

Symantec Enterprise Vault™

Setting up Domino Server Archiving

9.0

Symantec Enterprise Vault: Setting up Domino Server Archiving

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Last updated: 2011-10-21.

Legal Notice

Copyright © 2011 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, Veritas, Enterprise Vault, Compliance Accelerator, and Discovery Accelerator are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party ("Third Party Programs"). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the *Third Party Software* file accompanying this Symantec product for more information on the Third Party Programs.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
350 Ellis Street, Mountain View, CA 94043

<http://www.symantec.com>

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our Web site at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level

- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
 - Error messages and log files
 - Troubleshooting that was performed before contacting Symantec
 - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Contents

Technical Support	3
Chapter 1 About this guide	11
Introducing this guide	11
Where to get more information about Enterprise Vault	11
"How To" articles on the Symantec Enterprise Support site	13
Comment on the documentation	14
Chapter 2 Setting up Domino mailbox archiving	15
About Domino mailbox archiving	15
Preparation for Domino mailbox archiving	18
Check Enterprise Vault configuration of Domino server	18
Configure Enterprise Vault for Web connections in preparation for Domino mailbox archiving	19
Vault store group, vault store, and partition in preparation for Domino mailbox archiving	20
Configuring Domino targets, tasks and policies in Enterprise Vault	21
Checking the list of Domino forms	21
Adding Domino Server archiving targets	22
Configuring mailbox policies for Domino mailbox archiving	24
Domino mailbox archiving retention folders	31
Configuring desktop policies for Domino mailbox archiving	32
Creating a Domino Provisioning task	36
Creating a Domino Mailbox task	36
Reviewing the default archiving settings for the Site when setting up Domino mailbox archiving	37
Adding a Provisioning Group when setting up Domino mailbox archiving	38
Installing Enterprise Vault extensions for Lotus Notes and DWA clients	40
About Enterprise Vault clients for Lotus Notes and DWA clients	40
Installing Enterprise Vault client extensions for Lotus Notes and DWA clients	42

Setting up an account to use EVInstall.nsf to set up an Enterprise Vault Domino Gateway	42
Setting up an account to use EVInstall.nsf to set up a mail server	44
Granting Execution Control List permissions when setting up Lotus Notes and DWA clients	44
Installing the Lotus Notes and DWA client extensions	46
Changes made by EVInstall.nsf when setting up Domino mailbox archiving	48
Updating mail files with the new design after installing the Lotus Notes and DWA extensions	54
How users access Enterprise Vault Search features after installing the Lotus Notes and DWA extensions	55
Identifying internal Notes mail recipients	56
How to edit automatic messages after installing Domino mailbox archiving	56
Editing the Welcome message after installing Domino mailbox archiving	57
Enabling mailboxes for archiving after installing Domino mailbox archiving	57

Chapter 3	Setting up a Vault Cache for offline users	61
	About Vault Cache for Domino users	61
	Enabling users for Vault Cache with the Domino Desktop policy	62
	Setting permissions on the Enterprise Vault Domino Gateway when using Vault Cache	63
	Disabling Vault Cache using the Domino Desktop policy	63
	Troubleshooting setting up Vault Cache for Domino	64
	Newly-enabled Vault Cache for Domino is not populated	64

Chapter 4	Setting up Domino Journaling archiving	67
	Preparation for Domino Journaling archiving	67
	Adding a Domino domain	68
	Adding a Domino server	68
	Assigning a vault store for Domino Journaling	68
	Creating a Domino Journal archive	69
	Adding permissions to the Domino journal archive	70
	Creating a Domino Journal policy	70
	Creating a Domino Journaling task	71
	Adding a Domino Journaling location	71
	Identifying internal Notes mail recipients	72

	How to configure clients when setting up Domino Journal archiving	72
	Note on using a Lotus Notes client when setting up Domino Journal archiving	73
Chapter 5	Configuring filtering	75
	About filtering	75
	Configuring custom filtering	76
	About custom filtering in distributed Enterprise Vault environments	77
	Configuring registry settings for Domino server journal filtering	78
	About custom filtering ruleset files	80
	About controlling default custom filtering behavior	82
	About the general format of ruleset files for custom filtering	86
	About rule actions for custom filtering	89
	About message attribute filters for custom filtering	90
	Example ruleset file for custom filtering	101
	Configuring custom properties and content categories	105
	About the general format of Custom Properties.xml	108
	Defining additional Domino message properties in custom properties	110
	About content categories	112
	Defining how custom properties are presented in third party applications	115
	Summary of custom property elements and attributes	120
Index		125

About this guide

This chapter includes the following topics:

- [Introducing this guide](#)
- [Where to get more information about Enterprise Vault](#)
- [Comment on the documentation](#)

Introducing this guide

This guide describes how to set up Enterprise Vault so that you can archive items from Domino mail files and journal databases.

The guide assumes that you know how to administer the following Microsoft products:

- Microsoft Windows Server 2003 or Windows Server 2008
- IBM Domino Server
- IBM Lotus Notes client
- Microsoft SQL Server
- Microsoft Internet Information Services (IIS)

Where to get more information about Enterprise Vault

[Table 1-1](#) lists the documentation that accompanies Enterprise Vault.

Table 1-1 Enterprise Vault documentation set

Document	Comments
Symantec Enterprise Vault Help	<p>Includes all the following documentation so that you can search across all files. You can access this file by doing either of the following:</p> <ul style="list-style-type: none"> ■ On the Windows Start menu, click Start > Programs > Enterprise Vault > Documentation. ■ In the Administration Console, click Help > Help on Enterprise Vault.
<i>Introduction and Planning</i>	Provides an overview of Enterprise Vault functionality.
<i>Deployment Scanner</i>	Describes how to check the prerequisite software and settings before you install Enterprise Vault.
<i>Installing and Configuring</i>	Provides detailed information on setting up Enterprise Vault.
<i>Upgrade Instructions</i>	Describes how to upgrade an existing Enterprise Vault installation to the latest version.
<i>Setting up Exchange Server Archiving</i>	Describes how to archive items from Microsoft Exchange user mailboxes, journal mailboxes, and public folders.
<i>Setting up Domino Server Archiving</i>	Describes how to archive items from Domino mail files and journal databases.
<i>Setting up File System Archiving</i>	Describes how to archive the files that are held on network file servers.
<i>Setting up SharePoint Server Archiving</i>	Describes how to archive the documents that are held on Microsoft SharePoint servers.
<i>Setting up SMTP Archiving</i>	Describes how to archive SMTP messages from other messaging servers.
<i>Administrator's Guide</i>	Describes how to perform day-to-day administration, backup, and recovery procedures.

Table 1-1 Enterprise Vault documentation set (*continued*)

Document	Comments
<i>Reporting</i>	Describes how to implement Enterprise Vault Reporting, which provides reports on the status of Enterprise Vault servers, archives, and archived items. If you configure FSA Reporting, additional reports are available for file servers and their volumes.
<i>Utilities</i>	Describes the Enterprise Vault tools and utilities.
<i>Registry Values</i>	A reference document that lists the registry values with which you can modify many aspects of Enterprise Vault behavior.
Help for Administration Console	The online Help for the Enterprise Vault Administration Console.
Help for Enterprise Vault Operations Manager	The online Help for Enterprise Vault Operations Manager.

For the latest information on supported devices and versions of software, see the *Enterprise Vault Compatibility Charts* book, which is available from this address:
<http://www.symantec.com/docs/TECH38537>

"How To" articles on the Symantec Enterprise Support site

Most of the information in the Enterprise Vault administration manuals is also available online as articles on the Symantec Enterprise Support site. You can access these articles by searching the Internet with any popular search engine, such as Google, or by following the procedure below.

