**. This ensures that the encapsulation database is copied into the new document. Do not use the Create menu.

Databases Location tab

Is default: No Yes

Status: Enable

Databases Location | Encapsulation Settings | Agent Log Settings | Execution Settings | Logging

[Databases Location]


Domino Server(s)	HPGateway1\hparchive HPGateway2\hparchive
PreProcess Database	hprim\hp_preproc_miner.nsf
Reference Database	hprim\hp_riss_minerreferenc.nsf

Field	Description
Domino Server(s)	<ul style="list-style-type: none"> If this is the default Preprocessing Control document for the archiving type (Yes is selected for "Is default"), do not edit this field. If the document only applies to specific HP Gateway servers, click the arrow and select the names of the Gateway server(s) on which the preprocessing and reference databases are installed.
PreProcess Database	<p>The path and filename are pre-set for the default preprocessing databases:</p> <ul style="list-style-type: none"> hprim\hp_preproc_miner.nsf for selective archiving hprim\hp_preproc_journal.nsf for compliance archiving hprim\hp_preproc_blk.nsf for Bulk Upload
Reference Database	<p>Each preprocessing database has a corresponding reference database. The path and filename are pre-set for the default reference databases :</p> <ul style="list-style-type: none"> hprim\hp_riss_minerreferenc.nsf for selective archiving hprim\hp_riss_journalreferenc.nsf for compliance archiving hprim\hp_riss_blkupreferenc.nsf for Bulk Upload

Encapsulation Settings tab

Databases Location | **Encapsulation Settings** | Agent Log Settings | Execution Settings | Logging

[Encapsulation Settings]

Encapsulation Database  encap001.nsf

Temporary Work Area

Note: use OS format for filepath seperators - "\" for Windows and "/" for Unix

THIS DIRECTORY MUST EXIST ON THE SERVER.

CleanUp Purge Interval hours

Field	Description
Encapsulation Database	<p>We do not recommend editing this field.</p> <p>During preprocessing, a copy of the message is encased in an empty encapsulation database. The database is then renamed (for example, encap001.nsf, encap002.nsf) and added as an attachment to the message.</p> <p>It is possible to replace the empty encapsulation database in this field. However, the filename must remain the same and the replacement cannot contain any data. Alterations to the database, such as the addition of a form or view, significantly increase its storage size inside the IAP. HP does not support any functionality provided by changes to the encapsulation database.</p>

Field	Description
Temporary Work Area	<p>This field lists the directory on the HP Gateway server that temporarily stores the encapsulation databases while the messages are being encapsulated.</p> <p>Important! Always create a new directory for the work area, making sure the following conditions are met:</p> <ul style="list-style-type: none"> • Ensure that each preprocessing database (for compliance archiving, 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 sub-directories 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 <code>D:\Lotus\Domino\Data\RIM_TEMP</code> if that is the path to your Domino data root. Do not share this directory in your network. <p>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.</p> <p>For example, on a Windows-based Domino server, enter:</p> <pre>C: CD\ MKDIR RIM_TEMP CD RIM_TEMP MKDIR MNR</pre> <p>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:</p> <pre>chown domino:domino RIM_TEMP chmod 755 RIM_TEMP</pre>
CleanUp Purge Interval	<p>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.</p>

Agent Log Settings tab

Field	Description
Log Path and Filename	<p>Leave the EAs Domino log as the default: <code>hprim\hp_risslog.nsf</code></p>
Encapsulate Log ID	<p>Leave the default: Encapsulate.</p>
CleanUp Log ID	<p>Leave the default: Cleanup.</p>

Execution Settings tab

Databases Location | Encapsulation Settings | Agent Log Settings | Execution Settings | Logging

[Execution Settings]

Maximum Session Size 300M (*Size*)

Maximum Documents to Encapsulate 3000 (*Number*)

Perform Validation Yes No

Maximum number of retries if validation fail: 3 (*Number*)

Always Preserve File Attachments Yes No
(Only used if message Body must be converted from Rich Text to Text)

Field	Description
Maximum Session Size	<p>The maximum amount of data that the Encapsulate agent can process in one session. The default that is shown in this field depends on the type of archiving:</p> <ul style="list-style-type: none"> • Selective archiving: 300M • Compliance archiving: 300M • Bulk Upload: 500M <p>The default value is adequate for most environments.</p>
Maximum Documents to Encapsulate	<p>The maximum number of messages that can be processed by the Encapsulate agent in a session. The default that is shown in this field depends on the type of archiving:</p> <ul style="list-style-type: none"> • Selective archiving: 3000 (messages) • Compliance archiving: 3000 (messages) • Bulk Upload: 5000 (messages) <p>The default value is adequate for most environments.</p>
Perform validation	<p>Leave the default of Yes to ensure that a valid encapsulation database is attached to a message.</p>
Maximum number of retries if validation fails	<p>Enter the number of validation retries. The default is three retries.</p>

Field	Description
Always Preserve File Attachments	<p>Leave the default of Yes.</p> <p>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.</p> <p>While the conversion occurs, file attachments are temporarily detached and placed in the same temporary work area that is used by the encapsulation databases.</p> <p>Yes must be selected so that attachments can be preserved and reattached to the message.</p>

Logging tab

The logging 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 Logging Level is set to **None**, unless you are asked by HP support to enable logging.

Scheduling and enabling the preprocessing agents

The Encapsulate agent in the preprocessing database performs message encapsulation, using the settings configured in the Preprocessing Control document. The Remove Obsolete PreProcess Documents agent cleans up obsolete documents in the database.

These agents must be scheduled and enabled in each preprocessing database that is used for archiving.

1. In the Designer client, open the preprocessing database:
 - a. Click **Open an Existing Database**.
 - b. Select the server on which the preprocessing 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 (Journal) (`hp_preproc_journal.nsf`)
 - Bulk upload: HP EAs-D PreProcess (Blkupd) (`hp_preproc_blk.nsf`)
 - d. Click **Open**.
2. In the Design pane, select **Code > Agents**.
3. Double-click the Encapsulate agent to open it. Click **OK** if a warning message appears. The agent Properties 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.
The schedule should be set to more than once a day for the Encapsulate agent in the journal preprocessing database.
 - b. Click **Schedule** and set the run time to meet your requirements.
The Encapsulate agent in the journal preprocessing database 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. Click **Yes** to save the agent Properties.
7. Close the agent Properties and the agent, and then click **Enable**.
8. Repeat this process for the Remove Obsolete PreProcess Documents agent.
The agent only needs to run once a day.
9. To enable the agents on another server, repeat steps 1–8.
Preprocessing databases are not replicated, so the agents must be scheduled and enabled on each server used for archiving.

4.3 Configuring the archiving agents

The following topics describe the role played by HP EAs Domino agents in the archiving process:

- [Working with the Profile Agent](#), page 185
- [Enabling other HP EAs-D User agents](#), page 187
- [Enabling the preprocessing agents](#), page 190
- [Configuring Get Held Messages](#), page 190
- [Scheduling and enabling the archiving agents](#), page 191

 **NOTE:**

Always ensure that the agents are appropriately signed to execute on the HP Gateway servers. The last user ID to modify the agents will be the ID that the agents assume for access to the server.

Working with the Profile Agent

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

 **NOTE:**

If there is more than one HP Gateway server, run the Profile Agent on only one server.

Viewing Mail Detail documents

When the Profile Agent is run for a selective mining rule, it scans the User Membership settings in the rule to create and maintain a Mail Detail document for each user. Mail Detail documents import values from several fields in the Person or Mail-In Database documents in the Domino Directory.

During synchronization with the Domino Directory, the Profile Agent updates the Mail Detail records with any changes. It also refreshes the last synchronization date and other information such as the size of the user's mail file.

- 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 is no longer associated with the rule, the Module Status field is changed to No Profile Assigned.

Mail Details

CN=Barney Rubble/O= Org1

Database Details	Database Activity	Activity Log	Notes Archive Settings
[Database Details]			
First Name	Barney		
Middle Initial			
Last Name	Rubble		
Full Name	Barney Rubble/Org1		
Home Server	Server1/Org1		
Database Filepath	mail\barney		
Database used for Journaling	<input checked="" type="radio"/> No <input type="radio"/> Yes		
Mining Rule(s) Assigned	SelectiveArchiving		
Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <input type="radio"/> No Profile Assigned		

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

Database Details	Database Activity	Activity Log	Notes Archive Settings
[Database Activity]			
Database Title	BarneyR		
Database Template	Mail (R8.5)		
Creation Date	01/03/2010		
Replica ID	6525774A002F9		
Last Read	0 doc	Last Read Date	
Last Write	0 doc	Last Write Date	
Max Size	194304 MB	Logical size	0 MB
Current Size	53.75 MB	Percentage used	0 MB

- The **Activity Log** tab provides a brief summary of the mining activity in the user database, showing the date and time of mining, the number of messages mined, and their total size. This logging must be formally activated and should only be performed if your organization has a single HP Gateway server. For more information, see [“Purge Stats Selective Archive Log agent”](#) on page 189.
- 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.

Scheduling the Profile Agent

The Profile Agent must be scheduled and enabled so it can populate the HP EAs-D Users database. The Users database is replicated to all HP Gateway servers.

The Profile Agent is run only for selective archiving. It is not used for compliance archiving (where a journal's Mail Detail record is created manually) or Bulk Upload (where Mail Detail records are created by the Bulk Upload executable).

To schedule and enable the Profile Agent:

1. In the Designer client, open the HP EAs-D Users database in the `hprim` folder on any HP Gateway server.
2. In the Design pane, select **Code > Agents**.
3. Double-click **profileAgent**. Click **OK** to bypass the warning.
The agent Properties appears.
4. Ensure 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 an HP Gateway server. The agent must run on only one Gateway 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 Domino software is configured, you can force the Profile Agent to populate the EAs-D Users database by opening the server console and entering:

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

Enabling other HP EAs-D User agents

In addition to enabling the Profile Agent, enable the agents listed below when using selective archiving. You can also change some of the 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.

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 HP Gateway server with a copy of the database.

2. In the Design pane, select **Code > Agents**.
3. Double-click the agent name, and then click **OK** to bypass the warning.
4. In the agent Properties, 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, click **Yes** to save the changes, and then click **Enable** to enable the agent.

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 **Arg1: 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 Arg2.

6. Select **File > Save**, and then close the document.

Purge Not Synchronized person document agent

This agent removes the Mail Detail documents of users whose Person documents have been removed from the Domino Directory. It must be scheduled and enabled using the steps in ["Scheduling the agent"](#) on page 187.

By default, Mail Detail documents 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 **Arg1: How many days to be kept** double-click the **Value** field and change the number of days.
The user's Mail Detail record is deleted if the mail file is not synchronized for this number of days.
6. Select **File > Save**, and then close the document.

Purge Stats Selective Archive Log agent

HP EAs Domino can save a log in each user's Mail Detail record that records the activity of rissminer, the mining program, in the user's mail file. The activity log provides a brief summary that shows the date and time of mining, the number of messages mined, and their total size.

When this feature is activated, the Purge Stats Selective Archive agent must be enabled so it can periodically purge the entries in the activity log.

When to activate the activity log

Single HP Gateway server

If the organization has a single HP Gateway server, you can allow mining activity to be recorded in a user's Mail Detail record. This is done by adding an -l switch to the rissminer command. For example:

```
rissminer -k<profile name> -l
```

For information on adding the switch in the rissminer program document, see [“Scheduling the archiving job”](#) on page 193. For information on running the command in the server console, see [“Running an archiving job manually”](#) on page 195.

If the log is activated, schedule and enable the Purge Stats Selective Archive agent. Entries are purged based on the maximum amount of text that can be stored in the log. The agent **must** run before the log reaches a 64 KB limit. Otherwise the following error message appears:

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

Schedule the agent to run at least once a week. The default is once a day.

You can decrease the amount of text that is retained in the log. If you want to do this, follow the procedure in [Reducing the amount of text in the log](#) below.

Multiple HP Gateway servers

If the organization has multiple HP Gateway servers, it is important to prevent replication conflicts in the HP EAs-D Users database.

These conflicts can occur when rissminer is running on one HP Gateway server and the Purge Stats Selective Archive Log agent is enabled on a different Gateway server.

When the organization has multiple HP Gateway servers:

- Do not add the -l switch to the rissminer command. The rissminer activity will not be logged in the Mail Detail record's Activity Log tab.
- It is not necessary to enable the Purge Stats Selective Archive Log agent.

Reducing the amount of text in the log

If mining activity is logged in the Mail Detail records and the Purge Stats Selective Archive Log agent is enabled, the records must be purged at least once a week.

The maximum number of entries that can be kept in the log is 20 (one line per run). You can edit this value downward, but it cannot be increased.

To decrease the amount of text that is 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 **Arg1: Number of lines max**, edit the **Value** field to reduce the number of entries.
Legal values are 0–20 lines. 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.

Enabling the preprocessing agents

See [Scheduling and enabling the preprocessing agents](#), page 182 for the procedure to follow.

Configuring Get Held Messages

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

After the application recovers a held message from mail.box, it resubmits the message to the router several times, giving it more chances to be delivered. If the message still cannot be delivered, it is automatically reprocessed. Messages that remain in Get Held Messages after reprocessing are sent to HP support for diagnosis. See [“Processing held messages”](#) on page 317 for the procedure to use this database.

A unique instance of the Get Held Messages database must be configured on each HP Gateway server.

1. Using the Domino Administrator client, open the HP EAs-D Get Held Messages database (`hprim\hp_GetHeldMsgs.nsf`).
2. Ensure that the ACL has been set for the database.
See [“Setting access control \(ACL\)”](#) on page 80 for the settings that should be used.
3. Open the Setup Controls view in the database.
4. Double-click each setup control, adjust it as necessary for the installation, and then save the database.
Each control contains an explanation of how to use it.
5. Save the database.
6. Using the Domino Designer client, perform the following steps:
 - a. Open the Get Held Messages database.
 - b. Expand **Code**, select **Agents**, and open the **Get Held Messages** agent.
 - c. In the agent Properties, click **Schedule**.
By default, the agent runs every four hours. You can change the schedule so that it runs more frequently; for example, for testing purposes.
 - d. Select the HP Gateway server in the Where agent runs box.
 - e. Save your changes, and close the agent.
 - f. Enable the Get Held Messages agent.

Scheduling and enabling the archiving agents

Email messages are targeted for archiving by the rissminer program, using the associated mining profile. When rissminer is run, references to the targeted messages are created in the appropriate reference database (for selective archiving, compliance archiving, or Bulk Upload). For example, after a message is identified by the rissminer program and the selective archiving profile, a reference to the message is created in the HP EAs-D Reference (Miner) database.

The Archive agent in the reference database sends the referenced messages to the IAP. After the messages are successfully ingested, the Tombstone agent executes the action configured in the mining rule's [Tombstoning Settings tab](#).

Messages that are not archived, due to conversion or ingestion failure, are pulled from the Domino router into the HP EAs-D Get Held Messages database and reprocessed by the Reference Cleanup agent in the reference database. (See "[Processing held messages](#)" on page 317 for more information about message reprocessing.)

The Archive, Tombstone, and Reference Cleanup agents must be scheduled and enabled in each reference database that is used, on each HP Gateway server.

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 (Miner) (`hp_riss_minerreferenc.nsf`)
 - Journaling: HP EAs-D Reference (Journal) (`hp_riss_journalreferenc.nsf`)
 - Bulk upload: HP EAs-D Reference (Blkupd) (`hp_riss_blkupreferenc.nsf`)
 - d. Click **Open**.
2. In the Design pane, select **Code > Agents** in the reference database.
3. Double-click the agent name, and then click **OK** to bypass the warning.
The agent Properties 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 **Schedule** to set the run time.
 - By default, the Archive and Tombstone agents are set to run every hour. For selective archiving, you might want the agents to run less frequently. For compliance archiving, you might want the agents to run more frequently. If so, the times should be at least 20 minutes apart. Be sure that the schedule works with the schedule set in the rissminer program document. See "[Scheduling the archiving job](#)" on page 193.
 - The Reference Cleanup agent only needs to run once a day. The default setting is daily at 1:00 a.m.
 - b. Ensure that the server name appears in the **Where agent runs** box.
 - c. 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** to enable each agent.
8. Repeat steps 1–7 for each reference database and server used for archiving.

4.4 Running an archiving job

- [Scheduling the archiving job](#), page 193
- [Running an archiving job manually](#), page 195
- [Viewing reference documents](#), page 198

Scheduling the archiving job

Each mining rule has an associated program document that must be scheduled and enabled. This program document is used to launch the rissminer program. It is run with the command `-k<profile name>`, using the profile name established in the mining rule. The rissminer program runs against the mail files of users selected in the mining rule's User Membership tab. Each user mail file is examined for any messages that meet the rule's archiving criteria.

A selective archiving rule is typically run daily or weekly, while a compliance archiving rule is run throughout the day.

A mining job runs automatically after:

- Creating and enabling the mining rule
- Scheduling and enabling the Profile Agent
- Configuring the Preprocessing Control document.
- Scheduling and enabling the preprocessing and archiving agents
- Scheduling the job in the rissminer program document

To run the rissminer program manually (for example, for testing purposes), see ["Running an archiving job manually"](#) on page 195.

Follow these steps to schedule the mining job:

1. In the HP EAs-D API main view, select and open the mining rule for editing.
2. Click **Schedule Job** in the upper left corner of the mining rules document.



The rissminer program document appears.

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

Basics		Schedule	
Program name:	rissminer	Enabled/disabled:	Enabled
Command line:	-kSelective	Run at times:	04:00 AM each day
Server to run on:	Team Server 2/HP EAs	Repeat interval of:	0 minutes
Comments:	HP RIM for Domino / Selective Archiving - default profile: Selective	Days of week:	Sun, Mon, Tue, Wed, Thu, Fri, Sat

Field	Description
Basics	
Program name	Leave the default value: rissminer
Command line	<p>The -k command line switch and the name of the mining profile are automatically picked up in the command.</p> <ul style="list-style-type: none"> If multiple instances of rissminer are scheduled on a single HP Gateway server, we recommend that you add an -n switch to the command to prevent processing errors. For example: -kSelective -n If your organization has a single HP Gateway server, you can add an -l switch to allow rissminer activity to be recorded in a user's Mail Detail record. For example: -kSelective -l <p>To prevent replication conflicts, this switch must not be used if an organization has multiple HP Gateway servers.</p> <p>Note: When you add the -l switch, be sure to enable the agent that purges the activity log. See "Purge Stats Selective Archive Log agent" on page 189.</p>
Server to run on	The default is the current HP Gateway server. If you need to change the Gateway server, click the arrow and select another server.
Comments	Leave the default value.
Schedule	
Enabled/disabled	Click the arrow and select Enabled to enable the program document.
Run at times	<p>Enter a time period to run the program.</p> <p>The time period and repeat interval depend on the type of archive job you are running.</p> <ul style="list-style-type: none"> 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 compliance archiving, 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).

Field	Description
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 mail files and the size of the messages. 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 compliance archiving, be sure to select each day of the week. Click OK when you are finished.

- (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.

- Click **Save & Close** to save the program document.

Additional program documents

A rissminer program document must be created for each mining rule. Configure the program document on each server on which a mining rule is enabled.

- In the Domino Administrator client, open the server.
- Click the **Configuration** tab, expand **Server** and open the server document.
- Select **Create > Server > Program**.
- Complete the program document fields according to steps 3–5 in [Scheduling the archiving job](#) above.

Running an archiving job manually

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

1. Run the rissminer mining program:

```
load rissminer -k<profile>
```

(where <profile> is the name of the mining rule profile)

For example: `load rissminer -kSelective` for a selective archiving rule.

Ensure there is no space between the switch (-k) and the profile name (such as Selective).

Rissminer examines the mining rule and assigned Mail Detail records, searches for messages to archive, and creates a reference document for each message that meets the rule's criteria.

 **NOTE:**

- If you are running multiple instances of rissminer on a single HP Gateway server, we recommend that you add an -n switch to the command to prevent processing errors. For example:

```
load rissminer -kSelective -n
```

- If your organization has a single HP Gateway server, you can add an -l switch to allow rissminer activity to be logged in a user's Mail Detail record. For example:

```
load rissminer kSelective -l
```

When you add the -l switch, be sure to enable the agent that purges the log entries. See [“Purge Stats Selective Archive Log agent”](#) on page 189.

To prevent replication conflicts, the -l switch should not be used if your organization has multiple HP Gateway servers.

2. Open and review the reference database.

For example, `hp_riss_minerreferenc.nsf` for selective archiving.

Inspect the reference documents created by rissminer.

- Each reference will have an assigned status: Pending, Sent, Preprocess, or Error.
- Messages that are not signed or encrypted should be in the Pending state.
- Signed and encrypted messages should be in the Preprocess state.

See [“Viewing reference documents”](#) on page 198 for information on reference documents and [“Preprocessing messages”](#) on page 175 for information on preprocessing.

3. Run the Archive agent:

```
tell amgr run "hprim\hp_riss_<refname>referenc.nsf" 'archive'
```

The filename should be changed to reflect the reference database that is used. For example:

```
tell amgr run "hprim\hp_riss_minerreferenc.nsf" 'archive' for selective archiving.
```

In running this agent, and all EAs Domino agents, ensure that the file name is always enclosed in double quotation marks (" ") and the agent name is always enclosed in single quotation marks (' ').

The Archive agent uses the reference documents to find the source mail file and message, prepare the message for archiving, and send the message to the IAP.

4. Open and review the reference database.

For all messages that are not signed or encrypted, the reference document status should be Sent.

5. Run the Tombstone agent.

Change the filename to reflect the reference database that is used. For example: `tell amgr run "hprim\hp_riss_minerreferenc.nsf" 'tombstone'` for selective archiving.

When the agent is run, the mined messages in the user mail files are tombstoned. Messages in a journal or Bulk Upload database are removed.

6. Open and review the reference database.

Reference documents that were in the Sent state should be removed.

7. For signed, encrypted, or "clean envelope" messages:

a. Run the Encapsulate agent in the preprocessing database:

```
tell amgr run "hprim\hp_preproc_<archive-type>.nsf" 'encapsulate'
```

The filename should be changed to reflect the preprocessing database that is used. For example: `tell amgr run "hprim\hp_preproc_miner.nsf" 'encapsulate'` for selective archiving.

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

- For signed messages, ATT file attachments, and non Memo Reply items such as 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.

After encapsulation is complete, the document's status in the reference database is changed to Pending.

b. Run the Archive agent.

After the agent is run, the status of the documents in the reference database should be Sent.

Encapsulated messages are 84 KB while they are routed to the IAP. That size is reduced to 8 KB when the messages are stored on the IAP.

c. Run the Tombstone agent.

The archived messages in user mail files will be tombstoned. Messages in a journal or Bulk Upload database will be removed.

d. Open and review the reference database.

Reference documents that were in the Sent state should now be removed.

Viewing reference documents

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

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

The following references are shown by server.

▼ Pyroraptor/Org1			16
▼ mail t1user			14
2E5AAE447F8B53C185257615005A7672	PENDING	RISSMINER 2.1	
3135C6F0EE8E4814852576150071933A	PENDING	RISSMINER 2.1	
3F49B252583EB6EC852576750048DCFB	PENDING	RISSMINER 2.1	
4F0AB37775AB80A1852576170073688A	PENDING	RISSMINER 2.1	
562341E6304309DB8525758D0065FC2C	SENT	RISSMINER 2.1	
5E53D986B17236A685257624006248A8	SENT	RISSMINER 2.1	
6EF521B3D8A83DE18525759D0065EA59	SENT	RISSMINER 2.1	
7F7D5DDDD5E1C42885257657007779B7	SENT	RISSMINER 2.1	
959AA5826D66FB138525767500490A0B	SENT	RISSMINER 2.1	
A63818045C7FE98585257617007321FD	PREPROCESS	RISSMINER 2.1	
B78781A43D59696A852576580049E78E	SENT	RISSMINER 2.1	
E3CECDB89CB26988C85257615005D468A	PREPROCESS	RISSMINER 2.1	
EEAD9CF20A592A6E85257615005A69EE	PREPROCESS	RISSMINER 2.1	
F98BD9ED1DBAA8A78525761500707B18	PREPROCESS	RISSMINER 2.1	
▼ mail t2user			2
3F49B252583EB6EC852576750048DCFB	SENT	RISSMINER 2.1	
959AA5826D66FB138525767500490A0B	SENT	RISSMINER 2.1	
			16

These references are shown by state.

▼ PENDING	4
▼ Pyroraptor/Org1 !! mail tuser	4
2E5AAE447FB853C185257615005A7672	
3135C6F0EE8E4814852576150071933A	
3F498252583EB6EC852576750048DCFB	
4F0A837775AB80A1852576170073688A	
▼ PREPROCESS	4
▼ Pyroraptor/Org1 !! mail tuser	4
A63819045C7FE96585257617007321FD	
E3CECD89CB26988C85257615005D468A	
EEAD9CF20A592A6E85257615005A69EE	
F98BD9ED1DBAA8A78525761500707B18	
▼ sent	8
▼ Pyroraptor/Org1 !! mail tuser	6
7F7D5DDDD5E1C42B852576570077987	
B78781A43D59696A852576580049E78E	

Messages can be in one of the following states:

- **Sent:** A message has been sent to the IAP from the HP Gateway server.
When a message is in Sent status, the software has not yet confirmed the IAP has stored the message. That occurs after the Tombstone agent runs and verifies a message has been stored successfully. The associated reference document is then removed from the reference database. The message itself is either tombstoned or removed from the journal or mail file, depending on the action specified in the mining rule's tombstone settings.
(In some cases, references can also be removed from the database after the Reference Cleanup agent is run. See [“Message reprocessing rules”](#) on page 318 for more information.)
- **Pending:** A message has not been sent to the IAP. It is still located in the journal or mail file.
- **Preprocess:** An encapsulated message is being processed.
- **Error:** An error occurred and the message was not processed.

3. Double-click the reference document for more information.

Mail Reference	
Status: Sent	Session Server: Pyroraptor/Org1
Server: pyroraptor/org1	File Path: mailt1user
Replica ID: 85257674007E761F	UNID: 85257674007E761F85257624006248A8
Original Server: pyroraptor/org1	
Original Replica ID: 8525758D00642F7D	Original UNID: 5E53D986B17236A685257624006248A8
Message Source:	Message Flags:
Preproc Reason: <input type="checkbox"/> Signed Message <input type="checkbox"/> Encrypted Message <input type="checkbox"/> System Generated Forms <input type="checkbox"/> Forced (rissminer -e) <input type="checkbox"/> Stored Form <input checked="" type="checkbox"/> Unsupported Form <input type="checkbox"/> Bad or ATT Attachment <input type="checkbox"/> Layout Region in Body	
Preproc Actions:	Preproc Done: encapsulate

4.5 Configuring compliance (journal) archiving

- [Configuring the mail server for compliance archiving](#), page 201
- [Advanced Filtering installation](#), page 202
- [Lotus Domino native journaling](#), page 211
- [Configuring Advanced Filtering and Domino native journaling on the same server](#), page 217
- [Archiving journaled messages](#), page 217

Configuring the mail server for compliance archiving

HP EAs Domino archives messages that are journaled using:

- Advanced Filtering (EAs Domino journaling)
- Domino native journaling

In both types of journaling, messages are captured and sent to the mail recipient and to a mail-in journal database on the mail server or journal server. The mail-in database is then mined remotely by the HP Gateway server. Pointers to the mined messages are placed in the HP EAs-D Journal Reference database on the Gateway server and acted on by agents in the journal reference database and the journal preprocessing database, HP EAs-D PreProcess.

To create the mail-in database, use the HP EAs-D Mail Journal template or the standard journal template that ships with Domino. Do not use another, customized, journal template. Customized templates can cause the mining program to report an incorrect number of message processes, along with other potential problems.

The HP EAs-D Mail Journal template (`hp_mailjrn.ntf`) is located in the `Templates` folder on the EAs Domino installation media. 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.

HP EAs Domino only supports the mail-in method of journaling.

 **NOTE:**

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

Advanced Filtering installation

If EAs Domino Advanced Filtering is used to journal messages, follow the steps below.

1. Install Advanced Filtering on the mail servers to be journaled.
See “[Installing the Advanced Filtering module](#)” on page 202.
2. Create a journal database on each mail server to be journaled and set the journal ACL.
See “[Creating the mail-in journal database](#)” on page 204.
3. Set the ACL for the HP EAs-D API and HP EAs-D Users databases installed on the mail servers.
See “[Setting the permissions for other Advanced Filtering databases](#)” on page 205.
4. Create the Mail-In Database document.
See “[Creating the Mail-In Database document](#)” on page 205.
5. Configure the Advanced Filtering journaling rules.
See “[Creating journaling rules \(Advanced Filtering\)](#)” on page 206.
6. Restart the Domino server.

Installing the Advanced Filtering module

When messages are journaled using the Advanced Filtering method, several files must be installed on the Lotus Domino mail server using the EAs Domino installer. If more than one mail server is being journaled, use the installer to deploy the initial installation.

Before installing the Advanced Filtering module, ensure that all non-Lotus Notes applications are closed.

Advanced Filtering must be installed from a Windows client.

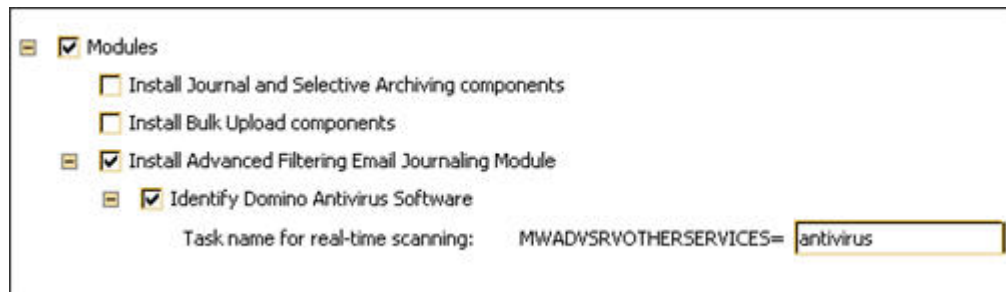
1. Open the Domino Administrator client using a Notes ID that can be used to create databases and run agents.
2. Open Windows Explorer, and navigate to the folder where the EAs Domino installation files were extracted. Locate the `server` directory and double-click the `Setup.exe` file.
3. Click **Next** at the 1. Welcome window.
4. Click **Next** at the 2. Load installation window.
The 3. Master window appears.

5. In the 3. Master window, perform the following actions:
 - a. In the Server name drop-down list, select the mail server to be journaled.
 - b. Select the **Modules** check box, and then select **Install Advanced Filtering Email Journaling Module**.
 - c. To allow antivirus scanning to be executed before the journaling capture:
 1. Select the **Identify Domino Antivirus Software** check box.
 2. Enter a name for the antivirus scanning task. For example:
antivirus

 **NOTE:**

If the organization uses Norton antivirus software (for example, `rtvscan.exe` from the Symantec Internet Security Suite, manually add another entry to `notes.ini` after the installation:

```
MWADVSRVOTHERSERVICESAO=[anti-virus-real-time-task-name]
```



- d. Click **Next**.
6. If a password dialog box appears, enter the password for the Notes ID.
7. In the 4. Deployment window, click **Next**.
8. In the 5. Remove Base window, select whether to delete the temporary installation base (`hp_riss_install.nsf`) on the server, and then click **Next**.
 - If you want to save the installation base, click **No**.
Selecting No leaves the install base so you can review status messages recorded during the installation.
 - If you do not want to save the installation base, click **Yes**.
9. In the 6. Save Installation window, select the **Save this installation** check box if you want to save the installation for future deployment. Browse for a location in which to save the installation.
The installation configuration is saved as an XML file.
10. In the 7. Readme window:
 - Verify that the View readme check box at the top of the window is selected.
 - Verify that the installation information is correct.
Make sure that Install on master server has been set to **Yes**.
11. Click **Install**.
An installation progress bar is displayed.
After the software is successfully installed, the Readme appears on screen.

12. Click **Finish** to complete the installation.
13. If more than one mail server is being journaled, use the installer to deploy the initial installation. Ensure that the HP EAs-D API and HP EAs-D Users databases are replicated.

The journaling rules filter and listening agent are installed in the Domino data directory on the mail server. See “[HP EAs Domino binaries](#)” on page 74.

For changes that are made to `notes.ini` on the mail server, see “[HP EAs Domino notes.ini entries](#)” on page 73.

Unix-based systems

If the software is installed on a UNIX-based operating system, set the following privileges for the Advanced Filtering rules filter and listening agent:

- `mwadvt` : `+x`
- `libadvsvr.a` or `libadvsvr.so` : `+r`

Creating the mail-in journal database

1. Create a journal database for each mail server that is being journaled.

Use the HP EAs-D Mail Journal template (`hp_mailjrn.ntf`) located in the Templates directory in the EAs Domino installation media.

Follow the installation instructions in “[Creating new EAs Domino applications](#)” on page 353. The journal's location is determined by the Domino administrator. It should not be placed in the `hprim` folder with the EAs Domino files.

2. Set the journal's ACL.

Because the contents of the journal are extremely sensitive and encryption cannot be used to protect journals in EAs Domino, the ACL is the primary protection mechanism for the journal. Organizations should designate a small number of users who have access to the journal and set the ACL accordingly. Journals can be placed on special servers (not HP Gateways) that are accessible to a limited number of administrators.

Avoid using groups (other than `LocalDomainServers`) in the journal ACL. Groups should be used only if the organization limits the right to edit groups in the Domino Directory, and all users with this right are trusted with access to the journals.

We recommend the following access for journals:

- List LocalDomainServers, with a **Server group** user type.
Servers should have **Depositor** access with the Admin role and rights to replicate or copy documents.
- List individual users, with a **Person** user type, instead of LocalDomainAdmins or an equivalent group.
Users should have **Manager** access with the Admin role and rights to replicate or copy documents.
- List each HP Gateway server by name, with a user type of **Server**. Do **not** use OtherDomainServers.
The Gateway servers should have **Editor** access with the Admin role and rights to replicate or copy documents.
- List the ID that signed the agents, by name. The user type should be **Person** if the agents were signed with user ID.
The ID should have **Editor** access with the Admin role and rights to delete and replicate or copy documents.
Do **not** add the HP Gateways and the agent signing ID into one group and make it a Mixed group.
- Anonymous: **No access**.
- Default: **No access**.

 **NOTE:**

These recommendations apply to the ACL on all journal replicas.

Setting the permissions for other Advanced Filtering databases

Set the access for the HP EAs-D API and HP EAs-D Users databases installed on the mail server. Use the settings in “[ACL for EAs Domino databases on customer servers](#)” on page 70.