To access the "How To" articles on the Symantec Enterprise Support site

- 1 Type the following in the address bar of your Web browser, and then press **Enter**:
http://www.symantec.com/business/support/all_products.jsp
- 2 In the Supported Products A-Z page, choose the required product, such as Enterprise Vault for Microsoft Exchange.
- 3 In the **Product Support** box at the right, click **How To**.
- 4 Search for a word or phrase by using the Knowledge Base Search feature, or browse the list of most popular subjects.

Comment on the documentation

Let us know what you like and dislike about the documentation. Were you able to find the information you needed quickly? Was the information clearly presented? Report errors and omissions, or tell us what you would find useful in future versions of our guides and online help.

Please include the following information with your comment:

- The title and product version of the guide on which you want to comment.
- The topic (if relevant) on which you want to comment.
- Your name.

Email your comment to evdocs@symantec.com. Please only use this address to comment on product documentation.

We appreciate your feedback.

Setting up Domino mailbox archiving

This chapter includes the following topics:

- [About Domino mailbox archiving](#)
- [Preparation for Domino mailbox archiving](#)
- [Configuring Domino targets, tasks and policies in Enterprise Vault](#)
- [Installing Enterprise Vault extensions for Lotus Notes and DWA clients](#)
- [Identifying internal Notes mail recipients](#)
- [How to edit automatic messages after installing Domino mailbox archiving](#)
- [Enabling mailboxes for archiving after installing Domino mailbox archiving](#)

About Domino mailbox archiving

The Enterprise Vault Domino Gateway provides the interface between Lotus Notes and Enterprise Vault. Although archiving does not use the Enterprise Vault Domino Gateway, actions on archived data, such as opening, restoring, deleting and searching, are handled by the Enterprise Vault Domino Gateway.

[Figure 2-1](#) illustrates the process when archiving an item from a Domino mail file.

Figure 2-1 Archiving an item

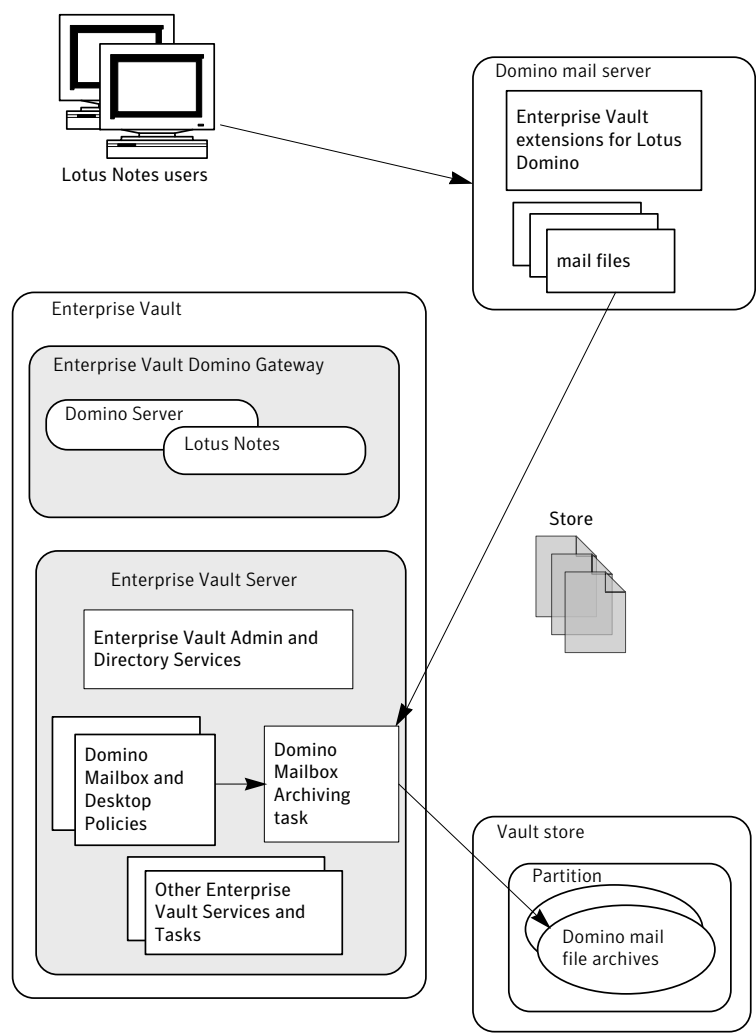
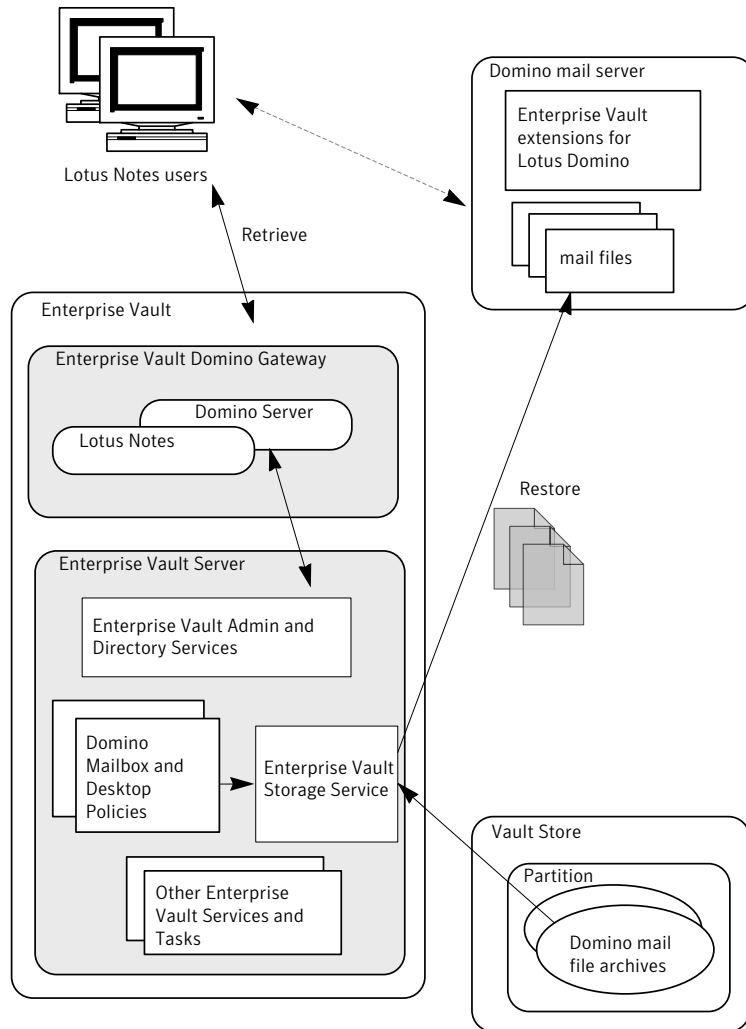


Figure 2-2 illustrates the process when viewing or restoring an archived item.

Figure 2-2 Retrieving or restoring an archived item



Enterprise Vault Extension Manager, which Enterprise Vault installs on the Enterprise Vault Domino Gateway provides the main functionality of the Enterprise Vault Domino Gateway. Enterprise Vault Extension Manager is a server-side

extension that processes requests from Lotus Notes and DWA clients and passes them on to Enterprise Vault. In order for the extension manager to have unrestricted access to Enterprise Vault data, the Domino server must run under the Vault Service account.

Preparation for Domino mailbox archiving

Before proceeding, ensure that you have done the following:

- Checked that software prerequisites are satisfied.
- Installed and configured Domino server on the Enterprise Vault Domino Gateway computer.
- Installed Enterprise Vault and run the configuration wizard.

See *Installing and Configuring* for instructions on how to perform these tasks.

Check Enterprise Vault configuration of Domino server

Now you can check the changes made to the Domino server configuration on the Enterprise Vault Domino Gateway.

Enterprise Vault installs the following binary files in the Domino program directory:

- EVRT.dll
- nEVDominoEM.dll
- EVDominoTrace.dll
- EVNoteStream.dll
- nEVDominoHousekeeping.exe

Enterprise Vault installs the following mail template and database files in the Domino data directory:

- EVAttach.ntf
- EVinstall.nsf
- help*help.nsf
- EV\EVDomino.nsf

The Enterprise Vault configuration wizard edits the notes.ini file in the Domino program directory. This file should then contain the following entries:

```
ExtMgr_Addins=EvDominoEM.dll
```

```
ServerTasks= ... ,EVDominoHouseKeeping
```

Now start the Domino server on the Enterprise Vault Domino Gateway. If the Enterprise Vault Directory Service is running, the following lines are displayed in the console during start-up:

```
Symantec Enterprise Vault Extension Manager: SERVER
```

```
...
```

```
EV Housekeeping: Initialization complete.
```

```
Symantec Enterprise Vault Extension Manager: HTTP
```

Configure Enterprise Vault for Web connections in preparation for Domino mailbox archiving

When Lotus Notes users start an archive search, a Web connection is made to the Enterprise Vault Domino Gateway. You need to perform the configuration tasks described in this section to support these connections.

A new IIS virtual directory called EnterpriseVaultDomino is used to authenticate user access to Enterprise Vault archives when users perform an archive search. The virtual directory points to the Enterprise Vault\WebApp folder and has anonymous access enabled. For security, a Web account is required for this virtual directory. It is advisable to create an account specifically for the purpose of Web access.

Do not change the name of the virtual directory, EnterpriseVaultDomino.

If you have already configured an account for Exchange Server OWA access, then you must use the same account for Domino mailbox archiving.

Create a Windows domain user account to use as the Enterprise Vault Data Access account. This should be a basic domain account specifically created for the purpose; a local machine account cannot be used. The account must not belong to any administrative group.

To configure the Enterprise Vault Data Access account

- 1 Log on to the Enterprise Vault Domino Gateway computer using the Vault Service account.
- 2 Start the Enterprise Vault Administration Console.
- 3 Expand the tree and right-click the **Directory** container.
- 4 Select **Properties**.
- 5 In the **Directory Properties** window, click the **Data Access Account** tab.

- 6 In the **Account** box, select the Enterprise Vault Data Access account.
- 7 Enter and confirm the password for the account.
- 8 Click **OK**.

The EnterpriseVaultDomino virtual directory is created and Anonymous access is granted automatically to the account specified.

To check the configuration of the Data Access account

- 1 On a computer that is not a domain controller, open Local Security Policy in Administrative Tools. On a domain controller, open Domain Controller Security Policy.
- 2 Click **Local Policies > User Rights Assignment**.
- 3 The following permissions should be set:
Access this computer from the network (SeNetworkLogonRight).
Bypass traverse checking (SeChangeNotifyPrivilege).
Log on as a batch job (SeBatchLogonRight).
Allow log on locally (SeInteractiveLogonRight).
- 4 The following registry value is also created containing the Enterprise Vault Data Access account. This ensures that only this user can obtain a list of archives accessible by a Domino User:

```
HKEY_CURRENT_USER
\Software
\KVS
\Enterprise Vault
\AnonymousUser
```

HKEY_CURRENT_USER is the Vault Service account. The value of this setting is the full name, including the Windows domain, of the anonymous user, for example, mydomain\DomAnonUser.

Vault store group, vault store, and partition in preparation for Domino mailbox archiving

A vault store group, vault store, and vault store partition must exist before you enable mailboxes for archiving. After you enable the target mailboxes for archiving, Enterprise Vault automatically creates an archive for each mailbox in the selected vault store.

A default vault store can be set for the Domino server, or for a Provisioning Group.

Note: The vault store is managed by the local Enterprise Vault Storage service.

See the "Setting up storage" chapter in the *Installing and Configuring* manual.

Configuring Domino targets, tasks and policies in Enterprise Vault

You can now configure Domino mailbox archiving in the Enterprise Vault Directory using the Administration Console. The following list summarizes the tasks which are described in more detail in the following sections:

- Check that the list of Domino forms available is correct for the items that you want to archive from mailboxes.
- Add the target Domino domain.
- Add the Domino servers hosting the mailboxes to be archived. Optionally, Domino Provisioning and Mailbox tasks can be added when you add the first target Domino server in the Administration Console.
- Configure Domino mailbox policies, to define how Enterprise Vault archives target Domino server mailboxes.
- Configure Domino desktop policies, to control the Enterprise Vault functionality available in the Lotus Notes client.
- Check the Enterprise Vault site settings.
- Create provisioning groups for the target mailboxes.

Checking the list of Domino forms

The types of items that can be archived from Domino server mailboxes are defined using Domino forms or form aliases. The list of forms available is displayed in the Directory Properties. You select the forms of items to archive in the Domino mailbox policy.

To check the list of available forms

- 1 Start Enterprise Vault Administration Console.
- 2 Expand the tree and right-click the **Directory** container.
- 3 Select **Properties**.
- 4 In the Properties window, select the **Domino Forms** tab.
- 5 Ensure the list includes all the required forms for the types of documents to be archived. If necessary, use **Add** to add forms to the list.

Adding Domino Server archiving targets

In the Administration Console you need to add the Domino domain and Domino Servers that you want to archive.

Adding a Domino domain

You can now configure the target Domino domain in the Enterprise Vault Administration Console.

To add a Domino domain

- 1 In the left pane of the Administration Console, expand the **Targets** container.
- 2 Right-click **Domino** and, on the shortcut menu, click **New** and then **Domino Domain**.

The **New Domino Domain** wizard starts.

- 3 Work through the wizard.

You will be asked for the following information:

- The name and password for the ID file that will be used to access Domino domain. This will typically be the ID of the Domino archiving user that you created.
- The fully-distinguished name of any Domino server in the domain that you are adding.

- 4 Copy the ID file to the following:

- Every Enterprise Vault server that runs a Domino mailbox archiving task.
- Every Enterprise Vault Domino Gateway.

Ensure that each ID file has the same file name on each server.

Adding target Domino mail servers

Next, add the target Domino mail servers in the Enterprise Vault Administration Console. A single Domino mailbox archiving task can archive several target Domino mailbox servers in a domain.

If you use secondary Domino servers to keep replicas of users' mail files, it is possible to archive from those secondary servers instead of from the mail servers. When there are many mail servers and only a few secondary servers this approach can simplify the configuration. If you want to use this method, add the secondary servers instead of the mail servers.

To add a target Domino mail server

- 1 In the left pane of the Administration Console, expand the **Targets** container.
- 2 Expand **Domino**.
- 3 Expand the Domino domain to which you want to add a server.
- 4 Right-click the Domino server container and on the shortcut menu, click **New** and then **Domino Server**.

The **New Domino Server** wizard starts.

- 5 Work through the wizard.

This wizard enables you to select the following:

- The Domino Server that you want to archive. In the wizard, the drop-down box under **Select the Domino server from which you want to archive** lists all the Domino servers in the domain.
 - Cluster options. If the server you are adding is in a Domino cluster, you can choose to add all servers in the cluster to the Enterprise Vault Site. Additionally, you can set the server you are adding to be the preferred server. The archiving task uses the preferred server when archiving from mailboxes, when possible. A mailbox that is on a different server must be replicated to this preferred server in order for the archiving task to be able to archive using this server. If a mailbox is not replicated to this preferred server, the task archives from the server that hosts the mailbox.
 - The Enterprise Vault tasks that you want created. If preferred, you can add these after adding the Domino mail server. There can be only one Domino Mailbox task on an Enterprise Vault server. There must be one (and only one) Domino Provisioning task for each Domino domain.
 - If the tasks are to be created on a different Enterprise Vault server in the site, you will need the name of the Enterprise Vault server.
 - The ID and password to be used to access the Domino mail server, if this is different from the ID used to access the domain. Typically, this will be the ID of the Domino archiving user that you created.
- 6 The Domino domain is then added to the Enterprise Vault directory and displayed in the tree. You can now add the Domino mail servers that you want Enterprise Vault to archive.
 - 7 If you have added a secondary server to archive replica mail files you must also define the DominoHubServers registry value on the Enterprise Vault server that runs the provisioning task.