 **NOTE:**

The instance of the HP EAs-D API database in the mail domain is separate from the instance in the HP Gateway domain. The mail domain instance should be replicated to any other Domino servers on which EAs Domino software is installed.

Creating the Mail-In Database document

The Domino administrator is responsible for creating the Mail-In Database document for each journal.

1. Open the Domino Administrator client using a Notes ID that can be used to create databases and documents.
2. Open the mail server.
3. In the People & Groups tab, select **Mail-In Databases and Resources**.
4. Click **Add Mail-In Database**.

5. In the Basics tab, ensure that **Encrypt incoming mail** is set to **No**.

❗ **IMPORTANT:**

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.

6. In the Administration tab, ensure that **Allow foreign directory synchronization** is set to **Yes**.
7. Complete the remaining fields in the Mail-In Database document.
8. Click **Save & Close**.

Creating journaling rules (Advanced Filtering)

The journaling rules determine which messages are copied to the journal mail-in database. The method for creating EAs Domino journaling rules is described in this section.

❗ **IMPORTANT:**

If you are deleting or disabling an existing rule to replace it with a new journaling rule, or if you are editing a journaling rule, stop the Advanced Filtering task (mwadvf) before continuing. See the instructions in [“Editing journal rules \(Advanced Filtering\)”](#) on page 210.

A default journaling rule has been created in the HP EAs-D API database. Edit the rule by following these steps:

1. In the Domino Administrator client, open the HP EAs-D API database on the mail server.
2. In the main view, double-click the default document under **Journaling Rules**.
The Journaling Rules document appears.
3. Configure the rule by completing the settings in each tab:
 - [“Traffic Definition tab”](#) on page 207
 - [“Sender/Receiver Exceptions tab”](#) on page 208
 - [“Content Exceptions tab”](#) on page 208
 - [“Journal Database tab”](#) on page 209
 - [“Rules Status tab”](#) on page 209
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, you can prioritize execution of the rules:
 - a. In the EAs-D API 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 messages.

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

Journaling Rules:

Comments:
 Top Managers - incoming traffic

Traffic Definition | Sender/Receiver Exceptions | Content Exceptions | Journal Database | Rules Status

[Traffic Definition]

From : * _ _ _ _ _ User Group Meta Meta Grp (?)

To : Acme Mgmt Team Users _ _ _ _ _ User Group Meta Meta Grp

Field	Description
From	<p>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.</p> <ol style="list-style-type: none"> 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. <p>The Meta and Meta group categories use wildcards. For more information, see "Defining wildcard patterns" on page 167.</p>
To	<p>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.</p> <ol style="list-style-type: none"> 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. <p>The Meta and Meta group categories use wildcards. For more information, see "Defining wildcard patterns" on page 167.</p>

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.

Traffic Definition | **Sender/Receiver Exceptions** | Content Exceptions | Journal Database | Rules Status

[Sender/Receiver Exceptions]

Except From : User Group Meta Meta Grp

Except To : User Group Meta Meta Grp

Field	Description
Except From	<p>Messages from this user or group should not be journaled.</p> <ol style="list-style-type: none"> 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. <p>The Meta and Meta group categories use wildcards. For more information, see "Defining wildcard patterns" on page 167.</p>
Except To	<p>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 that was entered in the Server Definition document when the software was installed. For example, if the IAP email address is AcmelAP01Admin@iap01.acme.com, the value in this field would be AcmelAP01Admin (everything before @). The IAP email address is listed in the Session Settings of the Server Definition document.</p> <p>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.</p>

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_maihtome)
```

- 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.

Traffic Definition | Sender/Receiver Exceptions | Content Exceptions | Journal Database | Rules Status

[Content Exceptions]

▶ Formula must returns TRUE or FALSE - no formula = TRUE

Wizard . Check Formula

@IsUnavailable(x_pt_maitome)

Journal Database tab

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

Traffic Definition | Sender/Receiver Exceptions | Content Exceptions | Journal Database | Rules Status

[Journal Database]

▶ Email will be routed to 'Mail-in'. BCC and From fields will be mapped to JRN_...

Journal this email in mail-in : hprimhp_riss_journal.nsf

Field	Description
Journal this email in mail-in	Click the arrow and select the name of the journal mail-in database that was created. Note: Ensure that the Mail-In Database document specifies the settings listed in "Creating the Mail-In Database document" on page 205.

Rules Status tab

Traffic Definition | Sender/Receiver Exceptions | Content Exceptions | Journal Database | Rules Status

[Rules Status]

Expiration Date : Start Date : 01/01/2010

>>> This rule terminates => do not check other rules : . <<<

Server(s) : dnmomail/zkodom Active on servers (* for all)

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 Managers – Incoming.
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.

Field	Description
This rule terminates ...	All rules that match an email are applied in sequence unless this check box is selected. When the check box is selected, no other journaling rules are applied to an email.
Sever(s)	Enter the mail server(s) on which this journaling rule is active.

Editing journal rules (Advanced Filtering)

Before editing journaling rules

❗ IMPORTANT:

Stop the mwadvt task on the Domino server before editing journaling rules.

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.

Making changes to a journal rule

If a journaling rule requires modification, follow these steps:

1. Stop the mwadvt task by using the Domino server console 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.

After the task is stopped, all incoming and outbound messages are held in the server's mail.box until the task is reloaded.

2. Make the necessary changes to the rule:
 - a. Open the HP EAs-D API database, and double-click the Journaling Rules document in the main view.
 - b. Double-click the relevant settings and make the changes.
 - c. Click **File > Save** to save the changes.
 - d. Close the document and the EAs-D API database.
3. From the server console, issue the command:

```
load updall hprim\hp_rissapi.nsf
```
4. In a multi-server environment, wait for HP EAs-D API to replicate to all relevant Domino servers.
5. Restart the mwadvt task by using the command `load mwadvt` on all relevant servers.

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.

Lotus Domino native journaling

If Domino native journaling is used to journal messages, follow the steps below. Only the mail-in style of Domino native journaling is supported by HP EAs Domino archiving.

NOTE:

The Domino administrator is responsible for creating the mail-in journal database and Mail-In Database document, configuring the journaling rules, and enabling journaling in the Configuration Settings document.

1. Create the mail-in journal database.
See [“Creating the mail-in journal database”](#) on page 211.
2. Create the Mail-In Database document.
See [“Creating the Mail-In Database document”](#) on page 205.
3. For each Domino server that has the SMTP Listener enabled, set the Inbound Message Options.
See [“Configuring the Advanced Inbound Message Options”](#) on page 213.
4. Configure the journaling rules and enable journaling.
See [“Enabling journaling”](#) on page 214.
5. Restart the Domino server.
6. On the HP Gateway server, create and configure the HP EAs-D Tools database to remove Mail-To-Me messages from the journal.
See [“Removing Mail-To-Me messages from the journal”](#) on page 215.

Creating the mail-in journal database

1. Create the journal database using the standard journal template that ships with Domino or the HP EAs-D Mail Journal template (`hp_mailjrn.ntf`) located in the Templates directory on the EAs Domino installation media.

If using the EAs Domino journal template, follow the instructions in [“Creating new EAs Domino applications”](#) on page 353. The journal should not be placed in the `hprim` folder.

2. Set the journal's ACL.

Because the contents of the journal are extremely sensitive and encryption cannot be used to protect journals in EAs Domino, the ACL is the primary protection mechanism for the journal. Organizations should designate a small number of users who have access to the journal and set the ACL accordingly. Journals can be placed on special servers (not HP Gateways) that are accessible to a limited number of administrators.

Avoid using groups (other than LocalDomainServers) in the journal ACL. Groups should be used only if the organization limits the right to edit groups in the Domino Directory, and all users with this right are trusted with access to the journals.

We recommend the following access for journals:

- List LocalDomainServers, with a **Server group** user type.
Servers should have **Depositor** access with the Admin role and rights to replicate or copy documents.
- List individual users, with a **Person** user type, instead of LocalDomainAdmins or an equivalent group.
Users should have **Manager** access with the Admin role and rights to replicate or copy documents.
- List each HP Gateway server by name, with a user type of **Server**. Do **not** use OtherDomainServers.
The Gateway servers should have **Editor** access with the Admin role and rights to replicate or copy documents.
- List the ID that signed the agents, by name. The user type should be **Person**, if the agents were signed with user ID.
The ID should have **Editor** access with the Admin role and rights to delete and replicate or copy documents.
Do **not** add the HP Gateways and the agent signing ID into one group and make it a Mixed group.
- Anonymous: **No access**.
- Default: **No access**.

NOTE:

These recommendations apply to the ACL on all journal replicas.

- ## 3. After creating the mail-in journal database, create the Mail-In Database document.
- See [“Creating the Mail-In Database document”](#) on page 205.

Configuring the Advanced Inbound Message Options

Each Domino server that has the SMTP Listener enabled must have the Advanced Inbound Message Options set in the server's Configuration Settings document.

1. In the Domino Administrator client, switch to a Notes ID that can be used to create databases and documents.
2. Click the **Configuration** tab, expand **Messaging**, and click **Configurations**.
3. Select the Configuration Settings document for the server, and then click **Edit Configuration**.
4. Click the **MIME** tab, then click **Advanced > Advanced Inbound Message Options**.
5. Select **Yes** in the field labeled "If each recipient's address does not appear in any address header, then add their address to the BCC list."

This ensures that every address found in SMTP RCPT TO will be checked. Any address that is not in one of the RFC822 address headers will be added to the BCC.

Configuration Settings

Basics | Security | Client Upgrade | Router/SMTP | MIME | NOTES.INI Settings

NOTE: All International MIME settings will only have an effect if you enable 'International MIME'.

Basics | Conversion Options | Settings by Character Set Groups | Advanced

Advanced Inbound Message Options | Advanced Outbound Message Options

Advanced Inbound Message Options

Resent headers take precedence over original headers:	Disabled
Remove group names from headers:	No
If each recipient's address does not appear in any address header, then add their address to the BCC list:	Yes
For non-MIME messages or MIME messages with an unknown character set, 8-bit character set is assumed to be:	Default
Character set name aliases maps to:	

6. Perform one of the following actions:
 - If the server has mail files to be journaled, leave the Configuration Settings document open and continue to the next section.
 - If the server will not be journaled, click **Save & Close**, and then restart the server.
7. Repeat these steps for each Domino server with the SMTP Listener enabled.

Enabling journaling

Follow these steps to enable native journaling on a Domino server:

1. In the Configuration Settings document for the server, select **Router/SMTP > Advanced > Journaling**.
2. Configure the following settings:
 - Journaling: **Enabled**
 - Method: **Send to Mail-in Database**

EAs Domino does not support the Copy to local database option because it requires encryption. Standard journaled messages cannot be encrypted when they are sent to the IAP. An extra layer of encryption cannot be added to previously-encrypted messages when they are sent to the IAP.
 - Mail Destination: Click the arrow and select the mail-in database in the Domino Directory.

Configuration Settings

Basics | Security | Client Upgrade | Router/SMTP | MIME | NOTES.INI Settings | Domino Web Access | IMAP

Basics | Restrictions and Controls... | Message Disclaimers | Message Tracking | Message Recall | Advanced...

Journaling | Commands and Extensions | Controls

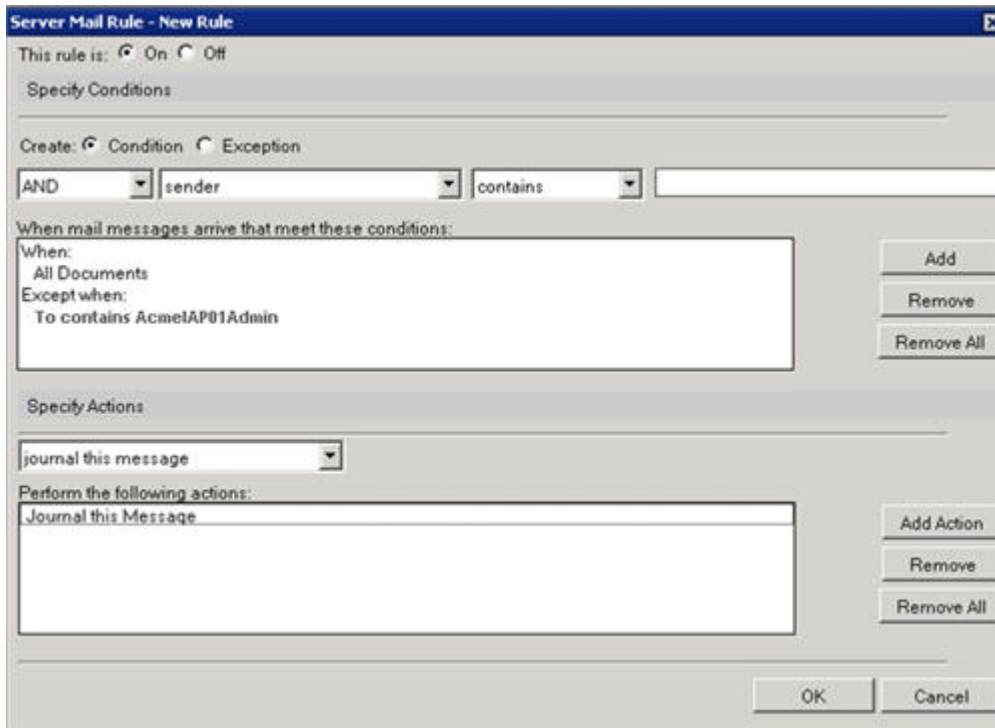
Basics

Journaling:	Enabled
Field encryption exclusion list:	Form; From; Principal; PostedDate
Method:	Send to mail-in database
Mail Destination:	journaldb
Journal Recipients:	Disable

***Reminder: A journaling mail rule is needed to properly enable message journaling.

3. Select **Router/SMTP > Restrictions and Controls > Rules**.

4. Click **New Rule** and create a journaling rule to ensure that messages sent to the IAP are not journaled again.



- a. Specify the conditions for the rule:
 - Create: **Condition**
 - **AND Sender contains**
 - When: **All Documents**
 - Except when: **To contains <iapaddress>**
Use the address listed in the IAP email address field of the Server Definition document's [Server Settings](#) tab. Enter the value as everything before @ in the IAP email address field. For example, if the IAP email address is AcmeIAP01Admin@iap01.acme.com, the value in this field would be AcmeIAP01Admin (everything before @).
 - b. Click **Add**.
 - c. Specify the action: **Journal this message**.
 - d. Ensure the rule is turned **On**, and then click **OK**.
5. If necessary, create other journaling rules to define which messages to capture or exclude.
Follow the instructions in the Domino documentation to create the journaling rules.
 6. Click **Save & Close**.
 7. Restart the server.

Removing Mail-To-Me messages from the journal

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 Domino mining agents skip them and leave them in the journal. HP EAs-D Tools provides an automated process for removing Mail-to-Me

messages from the journal. (In EAs Domino Advanced Filtering, Mail-To-Me messages are handled in the journaling rules content exceptions.)

Follow these steps to create and configure the HP EAs-D Tools database on the HP Gateway server:

1. In the Notes client:
 - a. Create the HP EAs-D Tools database using the instructions in [“Creating new EAs Domino applications”](#) on page 353.
Use `hp_tools.ntf` for the template and `hp_tools.nsf` for the filename. Place the file in the `hprim` folder in the Domino data directory.
 - b. Set the ACL for the database:
Click **Add**, add the following users if they are not already listed, and set user access as shown:
 - LocalDomainAdmins (or substitute): **Manager**
Must have rights to delete and replicate or copy documents.
 - LocalDomainServers: **Manager**
Must have rights to delete and replicate or copy documents.
 - Notes ID that signed the EAs Domino databases and agents during installation.
If the Notes ID is part of LocalDomainAdmins (or substitute), do not add it as a separate user.
If the Notes ID is not part of LocalDomainAdmins and you do not want to include it in the group, add the ID and give it **Manager** access. The user must also have rights to delete and replicate or copy documents.
 - Default: **Manager**
 - c. Ensure that the database has been signed.
2. In the Domino Administrator client:
 - a. Open the HP Gateway server and then open HP EAs-D Tools.
 - b. Select **Mail to Me Administration** in the left menu.
 - c. Click the **Mail-to-Me Admin** button, and select **New Admin Doc** to create a new administration document.
 - d. Complete the document:
 - Domino Server: Enter or select the mail server to monitor.
 - Journal Database: Enter the name of the mail-in journal database on the mail server.
 - Cleanup Action: Select **Delete**.
 - Scheduled Execution: Select **Enable**.
3. In the Domino Designer client, schedule and enable the Email Miner MTM Cleanup agent in HP EAs-D Tools.
The default schedule is to run the agent once a day at 1:00 a.m.

Configuring Advanced Filtering and Domino native journaling on the same server

Running both EAs Domino journaling and Domino native journaling on the same Domino 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.

- Advanced Filtering rules: Add an exception to prevent messages that are routed to the native journaling database from being journaled by EAs Domino Advanced Filtering. Add the entry in the Except To field in the [Sender/Receiver Exceptions tab](#).

 **NOTE:**

The Except To field must also contain an entry to exclude messages sent to the IAP. To support multiple entries in this field, create a group in the Domino Directory with the IAP, the native journal, and any other exceptions as members. In the Except To field, click the arrow and select the new group.

- Native Domino journaling rules: Add an exception to prevent messages addressed to the EAs Domino mail-in journal database from being journaled.

Archiving journaled messages

On the HP Gateway server, perform the following steps so the messages in the mail-in journal can be archived to the IAP.

These steps must be followed whether messages are journaled using Advanced Filtering or Domino native journaling.

1. Configure the journal mining rule.
See [“Configuring the journal mining rule”](#) on page 218.
2. Add the journal mail-in database as a user in the HP EAs-D Users database.
See [“Adding a journal user”](#) on page 220.
3. Configure the Preprocessing Control document.
See [“Editing the Preprocessing Control document”](#) on page 221.
4. Schedule and enable the preprocessing and archiving agents.
See [“Enabling the preprocessing and archiving agents”](#) on page 221.
5. Schedule the compliance archiving job in the rissminer program document.
See [“Scheduling the compliance archiving job”](#) on page 221.

Additionally, ensure that the following agents have been scheduled and enabled:

- Get Held Messages agent.
See “[Configuring Get Held Messages](#)” on page 190.
- Purge_Document agent in the HP EAs-D Log, HP EAs-D Alert, and HP EAs-D Stats databases.
This agent removes old documents from these databases.

Configuring the journal mining rule

1. Open the HP EAs-D API database on the HP Gateway server.
2. In the main view, under Mining Rules, double-click **Mining Rule: Journaling**.
3. Complete the following fields at the top of the mining rule:

Field	Description
Policy Status	Select Enable when you are ready to activate the rule and begin mining the mail-in journal database.
Profile	The default name for the mining rule is Journaling. If you rename the profile, the profile name cannot include spaces or dashes.

4. Set the following options in the mining rule:

Tab	Description
Time Conditions	Ensure that: <ul style="list-style-type: none">• Memo, Reply type of document is set to Creation Date.• Archiving Date for not Foldered doc... is set to 0.• Archiving Date for Foldered doc.. is set to 0.
Folders Settings	Do not edit.
Exceptions Settings	Do not edit.

Tab	Description
User Membership	<p>Edit the fields on the tab as follows:</p> <ul style="list-style-type: none"> • Active for Profile Agent: Ensure that No is always selected. • Include Users on selected Mail server(s): Set to All servers or Only Selected servers. • Active for database(s): Ensure that only Mail in Db is selected. • Use Alternate Server: If the mining configuration uses replicated journaling, select Yes. In the Alternate Server field that appears, select the server with the replicated journal(s). • In Person entry, select the mail-in journal database(s) to be mined. Note: If <code>rim_journaling_*</code> appears in the String pattern matching field, it can be deleted. This value is simply an example. <p>For more information on the settings, see “User Membership tab” on page 165.</p>
Reference Database	<p>Edit the following settings:</p> <ul style="list-style-type: none"> • Select Extended. • The default Reference Database path and name is hprim/hp_riss_journalreferenc.nsf. • Leave the Reference Database Server name field blank. • In the Preserve References for auditing field, ensure No is selected. Auditing is not enabled in EAs Domino 2.1.x. • In Original field(s) to be added to the Reference record, do not add entries. This field is used for auditing, which is not enabled.
Tombstone Settings	<p>Verify that Delete message is selected in Actions.</p>
Session Settings	<p>Edit the following settings:</p> <ul style="list-style-type: none"> • Allow Remote Mining of databases: Ensure Yes is selected. • Archive strategy: Ensure None is selected. (Messages do not need to be sorted before they are archived.) • Do not archive document older than: Leave this field blank.
User Notification	<p>Do not edit.</p>
Administration Alert	<p>Configure these settings if you want an alert to be sent to the Domino administrator when mining does not start. For more information, see “Administration Alert tab” on page 173.</p>

5. Save the mining rule.

Adding a journal user

Add the mail-in journal database as an EAs Domino user by manually creating a Mail Detail record in the HP EAs-D Users database.

If the journal is replicated, manually create a Mail Detail record for each replica.

1. In the Domino Administrator client, open the HP EAs-D Users database in the `hprim` folder.
2. In the **Create** menu, select **Mail Details > Database Details**.

A new Mail Detail record appears.

3. On the **Database Details** tab, set the following values:

The screenshot shows the 'Database Details' tab in the Domino Administrator client. The form contains the following fields and values:

[Database Details]	
First Name	
Middle Initial	
Last Name	
Full Name	HP EAsD Journal
Home Server	Mailserver 2/acme
Database Filepath	hp_mailrn.nsf
Database used for Journaling	<input type="radio"/> No <input checked="" type="radio"/> Yes
Mining Rule(s) Assigned	Journaling
Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <input type="radio"/> No Profile Assigned

Field	Description
FullName	Enter the mail-in journal database name; for example HP EAsD Journal.
Home Server	Click the arrow and select the server on which the database is located.
Database Filepath	Enter the file path (from the Domino data directory) and the file name of the mail-in journal database.
Mail File used for Journaling	Always click Yes . Note: This setting is essential for journal mining to occur.
Mining Rule(s) Assigned	Enter the name of the mining rule for journaling.
Module Status	Click Enable .

4. Save the record.

Editing the Preprocessing Control document

In the HP EAs-D API main view, open the Preprocessing Control document for journaling and edit the settings according to the steps in “[Configuring the Preprocessing Control document](#)” on page 177.

Enabling the preprocessing and archiving agents

Schedule and enable the preprocessing and archiving agents. For the steps to follow, see “[Scheduling and enabling the preprocessing agents](#)” on page 182 and “[Scheduling and enabling the archiving agents](#)” on page 191.

For compliance archiving, the Encapsulate, Archive, and Tombstone agents should run frequently, all day. The times should be at least 20 minutes apart. The Reference Cleanup agent only needs to run once a day.

Scheduling the compliance archiving job

Schedule the archiving job using the instructions in “[Scheduling the archiving job](#)” on page 193.

For compliance archiving, run the program throughout the day:

- In the Run at time field, enter a time period of **12:00 AM–11:59 PM**.
- In the Repeat interval field, enter a brief repeat interval (not less than 10 minutes).

Program: rissminer

Basics | Administration

Basics	Schedule
Program name: rissminer	Enabled/disabled: Enabled
Command line: -kJournaling	Run at times: 12:00 AM - 11:59 PM each day
Server to run on: HPGateway1/hparchive	Repeat interval of: 20 minutes
Comments: HP RIM for Domino / Selective Archiving - default profile: Journaling	Days of week: Sun, Mon, Tue, Wed, Thu, Fri, Sat

Journalled messages are archived automatically after the mining rule is enabled and the agents are scheduled.

To run the rissminer program manually (for example, for testing purposes), see “[Running an archiving job manually](#)” on page 195.

4.6 Using Bulk Upload

Bulk Upload is a utility that identifies mail file ownership. Typically, the owners are no longer employed by the organization and their Person documents have been removed from the Domino Directory.

Bulk Upload scans inactive mail files, discovers a mail file's owner, and creates a Mail Detail record for each mail file in the HP EAs-D Bulk Upload database. The Bulk Upload database is replicated to the HP Gateway server, and the mail files are mined by the Gateway server.

- [Installing the Bulk Upload software](#), page 223
- [The Bulk Upload process](#), page 226
- [Editing the bulk upload mining rule](#), page 226
- [Editing the Preprocessing Control document](#), page 226
- [Enabling the agents](#), page 227
- [Scanning the databases](#), page 227
- [Reviewing the Mail Detail records](#), page 228
- [Replicating the Bulk Upload database](#), page 229
- [Archiving the mail files](#), page 229

Installing the Bulk Upload software

The files to run Bulk Upload are installed on a Lotus Domino application server in the mail domain. (The server should not be a production application server or a mail server.) The files to archive the mail files are installed on an HP Gateway server.

Installing the local Bulk Upload files

Before installing the Bulk Upload software, ensure that:

- The inactive mail databases have been copied to the server from local mail servers.
- The Router task is running on the server.
- All non-Lotus Notes applications are closed.

The EAs Domino installer must run on a Windows client.

ⓘ **IMPORTANT:**

If the Bulk Upload software is being installed on a 64-bit AIX server, the `script.xml` file located in `\server\resources\applications\hpRimServerInstall_2.1.2.x\data` must be replaced before the installer is run. Contact HP technical support for an updated `script.xml` file, which sets the execution privileges to run Bulk Upload.

Follow these steps to install the software:

1. Open the Domino Administrator client using a Notes ID that can create databases and agents.

2. Open Windows Explorer, and navigate to the folder where the EAs Domino installation files were extracted. Locate the `server` directory and double-click the `Setup.exe` file.
3. Click **Next** at the 1. Welcome window.
4. Click **Next** at the 2. Load installation window.
The 3. Master window appears.
5. In the 3. Master window, perform the following actions:
 - a. In the Server name drop-down list, select the application server in the mail domain.
 - b. Select the **Modules** check box, and then select **Install Bulk Upload Components**.
 - c. Under Choose an installation mode, select **Install HP EAs Domino on the master server**.
Verify that the correct operating system is shown for the application server.
 - d. Click **Next**.
6. If a password dialog box appears, enter the password for the ID.
7. In the 4. Deployment window, click **Next**.
8. In the 5. Remove Base window, select whether to delete the temporary installation base (`hp_riss_install.nsf`) on the server, and then click **Next**.
 - If you want to save the installation base, click **No**.
Selecting No leaves the install base so you can review status messages recorded during the installation.
 - If you do not want to save the installation base, click **Yes**.
9. In the 6. Save Installation window, select the **Save this installation** check box if you want to save the installation. Browse for a location in which to save the installation.
10. In the 7. Readme window:
 - Verify that the View readme check box at the top of the window is selected.
 - Verify that the installation information is correct.
Make sure that Install on master server has been set to **Yes**.
11. Click **Install**.
An installation progress bar is displayed.
After the software is successfully installed, the Readme appears on screen.
12. Click **Finish** to complete the installation.
13. Ensure that only one instance of the HP EAs-D API database (`hprim\hp_rissapi.nsf`) is running in the Domino mail domain.
14. Set the ACL for the relevant databases in the Domino data directory `hprim` folder using the instructions in the next section.
15. Restart the Domino server.

Setting the ACL for the local files

Set the access for the HP EAs-D Bulk Upload, HP EAs-D API, and HP EAs-D Log databases using the settings in [“ACL for EAs Domino databases on customer servers”](#) on page 70.

Installing the Bulk Upload files on the HP Gateway server

The files to archive the inactive users' mail files are already installed on the HP Gateway server.

The Bulk Upload process

Bulk Upload involves the following steps:

1. “Editing the bulk upload mining rule” on page 226.
2. “Editing the Preprocessing Control document” on page 226
3. “Enabling the agents” on page 227.
4. “Scanning the databases” on page 227.
5. “Reviewing the Mail Detail records” on page 228
6. “Replicating the Bulk Upload database” on page 229
7. “Archiving the mail files” on page 229.

Editing the Bulk Upload mining rule

The mining rule for Bulk Upload is similar to a mining rule created for active users.

A default Bulk Upload mining rule has been created in the HP EAs-D API database on the HP Gateway server.

To use the default rule:

1. In the Domino Administrator client, open the HP EAs-D API database on the HP Gateway server.
2. In the Mining Rules area of the EAs-D API main view, double-click **Mining Rule: Bulk**.
3. On the User Membership tab, configure the following settings:
 - Active for Profile Agent: Ensure that **No** is selected.
(The Profile Agent is only used to create or update records for active users who are listed in the Domino Directory.)
 - Include Users on selected Mail server(s): Click **Only Selected server(s)** and select the application server with the mail files to be mined.
4. Configure the Reference Database tab:
 - Reference document: Click **Extended**.
 - Reference Database Server name: Leave the field blank.
5. On the Session Settings tab:
 - Select **Yes** to allow remote mining of databases.
 - Ensure the Archive Strategy is set to **None**. In Bulk Upload, messages do not need to be sorted before they are archived.
6. Do not edit the settings on the remaining tabs.
7. Enable and save the mining rule.

Editing the Preprocessing Control document

A default Bulk Upload Preprocessing Control document has been created in the HP EAs-D API database on the HP Gateway server.

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 **Encapsulation Settings** tab, edit the path for the temporary work directory if necessary. For more information on the temporary work area, see “[Encapsulation Settings tab](#)” on page 179.
4. 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 on the HP Gateway server.

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

The Tombstone agent deletes the messages in the inactive mail files after they are successfully archived.

Scanning the mail files

Run the Bulk Upload executable to scan the inactive mail files and determine mail file ownership.

Bulk Upload is run from the server console on the application server. The Mail Detail records that are created are placed in the HP EAs-D Bulk Upload database on the server. These documents are similar to the Mail Detail records created for active users in the HP EAs-D Users database.

Bulk Upload determines the owner of a mail file using the process in [Discovering a mail file owner](#).

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 owners of mail files in the Terminated directory of the Domino data directory, create Mail Detail records in the default Bulk Upload database, and associate the records with the Bulk Upload mining profile, enter:

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

To locate the owner of the smithj mail file in the Mail directory of the Domino data directory, create a Mail Detail record in the Bulk Upload database, and associate the record with the Bulk Upload mining profile, enter:

```
load hpblkupd -dmail/smithj.nsf -kbulk
```

NOTE:

When you scan mail files, ensure there is no space between the switch and the filename or profile name. The file name is not enclosed in quotation marks.

For example:

```
-dmail/smithj.nsf  
-kbulk
```

The following parameters can be used to scan mail files:

Parameter	Description
-d<db/dir>	The database or directory to search in the Domino data directory. You can run the process on a single database or a directory. If you do not specify a value for -d, the utility searches every database in the server's Domino data directory.
-r<db>	The database to store the Mail Detail records that are created. The default Bulk Upload database (no -r switch) is: hprim/hp_rissblkupd.nsf
-k<profile>	The name of the mining rule profile. If you use the default Bulk Upload rule, this value is: bulk
-v	Verbose mode, which also displays the scanned mail files.

Discovering a mail file owner

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

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 mail file's access control list. The process looks for a user with at least READER access.

You can manually set an owner for a mail file by using the parameter -o<x@xx.xx>, where <x@xx.xx> is the Internet address of the owner.

For example, if you want to set Joe Smith as the mail file owner, you might enter:

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

Reviewing the Mail Detail records

To review the Mail Detail records that are created during the Bulk Upload process:

1. In the Domino Administrator client, open the HP EAs-D Bulk Upload database on the application server.
2. 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 records the owner's name, the mail file name, the server where the mail file resides, and the mining rule that the mail file is associated with.
 - 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.

Replicating the Bulk Upload database

After the Bulk Upload executable is run and the HP EAs-D Bulk Upload database is populated, replicate the database to a HP Gateway server on which the Bulk Upload mining rule is enabled.

Archiving the mail files

To archive the messages in the inactive mail files, follow these instructions.

1. In the Domino Administrator client, open the HP Gateway server.
2. Navigate to **Server > Status > Server Console**.
3. Issue one of the following commands to run the mining program:
 - `load rissminer -r -v -kbulk`
This command instructs rissminer to archive messages in the mail files listed in the replicated Bulk Upload database. The command assumes that you are using the default database (`hprim/hp_rissblkupd.nsf`), which is listed in the Global Configuration document's Additional Modules tab.
 - `load rissminer -r<db> -v -kbulk`
If you renamed the Bulk Upload database or created another Bulk Upload database, use this command. It instructs rissminer to archive messages in the mail files listed in the alternate Bulk Upload database. Enter the relevant path and database value in `<db>`.
4. Open the Bulk Upload reference database (`hprim\hp_riss_blkupreferenc.nsf`) to view the references that were created.
5. Run the Archive and Tombstone agents:

```
tell amgr run "hprim\hp_riss_blkupreferenc.nsf" 'archive'
tell amgr run "hprim\hp_riss_blkupreferenc.nsf" 'tombstone'
```

In Bulk Upload, the tombstoning process deletes archived messages from the mail files.
6. If any reference documents are in the preprocessing state, issue the following command:

```
tell amgr run "hprim\preproc_blk.nsf" 'encapsulate'
```
7. Run the Archive and Tombstone agents to archive the encapsulated messages.

4.7 Working with log files

You can view a log of archiving activity on the HP Gateway servers and change the number of days that log entries are kept.

- [HP EAs-D Log database](#), page 231
- [Viewing log files](#), page 231
- [Purging log entries](#), page 236

HP EAs-D Log database

Logging is configured in the Logging tab of the Server Definition document. (See “[Logging tab](#)” on page 155.) On that tab, you can choose to record HP Gateway server activity in the Domino log (`log.nsf`) or the HP EAs-D Log Database (`hprim\hp_risslog`).

When you select the HP EAs-D Log database, the following items are recorded:

- Activity of the mining program (`rissminer`) and the EAs Domino archiving agents on the HP Gateway servers
- Errors, warnings, and other messages (depends on the logging level that is configured)
- Any debugging that you are asked to perform by HP support
- Output generated from the HP EAs-D API database's Actions > Tools > 2. Export configuration to log, which is used by HP support to examine the API database configuration

Viewing log files

To view the log files, open HP EAs-D Log in the `hprim` folder, or open HP EAs-D API and click **Module Logs** in the left menu of the HP EAs-D API main view.

The All Log view appears, showing logs filtered by HP Gateway server and date.

Server	Start Date	Type	StartTime	End Time	Elapse Time	
▼ Gw01						
▼ 05/17/2011						
		Agents printing\Tombstone\Errors	05/17/2011 04:26:34 PM	05/17/2011 04:26:34 PM	0 seconds	5/17/11 4:26:30 PM :
		Agents printing\Tombstone\Outputs	05/17/2011 04:26:34 PM	05/17/2011 04:26:34 PM	0 seconds	5/17/11 4:26:30 PM :
		Agents printing\Tombstone\Errors	05/17/2011 04:26:34 PM	05/17/2011 04:26:34 PM	0 seconds	5/17/11 4:26:30 PM :
		Agents printing\Tombstone\Outputs	05/17/2011 04:26:31 PM	05/17/2011 04:26:34 PM	3 seconds	5/17/11 4:26:30 PM : Tombstone hprim\hpriss_minireferenc.nc count = 10, 5/17/11 4:26:31 P 2.1.1.110 Build (2011-05-02) ru : Tue May 17 16:26:31
		Agents printing\Archive\Errors	05/17/2011 04:26:14 PM	05/17/2011 04:26:14 PM	0 seconds	5/17/11 4:26:12 PM :
		Agents printing\Archive\Outputs	05/17/2011 04:26:14 PM	05/17/2011 04:26:14 PM	0 seconds	5/17/11 4:26:12 PM :
		Agents printing\Archive\Errors	05/17/2011 04:26:14 PM	05/17/2011 04:26:14 PM	0 seconds	5/17/11 4:26:12 PM :
		Agents printing\Archive\Outputs	05/17/2011 04:26:13 PM	05/17/2011 04:26:14 PM	1 seconds	5/17/11 4:26:12 PM : Archive. hprim\hpriss_minireferenc.nc count = 10, 5/17/11 4:26:13 P Append hash 'LDMtb+xFK'Ytwl Processed 1 document(5.193 K
		Encapsulate	05/17/2011 04:26:05 PM	05/17/2011 04:26:06 PM	1 seconds	
		Agents printing\Archive\Errors	05/17/2011 04:25:58 PM	05/17/2011 04:25:58 PM	0 seconds	5/17/11 4:25:36 PM :
		Agents printing\Archive\Outputs	05/17/2011 04:25:58 PM	05/17/2011 04:25:58 PM	0 seconds	5/17/11 4:25:36 PM :
		Agents printing\Archive\Errors	05/17/2011 04:25:58 PM	05/17/2011 04:25:58 PM	0 seconds	5/17/11 4:25:36 PM :
		Agents printing\Archive\Outputs	05/17/2011 04:25:37 PM	05/17/2011 04:25:58 PM	21 seconds	5/17/11 4:25:36 PM : Archive. hprim\hpriss_minireferenc.nc count = 10, 5/17/11 4:25:37 P Append hash 'LDM5JkKglq01 Append hash 'LDMfQrpxEtAAdr

You can also filter the logs by module, which lists the information by the type of activity (archiving agent, encapsulation, mining) or by the mining module, which lists the mining activity only.

The module view opens with all information displayed, but can be collapsed and expanded by activity, server, and date, as shown below.

Server	Start Date	Start Time
▼ Agents running		
▼ Archive		
▼ Errors		
▼ Gw01		
	05/17/2011	
	05/16/2011	
	05/13/2011	
	05/12/2011	
	05/11/2011	
▼ Outputs		
▼ Tombstone		
▼ Errors		
▼ Outputs		
▼ Gw01		
	05/17/2011	
	05/16/2011	
	05/13/2011	
	05/12/2011	
	05/11/2011	
▼ Encapsulate		
▼ Gw01		
	05/17/2011	
	05/16/2011	
	05/13/2011	
	05/12/2011	
	05/11/2011	
▼ RISSMINER 2.1.1		
▼ Gw01		
	05/17/2011	
	05/16/2011	
	05/13/2011	
	05/12/2011	
	05/11/2011	

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

- The 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 processing session
- The time, in seconds, 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

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

For the rissminer program, the entry shows:

Log - RISSMINER 2.1.1

```
Start : 05/17/2011 04:22:40 PM          Server: CN=Gw01/0=Rail
End   : 05/17/2011 04:23:16 PM
Elapsed Time : 35 seconds

Results:
RISSMINER 2.1.1 :    LIMIT ON REFERENC RECORDS 'hprim\hp_riss_minerreferenc.nsf' on
'CN=Gw01/0=Rail' has [0 doc] => MAX [100000 doc] => Max for this run [ 100000 doc]
RISSMINER 2.1.1
[ ARCH PROFILE    ] : TESTSA
-----
[ ARCHIVE SORT    ] : Oldest first
[ ARCHIVE STATUS  ]MEMO :          >> ENABLE <<
[ DOC MAX DAY     ]MEMO :          0
[ SESSION MAX    ]DOC  :          0          SIZE(MB) : 0          TOTAL DOC : 100000
TOTAL SIZE :          0
-----
[ Exception Fields ]
MAILSTATIONERYNAME
PROTECTFROMARCHIVE
REPEATINTERVAL
$ATTBYTESTRUNCATED
$DOCBYTESTRUNCATED
HPTOMBSTONED
-----
CN=one object/0=Dom Four          mail\oneobject.nsf          Archived :    100
Size :    115.09 MB
-----
TOTAL          Archived :    100
Size :    115.09 MB
-----[ Normal end ]-----
2011/05/17 - 16:23
```

- The server on which mining was performed
- The date the mining session took place
- The start time and end time of the mining session
- The time, in seconds, that it took to mine each journal or mail database
- The version of the mining program
- The name of the mining rule and the relevant settings, including the reference database name
- The name and size of the journal or mail file that was mined
- The number of messages that were mined

An agent log entry displays the following information:

Log - Agents printing\Archive\Outputs

```
Start : 05/17/2011 04:25:37 PM                               Server: CN=Gw01/0-Rail
End   : 05/17/2011 04:25:58 PM
Elapsed Time : 21 seconds

Results:
5/17/11 4:25:36 PM : Archive Agent version : 2.1.1.110 Build (2011-05-02) running in 'hprim\hp_riss_minerreferenc.nsf'
5/17/11 4:25:37 PM : Print stats count = 10
5/17/11 4:25:37 PM : Store stats count = 10
5/17/11 4:25:37 PM : NP_EAS-D_Control_IAP_Hashes_Collision is enabled
5/17/11 4:25:37 PM : Append hash 'LDHfQrrpxEtiAdn+7jdUIGqGSStcxF9=' : '652578330037D3EB' to table
5/17/11 4:25:38 PM : Append hash 'LDHfQrrpxEtiAdn+7jdUIGqGSStcxF9=' : '652578330037D3EB' to table
5/17/11 4:25:38 PM : Append hash 'LDHVPi08kUSMMZiYyPaeKjr8rruN7Y=' : '6525788B001B353E' to table
5/17/11 4:25:38 PM : Append hash 'LDHIjG8fsw05cqtq8XTQ59Wipat0r8=' : '652578330037D3EB' to table
5/17/11 4:25:38 PM : Append hash 'LDHuPHiuo7xuuANx8ZIkbiYqVRNDzQ=' : '652578330037D3EB' to table
5/17/11 4:25:38 PM : Append hash 'LDHc008QHCPGv0xjxnMAYanE7b30u=' : '652578330037D3EB' to table
5/17/11 4:25:38 PM : Append hash 'LDHb/OuY1jdet0VG3m6c7q7UWpnlAs=' : '6525788B001B353E' to table
5/17/11 4:25:38 PM : Append hash 'LDHwALDFaqqE20Aqxg0vWFHlJQ+j4=' : '6525788B001B353E' to table
5/17/11 4:25:41 PM : Append hash 'LDN3e2Jrx+tgIi8+4Y5BFT78ULkUuI=' : '652578330037D3EB' to table
5/17/11 4:25:41 PM :
5/17/11 4:25:41 PM : TemplateVersion . . . . . : Archive Agent version : 2.1.1.110 Build (2011-05-02) running in
'hprim\hp_riss_minerreferenc.nsf'
5/17/11 4:25:41 PM : ProcessStartTime . . . . . : Tue May 17 16:25:37 GMT+05:30 2011
5/17/11 4:25:41 PM : Status . . . . . : Running
5/17/11 4:25:41 PM :
5/17/11 4:25:41 PM : DBDocCountAfterCount . . . . . : 0
5/17/11 4:25:41 PM : DBDocCountBeforeCount . . . . . : 84
5/17/11 4:25:41 PM : DocMapperServletFailedCount . . . : 0
5/17/11 4:25:41 PM : DocMapperServletTimeAvg . . . . . : 16 ms
```

- The name of the agent
- The server on which the agent processing was performed
- The date the processing took place
- The start time and end time of the processing session
- The version and template version of the agent performing the processing
- Archiving statistics that were printed to the log or console
- Message hash cache statistics, including whether the cache is enabled or disabled
- The status of the process — running, done, or error
- The number of documents processed
- Statistics for the DocMapperServlet calls, which determine if a message has already been archived
- Statistics for the document processing time
- Statistics on the message hash calculation
- Statistics on address book lookup errors
- Statistics on metadata updates (metadata tracks a message's relationship with the IAP repositories)
- Statistics on the messages and references that were processed
- Statistics on remapped fields (remapping preserves data in fields as messages go through the Domino router and into the IAP)
- Statistics on the messages sent via SMTP

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

Log - Agents printing\Archive\Outputs

Start : 11/21/2009 05:36:42 AM	Server: CN=Pyroraptor/O= Org1
End : 11/21/2009 05:36:43 AM	
Elapsed Time : 1 seconds	
Results:	
Archive Agent version : 2.1 running in 'hprim\hp_riss_minerreferenc.nsf'	
11/21/09 8:36:42 AM : Ensuring owner receipt 'Test1User@org1.acme.net' for IAP 2.0 and above	
11/21/09 8:36:43 AM : ERROR: Processing E3CECDB9CB26988C85257615005D468A XML parse exception: org.jdom.input.	
Error on line 14: An invalid XML character (Unicode: 0x0) was found in the element content of the document.	
11/21/09 8:36:43 AM : Processed 1 document(3.909KB).	
11/21/09 8:36:43 AM :	

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

Log - Diag\Agent\MinerConfigExporter 2.1

Stat : 02/04/2010 10:32:43 PM	Server: CN=Server 2/O= Org1		
End : 02/04/2010 10:32:54 PM			
Elapsed Time : 11 seconds			
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	'{FAPIVIEW}' 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	DWA Sample	Mining rules	
> Minimum message size :	0 byte(s)		
> Enabled	true		
Action behavior			
> 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 behavior			
> 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. We recommend that the setting is changed to a period of 7–14 days on HP Gateway servers.

The Purge_Document agent must be scheduled and enabled.

To change the number of days that log records are kept, edit the Agent Parameters document:

1. Using the Domino Administrator client, open the HP EAs-D Log database (hprim\hp_risslog) on the 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 **Arg1: Purge record older than (n) Days** and change the number of days. Do not change the Form Name value in Arg2.
6. Click **File > Save**, and then close the document.

To schedule and enable the Purge_Document agent:

1. Open the Domino Designer client.
 - a. Open the HP EAs-D Log database in the `hprim` folder on the server.
 - b. In the Design pane, select **Code > Agents**.
 - c. Double-click **Purge_Document**.
 - d. In the agent Properties, make sure the Trigger is set to **On schedule** and the Target is set to **All documents in database**.
 - e. Click **Schedule** and set the agent's schedule.

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. Select the server in the **Where agent runs** box.
 - g. Save the changes, then close the agent Properties and the agent.
 - h. Click **Enable** to enable the agent.
2. Schedule and enable the log on each server on which it is installed.

4.8 Event monitoring and alerts

The HP EAs-D Alert database (`hp_rissalert.nsf`) is used to store system alerts. The events that generate an alert and/or define other actions to be taken are shown in the Monitoring Events view of the HP EAs-D API database. Events and alerts are activated only on the HP Gateway servers.

- [Monitoring events](#), page 239
- [Alerts](#), page 245

Monitoring events

A set of default events is displayed in the Monitoring Events view of the HP EAs-D API database. To open the view, select **View > Go to > Monitoring > Event**.

A partial list of events is shown below.

Name
Default
hp.archive.iap.credentials.requiresIAP2OrAbove
hp.archive.serverdefinition.notfound
hp.archive.iap.credentials.empty
hp.archive.statistics.init.failure
hp.archive.iap.credentials.invalid
hp.iap.http.invalid
hp.iap.smtp.invalid
hp.archive.reference.invalid
hp.archive.reference.view.invalid
hp.archive.fieldmapper.initconfig.failure
hp.archive.reference.document.invalid
hp.archive.templateVersion.print
hp.archive.serverdefinition.print
hp.fieldmapper.nameslookup.secondarydirectory
hp.archive.reference.print
hp.archive.reference.settings.print
hp.archive.exception.breakexception
hp.archive.selective.originaldocument.invalid
hp.archive.originaldocument.alreadyarchived
hp.archive.exception

Events can be reconfigured, other events can be added, and the text of alerts and log entries can be edited, but **only** in consultation with HP support.

When events are edited, use Lotus Notes version 8.51 or later. The Notes client on the HP Gateway server can be used for this purpose, either directly or via remote desktop protocol.

Monitoring Event document

Monitoring Event

Status : Enable Disable

Comments :

Event Name	hp.archive.compliance.originaldocument.invalid
Group	
Weight	1
Repetition Factor	1
Threshold	10
Actions summary	WHEN VALUE EXCEEDS <0.0> THEN <Log, Alert, Skip>
Start Date	[1299686531287]
Elaspe	[2803735]
Count	[0]

Open a Monitoring Event document by double-clicking the event. The following information is shown in each document.

Field	Description
Status	The event can be enabled or disabled. Events are enabled by default.
Event Name	The monitoring event name, used as the event identifier.
Group	An optional field that is used for design purposes, to group events in views.
Weight	The weight of an event, which is combined with the repetition factor to increment the event counter. This field is currently disabled.
Repetition Factor	This value is combined with the weight to increment the event counter. The higher the repetition factor, the faster the event counter is incremented. This field is currently disabled.
Threshold	The maximum value that an event counter can have.

Field	Description
Actions summary	A brief summary of the actions taken when the threshold is exceeded, and the order in which the actions occur. <ul style="list-style-type: none"> • Log: Add an entry to the log. • Alert: Create an alert in the HP EAs-D Alert database. • Skip: Do not process the document and go on to the next document. • Break: Stop processing.
Start date	The start of the last date (yyyy/mm/dd) and time (hh:mm:ss) the event occurred during an archiving or tombstoning process.
Elapse	The duration of the event.
Count	The number of times the event was triggered.

Event actions

An event can be performed globally or on a single HP Gateway or group of Gateway servers, as determined by the event's configuration.

There are currently four types of actions that can be executed:

- Log a message: Adds an entry to the HP EAs-D Log or the Domino log, depending on the log selected in the Server Definition's Logging tab. The text of the log entry is defined in the event.

NOTE:

The entries that appear in the log depend on the logging level that is defined. For example, if Basic Information (the default level) is selected, an event warning or error will not be logged.

- Create an alert: Creates a document in the HP EAs-D Alert database. The type of alert (Error, Warning, Information, Debug, Suggestion) and the text of the alert are configured in the event.
- Run a Notes formula: Specifies a Notes formula for the event. Depending on the event's configuration, the formula may be run on a document (the message or reference being processed).
- Change processing behavior: Changes an agent's behavior by reprocessing the document, ignoring (skipping) the document, or stopping document processing and then stopping the agent.

In addition, an alternative action can be defined. This action will be executed if the first action cannot be run.

Default monitoring events: Configuration issues

The default list of monitoring events includes events generated for the configuration issues listed in this section.

- [Configuration issues: Alerts are generated and processing stops](#), page 242
- [Configuration issues: Alerts are not generated but processing stops](#), page 242
- [Configuration issues: Alerts are generated but processing continues](#), page 242
- [Configuration issues: Alerts are not generated and processing continues](#), page 243

Configuration issues: Alerts are generated and processing stops

In the default event configuration, alerts are generated and errors are logged when the events below occur. The agent stops processing after the threshold is reached.

Monitoring event	Description
hp.archive.iap.credentials.empty	The credentials to log into the IAP are empty. The IAP credentials are the IAP login username and password, set in the server definition.
hp.archive.iap.credentials.invalid	The credentials to log into the IAP are invalid.
hp.archive.iap.credentials.requiresIAP2OrAbove	The IAP version is pre-2.0, but the agent is configured to require IAP 2.0 or later.
hp.archive.fieldremapper.initconfig.failure	An error occurred initializing the address book settings.
hp.archive.reference.invalid	The reference database is not valid.
hp.archive.reference.view.invalid	The default view in the reference database is invalid.
hp.archive.serverdefinition.notfound	The server definition cannot be found for an HP Gateway server.
hp.iap.http.invalid	The IAP HTTP portal is not responding. Note: A test is performed before document processing begins. A test is not performed before using HTTP protocol to compute the message hash or confirm End Owner Receipt.

Configuration issues: Alerts are not generated but processing stops

In the default event configuration for the following issues, an error is logged and processing stops when the event occurs. An alert is not generated.

Monitoring event	Description
Tombstone.HTTP	An error occurred on the IAP HTTP portal.
Tombstone.IAP.Credentials	The credentials to log into the IAP are invalid.
Tombstone.ServerDefinition	The server definition cannot be found for an HP Gateway server.
Tombstone.View	The default view in the reference database is invalid.

Configuration issues: Alerts are generated but processing continues

In the default event configuration, alerts are generated and warnings are logged, but processing continues for the following configuration problems.

Monitoring event	Description
hp.iap.smtp.invalid	The IAP SMTP portal is not responding.
hp.archive.statistics.init.failure	The HP EAs-D Stats database cannot be initialized.

Configuration issues: Alerts are not generated and processing continues

In the default event configuration, alerts are not generated for the configuration issues shown below. These two events are currently inactive.

Monitoring event	Description
hp.archive.serverdefinition.print	Server definition information is printed to the log.
hp.fieldmapper.nameslookup.secondarydirectory	An error occurred while readying the secondary Domino Directory.

Default monitoring events: Archiving issues

The default list of monitoring events includes events generated for the archiving issues listed in this section.

- [Archiving: Alerts are generated and processing stops](#), page 243
- [Archiving: Alerts are generated but processing continues](#), page 243
- [Archiving: Alerts are not generated and processing continues](#), page 244

Archiving: Alerts are generated and processing stops

In the default event configuration, alerts are generated and errors are logged for the following archiving problem. The agent stops processing after the 100th time that failure occurs.

Monitoring event	Description
hp.archive.exception.ioexception	The IAP is not responding to a query. After the first time that failure occurs, an error is logged and the document is reprocessed. After the 10th time that failure occurs, the Archive agent skips the document being processed. An error is logged and an alert is created. After the 100th time that failure occurs, the process is stopped. An error is logged and an alert is created.

Archiving: Alerts are generated but processing continues

In the default event configuration, an alert is generated and an error or warning is logged for the archiving issues listed below. The agent continues processing but, for some events, it skips a user mail file after the threshold is reached.

Monitoring event	Description
hp.archive.compliance.originaldocument.invalid	The reference points to an invalid message in a journal. The Archive agent skips the document.
hp.archive.eor.user.error	Ensure Owner Receipt (EOR) failure because the user repository is not found in the IAP. After the event occurs three times, the Archive agent skips all remaining references for the user.
hp.archive.eor.user.nointernetaddress	EOR failure because the user does not have a valid Internet Address. EAsD_Domain parameter is not found in the <code>notes.ini</code> file. EAsD_Domain is the organization's mail domain. For EOR, an entry is required in <code>notes.ini</code> ; see "Adding the EAsD_Domain parameter" on page 61. After the event occurs three times, the Archive agent skips all remaining references for the user.
hp.archive.originaldocument.alreadyarchived	The message is already archived and is skipped.
hp.archive.originalrepid.invalid	Cannot access a user's mail file. After the event occurs three times, the Archive agent skips the mail file.
hp.archive.reference.document.invalid	The reference document is invalid and is skipped.
hp.archive.selective.originaldocument.invalid	The reference points to an invalid message in a user mail file. The Archive agent skips the document being processed.
hp.archive.send.failure	Notes error when sending a message to the IAP. The Archive agent skips the document being processed.
Tombstone.OriginalDatabase	A user mail file cannot be found. After the event occurs two times, the Tombstone agent skips the mail file.
Tombstone.OriginalSelectiveMessage	The reference document points to an invalid message in a user mail file. The Tombstone agent skips the document being processed.

Archiving: Alerts are not generated and processing continues

For the following events, the default behavior does not generate alerts.

Monitoring event	Description
hp.archive.exception	An unexpected error has occurred. The action is configured per customer, usually as a workaround while a fix is being created by HP engineering.
hp.archive.exception.breakexception	An unexpected error has occurred. The action is configured per customer, usually as a workaround while a fix is being created by HP engineering.
hp.archive.exception.easdthrowable	An unexpected error has occurred. The action is configured per customer, usually as a workaround while a fix is being created by HP engineering.

Monitoring event	Description
hp.archive.reference.print	Prints reference database information (size, document count) to the log. Note: This event is currently inactive.
hp.archive.reference.settings.print	Prints reference database settings to the log. Note: This event is currently inactive.
hp.archive.templateVersion.print	Prints the reference database template version to the log. Note: This event is currently inactive.
Tombstone.ApplyAction	Failed to tombstone a message. This could be due to a corrupt document, Notes API problem, etc. The error is logged and the Tombstone agent skips the document being processed.
Tombstone.ComputeOriginalMessageHash	Could not compute the message hash. The error is logged and the Tombstone agent skips the document being processed.
Tombstone.OpenPreprocDatabase	Could not open a preprocessing database. The error is logged and the Tombstone agent skips the document being processed.
Tombstone.OriginalComplianceMessage	A reference document in the Sent state points to an invalid message in a journal, or there is a Notes error. The error is logged and the Tombstone agent skips the document being processed.
Tombstone.OriginalMessageHash	A reference document in the Sent state has no message hash. The error is logged and the Tombstone agent skips the document being processed.

Alerts

- [The HP EAs-D Alert database](#), page 245
- [Removing documents from the HP EAs-D Alert database](#), page 247

The HP EAs-D Alert database

The events that result in alerts are described above in [Monitoring events](#).

Alerts are logged in the HP EAs-D Alert database and can be filtered by:

- Level (such as Error or Warning)
- The HP Gateway server on which the alert was generated and the alert level

The Alert view displays the following information:

- Level: The alert level, configured in the event.
- Created: The date and time the event and alert were generated.
- Event: The name of the event.
- Log: The alert message, configured in the event.

The alerts below are sorted by server and level.

Level	Created	Event	Log
CN=Gw01/O=Rail			
▼ Error			
	03/28/2011 04:34:41 PM	hp.archive.iap.credentials.invalid	IAP credentials are invalid - IAP Login : afour@dom four
	03/28/2011 04:34:41 PM	hp.archive.iap.credentials.invalid	IAP credentials are invalid - IAP Login : afour@dom four

When an alert is opened, the following information is displayed:

Alert

Event:	hp.archive.eor.user.error.adminfour@easeqa2.qa
Process:	Archive
Server:	CN=Gw01/O=Rail
Database:	652578880031DE72
Level:	Error
Event Time:	05/06/2011 17:39:31
Alert Time:	05/06/2011 17:39:31
Original document:	
Referenc document:	

Unable to process EOR for user \${hp.archive.eor.owner}, error : \${hp.archive.eor.error}

- Event: The name of the event generating the alert.
- Process: The agent processing the document that precipitated the event.
- Server: The HP Gateway server on which the event occurred.
- Database: The ID of the database on which the agent ran.
- Level: The alert level.
- Event time: The time of the event that generated the alert.
- Alert time: The time the alert was generated.
- Original document (if applicable): A link pointing to the original document in the reference data-base.
- Referenc document (if applicable): A link pointing to the reference that was being processed when the event occurred.
- The text of the alert.

Removing documents from the HP EAs-D Alert database

The HP EAs-D Alert database must be purged regularly so it does not grow too large. The Purge_Document agent in the database, which removes the old alert documents, needs to be scheduled and enabled.

By default, alerts that are more than 15 days old are removed. However, you can change the number of days that alerts are kept by editing the Agent Parameters document in the database.

1. In the Designer client, enable the Purge_Document agent.
You can also reschedule the agent. By default, it is set to run daily at 1:00 a.m.
2. To change the number of days that alerts are kept:
 - a. Using the Domino Administrator client, open the HP EAs-D Alert database in the `hprim` folder on the HP Gateway server.
 - b. In the left menu, expand **Agent**, and select **Parameters**.
 - c. Double-click the document listed in PURGE_DOCUMENT.
 - d. Double-click the value in **Arg1: Purge record older than (no) Days** and change the number of days that EAs Domino alerts should be kept.
Do not change the Form Name value in Arg12.
 - e. Click **File > Save**, and then close the document.

The alert documents that are deleted are shown in the Log view of the HP EAs-D Alert database. The start time and end time of the purge process is shown, along with the number of alert documents that were deleted. Select **Agent > Log** in the left menu to open this view.

4.9 Archiving statistics

- [Configuring and enabling statistics collection](#), page 249
- [Viewing statistics in the HP EAs-D Stats database](#), page 249
- [Removing documents from the HP EAs-D Stats database](#), page 251

Configuring and enabling statistics collection

Archive and tombstone process metrics for the HP Gateway servers are logged when statistics collection is enabled. This is done in the **Logging > Statistics** tab in Server Definition documents.

When statistics collection is enabled, archiving metrics can be output to the console and/or to the HP EAs-D Stats database (`hp_easd_stats.nsf`) in the `hprim` folder.

To configure statistics collection, follow the instructions in “[Logging tab](#)” on page 155.

Viewing statistics in the HP EAs-D Stats database

When archiving statistics are logged in the HP EAs-D Stats database, they can be filtered by the following views:

- All Running Only: All archiving/tombstoning processes that are currently running
- All by Server by Start Time: The HP Gateway server on which the statistics were collected, and the start time of the process on the Gateway
- All by Start Time: The start time of the archiving/tombstoning process (on all HP Gateway servers)

Each statistics view shows the following information:

Field	Description
Process Name	Statistics are collected for the archive and tombstone processes. This field displays the relevant agent: Archive or Tombstone.
Server	The HP Gateway server on which the process is run.
Source DB	The reference database on which the process is run.
Total Ingestion & Updates	The number of messages ingested by the IAP. (Applies to the Archive process.)
Rate/Sec	The rate per second of message ingestion.
Start	The time the process started.
End	The time the process ended.
Last Mod	The time of the last modification made by the agent.
Duration	The length of the process.

Field	Description
Status	The process status — Running, Done, or Error.
Ref Count	The number of references that were processed. (Includes references where the action ended in error or the reference was skipped.)
Msg Read Count	The number of messages that were read in the source mail file or journal.
Msg Read Failed Count	The number of messages that could not be read in the source mail file or journal.
SMTP Sent Count	The number of messages sent via SMTP.
Doc Map Serv Tot Count	The total number of documentMapperServlet calls. These calls determine if a message has already been archived, so that archiving of new messages can take place or previously archived messages can be tombstoned.
Meta Data Update Total Count	The total number of metadata update calls, both failed and successful. These calls are made when there have been changes to the message metadata. (The metadata is used to track the message's relationship with the IAP repositories, over the "life" of the message on the IAP.)
Doc Map Serv Failed Count	The number of documentMapperServlet calls that failed due to errors in the call; for example, read time outs.
Doc Map Serv URL Found Count	The number of documentMapperServlet calls that returned a docURL. (The docURL, the URL of a message in the IAP, is used to determine if a message has been archived.)
Doc Map Serv URL Not Found Count	The number of documentMapperServlet calls that did not return a docURL.
Meta Data Update Failed Count	The number of metadata update calls that failed due to errors in the call; for example, read time outs.
Meta Data Update Success Count	The number of metadata update calls that were successful. (Message metadata successfully updated.)
Meta Data Update Errors Count	The number of errors returned by metadata update calls. These are not errors in the calls themselves.
Refs to Sent Count	The number of reference documents moved to Sent status.
Refs to PreProcess Count	The number of reference documents moved to Preprocess status.
Refs to Error Count	The number of reference documents moved to Error status.
Doc Map Serv Time Avg	The average time for documentMapperServlet calls, in milliseconds (ms).
Doc Map Serv Time Max	The maximum time for a documentMapperServlet call, in milliseconds (ms).
Doc Map Serv Time Min	The minimum time for a documentMapperServlet call, in milliseconds (ms).
Doc Map Serv Time Total	The total time for all documentMapperServlet calls.
Meta Data Update Time Avg	The average time for metadata update calls, in milliseconds (ms).
Meta Data Update Time Max	The minimum time for a metadata update call, in milliseconds (ms).

Field	Description
Meta Data Update Time Min	The maximum time for a metadata update call, in milliseconds (ms).
Meta Data Update Time Total	The total time for all metadata update calls.
Refs Deleted Count	The total number of reference documents that were deleted from the reference database.
Msgs Tombstoned Count	The total number of source messages that were tombstoned.
Msgs Deleted Count	The total number of source messages that were deleted.

You can open a Statistics document by double-clicking its entry in the database. Each document provides most of the information shown above, but uses slightly different field names.

Removing documents from the HP EAs-D Stats database

When collection of EAs Domino statistics is enabled, the HP EAs-D Stats database must be purged regularly so it does not grow too large. The Purge_Document agent in the database, which removes the old statistics documents, must be scheduled and enabled.

By default, statistics documents that are more than 15 days old are removed. However, you can change the number of days that statistics are kept by editing the Agent Parameters document in the database.

1. In the Designer client, enable the Purge_Document agent.
You can also reschedule the agent. By default, it is set to run daily at 1:00 a.m.
2. To change the number of days that statistics are kept:
 - a. Using the Domino Administrator client, open the HP EAs-D Stats database in the `hprim` folder on the HP Gateway server.
 - b. In the left menu, expand **Agent**, and select **Parameters**.
 - c. Double-click the document listed in PURGE_DOCUMENT.
 - d. Double-click the value in **Arg1: Purge record older than (no) Days** and change the number of days that EAs Domino statistics documents should be kept.
Do not change the Form Name value in Arg2.
 - e. Click **File > Save**, and then close the document.

The statistics documents that are deleted are shown in the Log view of the HP EAs-D Stats database. The start time and end time of the purge process is shown, along with the number of statistics documents that were deleted. Select **Agent > Log** in the left menu to open this view.

Part 5. Retrieving email from the IAP

- [Configuring DWA Extension](#), page 255
- [Using Export Search](#), page 269
- [Configuring IAP single sign-on](#), page 289
- [Working with HP EAs Domino client applications](#), page 299

5.1 Configuring DWA Extension

This chapter describes the steps required to retrieve archived email in Domino Web Access (iNotes), if your organization uses this HP EAs Domino option.

- [Introduction](#), page 255
- [Installing DWA Extension](#), page 256
- [DWA Extension configuration steps](#), page 259
- [Configuring the Proxy Gateway document](#), page 260
- [Configuring the Tombstone Prototype document](#), page 261
- [Editing the Tombstone Settings tab](#), page 266

(See [“Working with HP EAs Domino client applications”](#) on page 299 if users retrieve archived messages in Lotus Notes.)

Introduction

DWA Extension allows archived messages to be retrieved from the IAP and opened in DWA. When users open a tombstoned message in DWA, text such as “Click here to retrieve the full message” is displayed in the browser. 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.

Messages that are retrieved from the IAP are cached in a user's mail file. The amount of time to keep the cached messages is specified in the Global Configuration document, located in the mail domain version of the HP EAs-D API database.

The Lotus Domino server(s) used for DWA message retrieval can be Domino mail servers (usually dedicated to DWA) or an application server that is used as a proxy. (In EAs Domino, the proxy server is known as the Proxy Gateway.)

We recommend the use of a proxy if the organization supports a DWA user community where performance and server stability are critical. The Proxy Gateway is usually in the same Domino domain as the mail server(s) that are being supported. It must not be in the HP Gateway domain.

Installing DWA Extension

Follow the steps below to install DWA Extension. The EAs Domino installer must run on a Windows client.

Installation on the DWA/proxy server

1. In the Domino Administrator client, switch to a Notes ID that can be used to create databases and run restricted and unrestricted agents.
2. Using Windows Explorer, navigate to the folder where the EAs Domino installation files were extracted. Locate the `server` directory and double-click the `Setup.exe` file.
3. Use the HP EAs Domino installer to install the EAs Domino databases on the DWA or proxy server. The following databases are used by DWA Extension:
 - HP EAs-D DWA Index database (`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. It should not be replicated.
 - HP EAs-D API database (`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.
If the mail domain instance of EAs-D API has already been installed on another server, replicate it to this server.
4. If using a Proxy Gateway server, use the Deploy and Replicate options in the EAs Domino installer to install HP EAs-D API on the mail server(s) that redirect user requests to the proxy.
The mail servers must have a copy of the EAs-D API database to dynamically generate tombstone URLs.
5. Set the access permissions for each EAs Domino database that is installed.
See "[Setting ACL for DWA Extension](#)" on page 258.
6. Configure a security setting for the EASWEB agent in the DWA Index database:
 - a. In the Domino Designer client, open the HP DWA Index database and select **Code > Agents**.
 - b. Double-click **EASWEB**, and then click **OK** to bypass the warning.
 - c. In the agent Properties, click the **Security** tab.
 - d. In the **Run on behalf of** field, select a Notes ID that is listed in the Server document's **Security > Programmability Restrictions > Run restricted LotusScript/Java agents** field.
HP engineering recommends specifying the server on which the agent will run.
 - e. Ensure **Allow restricted operations** is selected.
 - f. Save the settings, and close the Properties and the agent.

7. If a Proxy Gateway server is used, ensure that:
 - A trust relationship is established with the mail server(s) that the proxy is servicing.
 - If the proxy is not in the same Domino domain as the mail servers, OtherDomainServers is granted the same rights as LocalDomainServers in the database ACL.
 - 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.
8. Restart the Domino server(s).
9. Create a link to the IAP so that users have a quick way to search for archived messages.

You can create a Search the IAP link on the organization's Intranet portal, and/or send users the link in an email and have them bookmark it in their Web browser. The link is not created in DWA.

 - When IAP single sign-on (SSO) is not used, the URL is:
<http://IAP-VIP-address-or-hostname>.
 - When SSO is used, the URL is:
<http://mailserver-address-or-hostname/hprim/rimsso.nsf/IAPWebSearch?OpenAgent>
To set up SSO, follow the instructions in “Setting up IAP SSO with DWA” on page 258.

 **NOTE:**

Retrieved DWA messages that are cached in user mail files are hidden from all standard views provided by the Lotus Notes Mail templates. To add a custom view to the mail template to display the cached messages, use the following selection formula:

```
SELECT @IsAvailable(HP_DWA_CACHE_DATE) | @IsAvailable(HP_DWA_CACHE)
```

Installation on the HP Gateway server

DWA Extension uses Tombstone Prototype and Mining Rule documents in the Gateway domain version of the HP EAs-D API database. Additionally, it uses the HP EAs-D SC Request database (`\hprim\hp_rissreq.nsf`) to convert tombstones, for example if a new tombstone prototype is added or if users retrieve messages that were archived with a pre-2.0 version of EAs Domino. These databases are automatically installed on the HP Gateway servers during the EAs Domino software installation.

Setting ACL for DWA Extension

Follow these instructions to set the access for the databases used by DWA Extension:

1. Complete the following steps on each customer server where a DWA Index database is installed:
 - a. In the Domino Administrator client, click the **Files** tab and select the `hprim` folder.
 - b. Right-click `hp_dwaindex.nsf` in the folder, and select **Access Control > Manage**.
 - c. Click **Add**, add the following users, and set their access as shown:
 - LocalDomainAdmins (or substitute): **Manager**
Must also have Admin access and rights to delete and replicate or copy documents.
 - LocalDomainServers: **Manager**
Must also have Admin access and rights to delete and replicate or copy documents.
 - Each Notes ID that is listed in step 6d in [Installing DWA Extension](#): **Editor**
 - All DWA users: **Depositor**
Add users with one or more group entries.
 - d. Set Default to **Manager**.
 - e. Click **OK**, and close the window.
2. Edit the ACL in the mail files of all users who access DWA.

Add each Notes ID that is listed in step 6d in [Installing DWA Extension](#) and grant the ID **Editor** access.

If the mail files are replicated, ensure the ACL is also changed in the replicated files.
3. Modify the ACL for the HP EAs-D API database in the mail domain:
 - a. Provide DWA users with **Reader** access.
Add users with one or more group entries.
 - b. Add the Notes ID that is listed in step 6d in [Installing DWA Extension](#) and grant the ID **Reader** access.

If the Notes ID is the same as the server ID, grant the ID **Manager** access, and select the **Delete documents** check box.

The correct access control settings should already be configured for the HP EAs-D API and HP EAs-D SC Request databases on the HP Gateway server.

Setting up IAP SSO with DWA

If users access email only in DWA, follow the steps below to add support for IAP single sign-on. If users access email using Lotus Notes and DWA, follow the instructions in [“Configuring IAP single sign-on”](#) on page 289.

1. Copy the HP EAs-D SSO template (`hp_sso.ntf`) from the Templates directory on the installation media.
2. Create the HP EAs-D SSO database following the instructions in [“Creating the HP EAs-D SSO database”](#) on page 289 and [“Configuring the HP EAs-D SSO database and the Generate SSO Tokens agent”](#) on page 290.
3. Configure SSO on the IAP. See page 297.

4. Create a Search the IAP link on the Intranet portal, or email the link to users.

Use the following URL:

<http://mailserver-address-or-hostname/hprim/rimsso.nsf/IAPWebSearch?OpenAgent>

We do not recommend creating an IAP link or button directly in DWA.

DWA Extension configuration steps

DWA Extension is configured on both the DWA/proxy server and the HP Gateway server.

Configuration steps on the DWA/proxy server

1. Open the HP EAs-D API database and create a Server Definition document for the DWA server or Proxy Gateway(s).

If a proxy is used, include each server that redirects user requests to the proxy.

Configure the following tabs in the Server Definition document:

- “[Server Settings tab](#)” on page 148
 - “[DWA Settings tab](#)” on page 153
2. In the Global Configuration document, set the amount of time to retain retrieved messages in a user mail file cache.
See “[DWA Index Settings tab](#)” on page 144.
 3. Configure a Proxy Gateway document, if a proxy server is used.
See “[Configuring the Proxy Gateway document](#)” on page 260.

Configuration steps on the HP Gateway server

1. Configure the Tombstone Prototype document.
See “[Configuring the Tombstone Prototype document](#)” on page 261.
2. (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.
3. Configure the Tombstone Settings tab in the mining rule.
This tab must be configured whether you use a DWA mining rule or a selective mining rule for mail files accessed by both the DWA and Notes user communities.
See “[Editing the Tombstone Settings tab](#)” on page 266.
4. Configure the remaining settings in the mining rule according to the steps in “[Configuring mining rules](#)” on page 160.
5. Enable the Purge_Document agent in the HP EAs-D SC Request database.
If you want to change the number of days that tombstone conversion requests are kept in this database, see “[Removing conversion requests from the HP EAs-D SC Request database](#)” on page 267.

Configuring the Proxy Gateway document (optional)

We recommend the use of a Proxy Gateway if you support a DWA user community where performance and server stability are critical. The Lotus Domino server used for the Proxy Gateway is usually in the same Domino domain as the mail server(s) that are being supported. The proxy server must not be in the HP Gateway domain.

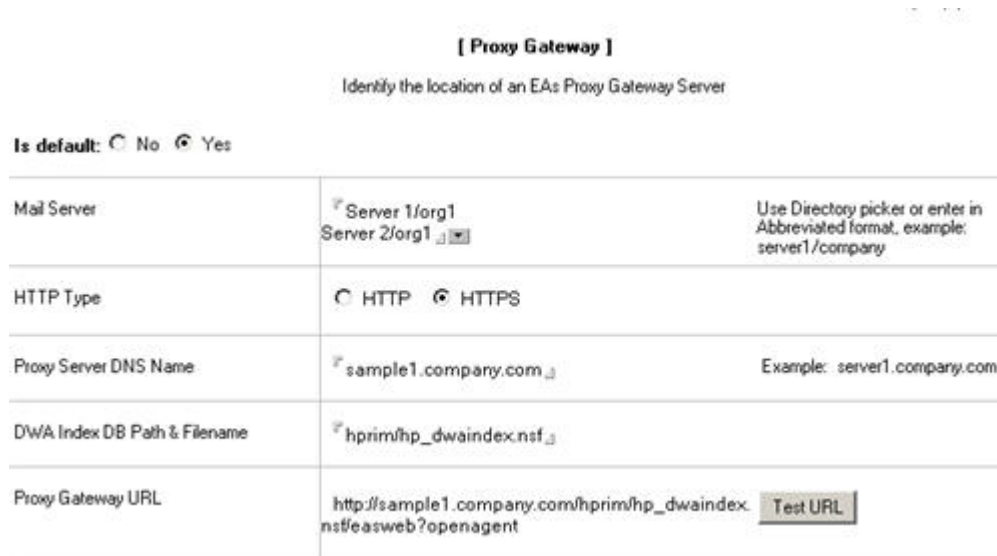
The Proxy Gateway document specifies the server that is being used as the proxy. By itself, this document has no effect on DWA message retrieval. It must be leveraged by a Tombstone Prototype document, which is created in “[Configuring the Tombstone Prototype document](#)” on page 261.

NOTE:




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

To configure the Proxy Gateway document:

1. In the Domino administrator client, open the mail domain version of the HP EAs-D API database file.
2. Under Proxy Gateway in the main view, open **Proxy Gateway Default**.



The screenshot shows the configuration form for the Proxy Gateway. The title is "[Proxy Gateway]" and the subtitle is "Identify the location of an EAs Proxy Gateway Server". There are two radio buttons for "Is default": "No" and "Yes", with "Yes" selected. The form contains five rows of configuration fields:

[Proxy Gateway]	
Identify the location of an EAs Proxy Gateway Server	
Is default:	<input type="radio"/> No <input checked="" type="radio"/> Yes
Mail Server	<input type="text" value="Server 1/org1"/> <input type="text" value="Server 2/org1"/>  <small>Use Directory picker or enter in Abbreviated format, example: server1/company</small>
HTTP Type	<input type="radio"/> HTTP <input checked="" type="radio"/> HTTPS
Proxy Server DNS Name	<input type="text" value="sample1.company.com"/>  <small>Example: server1.company.com</small>
DWA Index DB Path & Filename	<input type="text" value="hprim/hp_dwaindex.nsf"/> 
Proxy Gateway URL	<input type="text" value="http://sample1.company.com/hprim/hp_dwaindex.nsf/easweb?openagent"/> <input type="button" value="Test URL"/>

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. If you need to create a new document from the API main view, select **Create > Retrieval > 1. Proxy Gateways**.

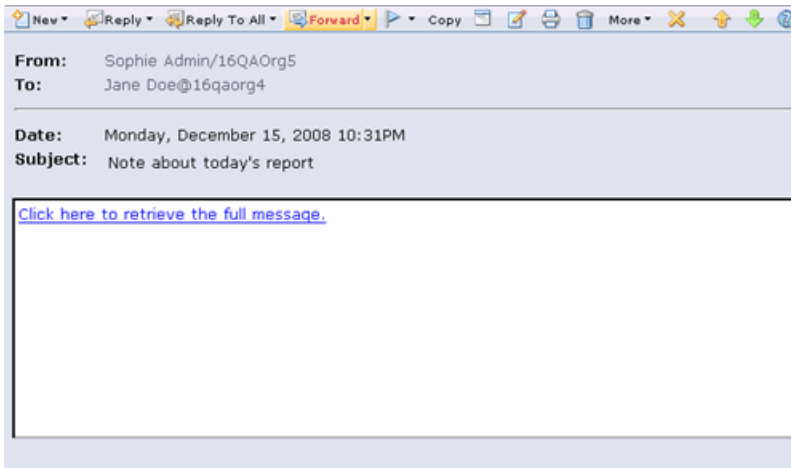
Configuring the Tombstone Prototype document

A Tombstone Prototype document must be configured in the HP EAs-D API database on the HP Gateway server so that tombstoned messages can be retrieved in DWA. It must also be configured if users access messages in both DWA and the Notes client.

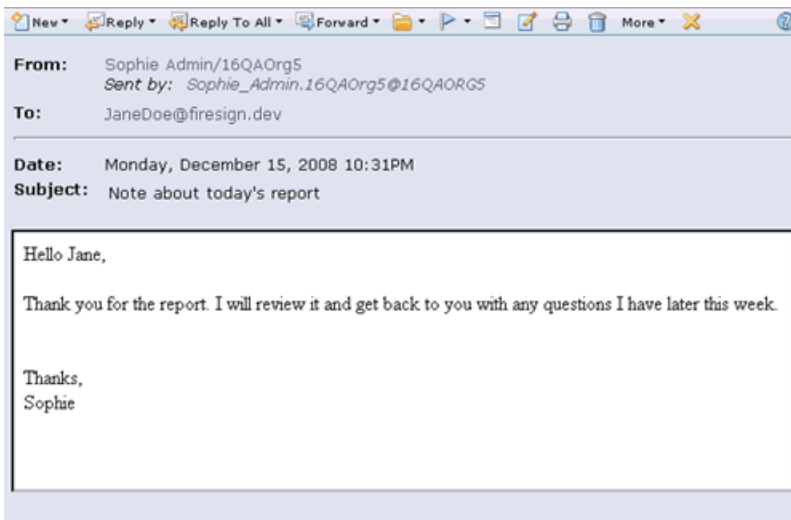
The prototype document includes a Rich Text field with a Computed Text or Computed Link Hotspot element. This element contains a Notes formula that is used to generate the link used during DWA tombstone retrieval.

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 266). 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.



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:

If users retrieve tombstoned messages from servers running Domino version 8.5.1 or later and/or retrieve tombstoned messages in EAs Domino Local Cache as well as DWA, use one of these prototype keys:

- TSKey2.1-1, for use with a Proxy Gateway, generates tombstones that are approximately 4 KB.
Use this formula if user requests can be directed to the default proxy server listed in the Proxy Gateway document.
- TSKey2.1-2, for use with a Proxy Gateway, generates tombstones that are approximately 5 KB.
This formula does not list the default proxy server.
- TSKey2.1-3, for use with a local host, generates tombstones that are approximately 3.5 KB.

 **NOTE:**

When messages are retrieved in both DWA and Local Cache, it is important to start with a TSKey2.1-x sample. The code in these samples creates unified tombstone links that work for both DWA access and Local Cache access in the Notes client. Prototypes from previous EAs Domino releases created links that only worked for DWA, and the use of Local Cache interfered with those links.

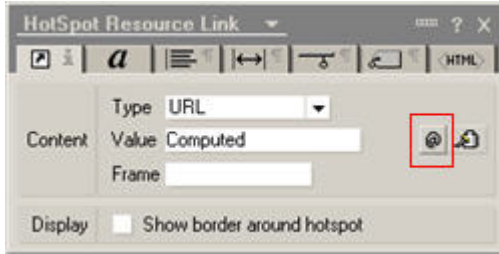
For more information about the Local Cache application, see [“Using Local Cache”](#) on page 301.

If users do not retrieve tombstoned messages in Local Cache as well as DWA and/or the DWA server runs a pre- 8.5.1 version of Domino, you can use one of the prototype keys below. However, do not use these keys if you plan to upgrade the server to Domino 8.5.x in the future.

- TSKey1, for use with a Proxy Gateway, generates tombstones that are approximately 3 KB.
Use this formula if user requests can be directed to the default proxy server listed in the Proxy Gateway document.
 - TSKey2, for use with a Proxy Gateway, generates tombstones that are approximately 2 KB.
This formula does not list the default proxy server.
 - 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 Local Cache compatibility field, ensure that:
 - **Yes** is selected if the key was copied from TSKey2.1-x.
 - **No** is selected if the key was copied from TSKey1, 2, or 3.
 7. In the **Comments** field, enter any comments about the key or the document.

8. Perform one of these actions:

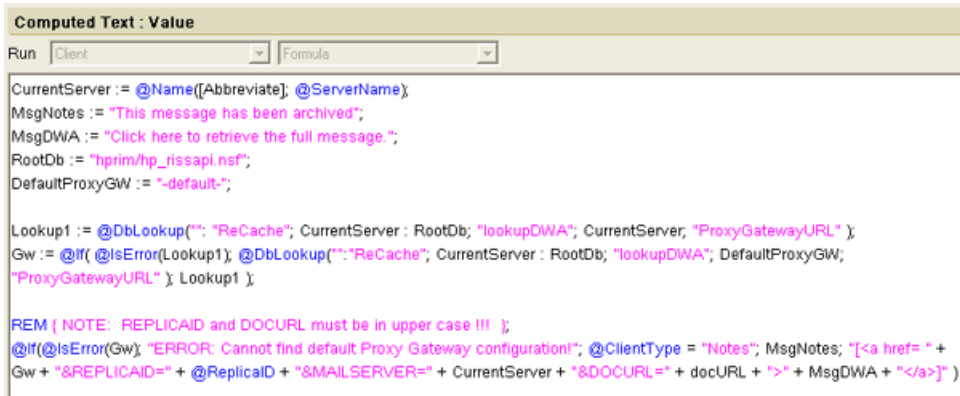
- Keys copied from TSKey2.1-x: Place the cursor in the Hotspot link in the **Tombstone Body** field. In the **Hotspot** menu, select **Hotspot Properties** and then click the formula icon.



- Keys copied from TSKey1, 2, or 3: Place the cursor in the **Tombstone Body** field. 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.)



9. Edit the formula values:

- (Proxy Gateway keys only) Edit the **CurrentServer** value if the 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 clickable link text if you want to change the sample, "Click here to retrieve the full message." This is the message that appears in DWA when users open a tombstoned message. In TSKey1, 2 or 3, change the **MsgDWA** value.

In TSKey2.1-x, place the cursor inside the Hotspot text in the **Tombstone Body** field and make the change directly in the text. Be careful when changing the text in TSKey2.1-x prototypes. Do not add or delete any lines, and do not select an entire line and type over the text.

[Tombstone Prototype]

Define the content of a rich text tombstone

Prototype key	TSKey 2.1-1 - US English
Local Cache compatibility	<input checked="" type="radio"/> Yes <input type="radio"/> No
Comments	Example - 8.51 & LC Compatible TSKey

Tombstone Body - enter Rich text

Click here to retrieve the full document.
This message has been archived.

- Edit the text if messages are retrieved in Lotus Notes as well as DWA and you want to change the sample, "This message has been archived."

This static message only appears in Lotus Notes if the computer or the IAP is offline and tombstoned messages cannot be retrieved and opened.

In TSKey1, 2 or 3, change the **MsgNotes** value.

In TSKey2.1-x, place the cursor inside the plain text in the **Tombstone Body** field and make the change directly in the text. Do not add or delete any lines, and do not select an entire line and type over the text.

Tombstone Body - enter Rich text

Click here to retrieve the full document.
This message has been archived.

- If you make changes to the formula or create your own formula, ensure that the following parameters are always in upper case: REPLICID, MAILSERVER, DOCURL. These URL parameters are case-sensitive.

For example:

```
https://<host_name>/hprim/hp_dwaindex.nsf/easweb?openagent&REPLICID=
<mailfile_replicaID>&MAILSERVER=<mailserver_name>&DOCURL=<docURL>
```

- More information on completing the formulas is shown in the prototype key instructions.

10. 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=
DWN03JI51C21loMWpNmnAmaY1kIHikUWYWame32EQekoce13WWnPKfdRJQ9w9MCj
DHUqT21gcwn99SNb-I5vBgi5dUFpvpuoXQPlkAFWbKswEgMgw1RsEikjlcJXsHcX8
J2gt4MTTgN9OYS7-uc23RuUgaVR4aKiNLHucf1J0M3U5ZoiNZ1TXeGmui3nTcOby
1lXLmFjx4N6F6gDpc4ZAg
```

11. Save the edited Tombstone Prototype document.

 NOTE:

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

```
https://<host_name>/hprim/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 must be specified in the Tombstone Settings tab in the mining rule. 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.

We recommend that you choose this option.

[Tombstone Settings]

Control the creation of tombstones for archived messages, determine size and functionality.

Actions:	Style
<input type="radio"/> None <input checked="" type="radio"/> Shrink Body and remove attachments <input type="radio"/> Remove attachments only <input type="radio"/> Clear body and remove attachments <input type="radio"/> Delete message [Shrink to : 100 Bytes]	<input type="radio"/> Text <input checked="" type="radio"/> Rich Text [Prototype: TSKey 2.1-3 - US English]
Operate only if document is greater than	3500 Bytes
Reference Document Retry interval	10 Days

- **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. On the HP Gateway server, open the **HP EAs-D API** database file.
2. Under Mining Rules in the main view, open the selective mining rule or 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 168.
 - Ensure that **Rich Text** is selected for the Style and a Tombstone Prototype key is selected.
 - Ensure that the **Operate only if document is greater than** value is set to a size of 2000–5000 bytes, depending on the Tombstone Prototype key. When DWA Extension is implemented, tombstoned items are a minimum of 2–3 KB for TSKeys 1, 2 or 3 and 3.5–5 KB for TSKeys 2.1-x.

Removing conversion requests from the HP EAs-D SC Request database

The Purge_Document agent in HP EAs- D SC Request is used by DWA Extension to remove tombstone conversion requests that are older than a certain number of days. By default, requests that are more than 30 days old are removed.

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

1. In the Designer client, schedule and enable the Purge_Document agent.
2. To change the number of days that conversion requests are kept:
 - a. Using the Domino Administrator client, open the HP EAs-D SC Request database in the `hprim` folder on the HP Gateway server.
 - b. In the **View** menu, select **Go To**, and then select **Agent**.
 - c. Expand **Agent**, select **Parameters**, and then click **OK**.
The Agent\Parameters view appears.
 - d. Double-click the document listed in PURGE_DOCUMENT.
If PURGE_DOCUMENT is not displayed, follow the instructions below in [Adding the Agent\Parameters document](#).
 - e. Double-click the value in **Arg1: Number of Days** and change the number of days conversion requests should be kept.
Do not change the Form Name value in Arg2.
 - f. Click **File > Save**, and then close the document.

Adding the Agent\Parameters document

If the Agent\Parameters document is not displayed in the HP EAs-D SC Request database, follow these instructions to create the document:

1. Using the Domino Administrator client, open the HP EAs-D SC Request database in the `hprim` folder on the HP Gateway server.
2. In the menu, select **Create > Agent > Parameters**
3. Complete the fields in the document that appears:
 - a. For Agent name, enter **PURGE_DOCUMENT**.
 - b. For Arg1, enter **Number of Days**.
 - c. For the Arg1 Value, enter the number of days that the conversion requests should be kept.
 - d. For Arg2, enter **Form Name**.
 - e. For the Arg2 Value, enter **AGENT_LOG**.
4. Click **Close**, and then click **Yes** to save the document.

5.2 Using Export Search

- [Introduction](#), page 269
- [Using the Export Search Desktop tool to export messages](#), page 269
- [Using the server to export messages](#), page 272

Introduction

Export Search is a tool that is typically used by compliance officers to retrieve messages for litigation-related review. With Export Search, links to archived messages are exported from the IAP Web Interface into a DLD file. The linked messages are then downloaded into a standard Notes database 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. The extraction of the DLD message links to a Notes database can be performed on a client system or a Lotus Domino server.

If messages are exported to a client, an Export Search Desktop tool must be installed on the machine. This tool runs as a standalone Java-based program on the user's desktop. It allows the user to specify the location of the DLD file, the output location for the exported messages, and other options.

The server version runs as a Java agent in the Export Search database, which is installed on a Domino server in the mail domain. If a large number of messages will be exported, the server option is the better choice. To export messages, a user completes an Export Search request form specifying an output database on a Domino server. The DLD file is attached to the form to trigger the export agent. The request form can be completed using the Lotus Notes client or the Export Search Web Interface.

Using the Export Search Desktop tool to export messages

The client-side option can be used by compliance officers to export messages from the IAP to the mail file on their computer, or to another mail file to which they have access.

The EAs Domino Local Cache package must be installed on the client machine, with the IAP domain and IP address configured in the Local Cache settings. The Local Cache installation includes the Export Search Desktop tool that is used to export messages. See "[Installing Local Cache](#)" on page 302 and "[Configuring Local Cache](#)" on page 303 for details.

To export email copies from the IAP using the Export Search Desktop tool:

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

If the messages are being exported to another mail file, create a folder in that mail file.

2. In the IAP Web Interface:
 - a. Search for the relevant messages.

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

The search results are displayed on the Query Results page.
 - b. If there are more than 500 results, follow the steps in [“Saving query results”](#) on page 271.
 - c. On the Query Results page, select the check box next to each message you want to export. Skip this step if you are exporting all items.
 - d. Click **More Options** to open the Options menu.
 - e. To export all search results, click **Export All Items**. To export selected items, click **Export Checked Items**.

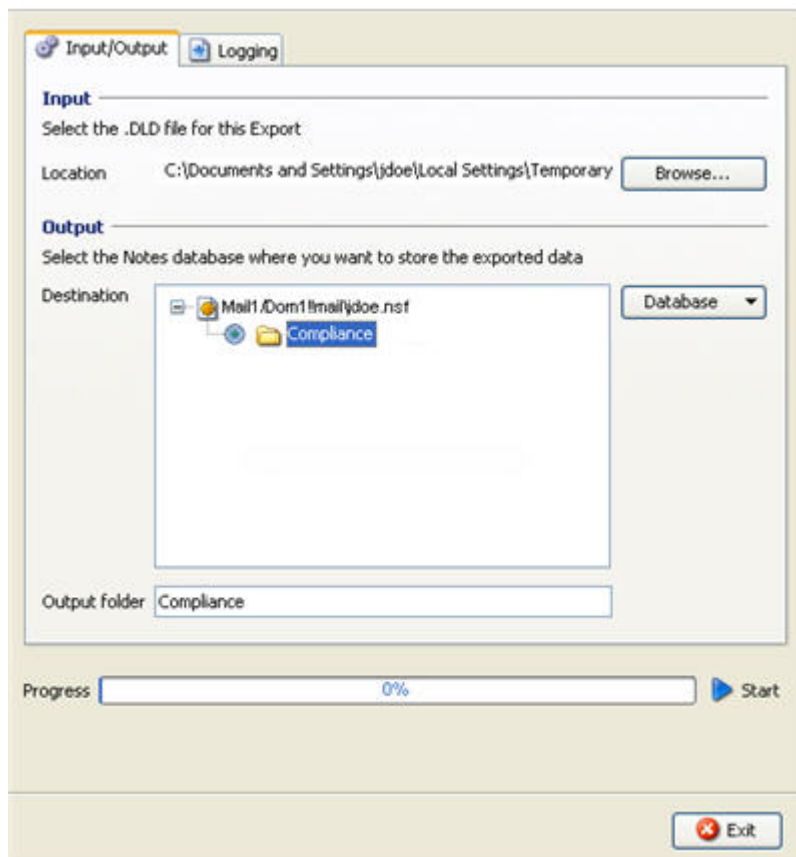
The file download dialog box appears.
 - f. Click **Open** to open the DLD file.

If you receive an error message, see [“Troubleshooting Export Search \(desktop tool\)”](#) on page 331 for information on solving the problem.
3. Enter the Notes password in the dialog box that appears, and then click **OK**.

The Export Search wizard appears.
4. In the **Output** area, select a Notes database to contain the downloaded messages.

The default database is the local mail database on the client machine.

5. Expand the mail file and select the folder you created in step 1.



6. Click the **Start** arrow next to the progress bar to start the download.
A log appears displaying the download results.
7. Review the log for any errors that might have occurred during the download process.
8. If the log shows a successful download, click **Exit** to close the Export Search wizard.
9. Use Lotus Notes to open the destination database and view the downloaded messages.

Saving query results

If your search returns more than 500 results, save the search results before exporting them. Saving the results allows all messages found in the search to be exported. If you do not save the results, only the current batch of 500 messages will be exported.

Results are saved in the IAP for one week. (The one-week period does not apply to search results that are placed in a legal hold. See "Using quarantine repositories" in the *HP Integrated Archive Platform User Guide* for more information on legal holds.)

To save your results:

1. From the Query Results page, click **More Options**, and then click **Save Current Results**.
The Save Results page is displayed.

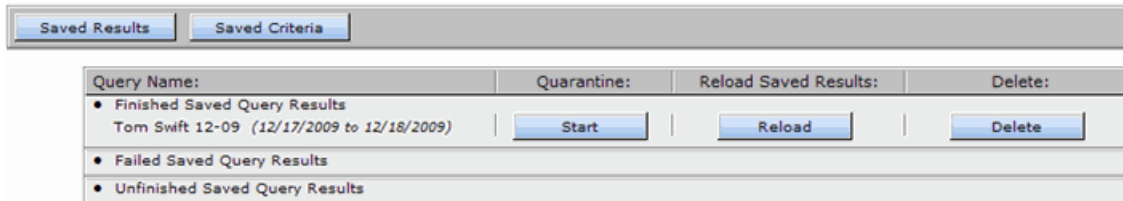
2. Enter the name of the results you are saving in the Save Search Results as field, and click **Save Now!**

The name should not exceed 60 characters.

Special characters @ \$ % ^ & * # () [] / \ { + } ` ~ = | are not allowed.

3. Click **Query Manager** in the Web Interface toolbar.

The default Query Manager page displays all saved results.



4. Select the results to export, and then click **Reload** to load the Query Results page.

Using the server to export messages

Follow the instructions in this section when there are a large number of messages to export.

An Export Search request can be created using the Lotus Notes client (see [“Using the Lotus Notes client to export messages”](#) on page 275) or the Export Search Web Interface (see [“Using the Export Search Web Interface to export messages”](#) on page 279).

Installing server-side Export Search

If you implement server-side Export Search, several files must be installed on the customer server(s) used to process export requests. Instructions are shown in the steps below.

The EAs Domino installer must run on a Windows client.

1. On the customer server, modify the `\Domino\jvm\lib\security\java.policy` file by adding the following entry at the top of the “standard extensions” properties list:

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

Security settings on the Domino server must be modified so that Export Search has permission to load the EAs Domino JAR files needed to interact with the IAP.

2. Open the Domino Administrator client and switch to a Notes ID that can be used to create databases and run restricted and unrestricted agents.
3. In Windows Explorer, navigate to the folder where the EAs Domino installation files were extracted. Locate the `server` directory and double-click the `Setup.exe` file.

4. Use the HP EAs Domino installer to install the EAs Domino databases on the customer server.
Export Search uses the following databases:
 - HP EAs-D API database (`hprim\hp_rissapi.nsf`)
If the mail domain instance of EAs-D API has already been installed on another customer server, replicate it to this server.
 - HP EAs-D Export Search database (`hprim\hp_rissexportsearch.nsf`)
This database contains the agent to process export requests.
 - HP EAs-D Locale Configuration database (`hprim\hp_localcfg.nsf`)
This localization database stores messages in a user's native language for Web-based export requests.
5. Set the access permissions for the EAs Domino databases.
See “[Setting ACL for Export Search](#)” on page 273.
6. If users will create Web-based export requests, configure the Export Search Destination document and the Export Search Template document in the EAs-D API database.
See “[Configuring the Export Search documents](#)” on page 280.
7. Schedule and enable the Export Search agents.
See “[Running the Export Search agents](#)” on page 285.
8. Restart the Domino server.
9. If users will create Web-based export requests, send them a link to the Export Search request form:
http://Domino-server-address-or-hostname/hprim/hp_rissexportsearch.nsf/EXPSEARCH?OpenForm

 **NOTE:**

Ensure that a template for the destination database is placed on customer servers where users view exported messages. This can be a mail, DWA, journal, or custom database template.

Setting ACL for Export Search

Follow these instructions to set the access for the databases used by Export Search:

1. For the HP EAs-D Export Search database:
 - a. Add the following users and set their access as shown:
 - LocalDomainAdmins (or substitute): **Manager**
Must also have the Admin role and rights to delete and replicate or copy documents.
 - LocalDomainServers: **Manager**
Must also have the Admin role and rights to delete and replicate or copy documents.
 - Export Search users: **Author** with **Create documents** permission
Users are compliance and legal officers, recipients of Export Search request notification email, and other staff determined by the organization. Users can be added with one or more groups.
 - b. Set the default to **Manager**.
Must also have the Admin role and rights to delete and replicate or copy documents.
2. In the HP EAs-D API and HP EAs-D Locale Configuration databases:
 - a. Add the following users and set their access as shown:
 - LocalDomainAdmins (or substitute): **Manager**
Must also have the Admin role and rights to delete and replicate or copy documents.
 - LocalDomainServers: **Manager**
Must also have the Admin role and rights to delete and replicate or copy documents.
 - Export Search users: **Reader**
 - b. Set the default to **Manager**.
Must also have the Admin role and rights to delete and replicate or copy documents.

Using the Lotus Notes client to export messages

Follow these instructions to complete an Export Search request using the Notes client.

Exporting the messages

1. In the IAP Web Interface:
 - a. Search for the relevant messages.

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

The search results are displayed on the Query Results page.
 - b. If there are more than 500 results, follow the steps in “[Saving query results](#)” on page 271.
 - c. On the Query Results page, select the check box next to each message you want to export. Skip this step if you are exporting all items.
 - d. Click **More Options** to open the Options menu.
 - e. To export all search results, click **Export All Items**. To export selected items, click **Export Checked Items**.

The file download dialog box appears.
2. In the file download dialog box, click **Save** to save the DLD file.

The DLD file should be saved in a directory that the server running Export Search can locate. You might want to create a network directory especially for these downloads.

Extracting the messages

To extract the messages to a mail database:

1. Using the Notes client, open a new Export Search request form using one of the following methods:
 - Open the HP EAs-D Export Search database in the `hprim` folder on the Domino server and click **New Export Search Request** at the top of the view.
 - Open the HP EAs-D API database, click **Export Search Req** in the left menu, and then click **New Export Search Request** at the top of the view.



The Export Search Request form appears.

- Complete the fields in the **IAP & DLD File** tab:

IAP & DLD File	Destination	Notification	Request Log
IAP host name / IP Address <input type="text" value="15.000.000.000"/>			
DLD file(s)  compliance_1-15-10.dld (Attach DLD file here)			

Field	Description
IAP host name/IP Address	Click the arrow, select the IAP hostname or IP address, and then click OK . This is the virtual IP address listed in the Server Definition document in the HP EAs-D API database.
DLD file(s)	Drag and drop the DLD file from the location where it was saved to this field.

- Click the **Destination** tab and complete the fields as shown below. The information in this tab determines where the exported messages are sent. The settings to be completed depend on the Destination Option that you select.

Destination Options	<input type="radio"/> Append data to an existing db <input checked="" type="radio"/> Create a new db <input type="radio"/> Create only if db does not exist
Domino Server	<input type="text" value="Server 1/Org1"/>
Database filename	<input type="text" value="Compliance/compliance_2010.nsf"/>
Folder name	<input type="text" value="Bennett_John"/>
New Database Title	<input type="text" value="Compliance 2010"/>
Database Design to Template (NTF)	<input type="text" value="mail85.ntf"/>
Database will inherit from Template	<input checked="" type="radio"/> yes <input type="radio"/> No

Field	Description
Destination options	<p>Choose whether to add the messages to an existing mail database or create a new database.</p> <ul style="list-style-type: none"> • Append data to an existing db Add the exported messages to a mail database that currently exists. • Create a new db Create a new mail database to hold the exported messages. • Create only if db does not exist Create a new mail database for the exported messages only if a database does not currently exist.
Domino server	<p>Click the arrow and select the name of the server where the mail database is located.</p> <p>Note: Make sure that users have access to this server and database so they can view the exported messages.</p>
Database filename	<p>Enter the name of the new or previously-created database, including the directory in which it is located.</p>
Folder name	<p>Enter the name of the mail file folder in which the messages will be extracted.</p>
New Database Title	<p>If you are creating a new database, enter the database title.</p>
Database Design to Template (NTF)	<p>If you are creating a new database, enter the name of the database template that is being used.</p>
Database will inherit from Template	<p>Click Yes.</p>

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

The notification email informs you (and any other recipients that are selected) when the exported messages are ready to be viewed. The email includes a link to the mail database containing the messages.

From/Sender Name	Administrator/Org1
Recipients	Org1 Compliance Users
Subject	EAsD to Domino Export Search notification
Hot Spot text for Database link	Double click to access to the EAsD Export Lotus Notes database
Additional Body text	Export Search is complete.

Field	Description
From/Sender Name	This field is automatically populated with the username of the Notes ID configuring the request.
Recipients	Add recipients by clicking the arrow, choosing one or more names from the list, and then clicking OK .
Subject	This box shows the text that will appear as the email subject. You can change the subject line from the default.
Text for Destination DB Link	This is the text for the live link to the exported messages. You can change the text from the default.
Additional Body text	Add any comments for the body of the message. For example, if the messages are exported into a new folder in the database, you can mention that the link will open the database to the Inbox and recipients must open another folder.

- Select **Save & Close** to save the request.

The request will be executed according to the schedule set for the Export Search agent. See ["Running the Export Search agents"](#) on page 285.

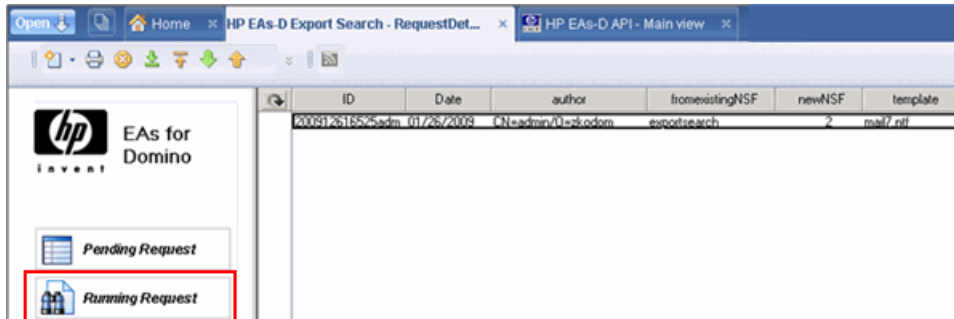
The **Request Log** tab shows the start and end time of the export, the number of URLs (DLD links to archived messages that were downloaded), and the total size of the export. Do not edit this tab.

You can limit the time that export requests are kept. See “[Removing requests from the Export Search log](#)” on page 285 for more information.

Editing or rerunning an export request

You can edit the settings in an Export Search request if the request is still running:

1. Using the Notes client, open the Export Search database.
2. Click **Running Request** in the left menu.
3. Open the running request.



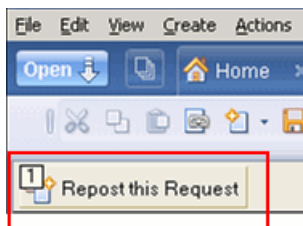
4. Double-click **break job** in the upper left corner of the request form.



5. Change the relevant settings and then repost the request.

Failed search requests can be reposted for processing by following these steps:

1. In the Export Search database, click **Request in Error** or **Request Cannot Start** from the left menu.
2. Open the request and double-click **Repost this Request**.



Using the Export Search Web Interface to export messages

The Export Search request can also be completed via a Web browser if the EAs Domino files are installed on a Domino Web server. Web-based exports download search results into a database in specially-designated network directories. When this method is used, two documents must be configured in the HP EAs-D API database.

Configuring the Export Search documents

1. In the Administrator client, open the HP EAs-D API database.
2. Open the Export Search Destination document, which is located in the Export Search area of the API main view.

This document is used to configure the server and directories that are allowed for message export.

3. Configure the destination server and directory settings, and then click **Save & Close**.

Export Search Allowed Directories

Destination Server	Server1/Org1 ▾
Destination Directories	Compliance_export1 Compliance_export2 Compliance_export3 ▾

- Destination Server: Click the arrow and select the server from the Domino Directory.
 - Destination Directories: Enter the name of the directory or directories where users can create mail databases to hold exported messages.
4. If an additional destination server will be used, create a new Destination document for the server by selecting **Create > Export Search > Destination Directories** in the EAs-D API main view.
 5. Open the Export Search Templates document in the EAs-D API main view.
This document lists the allowed Templates for Export Search Destination Database creation.
 6. In the Export Server Templates field, enter the allowable templates for the databases into which the messages will be exported. Use the format:
Template Title|Template Filename.ntf
For example: Mail(R8)|mail8.ntf

Creating the Export Search request

To create a search request, perform the following steps from the Web browser:

1. In the IAP Web Interface:
 - a. Search for the relevant messages.
If the search is a complex one, use the Advanced Search instructions in the *HP Integrated Archive Platform User Guide*.
The search results are displayed on the Query Results page.
 - b. If there are more than 500 results, follow the steps in “[Saving query results](#)” on page 271.
 - c. On the Query Results page, select the check box next to each message you want to export. Skip this step if you are exporting all items.
 - d. Click **More Options** to open the Options menu.
 - e. To export all search results, click **Export All Items**. To export selected items, click **Export Checked Items**.
 - f. In the file download dialog box, click **Save** to save the DLD file in a directory that has been designated for this purpose.
 - g. Log out of the IAP Web Interface.
2. Log in to the Export Search server.
3. In the menu, click **Create Export Request**.
The Export Request form appears.
4. Complete the settings in the IAP & DLD file area of the form.

Field	Description
IAP host name/IP Address	This field should already be populated. If it is not, click the arrow and select the IAP.
DLD File	Browse for the DLD file you saved in step 1f and click Open .

5. Complete the settings in the Destination Database area of the form.

This information determines where the exported messages are sent. The settings to be completed depend on the Destination Option that you select.

Messages can only be exported to mail databases in the specially-designated network directories.

Destination Database	
Destination Options	<input type="radio"/> Append data to an existing db <input checked="" type="radio"/> Create a new db <input type="radio"/> Create only if db does not exist
Server <input type="button" value="Select"/>	<input type="text" value="Server1/Compliance_export1"/>
Database filename	<input type="text" value="Compliance_2010.nsf"/>
Folder name(optional)	<input type="text" value="Bennett_John"/>
New Database Title	<input type="text" value="Compliance 2010"/>
DB Design to Template	<input type="text" value="mail85.ntf"/>
DB will inherit from Template	<input type="radio"/> yes <input checked="" type="radio"/> no

Field	Description
Destination options	<p>Select one of the following options:</p> <ul style="list-style-type: none"> • Append data to an existing db Add the exported messages to a mail database that currently exists. • Create a new db Create a new mail database to hold the exported messages. • Create only if db does not exist Create a new mail database for the exported messages only if a database does not currently exist. Users can select this option if they are not certain about the name of an existing mail database.
Server	<p>Click Select, select the server and directory where the archived messages will be exported, and click OK. The choices in this field are determined by the allowed directories configured in “Configuring the Export Search documents” on page 280.</p>
Database filename	<p>Enter the name the of the mail database to hold the exported messages. This can be the name of a previously-created database, or the name for a new database.</p>
Folder name (optional)	<p>If you want, enter the name of a mail folder to which the messages will be extracted. If a folder name is not entered, the messages will be exported into the All Documents view.</p>
New Database Title	<p>If you are creating a new database, enter the database title.</p>
DB Design to Template	<p>If you are creating a new database, click the arrow and select a template for the database. The choices in this field are determined by the Export Search Templates document. See “Configuring the Export Search documents” on page 280.</p>
Database will inherit from Template	<p>If you are creating a new database, click Yes.</p>

6. Complete the settings in the Notification area of the form.

The notification email informs you (and any other recipients that are selected) when the exported messages are ready to be viewed. The email includes a link to the mail database containing the messages.

The screenshot shows a 'Notification' form with the following fields and values:

- From/Sender Name:** Jack Smith/Org1
- Recipient:** A dropdown menu with a 'Select' button, currently showing 'Compliance Officers/Org1'.
- Subject:** EAsD to Domino Export Search notification
- Text for Destination DB Link:** Double click to access to the EAsD Export Lotus Notes database
- Additional Body Text:** A text area containing: 'Export Search is complete. The exported messages are located in the Bennett_John folder.'

Field	Description
From/Sender Name	This box displays your username.
Recipients	Your username is automatically listed in this box. To add other recipients, click Select , choose one or more names from the list, and then click OK .
Subject	This box shows the text that will appear as the email subject. You can change the subject line from the default.
Text for Destination DB Link	This is the text for the live link to the exported messages. You can change the text from the default.
Additional Body text	Add any comments for the body of the message. For example, if the messages are exported into a new folder in the database, you can mention that the link will open the database to the Inbox and recipients must open another folder.

The amount of time before the messages are exported, and email recipients notified, depends on the schedule that is set for the Export Search and PopulateFolderFiles agents.

7. Click **Submit** when the form is complete.
8. Export requests can be edited if they are in running status:
 - a. In the menu, click **Running Requests**.
 - b. Click the request to open it for editing.
 - c. Click **Edit Document**.
 - d. Make the necessary changes, and then click **Submit**.

Completed export jobs can be viewed by clicking **Success Requests** in the menu and viewing the Results area at the bottom of the form.

Export jobs that have encountered problems are listed in **Request in Error** in the menu.

Export requests that are missing information the Export Search agent needs to start processing are placed in **Request cannot start**.

Running the Export Search agents

Three agents in the HP EAs-D Export Search database must be scheduled and enabled:

- Export Search agent
- PopulateFolderFiles agent (only used with Web browser option)
- Purge_Documents agent

Export Search agent

The Export Search agent executes the Export Search request. It retrieves the archived messages referenced in the DLD file and exports the messages to the mail database configured in the search request. This agent must be enabled, using the Designer client.

By default, the Export Search agent is set to run every hour. You can change the schedule, using the instructions in [“Scheduling the Export Search agents”](#) on page 286.

You can also run the agent manually from the server console with the command:

```
tell amgr run "hprim\hp_rissexportsearch.nsf" `export search`
```

PopulateFolderFiles agent

The PopulateFolderFiles agent works with the Web-based export tool. It picks up the allowable server and directories configured in the Export Search Destination document, and the database file and folder information entered in the Export Search requests, to create a list of folders and files where messages can be exported. This list is used with the “Appending data to existing db” option in the export request. The PopulateFolderFiles agent must be scheduled and enabled, using the Designer client.

By default, the agent is set to run every six hours. You can change the schedule to have the agent run more frequently by using the instructions in [“Scheduling the Export Search agents”](#) on page 286.

You can also run the agent manually from the server console with the command:

```
tell amgr run "hprim\hp_rissexportsearch.nsf" `PopulateFolderFiles`
```

Removing requests from the Export Search log

The Purge_Document agent is used by the Export Search application to remove Export Search requests that are older than a certain number of days. By default, requests that are more than 30 days old are removed.

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

1. Using the Domino Administrator client, open the HP EAs-D Export Search database in the `hprim` folder on the Domino 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.
If PURGE_DOCUMENT is not displayed, follow the instructions below in [Adding the Agent\Parameters document](#).
5. Double-click the value in **Arg1: Number of Days** and change the number of days.
Do not change the Form Name value in Arg2.
6. Click **File > Save**, and then close the document.

Adding the Agent\Parameters document

If the Agent\Parameters document is not displayed in the HP EAs-D Export Search database, follow these instructions to create the document:

1. Using the Domino Administrator client, open the HP EAs-D Export Search database in the `hprim` folder on the Domino server.
2. In the menu, select **Create > Agent > Parameters**
3. Complete the fields in the document that appears:
 - a. For Agent name, enter **PURGE_DOCUMENT**.
 - b. For Arg1, enter **Number of Days**.
 - c. For the Arg1 Value, enter the number of days that Export Search requests should be kept.
 - d. For Arg2, enter **Form Name**.
 - e. For the Arg2 Value, enter **AGENT_LOG**.
4. Click **Close**, and then click **Yes** to save the document.

Scheduling the Export Search agents

Follow these instructions to schedule and enable the agents in the Export Search database:

1. In the Domino Designer client, open the HP EAs-D Export Search database in the `hprim` folder on the server used for search requests.
2. In the Design pane, select **Code > Agents**.
3. Double-click the agent.
4. In the agent Properties, make sure the Trigger is set to **On schedule**.

5. If necessary, change the default schedule for the agent:
 - Export Search agent:
The default runs the agent every hour
 - PopulateFolderFiles agent (only used with Web browser option):
The default runs the agent every six hours.
 - Purge_Documents agent:
The default runs the agent once a day at 1:00 a.m.
6. Select the server in the Where agent runs box.
7. Click **OK** to save the settings and close the agent Properties.
8. Click **Enable** to enable the agent.

5.3 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 Lotus 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.

- [Creating the HP EAs-D SSO database](#), page 289
- [Configuring the HP EAs-D SSO database and the Generate SSO Tokens agent](#), page 290
- [Configuring The Search the IAP Archive agent](#), page 294
- [“Configuring SSO on the IAP”](#) on page 297
- [Configuring the client computers](#), page 298

Creating the HP EAs-D SSO database

Copying the templates

Before you begin:

1. Copy the HP EAs-D SSO template (`hp_sso.ntf`) from the `Templates` directory on the installation media to the data directory in a Notes client. (For example, `C:\Program Files\lotus\notes\data`.)

This template is 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.

2. (Optional) Copy the following template from the installation media to the Notes client data directory:

HP EAs-D Mail (R6) with SSO (`hp_ssomail_sample.ntf`)

This template contains customized design elements that can be added to mail templates to create a link from users' mail files to the IAP. (These customized elements cannot be used with DWA templates.)

Creating the database

To create the HP EAs-D SSO database:

1. Ensure that HP EAs-D SSO (`hp_sso.ntf`) has been copied from the `Templates` directory on the installation media into the root data directory of the Notes client.
2. Open the Notes client and switch to an ID that has rights to create databases and run unrestricted agents on Domino servers in the mail domain(s).

3. Select **File > Application > New**.

The New Application window appears.

4. Create the HP EAs-D SSO database:

- a. In the **Server** box, specify the name of the 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 that participate in the SSO configuration.

- 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 294.

The Search the IAP Archive agent is only used in mail templates. If users access mail solely via DWA, you can name the file whatever you choose. For example, `hp_sso.nsf`.

5. Specify the template for the HP EAs-D SSO database:

- a. In the **Server** box, leave **Local** as the server.

- b. In the **Template** box, select **HP EAs-D SSO**, and then click **OK**.

6. In the **File** menu, select **Application > Access Control**.

7. Perform these steps to set the access control list (ACL):

- a. Configure the following settings for LocalDomainServers:

- For Access, select **Manager**.
- Select the **Replicate or copy documents** check box.
- In Roles, select the **RIM SSO Admin** check box.

- b. If all members of the LocalDomainAdmins group are trusted with SSO information, enter that group into the ACL, give it Manager rights with the RIM SSO Admin role, and select the **Replicate or copy documents** check box.

As an alternative, identify a group with a smaller list of members who are trusted with SSO information and enter that group instead.

- c. Click **Add** and add **Anonymous** to the ACL with access set to **No Access**.

- d. Set the Default access level to **Reader**.

- e. Click **OK** when all changes to the ACL are complete.

8. Close the database.

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

1. Start the Domino Administrator client and open the server on which the SSO database was created.

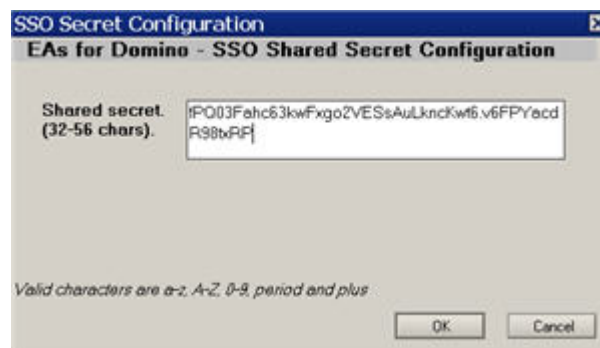
2. Perform the following steps to sign the HP EAs-D SSO database:
 - a. Click the **Files** tab.
 - b. In the **Show me** box, select **Databases only**.
 - c. Select the HP EAs-D SSO file.
 - d. With the file selected, right-click and select **Sign** from the context menu.
 - e. In the dialog box, select the Active User's ID or Active Server's ID and **All design documents**, and then click **OK**.
3. In the Notes client, open HP EAs-D SSO.
The following window appears.



4. Configure the SSO Shared Secret:
 - a. Click **Configure SSO Shared Secret**.

A sample secret is displayed.

Change the sample 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 297.)

- b. Click **OK** to save the secret.

5. 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**.

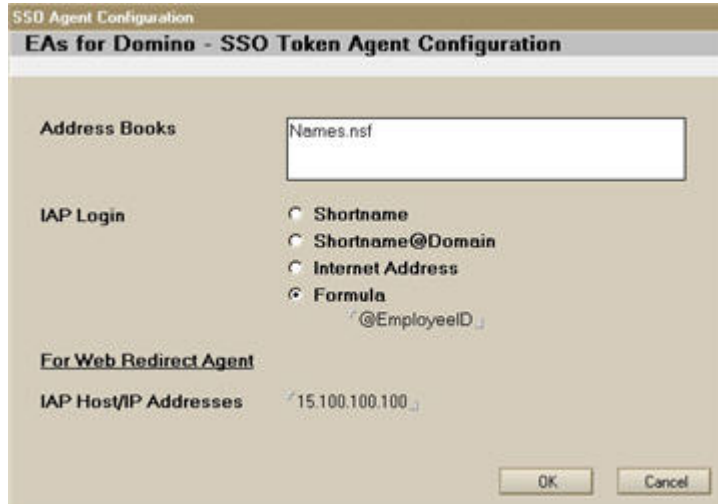
You will use the XML file as a reference when performing the IAP configuration for SSO (see step 2 in [“Configuring SSO on the IAP”](#) on page 297).

ⓘ **IMPORTANT:**

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

6. 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 IAP SSO.
The filenames should be separated by commas.
- b. In **IAP Login**, select the type of login used to access the IAP Web Interface.
- **Shortname:** Log in using the Notes ShortName.
 - **Shortname@Domain:** Log in using the ShortName and the mail domain.
 - **Internet Address:** Log in using the full email address (InternetAddress).
 - **Formula:** Log in using another field or fields from the consolidated directory.
The formula you enter must correspond to the IAP UID Mapping formula in the DAS Configuration document. (See “[Directory Entry Settings](#)” on page 91.) Do not enter the entire formula – only the value substituted for ShortName. For example, if the substituted value was EmployeeID, enter @EmployeeID.

The login type needs to work with the **LDAP Attribute to Map to Username** field in the DAS job configuration form. See “[Modifying the username mapping](#)” on page 298.

Additionally, if you select Internet Address as the login type, complete the steps in “[Modifying the Search The IAP Archive agent](#)” on page 296.

- c. In **IAP Host/IP Addresses**, enter the IAP hostname or virtual IP address used to perform the authentication.
- d. Click **OK**.

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

7. In the Designer client, open HP EAs-D SSO.
 - a. In the Code pane, click **Agents** and then open the **Generate User Tokens** agent.
 - b. Ensure that **On schedule** and **Daily** are selected in the Runtime area.
 - c. Click the **Schedule** button and select the server(s) where the agent will run.
 - d. Ensure the execution time is set close to 12:00 AM (for example, 12:05 AM).
 - e. Click **OK**.
 - f. Enable the agent.
8. Create replica copies of the SSO database 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.

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

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

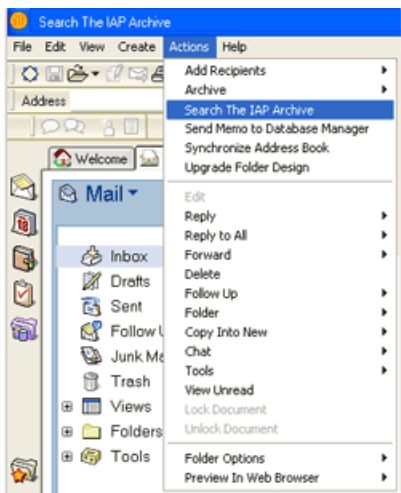
(where `rimsso.nsf` is the name of the SSO database)

Configuring the Search The IAP Archive agent

(Use only with mail database templates)

The HP EAs-D Mail (R6) with SSO template file (`hp_ssomail_sample.ntf`) is a modified version of the Lotus Domino 6 mail database template. The EAs-D SSO code in this template also works on Domino 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 SSO Mail Sample 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 SSO Mail Sample into individual user mail files for test purposes.
2. (Optional) Translate and develop alternative customizations (such as modified framesets, outlines, or smarticons) 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 modified mail file(s), using **File > Application > New Copy** from the Notes client menu. Deploy those templates 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](#). Standard Lotus Notes development and administration techniques should be used for steps 2 and 3.

Copying design elements from the template

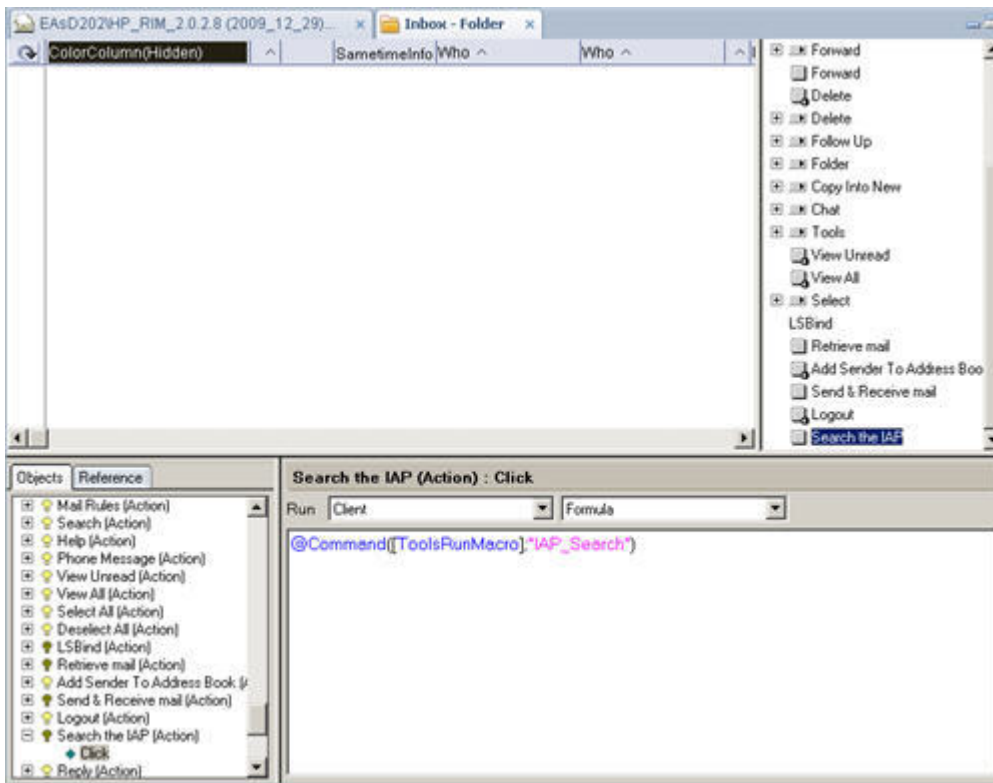
1. In the Designer client, open the following files:
 - HP EAs-D SSO Mail Sample (`hp_ssomail_sample.ntf`)
 - A user mail file
2. In the Code section of `hp_ssomail_sample.ntf`, open the Agents list and copy the Search The IAP Archive agent to the clipboard.
3. In the Code section of the user mail file,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

📝 **NOTE:**

If you changed the `rimssso.nsf` file name in “[Creating the HP EAs-D SSO database](#)” on page 289, 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 rimssso.nsf database on server**.

4. Expand the Folders section of `hp_ssomail_sample.ntf`, and then open the \$Inbox folder.

5. Open the Action pane, select the **Search The IAP** action, and copy the action to the clipboard.



6. Open the Folders section of the user's mail file, and then open the \$Inbox folder.
7. Open the Action pane, place your cursor inside the pane, and paste the Search The IAP action.
8. If you want, drag and drop the action to reorder within the sequence.

Note that the code for this action is a simple Notes @Function, which can be used 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 6 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 Code section of the user's mail file, open the Agents list and select the Search The IAP Archive agent.

2. Open the agent and in the Initialize section:

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, as shown below.

```
Initialize
Sub Initialize

.....
' Choose one of the following two statements to determine whether
' the code will prepopulate the InternetAddress or ShortName field
' onto the RISS Web UI login form.

'gConfigLoginItem = ITEM_INET_ADDR
'gConfigLoginItem = ITEM_SHORT_NAME

..... END CHOICE .....
```

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.

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 you exported earlier. (See step 5 in [Configuring the HP EAs–D SSO database and the Generate SSO Tokens agent](#)). Be sure to include only the secret key and datestamp text that is located in between the `<RIMSSO version="1.6">` and `</RIMSSO>` tags in the XML file. Do not include the text of the XML tags.

The example below shows the text in the XML file to be used for the SSO key.

```
<?xml version="1.0" encoding="utf-8"?>
<RIMSSO version="1.6">
FPQ03Fahc63kwFxqp2VESSAuLkncKwt6.v6FPYacdR98txRP20100826
</RIMSSO>
```

This example shows the correct insertion of the key into the `SSO_DOMINO.archive` file.

```
KEY:FPQ03Fahc63kwFxqp2VESSAuLkncKwt6.v6FPYacdR98txRP20100826
```

3. Navigate to the `/install/tools/registry/bin` directory and run the RegistryLoader using the following command:

```
regloader.pl -l
```

IAP 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 username mapping

Perform the following steps so that the IAP Login in the SSO Token Agent Configuration (step 6 in [Configuring the HP EAs–D SSO database and the Generate SSO Tokens agent](#)) matches the username mapping in the IAP.

1. Stop the current DAS job:
 - a. Log in to IAP PCC Web Administration and navigate to **User Management > Account Synchronization**.
 - b. In the DAS Available Jobs area of the Account Synchronization page, select the job and click **Stop**.
2. Select the DAS job and click **Edit**.
3. In the Mapping Information form, expand **Advanced Options**.
4. Locate the **LDAP Attribute to Map to Username** field at the bottom of the form.
5. Verify that the value in this field is correctly set for the IAP Login type:
 - **uid**: Use this value if the login type is Shortname, Shortname@Domain, or Formula.
 - **mail**: Use this value if the login type is Internet Address.
6. Click **Update**.
7. 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**.

5.4 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 Domino 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 mail accounts. These functions do not require software to be installed on client systems. A link to the Web Interface can be added in users' mail files.
- **Export Search:** Messages can also be exported from the IAP Web Interface into standard Notes databases. This feature is used primarily for legal or compliance purposes.
- **Local Cache:** A message 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 from Lotus Notes. The plug-in can be used in conjunction with Local Cache.
- **DWA Extension:** Software can be installed on DWA servers so that users can access archived messages in DWA.

These methods are explained in the following sections:

- [Using the IAP Web Interface](#), page 299
- [Creating a link in the Notes navigation pane](#), page 300
- [Using Local Cache](#), page 301
- [Using the Windows Notes Client Plug-In](#), page 308
- [Using the Windows Notes Client Plug-In with Local Cache](#), page 311
- [Adding the tombstone icon](#), page 312

For information on using the Export Search utility, see [“Using Export Search”](#) on page 269.

For information on setting up DWA Extension, see [“Configuring DWA Extension”](#) on page 255.

For information on the client operating systems that EAs Domino supports, see [“Supported Lotus Notes clients”](#) on page 38.

For information on working with signed and encrypted messages, see [“Retrieving and viewing encapsulated messages”](#) on page 313.

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 mail account.

The Web Interface portal is set up during IAP 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: Microsoft Internet Explorer version 7.x or 8.x or Mozilla Firefox version 3.x.

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: Virtual IP address of the IAP domain (configured in `Domain.jcml` on the IAP)
- Login:
 - Username: This can be the user's Notes Shortname, Shortname@MailDomain, or InternetAddress from the Domino Directory.
The value is set in the IAP DAS job advanced options, in the LDAP Attribute to Map to Username field. See “[Creating DAS jobs](#)” on page 372.
 - Password: The value is taken from the InternetPassword field in the user's Domino Directory Person document.
- 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 used primarily by compliance officers to export a large number of messages to a Notes database. For information on exporting email, see “[Using Export Search](#)” on page 269.

Creating a link in the Notes navigation pane

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

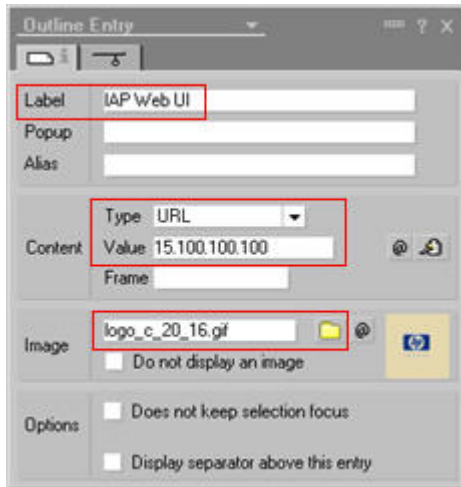
Use these instructions to create a link from Lotus Notes to the IAP Web Interface. This link must be created using a Windows client.

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 Domino server.
2. In the Design pane, expand **Resources**.
3. Right-click **Images**, select **New Image Resource**, and then select a graphic to use as an icon for the link.
4. In the Design pane, expand **Shared Elements**, expand **Outlines**, and then open **NotesMailOutline**.
5. Click **New Entry**.

6. Complete the following fields in the Outline Entry dialog box:
 - a. In the **Label** field, enter a name for the link.
 - b. In the **Type** list, select **URL**.
 - c. In the **Value** field, enter the URL or virtual IP address for the IAP Web Interface (the IAP domain).
 - d. Click the Folder icon in the **Image** area.
The Insert Image Resource dialog box is displayed.
 - e. Select the Image Resource you created in step 3, and then click **OK**.



7. Close the dialog box and save the outline. Click **Yes** to save the link.

Setting up single sign-on

See “[Configuring IAP single sign-on](#)” on page 289 to set up IAP single sign-on for Lotus Notes and the IAP Web Interface.

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 who are traveling with a laptop computer.

When client machines are online, users can pull 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 messages that are stored 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 a tombstoned 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 the Notes plug-in for no-click retrieval of messages. See [“Using the Windows Notes Client Plug-In with Local Cache”](#) on page 311.

During installation, Local Cache creates a Local Cache destination database (DefaultLCDestination.nsf) in the client system's \notes\data directory. This database holds the cached messages. It can be configured to set the message retention period, cache size, and other parameters.

Installing Local Cache

The Local Cache installer installs the Local Cache (LocalCache.exe) and the Export Search (ExportSearch.exe) applications into 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 client. You might need to manually add the program to the system variables path. (See [“Installing Java Runtime Environment”](#) on page 48.)

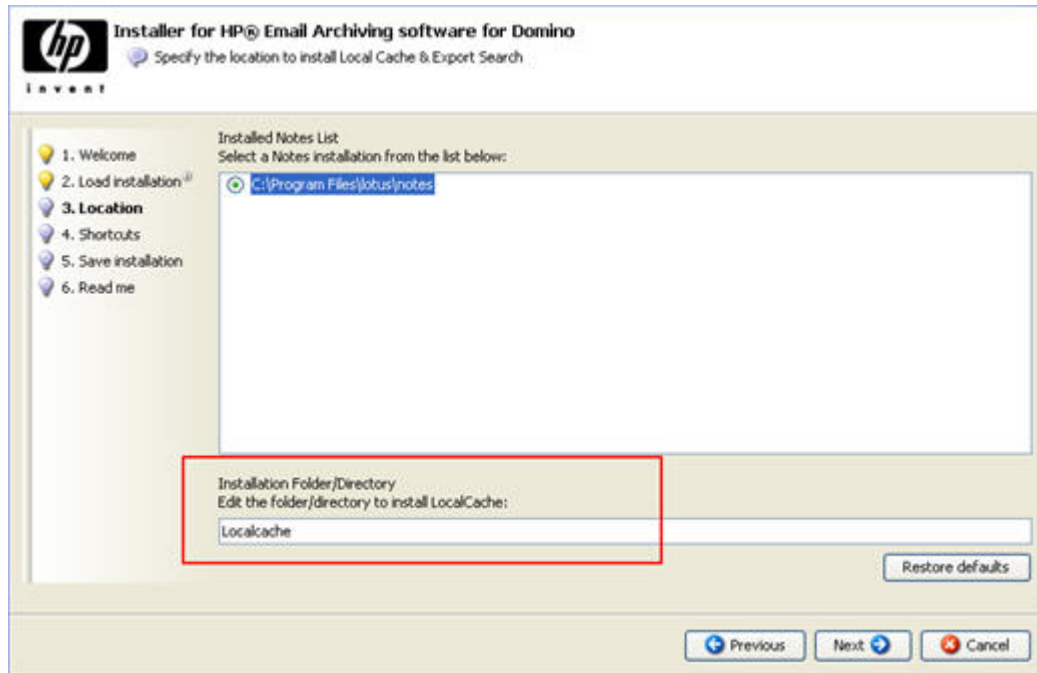
To install Local Cache on the client system:

1. Navigate to the client\Local Cache & Export directory on the installation media and double-click the Install.exe file.
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.

The Installation folder box displays the name of the Local Cache folder: Localcache.



4. Click **Next**.
5. 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.
6. 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 want to save the installation base, click **Next**.
7. 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.
8. Click **Install**.

The installation actions are displayed on screen.
9. 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\Localcache folder.



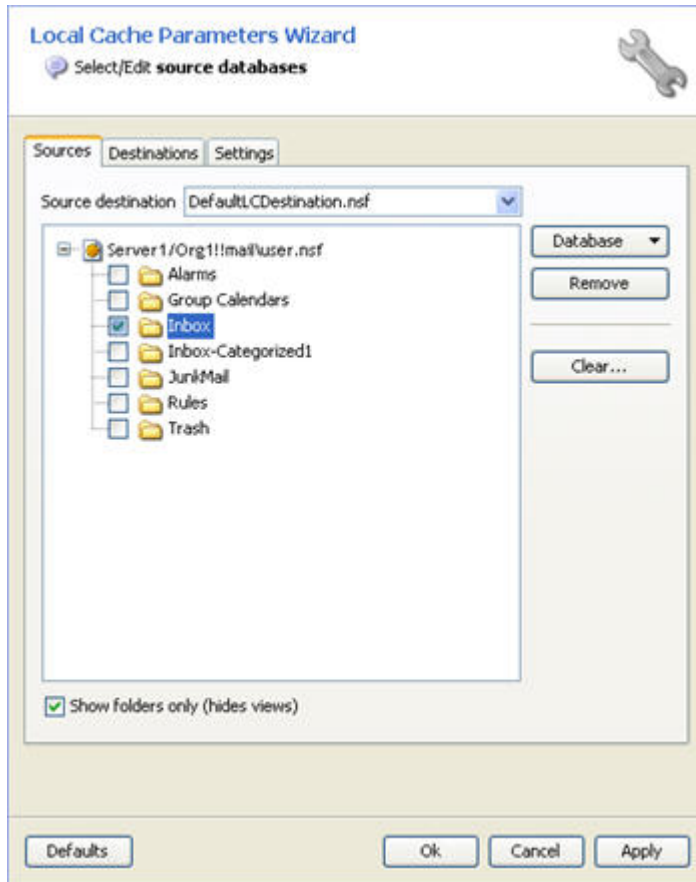
2. Open the **Options** drop-down list and select **Settings**.

The Local Cache Wizard appears.

3. On the **Sources** tab, click **Database**, select **Open**, and then browse to the user's live mail file on the mail server.

A confirmation dialog box appears.

4. In the confirmation dialog box, click **Yes** to create a default cache database (the destination database) on the user's machine.
5. The Local Cache destination database (`DefaultLCDestination.nsf`) appears on both the Sources and Destinations tabs. This is the database used for caching tombstoned messages retrieved from the IAP.
6. On the **Sources** tab, select the **Show folders only** check box, and then expand the user's mail file.
7. Select the mail folder(s) where the tombstoned messages are displayed, and click **Apply**.



8. Click the **Settings** tab and configure the cache:

The screenshot shows the 'Local Cache Parameters Wizard' dialog box with the 'Settings' tab selected. The dialog has three tabs: 'Sources', 'Destinations', and 'Settings'. The 'Settings' tab is active and contains three sections: 'Updates', 'Purge', and 'IAP'.
- The 'Updates' section has two radio buttons: 'Retrieve messages since last update' (unselected) and 'Only retrieve messages newer than' (selected). Below the second radio button is a spinner box set to '180' and a dropdown menu set to 'Day'. There is also a checked checkbox for 'Always retrieve up to last date time was updated' and another checked checkbox for 'Retrieve messages in background'.
- The 'Purge' section has a checked checkbox for 'Purge messages from local machine'. Below it are two rows: 'If older than' with a spinner box set to '180' and a dropdown menu set to 'Day'; and 'If cache size greater than' with a spinner box set to '500' and a dropdown menu set to 'M'.
- The 'IAP' section has a dropdown menu for 'IAP domain' set to 'iapdomain', a text box for 'IAP address' containing '15.100.100.100', and an unchecked checkbox for 'Use SSL'.
At the bottom of the dialog are four buttons: 'Defaults', 'Ok', 'Cancel', and 'Apply'.

- a. In the **Updates** area, select the age of the messages to be retrieved. The Local Cache retrieves and caches any tombstoned 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.

You can also choose to retrieve messages in the background.

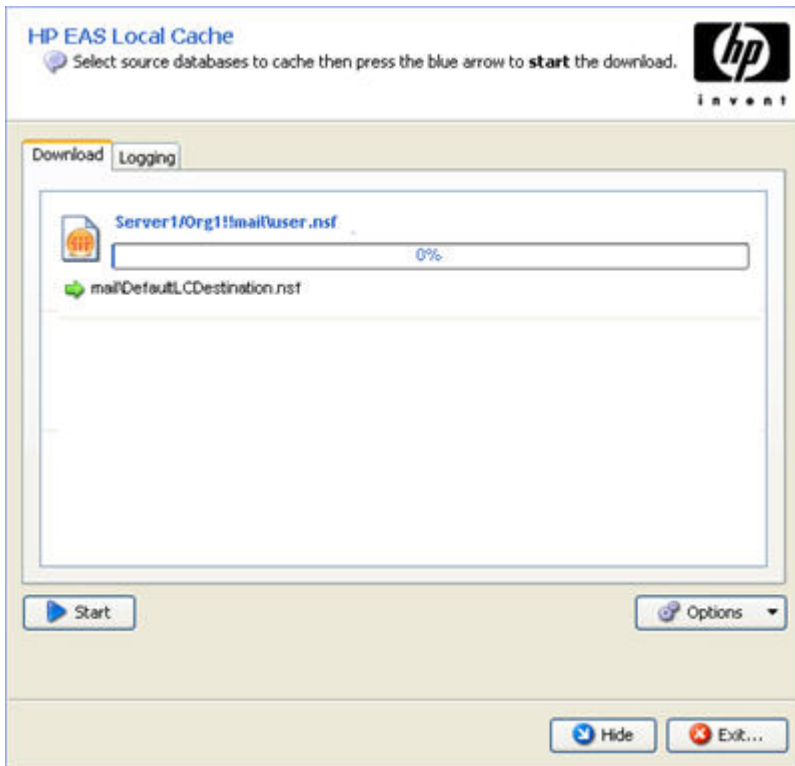
- b. In the **Purge** area, you can limit the scope and size of the cache. Select the **Purge messages from local machine** check box and enter a cutoff time and maximum cache size. Both options must be set.

The 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. Enter the IAP domain name and VIP address in the **IAP** area.
d. Make sure the **Use SSL** check box is not selected.

9. Click **OK**.

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







10. To use Local Cache:

- a. Click **Start** to import the archived messages 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 you choose to hide Local Cache, the icon remains in the system tray. Local Cache is closed automatically when you log out of Windows.

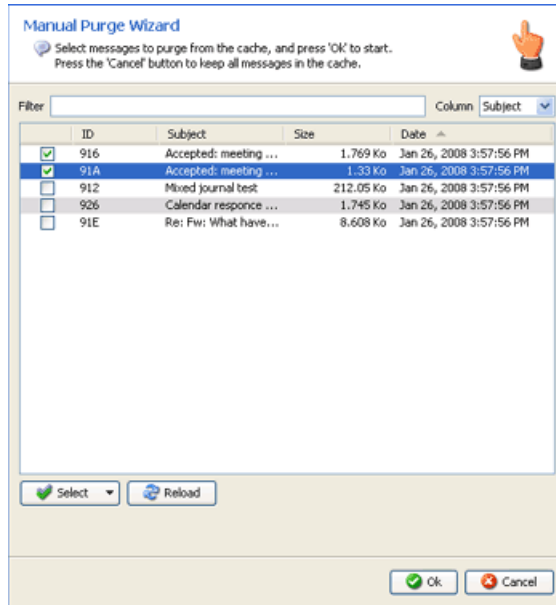
Deleting messages from the cache

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 message 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 so that users can automatically retrieve tombstoned messages in Lotus Notes. The plug-in can be installed on its own or, for mobile users, installed with Local Cache.

The plug-in gives users instant access to tombstoned messages when their computer is connected to the network. When they select a message, its content appears automatically.

The process works in a somewhat different way when the plug-in is installed with Local Cache. For more information, see [“Using the Windows Notes Client Plug-In with Local Cache”](#) on page 311.

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 mail 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:

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

To configure the installer:

1. Create a plug-in installation directory on your local hard drive.
2. Copy the `MakeNhpClientMSI` directory from the installation media to the new directory on your hard drive.

The directory contains the following items:

- `BinMakeMsi` (folder)
 - `NhpClientMsi` (folder)
 - `NhpClientSourceMsi` (folder)
 - `MakeNhpClientMsi.bat` (batch file)
3. Navigate to the `NhpClientSourceMsi` folder in the installation directory you created.
 4. Open `variableInstallation.ini` in a text editor.

5. 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 the 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 the <code>notes.ini</code> file.
HCLIENT_FROM_DOMAINTOREMOVE	This variable removes the extraneous FromDomain added to a message during archiving, so it does not appear if 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: HCLIENT_FROM_DOMAINTOREMOVE= EASCPE@usa.hp.com Example of multiple domains: HCLIENT_FROM_DOMAINTOREMOVE= bigcorp.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).
HCLIENT_HTTP_MAX_PLUGIN_FAILURE	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 IAP. 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 the 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 databases used in processing signed or encrypted messages. (See “ Preprocessing overview ” on page 175 for more information about these files.) If you want to keep the encapsulated files for a period of time, enter the number of days they should be kept. The default setting is 2 days.

Variable	Value
HPRIM_KEEP_ALL_ENCAP_FILES	<ul style="list-style-type: none"> • 0 keeps encapsulated files for the amount of time specified in the HPRIM_KEEP_ENCAP_FILE_DAYS variable. • 1 keeps all encapsulated files indefinitely. (Not recommended.) Be sure to keep = 0 after the number of days.
HPRIM_REMOVE_ALL_ENCAP_FILES	<ul style="list-style-type: none"> • 0 removes encapsulated files after the number of days specified in the HPRIM_KEEP_ENCAP_FILE_DAYS variable. • 1 forces the removal of all encapsulated files at Notes shutdown or at the next startup. Be sure to keep = 0 after the entry.
HPCLIENTEXCLUDE= localcache, taskldr, dyncfg, ExportSearch=0	Do not change this entry. It appears when Local Cache is installed in addition to the plug-in.
EXTMGR_ADDINS=hpclient=1	This variable registers the plug-in with the Notes Extension Manager. Do not change this entry.
NOTES_PATH	Do not change this entry, which helps the installation locate the notes.ini file.

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
HPCLIENTEXCLUDE=localcache,taskldr,dyncfg=0
EXTMGR_ADDINS=hpclient=1
NOTES_PATH=C:\Program Files\lotus\notes
```