See the *Registry Values* manual for details of how to create the DominoHubServers registry value.

Configuring mailbox policies for Domino mailbox archiving

Domino mailbox policies define how Enterprise Vault archives target Domino server mailboxes. You can create multiple policies if you want different groups of mailboxes to be archived using different policy settings. If you wish, you can create a custom mailbox policy for each provisioning group.

A default Domino mailbox policy is created in the Administration Console by the configuration wizard.

To view and modify the properties of the default Domino mailbox policy

- 1 Expand your Enterprise Vault site.
- 2 Click **Policies > Domino > Mailbox**.
- 3 Right-click **Default Domino Mailbox Policy** in the right pane and select **Properties**. You can modify the properties of this policy, as required, and also create new policies.

To create a new Domino mailbox policy

- 1 In the Administration Console, expand your Enterprise Vault site and then click **Policies > Domino > Mailbox**.
- 2 Right-click the **Mailbox** container and select **New > Policy** to launch the new policy wizard.
- 3 The new policy is displayed in the right pane.
- 4 To adjust the policy properties, right-click the policy and select **Properties**.

General tab (Domino mailbox archiving)

Table 2-1 lists the settings on the General tab. These settings provide a name and description for the policy.

Table 2-1 Domino mailbox policy General tab settings

Setting	Description	Default value
Name	A name for the policy.	None.
Description	An optional description for the policy, which you can change as often as you wish.	None.

Archiving Rules tab (Domino mailbox archiving)

Table 2-2 lists the settings on the Archiving Rules tab. Use these settings to control the archiving strategy.

Table 2-2 Domino mailbox policy Archiving Rules tab settings

Setting	Description	Default value
Young items	The minimum age limit at which items can be archived	2 weeks
Large items	Whether to archive larger items before smaller items and, if so, the minimum size of the items that are given priority.	Not selected.
Archiving strategy	Strategy for archiving the remaining items. This is based on the period of time since an item was modified.	Items that have not been modified for 6 months are archived.
Archive messages with attachments only	Archive an item only if it has an attachment, assuming all other archiving criteria are met. Note that this is not the same as archiving attachments only.	Not selected.
Archive encrypted messages	Archive messages that are encrypted. Note that Enterprise Vault cannot index encrypted messages. This means that it cannot display the body of an archived encrypted message, and users will not be able to find or view the body text when performing browser searches. However, users can view an encrypted message that is retrieved or restored from its shortcut, as normal.	Not selected.

Archiving Actions tab (Domino mailbox archiving)

Table 2-3 describes the settings on the Archiving Actions tab. Use these settings to configure whether the item in the mailbox is to be deleted and a shortcut created, and also whether to archive unread items.

Table 2-3 Domino mailbox policy Archiving Actions tab settings

Setting	Description	Default value
Delete original item after archiving	Original item is deleted from mailbox after archiving.	Selected.
Create shortcut to archived item after archiving	After it has been archived, the item in the mailbox is replaced with a shortcut.	Selected.
Archive unread items	Archive mailbox items even if they have not yet been read.	Not selected.

Shortcut Content tab (Domino mailbox archiving)

[Table 2-4](#) describes the settings on the Shortcut Content tab. Use these settings to configure what is to be included in shortcuts, and what is to be displayed when a shortcut is opened.

Note that Enterprise Vault does not create shortcuts for archived calendar or todo items. Instead, these are kept intact, although you can configure the mailbox archiving policy to strip calendar attachments.

See [“Advanced tab \(Domino mailbox archiving\)”](#) on page 28.

Table 2-4 Domino mailbox policy Shortcut Content tab settings

Setting	Description	Default value
Include recipient information	Whether to store recipient information (To: and Cc: details) in shortcuts. Shortcuts always contain the From and Subject information.	Shortcuts include recipient information.

Table 2-4 Domino mailbox policy Shortcut Content tab settings (continued)

Setting	Description	Default value
Shortcut body	<p>How much of the message body to store in shortcuts. Regardless of the setting value, the full message, with attachments, are still stored in the archive.</p> <ul style="list-style-type: none"> ■ None. None of the message text is stored in the shortcut. ■ Use message body. Shortcuts contain all of the message body text, but no attachments. ■ Customize. Select the amount of text and links that you want included in shortcuts. See “Using customized shortcuts for Domino mailbox archiving” on page 29. 	The first 1000 characters of the message body are stored in the shortcut.
When shortcut is opened	Whether double-clicking a shortcut displays the contents of the original item or the properties of the shortcut.	Show contents.

The file `LotusShortcutText.txt` is required if you configure customized shortcuts. You can also use this file to process standard shortcuts for untitled attachments. See [“Using customized shortcuts for Domino mailbox archiving”](#) on page 29.

Forms tab (Domino mailbox archiving)

The list shows the types of items that will be archived when the policy is applied. Select or clear Domino forms check boxes, as required.

If you need to edit the list of available forms, go to the Domino Forms tab of the Directory properties.

Shortcut Deletion tab (Domino mailbox archiving)

Shortcut deletion does the following:

- Deletes those shortcuts that are older than the age you specify on this page. Enterprise Vault uses the modified date or archived date to determine the age of a shortcut. You can specify which date to use on the **Storage Expiry** tab of **Site Properties**.

- Deletes orphaned shortcuts. These are those shortcuts that no longer have corresponding archived items. Typically users or storage expiry have deleted the archived items.
- Deletes those shortcuts for which the retention period has elapsed. Storage expiry may remove the corresponding archived items. It is possible to delete the shortcuts without deleting the archived items.

The Domino Mailbox Archiving task performs the shortcut deletion. When you run the task using **Run Now**, you can choose a Run mode that includes shortcut processing.

Table 2-5 describes the available settings.

Table 2-5 Shortcut Deletion settings

Setting	Description	Default value
Delete shortcuts	Select this option to make Enterprise Vault delete those shortcuts that are older than the age you specify. This option does not affect the corresponding archived items. Users can still search for the archived items. For example, you can choose to delete all shortcuts older than 12 months, but retain archived items for several years.	Not selected
Delete orphaned shortcuts	Select this option to make Enterprise Vault delete shortcuts in mailboxes if the corresponding archived item has been deleted. If the shortcuts contain text from the original message, those shortcuts might be useful to users even though the archived items have been deleted. However, deleting large shortcuts frees space in the mail files.	Not selected

Advanced tab (Domino mailbox archiving)

Table 2-4 briefly describes the settings on the Advanced tab. These settings enable you to change advanced archiving behavior. Information about each advanced setting is given in the *Administrator’s Guide*.

Table 2-6 Domino mailbox policy Advanced tab settings

Setting	Description
List settings from	<p>Controls the category of settings that are shown in the list. There is only one category:</p> <ul style="list-style-type: none"> ■ Archiving General. Settings that control archiving behavior. For example, you can configure the archiving task to strip attachments from calendar and todo items before archiving. <p>Information about each setting is given in the <i>Administrator's Guide</i>.</p>
Reset All	This returns all the settings in the list to their default values. There is a confirmation prompt that asks if you are sure you want to reset all the values.
Modify	Enables you to change the value for the selected setting. You can also double-click the setting to modify it.
Description	A brief description of what each setting controls.

Targets tab (Domino mailbox archiving)

Later, when you create provisioning groups to add mailboxes as archiving targets, you will assign the required Domino mailbox policy to each group. The associated provisioning groups will then be displayed in the Targets page of the policy.

Using customized shortcuts for Domino mailbox archiving

You can use custom shortcuts to change the information that is displayed in shortcuts.

In a new installation of Enterprise Vault, a default shortcut contains the following:

- From and Subject information.
- Recipient information: To, CC, BCC.
- A banner containing a link to the complete archived item.
- The first 1000 characters of the message body.
- No list of attachments or links to attachments.

You can change the settings so that shortcuts contain as much information as you require.

Note that the changes you make apply to shortcuts that are generated in the future, not to shortcuts that have already been created.

Details of custom shortcut content are held in the file, `LotusShortcutText.txt`, in the Enterprise Vault folder (for example `C:\Program Files (x86)\Enterprise Vault`). On a new installation, an English version of this file is placed in the Enterprise Vault folder. Language versions of the file are available in the language folders under `Languages\ShortcutText`.

To define custom shortcut content

- 1 Locate the required language version of the `LotusShortcutText.txt` file (under `Languages\ShortcutText`).
- 2 Open `LotusShortcutText.txt` with Windows Notepad. and make any required changes to the file.
See [“Layout of LotusShortcutText.txt for Domino mailbox archiving”](#) on page 30.
- 3 Save the file as a Unicode file.
- 4 Copy the file to the Enterprise Vault program folder (for example `C:\Program Files (x86)\Enterprise Vault`).
- 5 Copy the file to the Enterprise Vault program folder on all other Enterprise Vault servers in the Enterprise Vault Site.
- 6 If Domino Mailbox tasks are already created and running, you need to restart them to pick up the changes.

To apply the new content to new shortcuts

- 1 Start the Administration Console and go to the **Shortcut Content** tab in the **Lotus Domino Mailbox Policy** properties.
- 2 In the box beside **Content of shortcut body**, select **Customize** and then specify which options you want. Click **Help** on the tab for more information.

Layout of LotusShortcutText.txt for Domino mailbox archiving

`LotusShortcutText.txt` is laid out using the standard Windows `.ini` file format:

```
[Section]
Item1="value1"
Item2="value2"
```

You can change any of the values in the file. Remember to enclose each value in quotes.

The sections in `LotusShortcutText.txt` are as follows:

[Archived text]	<p>The entries in this section are displayed in the banner at the top of the shortcut.</p> <p>The entry that is used for the shortcut is the one that matches the archived item's Domino form or form alias.</p> <p>Values in this section all have a space before the final quote. This space separates the text from the link text.</p>
[Link]	<p>The entry in this section specifies the text in the banner that is a link to the archived item.</p>
[Attachment table]	<p>The Title entry in this section specifies the text immediately before the list of attachments.</p> <p>The OLERemoved entry lets you define the string to display in shortcuts when an embedded OLE object has been removed. In the default entry, the placeholder {0} in the string is replaced with the number of removed OLE objects. The combined size of the OLE objects is also displayed.</p>

Domino mailbox archiving retention folders

The Retention Folder feature enables you to create a single folder or a hierarchy of folders automatically in users' mail files. Enterprise Vault archives these folders according to policies that you assign. If a user deletes any folders in the retention folder hierarchy, Enterprise Vault automatically recreates them.

You specify the retention folders and their retention categories in retention plans. You can create as many retention plans as you require.

You use Enterprise Vault provisioning groups to apply retention plans to mail files. Thus, different users can have different retention folders with the appropriate retention categories. You can also define a default retention plan that Enterprise Vault applies to all users for whom a specific plan is not defined.

If a user moves a retention folder, the folder does not retain the retention plan settings. Items that are archived in the future will be archived according to the policy that applies to the folder in its new location. Items that have already been archived from the folder are unaffected and retain the original retention category.

If a user creates a subfolder beneath a retention folder, that subfolder inherits the retention folder settings. For example, if you create a 'Projects' folder users could then create a subfolder for each project. The subfolders would automatically use the retention folder settings from the parent 'Projects' folder.

You create an XML file in which you define the retention plans. You then use the `EVDominoRetentionPlans.exe` command line tool to upload the XML file to Enterprise Vault.

See the section 'Domino Retention Plan Tool' in the *Utilities* manual for details of how to create Domino retention plans.

Configuring desktop policies for Domino mailbox archiving

A Domino desktop policy defines the end user's experience when using the Enterprise Vault Lotus Notes client. It contains settings that determine the Enterprise Vault features and functionality that the client provides. You can create multiple policies if you want different provisioning groups to use different policy settings. If you wish, you can create a custom desktop policy for each provisioning group.

The desktop policy settings include following options:

- Show or hide Enterprise Vault menu options, such as Search, Store, Restore, and Delete.
- Control the availability of Vault Cache and its maximum size.
- Control advanced settings for Vault Cache.

A default Domino desktop policy is created in the Administration Console by the configuration wizard.

If you modify a desktop policy after setting up Domino mailbox archiving, then you need to synchronize the mailboxes using the button on the Synchronization tab in the Domino Provisioning task properties.

To view and modify the properties of the default Domino desktop policy

- 1 Expand your Enterprise Vault site.
- 2 Click **Policies > Domino > Desktop**.
- 3 Right-click **Default Domino Desktop Policy** in the right pane and select **Properties**. You can modify the properties of this policy, as required, and also create new policies.

To create a new Domino desktop policy

- 1 In the Administration Console, expand your Enterprise Vault site and then click **Policies > Domino > Desktop**.
- 2 Right-click the **Desktop** container and select **New > Policy** to launch the new policy wizard.
- 3 The new policy is displayed in the right pane.
- 4 To adjust the policy properties, right-click the policy and select **Properties**.

General tab (Domino desktop policy)

[Table 2-7](#) lists the settings on the General tab. These settings provide a name and description for the policy.

Table 2-7 Domino desktop policy General tab settings

Setting	Description	Default value
Name	A name for the policy.	None.
Description	An optional description for the policy, which you can change as often as you wish.	None, except in the case of an upgrade from Enterprise Vault 2007, in which case the description indicates which mailbox policy the desktop policy settings were copied from.

Options tab (Domino desktop policy)

The settings on the Options tab enable you to control the availability of Enterprise Vault menu options on the Domino clients.

The Enabled check box controls whether a feature is displayed as a menu option.

[Table 2-8](#) describes the settings on this tab. See the help on the desktop policy properties for more details on the effects of these settings.

Table 2-8 Domino desktop policy Options tab settings

Setting	Description	Default value
Search	Controls whether client users can search for archived items, by showing or hiding the 'Enterprise Vault Search' menu option.	Enabled.
Store and Cancel	Controls whether client users can perform manual archiving and cancel pending operations. Shows or or hides the 'Enterprise Vault Store' and 'Enterprise Vault Cancel' menu options.	Enabled.
Restore	Controls whether client users can restore items, by showing or hiding the 'Enterprise Vault Restore' menu option.	Enabled.

Table 2-8 Domino desktop policy Options tab settings (continued)

Setting	Description	Default value
Delete	Controls whether client users can delete archived items and their corresponding shortcuts, by showing or hiding the 'Enterprise Vault Delete' menu option.	Enabled.

Vault Cache tab (Domino desktop policy)

Table 2-9 describes the settings on the Vault Cache tab. These settings control the availability of Vault Cache, its maximum size and available features.