6. 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.

7. Execute MakeNhpClientMsi.bat to create the installer.

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



NOTE:

Additional variables can be added to troubleshoot the plug-in. See [“Troubleshooting the Notes client plug-in”](#) on page 330.

Installing the plug-in

It is the responsibility of the Domino administrator 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 the `variableInstallation.ini` file.
- 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 Web 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.

Uninstalling the plug-in

Use Add or Remove Programs in the Control Panel to remove the plug-in from a user's system.

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 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, dyncfg=0` variable is listed in the `notes.ini` file. 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 308 for more information.

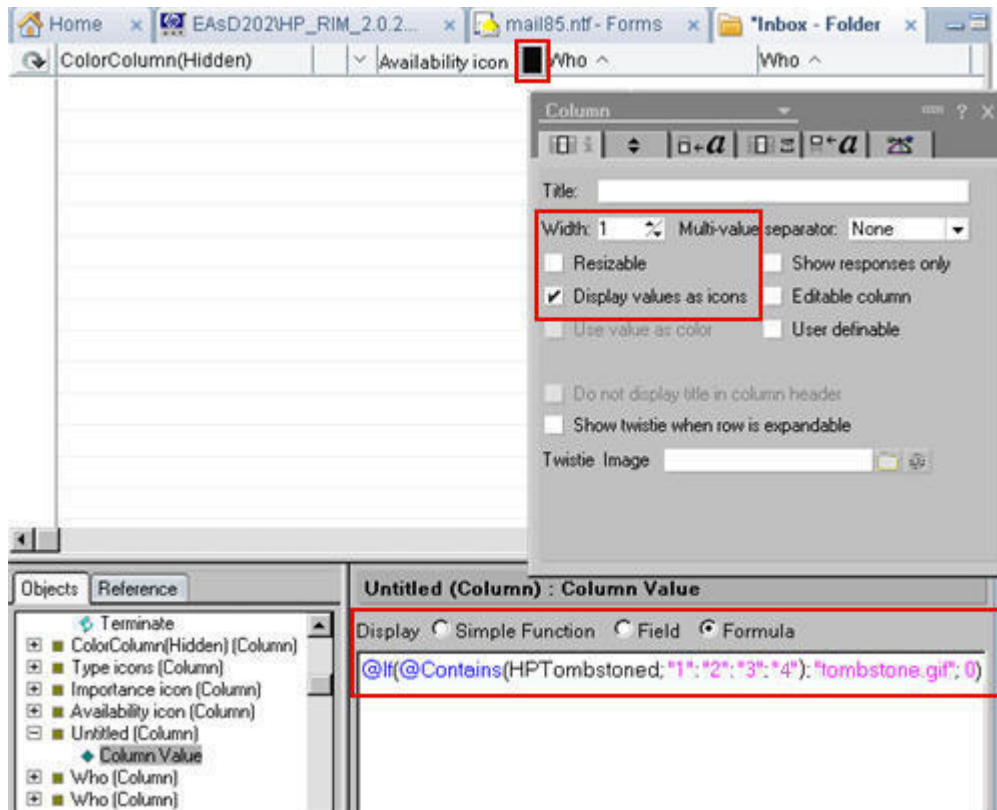
Adding the tombstone icon

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 added using a Windows client.

1. Copy HP EAs-D Shared Objects `hp_sharedobjects.ntf` from the `Templates` folder in the HP EAs Domino installation media to the Notes data directory in the Notes client.
2. In the Domino Designer client, open the Mail template and then open the `hp_SharedObjects.ntf` template.
3. In the left-hand navigation pane of `hp_sharedobjects.ntf`, expand **Resources**, and then expand **Images**.
4. Copy `Tombstone.GIF` and paste it into the Mail template in **Resources > Images**.
5. In the Mail template, select **Folders** in the navigation pane, and then double-click (**\$Inbox**) in the folder list.
6. Select the first **Who** column.
7. From the top menu bar, select **Create > Insert New Column**.
8. Next to the Column Value heading, click **Formula**.
 - a. Delete any existing value in the Column Value field.
 - b. Enter the following formula in the Column Value field:

```
@If(@Contains(HPTombstoned; "1" : "2" : "3" : "4"); "tombstone.gif"; 0)
```
 - c. In the Properties dialog box for the column, change the column width to **1**, clear the **Resizable** check box, and select the **Display values as icons** check box.
(If the Properties dialog box does not appear automatically, select **Design > Column Properties** from the menu.)



9. Close the Properties dialog box, and then click **Yes** to save the changes.

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 will not display the icon.

Retrieving and viewing encapsulated messages

In HP EAs Domino, signed and encrypted messages are encapsulated before they are archived. Several other types of Notes items are also encapsulated, including:

- Calendar notices
- Older messages with broken HTML links
- Some messages that contain custom forms, such as custom forms from workflow programs

Encapsulated messages are encased in a Notes database that is attached to the original message. This allows the messages to be archived in a format that preserves their data intact. "[Preprocessing overview](#)" on page 175 explains more about this process.

Retrieving and opening encapsulated messages in Lotus Notes and DWA

When the Notes plug-in or Local Cache is installed on a user's computer, an encapsulated message is unpacked automatically and restored with 100% fidelity. Users can open the message in the same way that they would open any other message. Encapsulated messages retrieved in DWA are also unpacked automatically.

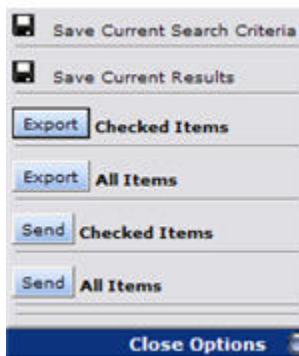
Encrypted messages are opened using the private key in the user's Notes ID. Signed messages are opened if the user has the sender's certified public key, which is stored in the Domino Directory or in the user's Address Book.

Opening and viewing encapsulated messages in the IAP Web Interface

- Users can view messages with ATT attachments and non Memo Reply items such as meeting requests in the IAP Web Interface.
- Users can view signed messages in the Web Interface, provided they have the sender's public key.
- Users cannot view encrypted files in the Web Interface. They can, however, view and open encrypted messages if they send or export a copy of the message to their Notes mailbox. When an encapsulated message is sent from the Web Interface, users must perform the steps described in the next section.

Opening encapsulated messages in Lotus Notes

Users can export or send encapsulated messages from the IAP Web Interface to their Notes mailbox. This is done by clicking **More Options** and selecting one of the Send or Export options in the Options menu.



If messages are exported, encapsulated messages can be opened and viewed like any other message.

If they are sent to the user's mailbox (as Mail-To-Me messages), the following steps are required to open the message in Lotus Notes:

1. In the Notes mailbox, double-click the file attached to 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 that is on the clipboard into the mail folder.
5. Open the message from the folder.

Part 6. Troubleshooting and performance improvement

- [Troubleshooting](#), page 317
- [Performance improvement](#), page 335

6.1 Troubleshooting

Use the topics in this section to troubleshoot problems with the system.

- [Capturing data for HP support](#), page 317
- [Preventing server instability](#), page 320
- [Mail routing issues](#), page 320
- [Dynamic Account Synchronization \(DAS\) issues](#), page 322
- [Archiving issues](#), page 326
- [Message retrieval issues](#), page 328

Capturing data for HP support

Information to collect

If you encounter problems archiving a message or retrieving a message from the IAP, collect the relevant pieces of information to help HP support troubleshoot the issue:

- The original message from a user mail file or journal (from a backup)
- The tombstone, if the message was selectively archived from a mail file
- The reference document and preprocessing document, if they exist in the reference and preprocessing databases
- The RFC-822 MIME version of the message, if it is archived in the IAP
- A copy of the message from the mail.box file on the HP Gateway server or the Get Held Messages database, if the message is not routing to the IAP

Processing held messages

A small percentage of messages sent to the IAP by EAs Domino fail during the MIME conversion process and are put into Hold status by the Domino router. Whether the error is generated by the router or the IAP, the router writes the error into the FailureReason field in the message and sets the Status field value to Hold.

The Get Held Messages application recovers mail.box messages in Hold status, and resubmits them for a specified number of times to the Domino router. (The number of times is configured in the Setup Controls view in the database.)

After the maximum number of retries, undelivered messages are saved in the Get Held Messages database and are reprocessed using [Message reprocessing rules](#) (described below). Any messages that remain in the Get Held Messages database after reprocessing are sent to HP support for diagnosis.

By default, the Get Held Messages agent is set to run every four hours, and can be run more often.

Message reprocessing rules

When the Reference Cleanup agent runs in a reference database, it first removes any obsolete or duplicate reference documents in the database. It then scans all reference documents with Sent status.

When a reference document is traced to a message in the Get Held Messages database, the Reference Cleanup agent uses a list of predefined rules to determine the action that should be performed. There are four possible actions:

- Resubmit the message to the Domino router.
- Flag the reference and original message for preprocessing and encapsulation. (See “[Preprocessing messages](#)” on page 175.)
- Flag the reference and original message for Clean Envelop preprocessing and encapsulation. (See “[Message Reprocessing](#)” on page 142.)
- Change the reference document’s Status field to Error, update the ErrorAgent field to Gateway, and write the FailureReason into the ErrorReason field.

Message reprocessing documents

Message Reprocessing documents define the action that should be performed for the following archiving errors. Changes to these documents are only made by HP support.

FailureReason	Class	Description	Message reprocessing action
3A:F2	Router	The message is corrupt and cannot be routed.	Mark reference with error Contact HP support for evaluation of the message failure.
Cannot convert Notes Rich Text message to MIME message	Router	MIME conversion error. For example, problems converting multi-byte characters such as those in the 2022-JP character code.	CD-to-MIME Failure The reference and original message are automatically flagged for preprocessing and encapsulation.
HTMLAPI Problem converting to HTML	Router	Failed conversion from Rich Text (RTF) to HTML.	CD-to-MIME Failure The reference and original message are automatically flagged for preprocessing and encapsulation.
Invalid or missing RFC822 header name	Router	The router found a badly-formatted message header.	Clean Envelop Encapsulation The reference and original message are automatically flagged for Clean Envelop preprocessing and encapsulation.

FailureReason	Class	Description	Message reprocessing action
Note item not found	Router	Generally indicates a broken attachment within the message structure. The message needs to be encapsulated. This FailureReason has been observed during Bulk Upload operations while ingesting older Notes mail data. For example, the message was initially processed by a Domino 5 router.	Corrupt File Attachment The reference and original message are automatically flagged for preprocessing and encapsulation.
Remote system no longer responding	Router	The IAP virtual IP, LoadBalancer, or SMTP portal is unavailable.	Resubmit to Router
Specified database is not currently open	Router	The database is not open, probably because the mail.box files are undergoing compacting or fixup.	Resubmit to Router
SMTP Protocol Returned a Permanent Error during archive process due to Internal Error in the Server	Router	The IAP rejected the message, probably due to internal issues.	Resubmit to Router
SMTP Protocol Returned a Permanent Error 551 Permanent Error	Router	The IAP returned parsing errors.	Clean Envelop Encapsulation The reference and original message are automatically flagged for Clean Envelop preprocessing and encapsulation.
SMTP Protocol Returned a Permanent Error 551	Router	The IAP rejected the message.	Resubmit to Router
SMTP Protocol Returned a Permanent Error	Router	The IAP rejected the message, probably due to internal issues.	Resubmit to Router

Collecting held messages for HP support

The following steps should be taken for messages that remain in the Get Held Messages database:

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

NOTE:

Be sure to disable local encryption of the database before clicking **OK**.

4. Send the Get Held Messages database copy to HP support for diagnosis of the held messages.

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

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 `Get Held Messages` string.

Reference database troubleshooting tools

Tools that help HP troubleshoot archiving problems are located in each reference database. These tools 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 document. The Hold status (for pending documents) and the Hold-P status (for documents being preprocessed) remove messages and their associated reference documents from the archiving execution path.
- Encapsulation Tools: The three message flag 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.

Preventing server instability

To avoid problems with server instability, make sure that the Agent Manager values are set correctly on the HP Gateway servers. For more information, see [“Editing the Agent Manager parameter values”](#) on page 57.

Mail routing issues

Checking mail backup

Use the mail statistics command `sh stat mail` on the HP Gateway's Domino server console to see where mail is backing up. Open `mail.box` and review the messages that are not routing. Be sure to change the `mail.box` setting from three mailboxes to one mailbox while troubleshooting. (See [Consolidating mail.box files](#) below.)

Messages in Hold or Dead state

Messages in the Hold or Dead state in `mail.box` are pulled into the Get Held Messages database on the HP Gateway server. This action occurs when the Get Held Messages agent runs, usually several

times a day. See [“Processing held messages”](#) on page 317 for information about Get Held Messages and message reprocessing.

Consolidating mail.box files

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

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

No route found from HP Gateway server to mail server

Check the Connection document on the HP Gateway server to verify that a connection has been created to the mail server. See [“Creating connection documents to the customer mail servers”](#) on page 57.

HP Gateway server not allowed to access Domino mail server

In the Domino Directory for the mail domain, ensure that each HP Gateway server has been added to the list of trusted servers. See [“Configure trusted servers”](#) on page 63.

HP Gateway server not allowed to access mail file

In the Domino Directory for the mail domain, ensure that each HP Gateway server has been added to the OtherDomainServers group, or a similar group that allows access to user mail files. See [“Granting access for the HP Gateway servers”](#) on page 63.

No route found from HP Gateway server to IAP

Ensure the Internet Domain and other settings have been properly defined in the Foreign SMTP Domain document and the SMTP Connection document on the HP Gateway server. See [“Creating and configuring the foreign SMTP domain document”](#) on page 58 and [“Creating and configuring the SMTP connection document”](#) on page 59.

Low priority messages remain in router on HP Gateway

Low priority messages are caught in the router if they are outside the low priority mail routing time range. These messages eventually route to the IAP when the low priority time range comes into force.

You can ensure that all mail is promptly routed to the IAP by setting the low priority time range to 24 hours:

1. In the HP Gateway's Server Configuration document, click the **Router/SMTP** tab.
2. Click the **Restrictions and Controls** tab, and then click the **Transfer Controls** tab.
3. Change the low priority mail routing time range from 12:00 AM – 6:00 AM to **12:00 AM - 11:59 PM**.

Domino debug parameters

These are very helpful Domino debug parameters to add to `notes.ini` on HP Gateway servers:

- Set `config SMTPCLIENTDEBUG=1`
Enables verbose logging of outbound SMTP traffic. This is helpful in monitoring SMTP conversations with the IAP.
- Set `config SmtptSaveOutboundToFile=1`
Writes the MIME of outbound messages to individual text files in the HP Gateway server's temp directory. This is helpful to see what is being sent to the IAP.

NOTE:

When you are finished troubleshooting, always reset the debug parameter to `=` or `=0` (blank or zero).

Dynamic Account Synchronization (DAS) issues

Problems copying data from customer Domino Directories to HP Gateway consolidated directory

Check the following:

- Ensure that the Notes ID and/or the master HP Gateway server are allowed to access the mail server. See [“Creating connection documents to the customer mail servers”](#) on page 57.
- Ensure that the Notes ID and/or master HP Gateway server are authorized to open/replicate `names.nsf` on the mail server.
Check the ACL for the `names.nsf` file. The Notes ID and/or HP Gateway server (or groups of which they are members) need Reader permission.
- Check the Server document on the mail server to see who can access the server and who cannot. See [“Configure trusted servers”](#) on page 63.
- Check if replication is temporarily disabled in `names.nsf` on the mail server. Remove the check mark from Replication Settings (Other) in the `names.nsf` file.

DAS does not load users

Back-trace the process:

- Check the DAS job parameters and DAS log files on the IAP.

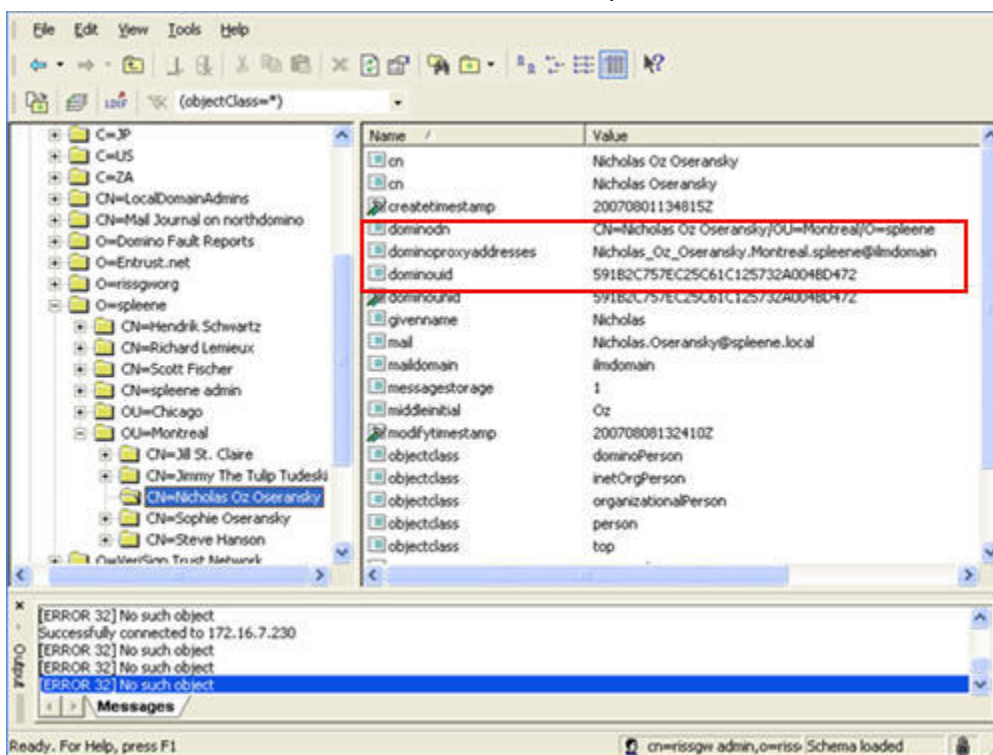
User Management / Account Synchronization Error Recovery

Search for: User Group Membership

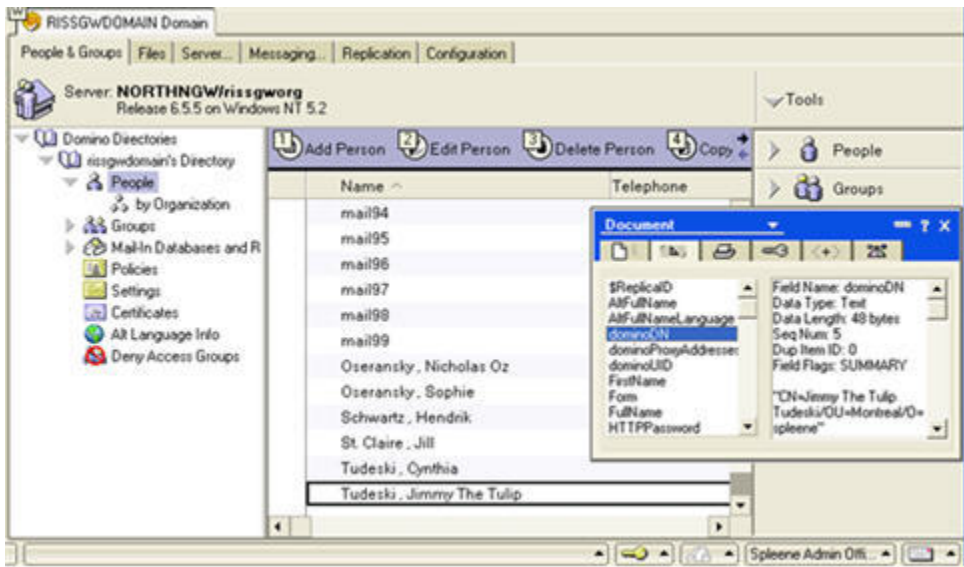
Date	Error	USN	UserName	Object GUID LDAP DN
Fri, 2007.08.24 14:21:35 CEST	ADD:ENTRY_EXISTS	20070824121529	jl@lndomain	00A55445B5D0D378C12573410041D92B CN=Jl St. Claire2/OU=Montreal/O=spleene
Fri, 2007.08.24 14:21:35 CEST	ADD:OTHER_ERROR	0		

Notes user with NULL username – check DAS logs on HTTP portal

- Verify that the dominoDN, dominoUID and dominoProxyAddresses attributes are included in the HP EAs-D DAS Names database record. (Check the document properties.)
 - Check Lotus Notes for Replication or Save conflicts that appear in the Domino Directory.
 - Confirm the LDAP configuration using an LDAP tool.
- Ensure the dominoDN, dominoUID, and dominoProxyAddresses LDAP attributes are available.



- Check the dominoDN, dominoUID, and dominoProxyAddresses attributes from within Lotus Notes, looking at the properties in the Person document.

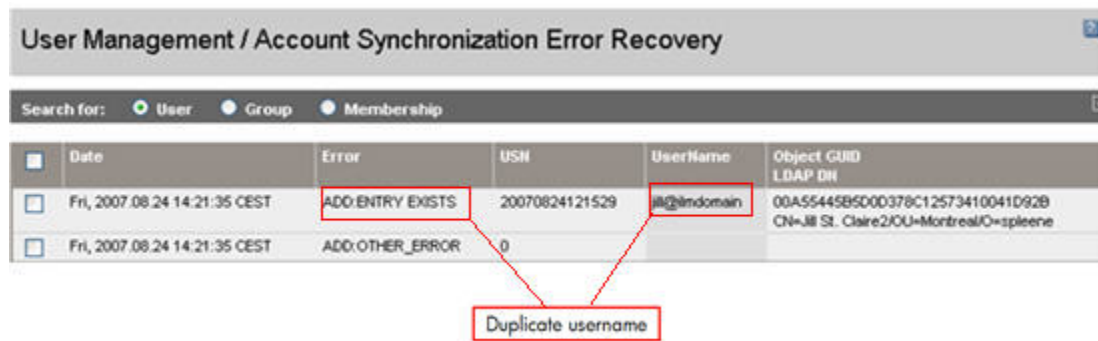


User already exists in the IAP

This error can be caused by:

- A Replication or Save Conflict in DAS Names.
- Manually running the Populate DAS Names agent while the agent is scheduled.
- An EAs Domino limitation with regard to deleted users. Users deleted from the Domino Directory are not automatically deleted from the IAP when the DAS job runs. When new users are added to the Domino Directory and the old IDs are reused, the new users cannot be added to the IAP because users with those IDs already exist.

The duplicates appear in the Account Synchronization Error Recovery page of the PCC.



	Date	Error	USN	UserName	Object GUID LDAP DN
<input type="checkbox"/>	Fri, 2007.08.24 14:21:35 CEST	ADD ENTRY EXISTS	20070824121529	j@domain	00A55445B5D00378C12573410041D92B CN=Jill St. Claire2/OU=Montreal/O=spleene
<input type="checkbox"/>	Fri, 2007.08.24 14:21:35 CEST	ADD OTHER_ERROR	0		

Duplicate username

To solve the problem, remove the duplicate users on the IAP. On the EAs Domino side, delete any duplicate Person or Mail-In documents from DAS Names and rerun the Populate DAS Names agent.

NOTE:

EAs Domino does not support the syncing of deletions through DAS. Users deleted from the Domino Directory **must** be manually deleted from the IAP.

Users deleted from the Domino Directory are not deleted in the IAP

Users deleted from the Domino Directory are not automatically deleted from the IAP when the DAS job runs. Users deleted from the Domino Directory **must** be manually deleted from the IAP.

User cannot log on to the IAP Web Interface

- Check if an Internet password has been set for the user in the Domino Directory. If not, have the user set the password and wait for replication to occur and the consolidated directory and the DAS Names database to be updated on the HP Gateway server. (DAS is not required to run again.)
- There might be a caching issue on the IAP HTTP portal. Enable debugging on the HTTP portal and look for the error reporting "UID not found" in DB2 (even though the UID does exist). Authentication will work a few hours later.

Archiving issues

Archiving tasks not executing

If archiving is not taking place, ensure that:

- The HP EAs Domino agents are signed or modified by a Notes ID with permission to execute agents and programs on the HP Gateway server. An agent runs on behalf of the user who last modified and saved the agent. (Check the column “Last modified by” in Domino Designer.)
- The Notes or server ID that signed the EAs Domino databases has permission to execute the task. Check the security settings in the Server document. See “[Setting up security on the HP Gateway server](#)” on page 56.
- The Notes or server ID that signed the EAs Domino databases has access to the mail files it needs to archive.

Email is not correct

If the messages archived on the IAP do not look correct (for example, sender/recipients missing, wrong date, wrong format):

- Make sure the archiving process is using an LNM enabled virtual IP (VIP). Each VIP address is tagged with a three-letter identifier that defines the function for which the VIP can be used. LNM indicates that the VIP address is used to store and access Lotus Notes Mail on the IAP. LNM is set in the `Domain.jcml` file. (Note that the identifier NBL does **not** work with Lotus Notes email.) See [“Setting LNM”](#) on page 365.
- Verify that the correct router and MIME settings are applied on the HP Gateway server. These options are set in the Server Configuration document. See [“Creating a configuration document for the HP Gateway server”](#) on page 59.

“Unable to open index table of Mail Details records” error

When multiple mining jobs are scheduled at close intervals on an HP Gateway server, the mining program can abort with the message “Unable to open the index table of the Mail Details records view task aborted.”

To prevent this error from occurring, open the `rissminer` program document on the Gateway server and add a `-n` switch to the command. For example:

```
-kSelective -n
```

(where `Selective` is the name of the mining profile)

For more information, see [“Scheduling the archiving job”](#) on page 193 or [“Running an archiving job manually”](#) on page 195.

Replication/save conflicts in HP EAs-D Users database

If you have multiple HP Gateway servers and are experiencing a large number of replication/save conflicts in the HP EAs-D Users database, disable updating of the Mail Detail records' Activity Log. See [“Scheduling the archiving job”](#) on page 193 or [“Running an archiving job manually”](#) on page 195.

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 Domino 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 in Lotus Notes”](#) on page 314.

Incorrect content-type

The File Identifications table is responsible for mapping file extensions in Notes \$FILE items to MIME content-type values, and vice-versa, for mail transmitted via SMTP.

The IAP indexes file attachments based on the MIME content-type value. If the HP Gateway has an improperly set or empty File Identifications table, attachments might be stamped with the incorrect content-type or labeled as application/octet-stream by default.

To verify that the table is present:

1. Open the Administrator client, select **File > Open Server**, and then select the HP Gateway server.
2. Click the **Configuration** tab.
3. Expand **Messaging**, and then click **File Identifications**.

The table should display a set of 90 default document types. If the table is empty, reload the default table:

1. Open the Lotus Notes client.
2. Select **File > Application > Open**.
3. Open the file named `pubnames.ntf` on the HP Gateway server.
4. Press **Ctrl + A** to select all documents, then **Ctrl + C** to copy them to the clipboard.
5. Return to the Administrator client File Identifications table.
6. Press **Ctrl + V** to paste the documents in the table.

See “[Indexed file types and MIME types](#)” on page 381 for a list of content-types supported by the IAP.

Message retrieval issues

The following topics describe how to troubleshoot problems that might occur when retrieving archived messages in DWA or when using the Notes Windows plug-in or the desktop version of Export Search.