Table 2-9 Domino desktop policy Vault Cache tab settings

Setting	Description	Default value
Make Vault Cache available for users	<p>Select this to make Vault Cache available in this Enterprise Vault site. If this setting is cleared, no new Vault Caches are created. Users will have access to existing Vault Caches, but no items will be added.</p> <p>If you make Vault Cache available, additional settings enable you to choose one of the following:</p> <ul style="list-style-type: none">■ Automatically enable Vault Cache for offline users.■ Allow users to enable Vault Cache by displaying the Enable Vault Cache option from the Tools button and on the Actions > Tools menu.	<p>Vault Cache is not available. No new Vault Caches are created. Users will have access to existing Vault Caches, but no items will be added.</p> <p>If you make Vault Cache available, the default is to automatically enable Vault Cache.</p>

Table 2-9 Domino desktop policy Vault Cache tab settings (continued)

Setting	Description	Default value
Limit size of Vault Cache	<p>Use these settings to limit the size of Vault Caches, either as a percentage of unused disk space (calculated dynamically), or as a size in megabytes.</p> <p>If a Vault Cache reaches the specified size, the oldest items are automatically deleted in order to make room for new items. The space is not allocated until it is needed.</p>	10% of the unused disk space.

Advanced tab (Domino desktop policy)

Table 2-10 briefly describes the settings on the Advanced tab, which provide advanced settings for the policy. Information about each advanced setting is given in the *Administrator's Guide*.

Table 2-10 Domino desktop policy Advanced tab settings

Setting	Description
List settings from	<p>Controls the category of settings that are displayed in the list. There is only one category:</p> <ul style="list-style-type: none"> ■ Vault Cache <p>Information about each advanced setting is given in the <i>Administrator's Guide</i>.</p>
Reset All	This returns all the settings in the list to their default values. There is a confirmation prompt that asks if you are sure you want to reset all the values.
Modify	Enables you to change the value for the selected setting. You can also double-click the setting to modify it.
Description	A brief description of what each setting controls.

Targets tab (Domino desktop policy)

Later, when you create provisioning groups to add mailboxes as archiving targets, you will assign the required Domino desktop policy to each group. The associated provisioning groups will then be displayed in the Targets page of the policy.

Creating a Domino Provisioning task

If you did not request Enterprise Vault to create the Domino Provisioning task in the New Domino Server wizard, you can create this task manually, as described in this section. A separate Provisioning task is required for each domain.

To add a Domino Provisioning task

- 1 In the left pane of the Administration Console, expand the Site hierarchy until the **Enterprise Vault Servers** container is visible.
- 2 Expand the **Enterprise Vault Servers** container.
- 3 Expand the name of the server to which you want to add the Domino Provisioning task.
- 4 Right-click **Tasks** and, on the shortcut menu, click **New** and then **Domino Provisioning Task**.

The **New Domino Provisioning Task** wizard starts.

- 5 Work through the wizard.

Creating a Domino Mailbox task

If you did not request Enterprise Vault to create the Domino Mailbox task in the New Domino Server wizard, you can create this task manually, as described in this section.

There can be only one Domino Mailbox task on an Enterprise Vault server. A single task can process several Domino servers in different Domino domains.

A single Domino server can be processed by several Domino Mailbox tasks on different Enterprise Vault servers; in this situation, the Domino mailbox archives would be distributed across multiple vault stores.

To add a Domino Mailbox task

- 1 In the left pane of the Administration Console, expand the Site hierarchy until the **Enterprise Vault Servers** container is visible.
- 2 Expand the **Enterprise Vault Servers** container.
- 3 Expand the name of the server to which you want to add the Domino Mailbox task.
- 4 Right-click **Tasks** and, on the shortcut menu, click **New** and then **Domino Mailbox Task**.

The **New Domino Mailbox Task** wizard starts.

- 5 Work through the wizard.

Reviewing the default archiving settings for the Site when setting up Domino mailbox archiving

Check the default settings configured in the Enterprise Vault Site properties.

To review the Site settings

- 1
- In the Administration Console, right-click your Enterprise Vault Site.
- 2
- On the shortcut menu, click **Properties**.
- 3
- Site properties include the following settings that are applicable to archiving from Domino servers. Note that you can override some of these at a lower level. For example, you can override the Site archiving schedule for a particular task by setting the schedule in the task properties. The indexing level can also be set at policy level and the default retention category can be set at provisioning group or policy level.

General	<div><div>■</div>The Site alias and description.</div> <div><div>■</div>The protocol and port to be used for Web Access application requests, for example, when users perform an archive search using integrated or browser search.</div> <div><div>■</div>A system message for users, if required.</div> <div><div>■</div>A system message for administrators, if required.</div>
Archive Settings	<div><div>■</div>The default level of indexing.</div> <div><div>■</div>The default retention category.</div> <div><div>■</div>Whether users can delete items from their archive. If you want users to be able to delete items from their archives, you must select the check box Users can delete items from their archives. The setting Enable recovery of user deleted items enables the retention of user-deleted items so that accidentally-deleted items can be recovered.</div>
Storage Expiry	<div><div>■</div>The schedule for running storage expiry to delete from archives any items that are older than the retention period assigned.</div>
Archive Usage Limit	<div><div>■</div>If required, you can set limits on the size of archives here or in the vault store properties.</div>
Site Schedule	<div><div>■</div>The schedule for running automatic, background archiving.</div>
Monitoring	<div><div>■</div>Performance counters for monitoring Enterprise Vault.</div>

- 4 Click **Help** on any of the Site properties screens for further information.
- 5 Now you can create provisioning groups for the mailboxes that are to be archived.

Adding a Provisioning Group when setting up Domino mailbox archiving

A provisioning group enables you to apply a Domino mailbox policy and a Domino desktop policy to any of the following:

- Individual users
- A group of Domino mailbox users
- A mail-in database

You can have a single provisioning group, comprising the whole corporate hierarchy, or multiple provisioning groups, if you want to assign different policies to different groups of users.

You can select any of the following target types to associate with a provisioning group:

- Directory group
- Mailbox
- Mail-in database
- Organizational Unit
- Corporate Hierarchy

Note: A mailbox must be added to a provisioning group, and mailboxes in the provisioning group must be configured and enabled by the Domino Provisioning task, before you can archive items from the mailboxes.

Note: Vault Cache is not available for mail-in databases. Enterprise Vault ignores Vault Cache policy settings in the case of mail-in databases.

If there are a large number of mailboxes, and automatic enabling of mailboxes is not configured for the provisioning group, then there could be a delay in the mailboxes being available to Enterprise Vault for enabling. If you do not want to wait, you can force an update. To force an update, run the following commands in the Domino server console:

```
LOAD UPDALL NAMES.NSF -T "($Users)"
LOAD UPDALL NAMES.NSF -T "($ServerConfig)"
```

```
LOAD UPDALL NAMES.NSF -T "($VIMGroups) "  

LOAD UPDALL NAMES.NSF -T "($VIMPeople) "  

LOAD UPDALL NAMES.NSF -T "($PeopleGroupsCorpHier) "  

LOAD UPDALL NAMES.NSF -T "($Certifiers) "
```

To add a Provisioning Group

- 1 In the left pane of the Administration Console, expand **Targets**.
- 2 Expand the Domino domain that you added.
- 3 Right-click **Provisioning Group** and, on the shortcut menu, click **New** and then **Provisioning Group**.

The **New Provisioning Group** wizard starts.

- 4 Work through the wizard to add a provisioning group.

You will need the following information:

- The domain containing the Domino Servers that you want to archive.
- The Domino desktop policy to apply.
- The Domino mailbox policy to apply.
- The default retention category to apply, when archiving from the mailboxes. The wizard enables you to create a new retention category, if required.
- The default vault store in which the mailbox archives are to be created by Enterprise Vault. If mailboxes in the provisioning group are automatically-enabled for archiving, the vault store will be used for any future mailboxes added to the provisioning group.
If you do not explicitly set the vault store for the provisioning group, the default vault store setting is inherited from the Domino Server properties.