Message retrieval error in DWA

If users receive the error “HP DWA Message Retrieval Error: can not open API database” when retrieving an archived message, the `hprim_api` setting is missing in `notes.ini` on the DWA server. Most often, this situation occurs when the databases for DWA Extension are installed manually on DWA servers and the required setting is not added to `notes.ini`.

If you install the databases manually on DWA/mail servers, be sure to manually add the setting `hprim_api=hprim\hp_rissapi.nsf` to the `notes.ini` file.

NullPointerException error in DWA

If messages with very large file attachments are archived, users can receive an Out of Memory (`java.lang.NullPointerException`) error when they attempt to retrieve those messages in DWA.

The messages can be retrieved without error in Lotus Notes if the Windows Plug-In and/or Local Cache are installed on users' machine. The messages can also be sent from the IAP Web Interface and opened in Lotus Notes.

You can allow messages with large attachments to be viewed in DWA by editing `notes.ini` as follows:

1. Open `notes.ini`.
2. Change the value of the `HTTPJVMMMaxHeapSize` parameter as shown below. Add this parameter if it does not exist.
 - To allow attachments up to 16 MB to be opened, set the value at 64M.
`HTTPJVMMMaxHeapSize=64M`
 - To allow attachments up to 40 MB to be opened, set the value at 128M.
`HTTPJVMMMaxHeapSize=128M`
 - To allow attachments up to 87 MB to be opened, set the value at 256M.
`HTTPJVMMMaxHeapSize=256M`

Archived messages with attachments over 87 MB cannot be opened in DWA.

3. Save the file, and then restart the Domino server.

 **NOTE:**

If your organization allows email with very large attachments, we recommend using a DWA proxy configuration and setting the `HTTPJVMMMaxHeapSize` value on the Proxy Gateway instead of the mail server.

For information on setting up a Proxy Gateway, see [“Installing DWA Extension”](#) on page 256 and [“Configuration steps on the DWA/proxy server”](#) on page 259.

The recipient's Internet Address is not displayed in the IAP Web Interface

When a user's Notes mail address does not include any spaces or other characters that are invalid in SMTP addresses, the archiving agents do not recognize that the recipient is internal, and the quoted full name is not added during ingestion to the IAP. The recipient's Internet Address is not displayed when the message is retrieved in the IAP Web Interface.

```
From: "user2/ou_mail3" <mary.doe@domino3.company.com>
To: joeuser/ou_mail3@dom3
Folder:
Subject: Mail 1
```

Adding the Domino mail domain to the list of SMTP domains in the Global Domain document causes the archiving agents to recognize that the message is internal. The quoted full name is now displayed in the Web Interface.

```
From: "user2/ou_mail3" <mary.doe@domino3.company.com>
To: joeuser/ou_mail3@dom3 <joe.user@domino3.company.com>
Folder:
Subject: Mail 1
```

To make this change, go to **Address Conversion Settings > SMTP Alias** in the Global Configuration document and add the mail domain to the **DNS domains/hostnames accepted for SMTP messages** field.

SendTo address is incorrect when replying to a Mail-To-Me message

When users send copies of archived email from the IAP Web Interface to their mail accounts, the messages are viewable, but actions on the email (such as reply or forward) might not work correctly. This situation can occur if the original message had a value in the FromDomain field, which results in the Domino domain being added to the end of the email address. For example, Joe User/Org1/MyCompany <joe.user@mycompany.com>@DominoDomain.

To correct the problem:

- If users retrieve email in Lotus Notes, install the Windows Notes Client Plug-In on their computers. See “Using the Windows Notes Client Plug-In” on page 308.
- If users only retrieve email in iNotes (DWA), or if they retrieve email in Notes but you do not want to deploy the plug-in:
 - When there is a single Domino domain, follow the steps below.
Note that any information in the FromDomain field in a message will be lost, since the router on the HP Gateway server will delete the item.
 - When there are multiple Domino domains, inform users that certain actions will not work on email sent from the IAP Web Interface.
The solution below does not work if there are multiple Domino domains (now or in the past). These domains can include foreign domains such as those used by FAX gateways, X.400 gateways, and the Lotus SMTP Gateway (pre-Domino 5.x).

To remove values in the FromDomain field when there is a single Domino domain:

1. Change the Advanced Outbound Message options in the Domino Configuration document:
 - a. Open the Domino Administrator client and then open the HP Gateway server.
 - b. If necessary, switch to a Notes ID that can be used to create databases and documents.
 - c. Click the **Configuration** tab, expand **Messaging**, and click **Configurations**.
 - d. Select the Configuration Settings document for the server, and then click **Edit Configuration**.
 - e. Click the **MIME** tab, then click **Advanced > Advanced Outbound Message Options**.
 - f. Enter **FromDomain** in the field labeled “Notes items to be removed from headers.”
 - g. Click **Save & Close**.
2. Edit the Archive agent options in EAs Domino:
 - a. In the Administrator client, open the HP EAs-D API database.
 - b. Open the Global Configuration document for editing.
 - c. Click the **Agent Settings** tab and then click the **Archive Agent** tab.
 - d. Add **FromDomain** to the list in Remapped Fields.
 - e. Click **Save & Close**.

Troubleshooting the Notes client plug-in

Two parameters can be added to `notes.ini` on the client to help HP support troubleshoot problems with the plug-in:

- `HPCLIENT_HTTP_FILE=1`
Saves the MIME downloaded from the IAP into the `hprimdump.eml` file.

- HPCLIENTVERBOSE=1
Enables verbose logging.

Only add these parameters at the direction of HP support.

Content appears twice in phone messages

Messages that are sent using the Phone Message form in Notes are selectively archived and tombstoned unless they are specifically excluded in the mining rule. 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 on the IAP.

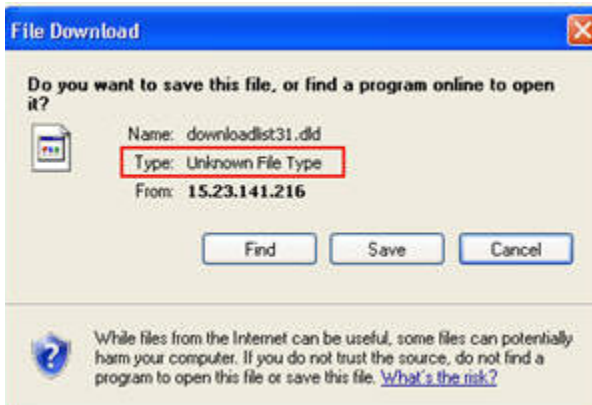
Error opening meeting request in Lotus Notes

A “Document Command is not Available” error can appear when users open archived meeting requests in Notes and the Windows plug-in is installed. After users click **OK** in the error dialog box, the meeting request opens properly.

This issue applies to requests that were archived using pre-2.1 versions of EAs Domino. In EAs Domino 2.1, meeting requests (notices) are always excluded from archiving. It can also apply if meeting requests are attached to messages as .ics files.

Troubleshooting Export Search (desktop tool)

If users receive the following error while exporting files, verify that the Windows system has associated the DLD file type with the Export Search Desktop tool.



Verifying the file type

To verify that the DLD file type is installed on the computer:

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

Creating a file type association

If DLD is not listed in the file type list, create an association for the DLD file type.

Windows Vista:

1. In the Web Interface Query Results page, click **More Options** and export the search results.
The file download dialog box appears.
2. Click **Save** and save the DLD file to the computer desktop.
3. Right-click the DLD file (for example, `downloadlist2.dld`), and select **Properties**.
4. In the **General** tab, click **Change**.
5. Click **Browse**, and then browse to the following location:
`\Program Files\Lotus\Notes\Localcache`
6. Select **ExportSearch.exe** and click **Open**.
7. Click **OK** to associate the DLD file type with the Export Search Desktop tool.
8. Double-click the DLD file to continue exporting the files.

Other Windows operating systems:

1. In the Control Panel, select **Tools > Folder Options**, and then click the **File Types** tab.
2. Click **New**.
3. In the File Extension box, enter **DLD**, and then click **OK**.
4. In the Details for 'DLD' extension area, click **Change**.
5. Click **Select the program from a list** in the dialog box that appears, and then click **OK**.
6. Click **Browse** in the Open With dialog box.
7. Browse to the following location:
`\Program Files\Lotus\Notes\Localcache`
8. Select **ExportSearch.exe**, and then click **Open**.
9. Click **OK** to associate the DLD file type with the Export Search Desktop tool.

Changing the file type association

If the DLD file type is associated with another program, change the file type association.

Windows Vista:

1. In the Control Panel, select **Default Programs** and then click **Associate a file type or protocol with a program**.
2. Select the **.dld** extension, and then click **Change program**.
3. Click **Browse** in the Open With dialog box.
4. Browse to the following location:
`\Program Files\Lotus\Notes\Localcache`
5. Select **ExportSearch.exe**, and then click **Open**.
6. Click **OK** to associate the DLD file type with the Export Search Desktop tool.

Other Windows operating systems:

1. In the Control Panel, select **Tools > Folder Options**, and then click the **File Types** tab.

2. Select the **DLD** extension in the File Types tab, and then click **Change**.
3. In the **Open With** dialog box, click **Browse**.
4. Browse to the following location:
`\Program Files\Lotus\Notes\Localcache`
5. Select **ExportSearch.exe**, and then click **Open**.
6. Click **OK** to associate the DLD file type with the Export Search Desktop tool.

6.2 Performance improvement

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

- [Compacting databases](#), page 335
- [Editing the HP Gateway server configuration](#), page 335
- [Monitoring the HP Gateway server](#), page 336

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 the HP Gateway server configuration

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

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.
- `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 HP Gateway server

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.

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 HP 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 EAs Domino, the Get Held Messages application and message reprocessing are used to troubleshoot routing issues. For more information, see "[Processing held messages](#)" on page 317.

Part 7. Appendices

- [Installation worksheets](#), page 339
- [Post-installation checklists](#), page 347
- [Software upgrade checklist](#), page 351
- [Creating and updating EAs Domino applications](#), page 353
- [HP EAs Domino scheduled agents](#), page 357
- [HP EAs Domino settings for Japanese data](#), page 361
- [IAP configuration](#), page 365
- [Indexed file types and MIME types](#), page 381
- [Support and other resources](#), page 383

A Pre-installation worksheets

- [Customer and product information](#), page 339
- [IAP information](#), page 340
- [HP Gateway environment](#), page 341
- [Domino servers to be mined](#), page 343
- [HP EAs Domino features \(Domino servers\)](#), page 344
- [HP EAs Domino features \(client systems\)](#), page 345

Customer information

Company name	
---------------------	--

Customer contacts for the delivery

Name/position	Telephone #	Cell phone #	Email

Customer contacts for post-delivery/support

Name/position	Telephone #	Cell phone #	Email

Installation site information: Site 1

Customer	
Installation site address	
Site phone	
Special instructions for site access	
Mailing address (if different from above)	

Installation site information: Site 2

Customer	
Installation site address	
Site phone	
Special instructions for site access	
Mailing address (if different from above)	

Installation site information: Site 3

Customer	
Installation site address	
Site phone	
Special instructions for site access	
Mailing address (if different from above)	

Installation site information: Site 4

Customer	
Installation site address	
Site phone	
Special instructions for site access	
Mailing address (if different from above)	

IAP information

Description	Value
IAP name (BlackBoxName)	
EAs Domino credentials for authentication with IAP: User Login ID Password This is not the user/password used to log into IAP PCC Administration. See the instructions for the IAP Login and Password fields in " Archiving Options tab " on page 149.	
IAP software version to be installed (include any patches or hotfixes to be installed)	

Description	Value
IAP domain names	
IAP domain IDs <i>Used in setting up DAS job.</i>	
Virtual IP addresses (VIPs)	
Replica IP name <i>(if replication used)</i>	
Retention periods: <ul style="list-style-type: none"> • Domain <i>(cannot be less than 30 days)</i> • Unregulated repositories <i>(cannot be less than domain retention period)</i> • Regulated repositories <i>(cannot be less than domain retention period)</i> 	Example: <ul style="list-style-type: none"> • 30 • 60 • 60
Estimated number of users to be loaded by DAS into the IAP	
Frequency (in hours) that IAP should perform account synchronization with master HP Gateway server	
Name of IAP repository to hold Clean Envelop encapsulated files	

HP Gateway environment

Use the information in this table to install and configure the Windows server software and Lotus Domino server software on HP Gateway servers.

See [“Preparing the HP Gateway environment”](#) on page 43.

Description	Value
Organizational unit certifier ID	Example: /ou=hparchive/o=acme
Certifier ID password <i>(both certifier ID and password need to be supplied by Domino administrator)</i>	
HP Gateway Domino domain name	Example: HPGateway
HP Gateway administrator ID	HPAdmin
HP Gateway administrator ID password <i>(to be supplied by Domino administrator)</i>	
Customer Windows domain <i>(optional)</i>	
Master HP Gateway server	
Master HP Gateway server ID <i>(used for DAS and EAs Domino software installation)</i>	
HP Gateway server name and title	Example: HPGateway1, HP Gateway 1

Description	Value
Master HP Gateway server fully qualified name (Domino ID name)	Example: HPGateway1/hparchive/acme
Master HP Gateway server fully qualified Internet (host) name	Example: HPGateway1.acme.com
Master HP Gateway server IP address	
Master HP Gateway server host name	

Additional HP Gateway servers

HP Gateway server 2

HP Gateway server 2 ID	
HP Gateway server 2 name and title	
HP Gateway server 2 fully qualified name	
HP Gateway server 2 fully qualified Internet name	
HP Gateway server 2 IP address	
HP Gateway server 2 host name	

HP Gateway server 3

HP Gateway server 3 ID	
HP Gateway server 3 name and title	
HP Gateway server 3 fully qualified name	
HP Gateway server 3 fully qualified Internet name	
HP Gateway server 3 IP address	
HP Gateway server 3 host name	

HP Gateway server 4

HP Gateway server 4 ID	
HP Gateway server 4 name and title	
HP Gateway server 4 fully qualified name	
HP Gateway server 4 fully qualified Internet name	
HP Gateway server 4 IP address	
HP Gateway server 4 host name	

Domino servers to be mined

List the mail and journal servers that will be mined by the HP Gateway servers.

Ensure that each server is supported for remote mining.

See “[Supported operating systems and Lotus Domino versions](#)” on page 35.

Description	Value
Domino mail domain name	
Hub server or server designated for communication with the customer's external domain	
Type of tombstoning to be implemented for selective archiving	
Mail server 1: Fully qualified name OS Lotus Domino version	
Mail server 2: Fully qualified name OS Lotus Domino version	
Mail server 3: Fully qualified name OS Lotus Domino version	
Mail server 4: Fully qualified name OS Lotus Domino version	
Journal server 1: Fully qualified name OS Lotus Domino version	
Journal server 2: Fully qualified name OS Lotus Domino version	

HP EAs Domino features (Domino servers)

Ensure that the customer server meets the EAs Domino system requirements.
See “Supported operating systems and Lotus Domino versions” on page 35.

See “Customer Domino server requirements” on page 35 for journaling and DWA Extension space requirements.

Category	Item	Description
Journaling	Mail journaled using: <ul style="list-style-type: none"> • Domino native journaling • HP EAs Domino Advanced Filtering 	
	Mail/journal server 1 hosting journal: <ul style="list-style-type: none"> • Fully qualified name of server • OS Lotus Domino version • Journal mail-in database name 	
	Mail/journal server 2 hosting journal: <ul style="list-style-type: none"> • Fully qualified name of server • OS Lotus Domino version • Journal mail-in database name 	
	(Advanced Filtering only) Name of anti-virus software (if any) used on the Domino server(s)	
Bulk Upload	Feature to be implemented?	
	Customer Lotus Domino application server: <ul style="list-style-type: none"> • Fully qualified server name • OS Lotus Domino version 	
DWA Extension	Feature to be implemented?	
	Installed on mail/DWA server or proxy server?	
	Customer Lotus Domino server: <ul style="list-style-type: none"> • Fully qualified server name • OS Lotus Domino version 	
Export Search	Feature to be implemented?	
	Customer Lotus Domino server: <ul style="list-style-type: none"> • Fully qualified server name • OS Lotus Domino version 	
	Use Export Search Web Interface?	

HP EAs Domino features (client systems)

See “Supported Lotus Notes clients” on page 38 for the client systems that are supported.

Category	Item	Description
Windows Notes Plug-In	Feature to be implemented?	
	Client OS/Lotus Notes version supported	
Local Cache/Export Search	Feature to be implemented?	
	Java Runtime environment installed?	
	Client OS/Lotus Notes version supported	
IAP Single Sign-On	Feature to be implemented?	
	Client OS/Lotus Notes version supported	

B Post-installation checklists

- [Installation: Master HP Gateway server](#), page 347
- [Installation: Additional HP Gateway servers](#), page 348
- [Configuration: Email archiving](#) , page 348

Installation: Master HP Gateway server

Description	
Ensure that the Java Runtime Environment is installed on the server.	
Set up security on the server.	
Adjust the Agent Manager values.	
Create connection documents to the customer server(s).	
Create connection documents to the IAP.	
Create a Server Configuration document. (Be sure to specify number of mail.box files and all router/SMTP and MIME settings.)	
Limit the size of the Domino log file on the server.	
Add the EAsD_Domain variable to <code>notes.ini</code> , if user mail files are selectively archived and Ensure Owner Receipt (EOR) is specified.	
Install the EAs Domino software and set the ACL for the databases.	
Create a consolidated directory and replicate it to any additional Gateway servers.	
Configure Directory Assistance.	
Edit the DAS Names Configuration document.	
Schedule and run the Populate DAS Names agent in the DAS Names database to populate from the consolidated directory.	
Restart the server. (If a mail.box file exists remove it during the server restart).	
Configure the Global Configuration document and configure and enable the Server Definition document.	

Installation: Additional HP Gateway servers

Description	
Ensure that the Java Runtime Environment is installed on the server.	
Create connection documents from the master HP Gateway to additional HP Gateway servers.	
Set up security on the server.	
Adjust the Agent Manager values.	
Create connection documents to the customer server(s).	
Create connection documents to the IAP.	
Create a Server Configuration document. (Be sure to specify the number of mail.box files and all router/SMTP and MIME settings.)	
Limit the size of the Domino log file on the server.	
Add the EAsD_Domain variable to <code>notes.ini</code> , if user mail files are selectively archived and Ensure Owner Receipt (EOR) is specified.	
Ensure the consolidated directory has been replicated from the master HP Gateway server.	
Ensure that the Directory Assistance database has been replicated to the Gateway server that will be used as the DAS backup.	
Deploy the EAs Domino software from the master HP Gateway server, replicating the HP EAs-D API and HP EAs-D Users databases. Replicate the DAS Names database to the DAS backup server.	
Set the ACL for the EAs Domino databases.	
Restart the server. (If a mail.box file exists remove it during the server restart).	
Ensure that the additional Gateway servers are added to the Server Definition document.	

Configuration: Email archiving

Description	
Confirm that the Global Configuration document and Server Definition document are correctly configured.	
Configure the mining rules document(s). (You can configure one rule and copy/paste as needed. Delete any mining rules that are not used.)	

Description	
<p>If selective archiving is used, run the Profile Agent to populate the HP EAs-D Users database. The Profile Agent should be run on only one HP Gateway server. (Verify that the User Membership tab settings are correct on each mining rule before running the agent. You can selectively add users for testing and verification by enabling or disabling the Profile Agent for a mining rule.)</p>	
<p>For selective archiving, schedule and enable the other agents in the HP EAs-D Users database.</p>	
<p>Configure the controls and agent in the Get Held Messages database.</p>	
<p>Schedule and enable the preprocessing agents.</p>	
<p>Schedule and enable the Archive, Tombstone, and Reference Cleanup agents.</p>	
<p>Schedule and enable the Purge_Document agent in the HP EAs-D Log, HP EAs-D Alert, and HP EAs-D Stats databases.</p>	
<p>Schedule the mining job.</p>	

C Software upgrade checklist

Before proceeding with an upgrade to EAs Domino 2.1.2, perform the tasks in this table.

Task description	Comments
<p>Enter the IAP VIP address as shown in the following documents in the existing EAs Domino installation:</p> <ul style="list-style-type: none">• Foreign SMTP Domain and SMTP Connection documents on the HP Gateway server. See “Creating and configuring the foreign SMTP domain document” on page 58 and “Creating and configuring the SMTP connection document” on page 59.• Server Definition document (IAP host name field). See “Configuring the Server Definition document” on page 147.	
<p>Enter the IAP store domain name, as shown in the Server Definition document (IAP domain field) in the existing EAs Domino installation.</p>	
<p>Enter the EAs Domino credentials for authentication with the IAP, as shown in the Server Definition documents in the existing installation:</p> <p>User Login ID Password</p> <p>This is not the user/password used to log into IAP PCC Administration. See the instructions for the IAP Login and Password fields in “Archiving Options tab” on page 149. Note that this information does not exist in older versions of EAs Domino.</p>	
<p>Complete the IAP Information section of the pre-installation worksheet. See “IAP information” on page 340.</p>	
<p>Make a backup copy of the EAs Domino databases.</p>	
<p>Ensure that you have physical or Remote Desktop Protocol (RDP) access to all HP Gateway servers involved in the upgrade. You might also need physical or RDP access to some customer mail servers, depending on the applicable upgrade scenario.</p>	

D Creating and updating HP EAs Domino applications

Use the instructions in this appendix to create new EAs Domino applications or to refresh or replace the design of an application.

- [Creating reference and preprocessing applications](#), page 353
- [Creating new EAs Domino applications](#), page 353
- [Refreshing the design of EAs Domino applications](#), page 354
- [Replacing the design of EAs Domino applications](#), page 355

Creating reference and preprocessing applications

To increase throughput, you can create additional mining rules, with additional reference and preprocessing databases, to distribute the agent processing load.

Use the `hp_referenc.ntf` and `hp_preproc.ntf` EAs Domino templates to create additional reference databases and corresponding preprocessing databases.

Schedule and enable the agents in the databases by following the instructions in [“Configuring the archiving agents”](#) on page 185.

Creating new EAs Domino applications

Use the EAs Domino templates to create new databases. See [“HP EAs Domino database templates”](#) on page 66 for a description of each template.

1. Copy the relevant templates from the `Templates` directory on the installation media into the root data directory of a Notes client that has access to the server. For example:

```
C:\Program Files\lotus\notes\data
```

(Do not copy EAs Domino templates into the Domino data directory on the server. The overnight Design process might use the templates to refresh agents, causing the agents to lose schedule information.)

2. Using the Notes client, create the database:
 - a. Select **File > Application > New**.
The New Application window appears.
 - b. In the **Server** box, specify the server where the database is being installed.
 - c. In the **Title** box, enter the name for the database.
 - d. In the **Filename** box, enter the database filename.
Files should be placed in the Domino data `hprim` folder, except when a journal is created using the HP EAs-D Journal template. In that case, create the journal in the Domino data directory.
 - e. In the Template for New Application area, select the Local server.
 - f. Select the relevant HP EAs-D template in the scroll box.
 - g. Click **OK** to create the database.
3. Select **File > Application > Access Control** and set the ACL for the EAs Domino database.
 - For journal databases, adjust the access control settings as described in:
 - [“Creating the mail-in journal database”](#) on page 204, or
 - [Creating the mail-in journal database](#)
 - For other databases used in the archiving process, adjust the access control settings as described in [“EAs Domino ACL for HP Gateway databases”](#) on page 67.
If the databases and agents will be signed with a server ID, make sure the server is in LocalDomainServers.
If the databases and agents will be signed with a user ID, add the ID to database ACL. Usually, this ID has the same access as LocalDomainAdmins.
 - For databases used in DWA Extension, Export Search, or IAP SSO, set the ACL according to the instructions in:
 - [“Setting ACL for DWA Extension”](#) on page 258
 - [“Setting ACL for Export Search”](#) on page 273
 - Step 7 in [“Creating the HP EAs-D SSO database”](#) on page 289
4. In the Domino Designer client, schedule and enable the relevant agents in the database.
5. In the Domino Administrator client, sign the new database:
 - a. If the database will be signed by the active user ID, switch to the relevant ID.
 - b. Select **File > Open Server** and then select the server where the new database was created.
 - c. Click the **Files** tab and select the database.
 - d. With the file selected, right-click and select **Sign** from the context menu.
 - e. In the dialog box, select the Active User’s ID or Active Server’s ID and **All design documents**, and then click **OK**.

Refreshing the design of EAs Domino applications

To refresh the design of an EAs Domino database:

1. Copy the relevant templates from the `Templates` directory on the installation media into the root data directory of a Notes client with access to the server.
For example:
`C:\Program Files\lotus\notes\data`
2. In the Domino Administrator client, open the server on which the database to be refreshed is installed.
3. Click the **Files** tab, navigate to the `hprim` folder, and select the database.
4. From the menu, select **File > Application > Refresh Design**.
5. In the dialog box that appears, select **Local** (or **On My Computer**) in the **With design from Server** box.



6. In the dialog box that appears, click **Yes** to allow the Refresh Design process to proceed.



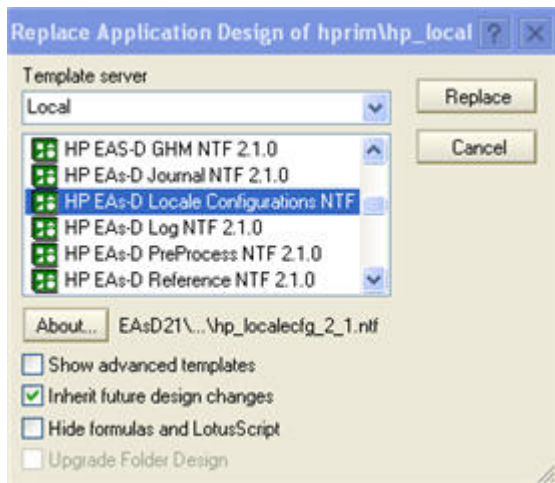
Replacing the design of EAs Domino applications

❗ IMPORTANT:

Replacing the design of a database with the wrong template can cause EAs Domino or Lotus Domino to function improperly. Only perform this operation when instructed to do so by this guide or other EAs Domino/IAP instruction documents.

1. Copy the relevant templates from the `Templates` directory on the installation media into the root data directory of a Notes client with access to the server.
For example:
`C:\Program Files\lotus\notes\data`
2. In the Domino Administrator client, open the server on which the database to be replaced is installed.
3. Click the **Files** tab, navigate to the `hprim` folder, and select the database.
4. From the menu, select **File > Application > Replace Design**.

5. In the Replace Application design dialog box:



- a. Select **Local** (or On My Computer) in the **Template server** box.
 - b. Select the template that contains the replacement design.
 - c. Click **Replace**.
6. In the dialog box that appears, click **Yes** to allow the Replace Design process to proceed.



E HP EAs Domino scheduled agents

Table 11 EAs Domino scheduled agents

Template	Agent name	Must be enabled (Y/N)	Recommended schedule	Description
HP EAs-D Alert	Purge_Document	Y	Once a day	Removes older alert documents from the database. To edit the retention time, see "Removing documents from the HP EAs-D Alert database" on page 247.
HP EAs-D DAS Names	Populate DAS Names	Y	Every 2 hours	Reads the consolidated directory and the DAS Names Configuration document to populate the DAS Names database. (The Archive/Tombstone agents, Profile Agent, and rissminer still use the consolidated directory; LDAP uses the DAS Names database.)
HP EAs-D Export Search (for server side Export Search)	Export Search	Y	Every hour	Retrieves messages referenced in the attached DLD file and exports them to a database configured in the Export Search request.
	PopulateFolder Files	Y (if Web based)	Every 6 hours	Picks up the allowable server and directories configured in the Export Search Destination document, and the database file and folder information in the Export Search request, to create a list of folders and files where messages can be exported. It is used with the "Append data to existing db" option in the export request.
	Purge_Document	Y	Once a day	Removes older Export Search requests from the database. To change the retention time, see "Removing requests from the Export Search log" on page 285.
HP EAs-D Get Held Messages	Get Held Messages	Y	Every 4 hours	Collects or reprocesses messages in mail.box files on the HP Gateway server that are rejected by the IAP's SMTP portal with coded errors.
HP EAs-D Log	Purge_Document	Y	Once a day	Removes older log entries based on retention value. To change the retention time, see "Purging log entries" on page 236.

Template	Agent name	Must be enabled (Y/N)	Recommended schedule	Description
HP EAs-D PreProcess	Encapsulate	Y	Every 2 hours *	Prepares messages for IAP ingestion using an encapsulated format to preserve the integrity of digital signatures, encrypted data, or other data that cannot be converted into RFC-822 format by the Domino router. * Schedule is recommended for systems with low volume for signed and encrypted messages. Busy systems may require more aggressive scheduling.
	Remove Obsolete PreProcess Documents	Y	Every 4 hours	Cleans up orphaned encapsulate documents and removes temporary files created by the Encapsulate agent, at the operating system level.
HP EAs-D Reference	Archive	Y	Every 30 minutes **	Creates a transient copy of an original message and sends it to the IAP, based on a reference record. ** Recommended for systems with moderate volume. Busy systems may require more aggressive scheduling.
	Reference Cleanup	Y	Every 4 hours	Removes any obsolete reference documents from the reference databases.
	Tombstone	Y	Every 30 minutes **	Validates that messages have been successfully archived to the IAP, before applying the tombstone settings configured in the mining rule. ** Recommended for systems with moderate volume. Busy systems may require more aggressive scheduling.
HP EAs-D Server Requests	Purge_Document	Y (if DWA Ext is used)	Once a day	Removes older tombstone conversion requests. To change the number of days that conversion requests are kept, see "Removing conversion requests from the HP EAs-D SC Request database" on page 267.
HP EAs-D SSO	Generate User Tokens	Y (if SSO is used)	Once a day	Generates secure date-stamped user credentials for single sign-on to the IAP.
HP EAs-D Stats	Purge_Document	Y	Once a day	Removes older statistics documents. To change the number of days that documents are kept, see "Removing documents from the HP EAs-D Stats database" on page 251.

Template	Agent name	Must be enabled (Y/N)	Recommended schedule	Description
HP EAs-D Users	profileAgent	Y (if selective archiving is used)	Once a day	Synchronizes the user database with the mining rule's membership definition and the Domino Directory. Updates all Mail Details records in the database. If there are multiple HP Gateway servers, the agent must run on only one Gateway.
	Purge Not synchronized 'person' document	Y (if selective archiving is used)	Once a day	Removes the Mail Detail records of users who have been removed from the Domino Directory. To change the number of days that Mail Detail records are kept after the last synchronization with the Domino Directory, see "Purge Not Synchronized person document agent" on page 188.
	Stats\Purge Selective Archive Log	Y (if there is only one HP Gateway and selective archiving is used)	At least once a week	Saves a mining activity log in each user's Mail Detail record. Do not enable if there are multiple HP Gateway servers. For more information, see "Purge Stats Selective Archive Log agent" on page 189.
	Stats\User Activity Alert	Y (if selective archiving is used)	Once a day	Flags a user's Mail Detail record if the mail file has not been mined for a certain number of days. To change the number of days, see "Statistics User Activity Alert agent" on page 187.

F HP EAs Domino settings for Japanese data

Email storage formats

Lotus Notes and Domino can use two formats for storing email message content:

- MIME format, which is the standard format used for Internet email
- Rich Text format, which is a native Notes data format

User preference settings and server settings can influence the actual format that is used for a particular message.

Messages stored in Rich Text format use an IBM character set called LMBCS to store all text characters. Messages stored in MIME format use standard character sets that are recognized by almost all email systems.

For interoperability between Domino and other email systems, the router in the Domino server converts Rich Text to MIME format and LMBCS characters to a variety of standard character sets. Trade-offs between message size and fidelity are inherent in the choice of standard character sets for a message, so Domino provides settings that allow administrators to control the choices on a language-by-language basis.

ISO-2022-JP and Hankaku-Kana characters

The default settings in the Domino server software that ships with an HP Gateway specify a standard character set known as ISO-2022-JP for email messages containing Japanese characters. This standard character set is used when Rich Text messages containing Japanese characters are ingested into the IAP.

The ISO-2022-JP character set, as implemented by IBM, does not support a subset of Japanese characters known as Hankaku-Kana, or half-width Katakana. The conversion of LMBCS data to ISO-2022-JP forces the Hankaku-Kana characters to be changed to full-width Katakana, or Zenkaku-Kana.

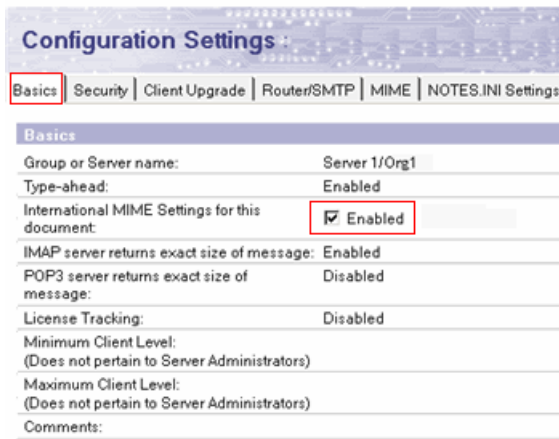
There are two differences between Hankaku-Kana and Zenkaku-Kana characters. In certain Japanese character sets, Hankaku-Kana take up only a single byte and are rendered as a narrow glyph, whereas Zenkaku-Kana characters take up two bytes and are rendered as a wide glyph.

IBM has chosen the ISO-2022-JP setting for efficiency and message size purposes. This does result in a loss of visual fidelity for Hankaku-Kana characters that are converted to the wider Zenkaku-Kana. Although there is no change in character meaning, EAs Domino customers might be concerned about the effects of the visual fidelity loss. One such effect is disruption of table column layout within a message containing Hankaku-Kana.

Changing the HP Gateway server configuration document

To preserve the fidelity of Hankaku-Kana characters, use the following procedure on each HP Gateway server:

1. Connect to the HP Gateway server using the Domino Administrator client.
2. Select the **Configuration** tab, expand **Server** in the navigation pane, and select **Configurations**.
3. Select the configuration document for the HP Gateway that you are modifying, and then click **Edit Configuration**.
4. Click the **Basics** tab and select the **International MIME Settings for this document** check box.



5. Click the **MIME** tab in the configuration document, and then click **Settings by Character Set Groups**.
6. Select **Japanese** in the **MIME settings by character set group** drop-down list.

7. In the Outbound Message Options section at the bottom of the form:
 - Change both Character Set options to **Shift_JIS**.
 - Change both Encoding settings to **Base 64**.