- The default Indexing Service that will be used for mailboxes in the provisioning group that are automatically-enabled for archiving.
If you do not explicitly set the Indexing Service for the provisioning group, the default Indexing Service setting is inherited from the Domino Server properties.

- Whether you want the Domino Provisioning task to enable new mailboxes for archiving automatically.

A new mailbox is one that is new to Enterprise Vault. When you first start using Enterprise Vault, all the mailboxes are new. With auto-enabling set, all existing mailboxes are enabled when the Domino Provisioning task next runs. All mailboxes created in the future will also be enabled and the associated archives created automatically.

If auto-enabling is not selected, you use the **Enable Mailbox** wizard to enable the mailboxes for archiving. You can use the **Disable Mailbox** wizard to explicitly disable individual mailboxes. This prevents the mailbox being enabled automatically, so the mailbox is never archived unless you choose to enable it.

See [“Enabling mailboxes for archiving after installing Domino mailbox archiving”](#) on page 57.

Ordering provisioning groups when setting up Domino mailbox archiving

If you create multiple provisioning groups, the order in which they are listed is significant; the groups are processed from the top of the list down. Mailboxes that appear in more than one provisioning group use the settings from the first group in which they appear.

Ensure that the most specific group is at the top of the list and the least specific is at the bottom.

To re-order provisioning groups

- 1 In Administration Console tree, right-click the **Provisioning Group** container and select **Properties**.
- 2 Use **Move Up** and **Move Down** buttons to rearrange the groups.

Installing Enterprise Vault extensions for Lotus Notes and DWA clients

This section describes the Enterprise Vault client functionality available for Lotus Notes and DWA users, and how to install the necessary mail file design templates to provide the functionality that you require.

About Enterprise Vault clients for Lotus Notes and DWA clients

The Enterprise Vault functionality for Lotus Notes and DWA is provided by design changes to the mail file. These design changes are applied using revised mail templates.

For Domino mail file users you can configure the following Enterprise Vault client features:

- Enterprise Vault extensions for Lotus Notes.

If you want users to have the Enterprise Vault client functionality available, you need to install the Enterprise Vault extensions for Lotus Notes on all the target Domino mail servers.

- **Enterprise Vault extensions for DWA.**
 If you want users to have the Enterprise Vault client functionality available in their DWA clients, you need to install the Enterprise Vault extensions for DWA on all the target DWA servers.

Enterprise Vault extensions for Lotus Notes

The Enterprise Vault Lotus Notes extensions have the following features:

- All folders and views are updated with a new column to indicate archived, and archive pending items with a special icon.
- If the user double clicks an archived item, the contents are retrieved (provided the associated Enterprise Vault mailbox policy is configured to retrieve the item).
- If an archived item has attachments, the paper clip icon is shown in all the views and folders.

The following options are added to the **Tools** action bar menu in Notes 7 and to the **More** action bar in Notes 8 and later:

- **Enterprise Vault Search.** Opens the integrated search application.
- **Enterprise Vault Store.** This marks the item for archiving but it is only archived at the next scheduled archiving run.
- **Enterprise Vault Cancel.** Cancels previous store requests and removes the pending icon from the view.
- **Enterprise Vault Restore.** Restores the item back to the mail file. (This action is synchronous).
- **Enterprise Vault Delete.** Deletes the shortcut and the archived item, if permitted. (Like restore, this action is synchronous). A prompt enables users to delete the shortcut or both the shortcut and the archived item.
- **Enterprise Vault Help.** Opens the Enterprise Vault help database.
- **About Enterprise Vault.** This shows version information and technical support information for Enterprise Vault.

Each of these options can be performed on one or multiple items.

If a user attempts to reply to or forward a shortcut, the content of the archived item is included, if requested.

If a user attempts to use **Copy Into a Memo**, **Calendar Item** or **To Do** item from a shortcut document, the archived content is copied in, not the shortcut.

Enterprise Vault DWA client features

Enterprise Vault DWA client provides similar functionality to the Enterprise Vault extensions for Lotus Notes.

Note that, in order for users to be able to open archived signed or encrypted MIME items, there must be an SSL connection to the Enterprise Vault Domino Gateway.

If there is no such connection, users receive the following message:

```
Unable to complete the current operation.  
SSL is required for secure mail,  
but is not enabled on Domino Server.  
Please notify your administrator.
```

Installing Enterprise Vault client extensions for Lotus Notes and DWA clients

If users are to have full Enterprise Vault functionality available in their Lotus Notes or DWA clients, then you need to install the Enterprise Vault client extensions on each of the target Domino mail servers and DWA servers.

The client extensions are installed using the Lotus Notes application, Symantec Enterprise Vault *version* - Domino Installer (the filename of the Lotus Notes database is `EVinstall.nsf`). During the Enterprise Vault installation, this database is installed in the Domino data directory of the Domino server on the Enterprise Vault Domino Gateway.

For both Enterprise Vault Domino Gateways and mail servers, if language packs are installed, `EVInstall.nsf` will install the required changes to support them.

Setting up an account to use `EVInstall.nsf` to set up an Enterprise Vault Domino Gateway

The account that will run `EVInstall.nsf` on the Enterprise Vault Domino Gateway must have permissions on a number of files, as described in this section. Note that, depending on the Domino version, not all the files will be present.

In order to run `EVInstall.nsf` on the Enterprise Vault Domino Gateway, the account must have the following on the Enterprise Vault Domino Gateway:

- The following permissions on the **Security** tab of the server document:

- Sign agents to run on behalf of the invoker of the agent. If this setting is blank then this permission is already granted by default. If the setting is not blank, add the name of the account.
- Create databases & templates. If this setting is blank then this permission is already granted by default. If the setting is not blank, add the name of the account. (This is not required if you choose the Full Access Administrator option.)
- Create master templates. (This is not required if you choose the Full Access Administrator option.)
- One of the following:
 - Be a Full Access Administrator on the Enterprise Vault Domino Gateway.
 - Manager access to the following files:
 - Mail85.ntf
 - Mail8.ntf
 - Mail7.ntf
 - DWA7.ntf
 - EVAttach.ntf
 - EV\EVDomino.nsf
 - EVinstall.nsf
 - All the Enterprise Vault help files in the Domino server help folder:
da_evhelp.nsf; de_evhelp.nsf; en_evhelp.nsf; es_evhelp.nsf;
fr_evhelp.nsf; he_evhelp.nsf; it_evhelp.nsf; ja_evhelp.nsf; ko_evhelp.nsf;
nl_evhelp.nsf; pl_evhelp.nsf; ru_evhelp.nsf; sv_evhelp.nsf;
zh-cn_evhelp.nsf; zh-tw_evhelp.nsf.
 - If you intend to select the option to modify Domino Web Access forms files you also need Manager access to the following files:
 - Forms85.nsf
 - Forms8.nsf
 - Forms7.nsf

EVinstall.nsf will automatically add the LocalDomainAdmins group to the access control lists (ACLs) of the following files, with Manager access:

- EVAttach.ntf
- EVOOffline.ntf

- EV\EVDomino.nsf
- EVinstall.nsf

Setting up an account to use EVInstall.nsf to set up a mail server

The account that will use EVInstall.nsf to set up a mail server must have permissions on a number of files, as described in this section. Note that, depending on the Domino version, not all the files will be present.