The screenshot shows the 'Configuration Settings' page for 'MIME'. The 'Settings by Character Set Groups' tab is selected, and the character set group is set to 'Japanese'. Under the 'Outbound Message Options' section, there is a table with two columns: 'Character Set' and 'Encoding'. The 'Header' row has 'Shift_JIS' and 'Base64' selected. The 'Body' row also has 'Shift_JIS' and 'Base64' selected. Red boxes highlight these four selections.

	Character Set	Encoding
Header:	Shift_JIS	Base64
Body:	Shift_JIS	Base64

8. Click **Save & Close**.
9. Click the **Server** tab. In the server console, shut down the Domino server.
10. Restart the Domino server.

G IAP configuration

The following topics describe the changes that must be made on the IAP to support an HP EAs Domino 2.1.x installation:

- [Setting LNM](#), page 365
- [Disabling folder support](#), page 365
- [Creating a repository for Clean Envelop encapsulated messages](#), page 365
- [Default LDAP attribute mapping](#), page 365
- [Directory Integration](#), page 366
- [Account security](#), page 370
- [Creating and running DAS jobs](#), page 371

Setting LNM

The VIP where email is sent must parse Lotus Domino email. Therefore, Lotus Notes Mail (LNM) must be set in `Domain.jcml` for each of the VIPs attributed to Notes mail.

The following example shows this setting:

```
ipToDomainInfo=172.16.7.226,172.16.7.227
172.16.7.226=LNM,CURRENT
172.16.7.227=RPL,CURRENT
```

Disabling folder support

IAP folder support must not be enabled on an IAP domain that supports messages archived from Lotus Domino. This feature is not supported in HP EAs Domino. If the folder support option is enabled, messages exported from the IAP cannot be opened with the Export Search utility.

Open `Domain.jcml` on the IAP kickstart server at `/install/configs/primary/` and ensure that the `FolderSupportEnabled` parameter is set to the default value of `false` for the IAP domain.

Creating a repository for Clean Envelop encapsulated messages

An IAP repository must be created to hold the messages processed during Clean Envelop Encapsulation. When enabled, this method of processing is used for messages that are rejected by the IAP's SMTP portal with 551 permanent errors. For more information, see "[Message Reprocessing](#)" on page 142.

Only compliance officers (and the IAP administrator, if required) should have access to this repository.

Default LDAP attribute mapping

A special DSE configuration file is required to provide a default mapping for the IAP user definition attributes.

Perform the following steps before setting up a DAS job for Domino:

1. SSH into the HTTP portal handling the DAS job and execute the following commands:

```
cd /opt/DAS/runtime
mv LoadChanges.dse LoadChanges.dse.orig
cp LoadChangesDomino.dse LoadChanges.dse
```
2. Repeat step 1 for all HTTP servers that handle a Domino job.

 **NOTE:**

You can now use the DAS job form in PCC Web administration to change the username mapping for IAP login. See [“Creating DAS jobs”](#) on page 372.

Directory Integration

HP EAs Domino 2.1 and IAP 2.1 include support for three new features:

- IAP repositories for shared mailboxes, which are represented as mail-in databases in the Domino Directory. Access control is provided via mappings from (Domino or LDAP) directory groups.
- An IAP repository retention period that is set via an attribute in the Domino Directory for each user or shared mailbox.
- Legacy email address support, which gives users access to messages archived under an old email address.

The DAS process has been changed to support this functionality.

On the EAs Domino side, support for these features is established in changes to the HP Gateway server configuration and the addition of the DAS Names database and DAS Names Configuration document. See [“Preparing the HP Gateway server for DAS”](#) on page 81.

On the IAP side, support for the shared mailboxes and repository retention attribute must be enabled in the PCC Service Tools. No changes are made on the IAP to add support for legacy email addresses. However, a DAS job does take longer to run when this feature is implemented.

Enabling the Integrated Directory features on the IAP

The shared mailbox and retention features are disabled by default in the IAP. To enable them, follow these steps:

1. Log into PCC Web administration as the IAP super user.
2. If the DAS job to import users has not been previously created, create the DAS job. Follow the instructions in [“Creating and running DAS jobs”](#) on page 371.
3. Navigate to **Service Tools > View Cell Space**.

4. In the Other Servers area of View Cell Space, open the HTTP server on which the DAS job is run and perform these steps.
 - a. Locate and click **name=DASMBean**.
 - b. In the list of MBean operations, locate:


```
enableRetentionAndAccessManagementViaLdap(String dasJob, int
minimumRetentionPeriod)
```
 - c. Set the following ParamName values:
 - DasJob: Enter the name of the DAS job.
 - MinimumRetentionPeriod: Enter the iapRepositoryRetention value, in days. This value cannot be less than the domain retention period.
 - d. Click **Invoke**.
5. Run the DAS job with the initialize option set to true.

DAS will now pull in the shared mailboxes and iapRepositoryRetention value.

Confirming success

After the DAS job has completed successfully, verify the importation of users and shared mailboxes by following these steps in PCC Web administration:

1. Check the job history log on the main Account Synchronization page.

You should see the expected number of imported users and groups.

The status message below states that eight users have been imported along with four groups (shared mailboxes).

Job(s) History Logs:

This log contains the job name, the number of Integrated Archive Platform users/groups that have been added, modified, or deleted, and the date/time the job was completed.

Previous DAS Job Runs						
Job Name	Added [User(s)/Group (s)]	Updated [User(s)/Group (s)]	Delete [User(s)/Group (s)]	Elapse time	State	Date
domino	8 / 4	0 / 0	0 / 0	4s	🟢 >>>>	2009-11-20 10:01:07

- Verify that the shared mailboxes have been imported as groups by clicking **Group** in the PCC Account Manager page.

User Management / Accounts Manager 9 Users.
4 Groups.
Domains: sparta.com

Search for: User Group Repository

Group Name: Email:

<input type="checkbox"/>	Group Name	Email
<input type="checkbox"/>	Shared Mailbox 4 with spaces_change (ShortName)@API1	sharedmailbox4withspaces@test11.com
<input type="checkbox"/>	SharedMailbox1 (ShortName)@API1	sharedmailbox1@test1.com
<input type="checkbox"/>	SharedMailbox2/Test/IAP (ShortName)@API1	sharedmailbox2@test1.com
<input type="checkbox"/>	SharedMailbox3 (ShortName)@API1	sharedmailbox3@test1.com

- Select one or more users and verify they have access to the shared mailbox of which they are members.

Click **User** on the Account Manager page, and check the user's repository access list.

User Management / Accounts Manager 9 Users.
4 Groups.
Domains: sparta.com

Search for: User Group Repository

User Name: First Name: Last Name: Email:

W X Y Z

Integrated Archive Platform Account Information:

Username:

Local

Password:

First Name:

Last Name:

Email Contact:

Mail To Me Address:

Comments:

Domain:

Mail Server:

Billing Group ID:

Personal Repository:

Direct Repositories:

LDAP information:

Membership:

WinDomain:

LDAP Dn:

Source:

ObjectGUID:

ObjectSID:

USNChange:

Created Date:

Last Modified:

All Repositories:

Proxies:

4. Verify that the repository retention period has been correctly set for a user or shared mailbox. Click **Repository** on the Account Manager page, select the user or group, and then check the retention value.

The screenshot shows the 'User Management / Accounts Manager' interface. At the top, there are search options for 'User', 'Group', and 'Repository', with 'Repository' selected. Below this, there are input fields for 'Repository for User:' and 'Repository Name:', followed by a 'Search' button. A navigation bar contains tabs for 'All', 'Regulated', 'Unregulated', 'Quarantine', and 'Other'. The main content area displays details for an 'IAP Repository':

- Name: GUID.6CEC0697FB177F7C8525764A006139B1.repository
- ID: 0b000c29b21b9912477c300f41
- Domain: sparta.com
- Retention: 250 (highlighted with a red box)
- Type: Unregulated
- E-Mail Routing: alice_balice@test1@test1

Below the repository details, there is a checkbox labeled 'Check this box to delete the selected EMail routings from list above.' and an 'Add EMail:' input field. At the bottom, there is an 'EMailDomain Routing:' input field.

Disabling the Integrated Directory features

Follow these steps to disable the shared mailbox and retention period features.

1. Log into PCC Web administration as the IAP super user and navigate to **Service Tools > View Cell Space**.
2. In the Other Servers area of View Cell Space, open the HTTP server on which the DAS job is run.
3. Locate and click **name=DASMBean**.
4. In the list of MBean operations, locate:
`disableRetentionAndAccessManagementViaLdap(String DasJob)`
5. For ParamName, enter the DAS job running the new features, and then click **Invoke**.
6. Navigate to **User Management > Account Synchronization**.
7. Run the DAS job with the initialize option set to true.

After the DAS job is run, the Integrated Directory features are disabled. DAS will not update or import shared mailboxes or use the `iapRepositoryRetention` attribute.

 **NOTE:**

The shared mailboxes, access lists, and repository retention periods that have already been imported into the IAP are not removed or changed when you disable the Integrated Directory features.

Troubleshooting

To troubleshoot installation of the shared mailbox and retention features:

1. On the HTTP portal where the DAS job is running:
 - a. Open the following log files using vim or another text editor:
 - `/var/log/jboss/stdout.log.X`
 - `/var/log/jboss/daslog.txt`
 - b. Check the logs for errors.
2. Verify that:
 - The new features are enabled.
 - `LoadChangesDomino.dse` was moved to the `LoadChanges.dse` file.
 - The configuration was enabled on the HTTP portal. See [“Assigning HTTP portals”](#) on page 374.

Account security

The Domino LDAP service provides authentication when HP EAs Domino users connect to the IAP Web Interface to search for and retrieve archived messages. It is very important that all users have a valid Internet Password. Domino LDAP authenticates users via the Internet Password field in the user's Domino Directory Person document. A blank Internet password would allow anyone to easily log into the user's IAP account.

This is particularly important in organizations that only use the Notes client to access Domino, and might not have had any prior reason to set Internet passwords.

Refer to the Domino Administrator help topics [“Setting up password verification,”](#) [“Managing Internet passwords,”](#) and [“Providing additional security for Internet passwords”](#) for information about setting up Internet passwords.

SSL is not supported for communication between the HP Gateway server and the IAP in HP EAs Domino release 2.1.x.

Creating and running DAS jobs

Use the instructions in this section to create and run a DAS job.

1. Log in to PCC Web Administration, and navigate to **User Management > Account Synchronization**.
2. Create an LDAP connection. See “[Creating LDAP server connections](#)” on page 371.
3. Create the DAS 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 DAS jobs](#)” on page 372.
4. Assign the job to an HTTP portal. See “[Assigning HTTP portals](#)” on page 374.
5. Run the job. See “[Starting, scheduling, and stopping DAS jobs](#)” on page 376.

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:

Connection Name	<input type="text" value="Domino LDAP"/>
Host Name	<input type="text" value="15.00.00.000"/>
Binder user	<input type="text" value="cn=Administrator,O=Company"/>
Binder password	<input type="password" value="*****"/>
Directory Server type	<input type="text" value="Lotus Domino"/>
Security Option	<input type="text" value="Simple LDAP"/>
Port	<input type="text" value="389"/>

- Connection Name: Name used to identify the LDAP connection.
- Host Name: 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 user objects.
For example, if the Notes address is CN=Administrator/O=Company the Binder user would be **cn=Administrator,O=Company**.

❗ **IMPORTANT:**

Be sure to use commas in the binder username for LDAP connections.

- 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 the 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 page and verify that the new LDAP server connection is listed under LDAP Server Connectors.

Creating DAS jobs

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, and then click **Next Step**.

Job Name:
(the field cannot be blank or contain a "*@ \$ % ^ & . , ; : * # () [] \ { + } ~ = - | " character.)

3. From the drop-down list, select the LDAP connection you want to use with the job.
The LDAP connection must already be created.
4. Click **Next Step**.
5. Complete the form by entering the following information:
 - LDAP Domain name: Domain to which the users belong. For example: dominoscale.com.
 - LDAP Starting Point: Root node where the user accounts are stored.
Leave this box empty to pull information from DAS Names.
 - 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 the `Domain.jcml` file.
 - Deletion Starting Point: The root node where deleted user objects are stored on the LDAP server.
Ignore this box because it is not enabled for Domino.

6. Click the Advanced Options icon (🔍) and edit the value in the **LDAP Attribute to Map to Username** box at the bottom of the form.

Parameter Value	
Job ID	DominoDASJob
LDAP Domain Name	dominoscale.com
LDAP Job Starting Point	
IAP Domain ID	domino1
Delete Starting Point	N/A
Advanced Options: 🔍	
USNChanged	1
Delete USNChanged	0
Audit Repository	R0000000
Update LDAP Filter	(objectclass=dominoPerson)(mail=*)
LDAP Query Return Attributes	uid,sn,modifytimestamp,createtimestamp,cn,givenName,mail,sn,dominoid,dominodn,dominoproxyaddresses,maildomain,iaprepositoryretention
Delete LDAP Filter	N/A
LDAP Attribute to Map to Username	uid
<input type="button" value="Update"/> <input type="button" value="Back To Main Page"/>	

The other advanced options should not be changed.

Field	Description
USNChanged	This box is not enabled for Domino.
Delete USNChanged	This box is not enabled for Domino.
Audit Repository	Do not change.
Update LDAP filter	Criteria to include or exclude specific users. (Cannot be edited.) For Domino users: (objectclass=dominoPerson)(mail=*) . For shared mailboxes: (objectclass=dominoServerMailInDatabase)(mail=*)
LDAP Query return attributes	List of return attributes. (Cannot be edited.) The following LDAP attributes may be used: uid, sn, modifytimestamp, givenName, mail, sn, dominoid, dominodn, dominoproxyaddresses, maildomain, iaprepositoryretention.
Delete LDAP Filter	This box is not enabled for Domino.

Field	Description
LDAP Attribute to Map to Username	<p>Click the arrow and select one of the following LDAP attributes to determine how users log into the IAP Web Interface:</p> <ul style="list-style-type: none"> uid: This is the default attribute, which corresponds to the Notes ShortName. Select uid if users log into the IAP using their ShortName or ShortName@MailDomain. In EAs Domino 2.1.2, a Notes formula can be used to substitute other consolidated directory field(s) for ShortName. For example, users could log in to the IAP using their Employee ID. See “Directory Entry Settings” on page 91 for information on creating the formula. mail: This attribute corresponds to the Notes InternetAddress. Select mail if users enter their full email address to log into the IAP.

7. Click **Next Step**.

A status page appears, stating that the mapping has been updated for the new job. You are asked if you want to attach the job to a HTTP portal.

8. Click **Assign Job** to continue, then follow the instructions in [Assigning HTTP portals](#) below.

If a HTTP portal is not available for the new job because it is being used for another job, click **Back to Main Page**, and unassign the HTTP portal. See “[Unassigning and reassigning a portal](#)” on page 376 for the steps to take.

Assigning HTTP portals

Before running a DAS job, assign a HTTP portal on which to run the job. Only one job can be assigned to a HTTP portal. These steps are performed in the DAS Available Jobs area of the Dynamic Account Synchronization page.

Assigning a portal

When you click **Assign Job** after creating a new job, the Assign a Job page appears:

Job Name	DominoDASJob
DAS server IP	10.0.71.2
Configuration Enabled	<input checked="" type="radio"/> Yes <input type="radio"/> No
Configuration running state	0
Period (minutes)	0
DAS server running state	

Complete the form to assign a HTTP portal to the job.

1. Enter the following information:
 - 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.
2. Click **Save**.

Unassigning and reassigning a portal

If all HTTP portals are being used for other jobs and none are available for a new job, reassign a HTTP portal from another job.

To reassign a HTTP portal:

1. Select an existing DAS job in DAS Available Jobs, and then click **Unassign HTTP**.
2. Select the new job.

The Job Update page appears.

Job Update page:

Job Name	DominoDASJob	
LDAP Server Name	DominoLDAP	Edit
Mapping Domain	dominoscale.com	
LDAP Starting Point		Edit
HTTP Server State		Edit

Back To Main Page Delete

3. Click **Edit** in **HTTP Server State**.
The Assign a Job page appears.
4. Complete the form by following the instructions in [Assigning a portal](#).
5. Start the job by following the instructions in the next section.
The DAS setup must be initialized whenever a new HTTP portal is assigned to a job.

Starting, scheduling, and stopping DAS jobs

If you are running DAS for the first time or have assigned a DAS job to a new HTTP portal, follow these steps:

1. In DAS Available Jobs, select the job and click **Stop/Start**.
The job control page appears.
2. Schedule the job:
 - a. Click **Schedule**.
 - b. Enter the number of minutes between job runs.
To run a job once, enter **0**. To run a job continuously, set the interval so that it is equal to or greater than 60 minutes.
 - c. Click **Confirm Schedule** to save your changes.
You are returned to the job control page.

3. Click **Yes** in **Initialize DAS setup**.

Initialize DAS setup: Yes No

Launch the Selected Job: **Start**

Set the Job Schedule: **Schedule**

Stop the selected Job: **Stop**

4. Click **Start**.
A notice appears stating that the job started successfully.
5. Click **Back to Main Page**.

To start a DAS job when DAS has already been initialized and the HTTP portal has not changed:


1. Select the job in DAS Available Jobs.
2. Schedule the job if you have not already done so:
 - a. Click **Schedule**.
 - b. Enter the number of minutes between job runs.
To run a job once, enter **0**. To run a job continuously, set the interval so that it is equal to or greater than 60 minutes.
 - c. Click **Confirm Schedule** to save your changes.
3. Click **Start**.
4. If necessary, click **Back to Main Page**.

To stop a DAS job from running:

1. In DAS Available Jobs, select the job, and then click **Start/Stop**.
2. In the job control page, click **Stop**.
A notice appears stating that the job has stopped. When the DAS job is stopped, DAS will unschedule itself and will not run the DAS job any more. (A currently running DAS job will not stop.)
3. Click **Back to Main Page**.

Editing or deleting jobs

To edit an active or configured DAS job:

1. In DAS Available Jobs, select the job and click **Edit**.
2. Make any changes needed for the job mapping.
3. Click the Advanced Options icon () to edit any advanced options.
See "[Creating DAS jobs](#)" on page 372 for information about job options.
4. Click **Update**.
A confirmation page appears.

5. Click **Assign Job** and ensure that a HTTP portal is selected and the configuration is enabled.
If you are changing the HTTP portal on which a job is running, select the new portal from the drop-down list.
6. Click **Save**.
7. If you changed the HTTP portal for the job:
 - a. Click **Back to Main Page**.
 - b. Follow the steps in “[Starting, scheduling, and stopping DAS jobs](#)” on page 376.
The DAS setup must be reinitialized whenever the HTTP portal is changed.
8. If you did not change the HTTP portal, you can click **Back to Main Page** or click **Run Job** to start the job.

To delete a DAS job:

1. In DAS Available Jobs, select the name of the job to delete.
2. Click **Delete**.
3. If you are deleting a job without an assigned HTTP portal:
 - a. In DAS Available Jobs, click the job.
 - b. On the Job Update page, click **Delete**, and then click **Delete Job**.
 - c. Click **Back to Main Page**.

Managing available HTTP portals

To assign or unassign a HTTP portal for a job, see “[Unassigning and reassigning a portal](#)” on page 376.

Editing or deleting available LDAP connections

To edit or delete an LDAP connection:

1. In the LDAP Server Connectors area of the DAS page, click the name of the connection you want to edit or delete.
2. To edit the connection, click **Edit**, complete the form, and click **Save**.
3. To delete the connection, click **Delete**.
4. Click **Back to Main Page** when you are finished.

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 or 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 page.

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.

 **NOTE:**

In EAs Domino, a DAS job adds IAP users or modifies the account information for existing users. It does not delete users.

Users who are deleted from the Domino Directory are not automatically deleted from the IAP when the DAS job runs. Any users deleted from the Domino Directory **must** be manually deleted from the IAP.

H Indexed file types and MIME types

The following file types and MIME content-types are indexed by the IAP. You can search the contents of archived files or email attachments if their file type is listed in this table.

Table 12 IAP indexed file types and MIME types

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

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

I Support and other resources

Related documentation

In addition to this guide, HP provides the following documentation for HP EAs Domino and the IAP:

- *HP Email Archiving software for IBM Lotus Domino User Guide*
- *HP Email Archiving software for IBM Lotus Domino Release Notes*
- *HP Integrated Archive Platform Installation Guide*
- *HP Integrated Archive Platform Administrator Guide*
- *HP Integrated Archive Platform User Guide*

Additional information

For more information on the HP Integrated Archive Platform, visit:

www.hp.com/go/ILM

To learn more about HP's award winning industry hardware, visit the HP Web site at:

www.hp.com

Visit HP ActiveAnswers Web site at:

www.hp.com/solutions/activeanswers/

Support

You can visit the HP Software Support Web site at: <http://www.hp.com/go/hpsupport>

HP Software Support Online provides an efficient way to access interactive technical support tools. As a valued support customer, you can benefit by using the support site to:

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

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

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

Subscription service

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

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

Document conventions and symbols

Table 13 Document conventions

Convention	Element
Medium blue text: Related documentation	Cross-reference links and email addresses
Medium blue, underlined text (http://www.hp.com)	Web site addresses
Bold font	<ul style="list-style-type: none">• Key names• Text typed into a GUI element, such as into a box• GUI elements that are clicked or selected, such as menu and list items, buttons, and check boxes
<i>Italic font</i>	Text emphasis
Monospace font	<ul style="list-style-type: none">• File and directory names• System output• Code• Text typed at the command line
<i>Monospace, italic font</i>	<ul style="list-style-type: none">• Code variables• Command-line variables
Monospace, bold font	Emphasis of file and directory names, system output, code, and text typed at the command line

! **IMPORTANT:**

Provides clarifying information or specific instructions.

📝 **NOTE:**

Provides additional information.

Index

unable to open index table of Mail Details records, [327](#)

A

Access Control List

Advanced Filtering, [205](#)

DWA Extension, [258](#)

EAs Domino databases on HP Gateway server, [80](#)

Export Search, [273](#)

Advanced Filtering

configuration, [29](#)

definition, [19](#)

installation, [202](#)

journaling rules, [206](#)

server requirements, [35](#)

Agent Manager, recommended options, [57](#)

Archive agent, [191](#), [221](#), [227](#)

archive document size limitations, [164](#), [201](#)

archive references, viewing, [198](#)

archive traffic, [170](#)

archiving configurations, [24](#)

archiving instructions, [159](#)

archiving statistics, [249](#)

ATT attachments, [327](#)

attachments, message, [164](#), [313](#)

B

binaries, EAs Domino, [74](#)

Bulk Upload

configuration, [32](#)

defined, [223](#)

definition, [19](#)

determining mail file owner, [228](#)

mining files, [229](#)

mining profile, [226](#)

scan mail files, [227](#)

C

certifier ID, [44](#)

collecting held messages, [190](#), [317](#)

compliance archiving, [201](#)

Advanced Filtering, [202](#)

archiving steps, [217](#)

definition, [19](#)

mail-in database, [165](#)

mining rule, [218](#)

native journaling, [211](#)

consolidated Domino Directory, [83](#)

D

DAS

changes in EAs-D 2.1, [81](#)

changes on IAP, [366](#)

consolidated directory, [83](#)

creating and running jobs, [371](#)

DAS backup server, [97](#)

DAS Names Configuration document, [89](#)

DAS Names database, [81](#)

definition, [20](#)

Directory Assistance, [86](#)

editing or deleting jobs, [377](#)

group mailbox support, [81](#), [366](#)

LDAP server connection, [371](#)

Populate DAS Names agent, [96](#)

preparing HP Gateway, [81](#)

repository retention attribute, [81](#), [366](#)

scheduling jobs, [376](#)

starting jobs, [376](#)

stopping jobs, [376](#)

troubleshooting, [322](#)

verifying LDAP configuration, [88](#)

data

archiving, [17](#)

querying, [17](#), [271](#)

database templates, EAs Domino, [65](#), [66](#)

databases, compacting, [335](#)

databases, EAs Domino, [65](#)

debugging options, [155](#), [182](#), [266](#)

deploying HP Gateway installation, [100](#)

Directory Assistance, [86](#)

distribution lists, expanding, [150](#)

DLD download file

associating with Export Search, [269](#)

DLD file type association, [331](#)

DWA Extension, 153
cache retention, 144
configuration, 30
configuration steps, 259
definition, 19
installing, 256
server definition settings, 153
server requirements, 35
Tombstone Prototype document, 170, 261
tombstone settings, 170, 266

E

EAs Domino
administrative applications, 17
Agent Manager values, 57
binaries, 74
client applications, 18
compliance archiving, 201
configuring, 137
creating new databases, 353
database templates, 66
databases, 65
definition, 17, 18
deploying server software, 100
Global Configuration document, 139
installing archiving software (new installation), 77
installing software on HP Gateway, 77
migrating to new HP Gateway server, 127
notes.ini entries on server, 73
opening, 137
post-installation tasks, 131
preprocessing databases, 177
selective archiving, 159
Server Definition document, 147
uninstalling software, 131
upgrading components on customer servers, 123
upgrading existing remote mining configuration, 110
upgrading from earlier version, 105
upgrading to remote mining, 106
EAs-D API main view, 137
EAs-D Users database, 185
email distribution lists, expanding, 150
Encapsulate agent, 182, 221, 227
encapsulated files, 175, 182, 310, 313, 327
temporary work area, 179
temporary work area for DWA, 153
Encapsulation Tools, 320
encrypted messages, 206, 257, 310, 313
EnsureOwnerReceipt, 150
error messages, IAP, 318
exception settings, 163

Export Search, 269, 299
ACL, 273
configuration, 31
installing server files, 272
troubleshooting, 271, 331
using the Desktop tool to export messages, 269
using the server to export messages, 272
Web Interface, 39
Extended Directory Catalog, 85, 90
extracting exported messages from DLD file, 275

F

File Identification table, 328
file types, indexed, 381
Find Parent tool, 320
folder settings, 162
folder support, disabling, 365
foreign SMTP domain documents, 58

G

Get Held Messages, 190, 317
Global Configuration document, 139

H

held messages, 190, 317, 336
help
obtaining, 383
HP
Subscriber's choice Web site, 384
technical support, 383
HP Gateway
improving server performance, 335

- HP Gateway server, 21
 - compacting databases, 335
 - configuring, 55
 - configuring foreign SMTP domain documents, 58
 - Connection documents to customer servers, 57
 - creating configuration document, 59
 - creating SMTP connection, 59
 - definition, 18
 - Directory Assistance, 86
 - Gateway server connection documents, 52
 - installing additional HP Gateway servers, 49
 - installing Domino server software, 44
 - installing Java Runtime Environment, 48
 - installing Lotus Notes client software, 48
 - installing Windows server software, 43
 - limiting Domino log size, 60
 - monitoring, 336
 - setting security, 56
- HP_ReferenceInfo, 168
- HP_SessionInfo, 168

I

- IAP
 - applications, 17
 - definition, 18
- IAP Web Interface, 18, 299
 - creating link in navigation pane, 300
 - defined, 299
 - exporting messages, 269, 299
 - supported browsers, 38
 - viewing signed and encrypted messages, 313
- improving EAs Domino performance, 335
- installation worksheets, 339, 347
- installing
 - additional HP Gateway servers, 49
 - Advanced Filtering, 202
 - Bulk Upload, 223
 - DWA Extension, 256
 - EAs Domino software on HP Gateway, 77
 - Export Search server files, 272
 - Local Cache, 302
 - Lotus Domino server software on HP Gateway, 44
 - Windows Notes Client plug-in, 308

J

- Japanese data issues, 361
- Java Runtime Environment, 48, 302

- journaling, 201
 - EAs Domino, 201
 - EAs Domino (Advanced Filtering), 206
 - EAs journal database, 201, 209
 - enabling mining agents, 191
 - enabling preprocessing agent, 182
 - exceptions, 208
 - incoming messages, 207
 - mail-in database, 209
 - messages, maximum size, 201
 - native Domino, 201
 - outgoing messages, 207
 - preprocessing files, 199
 - preprocessing messages, 175
 - rules, 140, 206
 - rules, Advanced Filtering, 209, 210
 - schedule, 193, 221

L

- large distribution lists, 150
- LDAP
 - changes to DAS process, 81, 366
 - mapping IAP user attributes, 365
 - server connection, 371
 - synchronization, 86
 - user authentication, 370
 - verifying configuration, 88
- LDAP connection to IAP
 - IAP configuration, 371
- legal hold, 271
- LNLM, setting in Domain.jcml, 365
- LoadChanges file, 298, 365
- Local Cache, 299, 308, 311
 - configuring, 303
 - defined, 301
 - installing, 302
 - SSL support, 305
- log files, 140, 231, 331
 - purging mining entries, 236
- logging, 322
- Lotus Domino
 - releases supported, 35
 - server requirements, 35
- Lotus Domino network architecture, 21
- Lotus Domino server software
 - installing on HP Gateway, 44

Lotus Notes clients
adding tombstone icon, [312](#)
creating link to IAP Web Interface, [300](#)
EAs Domino applications, [299](#)
Local Cache, [301](#)
retrieving signed and encrypted messages, [313](#)
supported versions, [38](#)
Windows Notes Client Plug-in with Local Cache, [311](#)
Windows plug-in, [308](#)

M

Mail Detail records, [185](#), [220](#)
enabling activity log, [189](#)
Mail Detail records, Bulk Upload, [226](#)
mail-in database, [166](#), [201](#), [209](#), [220](#)
Mail-To-Me messages, [208](#), [215](#)
mail.box
backup, [320](#)
consolidating, [321](#)
setup in configuration document, [60](#)
mailboxes, user, [185](#)
message reprocessing, [318](#)
messages, maximum size, [159](#), [164](#), [201](#)
MIME content type, [381](#)
mining agents, [191](#), [221](#)
mining configurations
Active Gateway, [25](#)
dedicated journal server, [26](#)
replicated journal, [27](#)
scalable multi-Gateway, [28](#)
mining job, [193](#), [221](#)
running, [195](#)
mining log, [140](#), [231](#)
MTM Cleanup agent, [216](#)
mwadv task, [210](#)

N

native journaling, [211](#)
notes.ini, EAs Domino entries on server, [73](#)

O

on demand archiving, [162](#)
operating systems supported, [35](#)
organization unit certifier, [44](#)

P

PCC, [18](#)
pending transactions, [199](#)

performance, improving, [335](#)
compacting databases, [335](#)
limiting Domino server log size, [60](#)
monitoring HP Gateway server, [336](#)
performance, improving HP Gateway, [335](#)
phone message form, [331](#)
PKI encryption, [313](#)
platforms supported, [35](#)
Preprocessing Control document, [177](#), [226](#)
preprocessing databases, [177](#), [182](#)
preprocessing temporary directory, [177](#)
prerequisites for installation, [17](#)
Profile Agent, [185](#)
program document, rissminer, [193](#)
Proxy Gateway document, [260](#)
Purge Not Synchronized person document agent, [188](#)
Purge Stats Selective Archive Log agent, [189](#)
purging alerts, [247](#)
purging export requests, [285](#)
purging statistics, [251](#)
purging tombstone conversion requests, [267](#)

Q

Quattro Pro, [382](#)
query results, saving, [271](#)
querying data, [17](#)

R

reference databases, [167](#), [182](#), [191](#), [198](#), [221](#)
refreshing design of EAs Domino applications, [354](#)
related documentation, [383](#)
remote mining, [24](#)
definition, [19](#)
replacing design of EAs Domino applications, [355](#)
repositories, IAP
definition, [18](#)
Reset Status tool, [320](#)
rissminer
definition, [19](#)
rissminer program, [193](#)

S

S/MIME encryption, [313](#)
saving query results, [271](#)
security, HP Gateway server, [56](#)

- selective archiving
 - adding users to profile, 185
 - archive traffic, 170
 - archiving dates, 161
 - configuring, 159
 - creating profile, 160
 - definition, 19
 - document size limitations, 164
 - enabling mining agents, 191, 221
 - enabling preprocessing agent, 182
 - error alert, 173
 - exceptions, 163
 - folder settings, 162
 - instructions, 159
 - log files, 140, 231
 - message attachments, 164
 - messages, maximum size, 159
 - on demand archiving, 162
 - preprocessing files, 199
 - preprocessing messages, 175
 - profile, 166
 - Profile Agent, 185
 - Purge Not Synchronized person document agent, 188
 - Purge Stats Selective Archive Log agent, 189
 - reference database, 167, 191, 198
 - running job, 195
 - scheduling jobs, 193, 221
 - synchronizing users, 185
 - Time Conditions, 161
 - User Activity Alert agent, 187
 - user mailboxes, 185
 - user notification, 172
 - user profile, 165
 - viewing archiving references, 198
- server crashes, avoiding, 57, 320
- server definition document
 - debugging options, 155
- server ID
 - backing up, 53
 - creating, 49
- session settings, 170
- session size, 152, 181
- signed and encrypted messages, 153, 175
- signed messages, 310, 313
- single sign-on
 - configuring EAs Domino files, 289
 - configuring on the IAP, 297
 - Generate SSO Tokens agent, 290
 - Search the IAP Archive agent, 294
 - secret key lost when IAP kickstarted, 298
- SMTP connection, HP Gateway to IAP, 59
- statistics, archiving, 249
- Subscriber's choice, 384
- synchronizing users, 185

T

- technical support
 - HP, 383
- tombstone
 - definition, 19
- Tombstone agent, 191
- tombstone icon, 312
- tombstone settings, 168
- traffic, archive, 170
- troubleshooting, 317
 - archiving issues, 326
 - avoiding server crashes, 320
 - capturing data for HP support, 317
 - DAS, 322
 - Export Search desktop tool, 331
 - held messages, 317
 - IAP DAS installation, 370
 - IAP error messages, 318
 - Japanese data issues, 361
 - mail routing issues, 320
 - message reprocessing, 318
 - Notes Client plug-in, 330
 - Notes plug-in, 331
 - reference database tools, 320
- troubleshooting tools, 155, 320

U

- unable to open index table of Mail Details records, 327
- uninstalling EAs Domino software, 131
- upgrading database design, 354, 355
- upgrading EAs Domino software, 105
 - migrating to new HP Gateway server, 127
- upgrading components on customer servers, 123
 - upgrading existing remote mining configuration, 110
 - upgrading from local to remote mining, 106
- User Activity Alert agent, 187
- user database agents, 187
- Users database, 185

W

- Web browsers, supported
 - Export Search Web Interface, 39
 - IAP Web Interface, 38
- Web sites
 - HP Subscriber's choice, 384
- wildcards, 166, 167, 207, 208
- Windows Notes Client Plug-in, 299, 308
 - configuring, 308
 - phone message form, 331
 - troubleshooting, 330

Windows Notes Client Plug-in with Local Cache, [311](#)
Windows users, [301](#), [311](#)
WordPerfect, [382](#)
WordPerfect Presentations, [382](#)
worksheets, installation, [339](#), [347](#)