In order to use EVInstall.nsf to set up a mail server, the account must have the following permissions on the mail server:

- The following permissions set on the Security tab of the server document:
 - Sign agents to run on behalf of the invoker of the agent
 - Create master templates. (This is not required if you choose the Full Access Administrator option.)
- One of the following:
 - Be a Full Access Administrator on the mail server.
 - Manager access to the following files:
 - Mail85.ntf
 - Mail8.ntf
 - Mail7.ntf
 - DWA7.ntf
 - If you intend to select the option to modify Domino Web Access forms files you also need Manager access to the following files:
 - Forms85.nsf
 - Forms8.nsf
 - Forms7.nsf

Granting Execution Control List permissions when setting up Lotus Notes and DWA clients

You must grant ECL permissions so that users do not receive Execution Security Alerts when they use the Enterprise Vault client.

You must grant permissions to the following accounts:

- The account that you use to run EVInstall.nsf

See [“Granting permissions to the account that will run EVInstall.nsf”](#) on page 45.

- The Enterprise Vault Domino Gateway server account
See [“Granting permissions to the Enterprise Vault Domino Gateway server account”](#) on page 45.
- If you intend to run NSF Migration, the Domino archiving user account.
See [“Granting permissions to the archiving user account”](#) on page 45.
- Each user who will use Vault Cache.
See [“Granting permissions to users of Vault Cache”](#) on page 45.

Granting permissions to the account that will run EVInstall.nsf

The account that runs EVInstall.nsf requires the following:

- Ability to export data
- Ability to modify other databases
- Ability to read other databases
- Ability to send mail
- Access to current database
- Access to environment variables
- Access to external code
- Access to file system

Granting permissions to the Enterprise Vault Domino Gateway server account

The Enterprise Vault Domino Gateway server account requires the following:

- Access to current database

Granting permissions to the archiving user account

For NSF Migration and for retention folders the Domino archiving user account requires the following:

- Access to current database

Granting permissions to users of Vault Cache

You must grant the following ECL permissions to Vault Cache users:

- Access to current database

- Access to environment variables
- Ability to read other databases
- Ability to modify other databases
- Access to external code

Installing the Lotus Notes and DWA client extensions

Now you can install the Lotus Notes and DWA extensions on the Enterprise Vault and a target Domino mail server, as described in this section.

To run EVInstall.nsf you must use the correct Notes client version. The minimum client version that you can use to run EVInstall.nsf is Notes 7.0.2 with appropriate hotfixes.

For the full details of supported versions of Domino software and the required hotfixes, see the *Enterprise Vault Compatibility Charts* book at the following address:

<http://www.symantec.com/docs/TECH38537>

Note: If the forms databases have replication enabled, the changes that EVInstall makes are replicated to all Domino mail servers. To prevent the replication to other mail servers, disable the replication of the Forms7.nsf, Forms8.nsf, and Forms85.nsf databases before you run EVInstall.nsf.

To run EVInstall.nsf to configure standard mail templates

- 1 Log on to Lotus Notes with the user ID that will run the EVInstall.nsf.

Note: If you do not use Notes on the Enterprise Vault Domino Gateway you must use a Notes client that is the same version as or newer than the Notes that is installed on the Enterprise Vault Domino Gateway.

- 2 Sign EVInstall.nsf.
- 3 Open the Symantec Enterprise Vault *version* - Domino Installer application (EVInstall.nsf).
- 4 In the application page, select the Enterprise Vault Domino Gateway and target Domino mail server.
- 5 If you intend to use the Enterprise Vault search applications (integrated search and browser search) or you require iNotes/DWA, select **Modify Domino Web Access Forms Files**.

- 6 If you want to use Vault Cache, select **Install Vault Cache**.
- 7 Click **Install Symantec Enterprise Vault *version* database design templates** to start the process.

The application should take several minutes to create the new Enterprise Vault templates.

- 8 When the update is complete, double-click each log line in the lower pane of the window and check that there were no errors reported.
- 9 If you had previously customized the templates, confirm that the templates still exist and function properly in the Enterprise Vault mail templates.
- 10 If you have other target mail servers with different Domino Server versions, do the following until you have deployed the templates to all mail server targets:

- Run `EVInstall.nsf` again.
- In the application page, clear the **Enterprise Vault Domino Gateway** selection.
- Select a target Domino mail server.
- If you require iNotes/DWA, select **Modify Domino Web Access Forms Files**.
- If you intend to make Vault Cache available to users, select **Install Vault Cache**.
- Click **Install Symantec Enterprise Vault *version* database design templates** to start the process.
The application takes several minutes to create the new Enterprise Vault templates.

- 11 If you want to do so, you can now use `EVInstall.nsf` to add Enterprise Vault customizations to a customized template.

See [“To run EVInstall.nsf to modify a customized database template or mail-in database template”](#) on page 48.

To run EVInstall.nsf to modify a customized database template or mail-in database template

- 1
- Before you run Enterprise Vault to modify a customized template you must previously have run EVInstall.nsf to configure standard mail templates.
- See “[To run EVInstall.nsf to configure standard mail templates](#)” on page 46.
- 2
- Log on to Lotus Notes with the user ID that will run EVInstall.nsf.

Note: If you do not use Notes on the Enterprise Vault Domino Gateway you must use a Notes client that is the same version as or newer than the Notes that is installed on the Enterprise Vault Domino Gateway.

- 3
- Open the Symantec Enterprise Vault *version* - Domino Installer application (EVInstall.nsf).
- 4
- Click the **Mail Template Customization** tab.
- 5
- In the **Domino mail server** list, select the server that has the template you want to modify.
- 6
- Next to **Template file name**, enter the name of the template. Click Browse if you want to select from the list of available templates.
- 7
- In the **Original mail template on which this template is based** list, select the type of template that was originally used to create the template that you have selected. For example, if the template was created from mail7.ntf, select mail7.ntf.
- 8
- In the **Original server version of base template** list, select the Domino version of the server from which the original mail template came. For example, if the original template was on a Domino 7.0.1 server, select 7.0.1.
- 9
- Click **Add Enterprise Vault Customizations** to apply the Enterprise Vault customizations to the template that you have chosen.

Changes made by EVInstall.nsf when setting up Domino mailbox archiving

This section describes the changes made by EVInstall.nsf.

EVInstall.nsf changes on a Domino 8.5 Enterprise Vault Domino Gateway

[Table 2-11](#) describes changes made by EVInstall.nsf.

Table 2-11 EVInstall.nsf changes on a Domino 8.5 Enterprise Vault Domino Gateway

File	Master Template	Comments
EVDGMail.ntf	EVDGMail	This is the template used by the temporary databases created in the EV folder on the Enterprise Vault Domino Gateway server during the item retrieval process. The master template name of EVDGMail.ntf is EVDGMail.
forms85.nsf		This is the iNotes/DWA forms database that is used by Domino 8.5 servers. For this database, the Enterprise Vault changes are inserted into the existing database instead of creating a new forms database.
forms85_x.nsf		This is the iNotes/DWA forms extension database that is used by Domino 8.5.1 (or later) servers. The Enterprise Vault changes are inserted into the existing iNotes/DWA forms extension database, if one exists. If the forms extension database does not exist, a new one is created.
evattach.ntf		Installed by the Enterprise Vault installation. It is used to display archived attachments in a separate window when the user clicks a link in a shortcut. This file must be signed. EVInstall.nsf has an option to perform the signing.
EVOOffline.ntf		This is the template that Enterprise Vault uses to create Vault Cache databases. This file must be signed. EVInstall.nsf has an option to perform the signing.
domcfg.nsf		The Domino Web Server Configuration database (domcfg.nsf) is a database that can contain customized logon forms that will be displayed when using single sign-on. This database is created on the Enterprise Vault Domino Gateway server so that a customized logon form can be displayed for searching Domino mailbox archives.
EV\evdomino.nsf		Installed by the Enterprise Vault installation. This file must be signed. EVInstall.nsf has an option to perform the signing.

Table 2-11

EVInstall.nsf changes on a Domino 8.5 Enterprise Vault Domino Gateway *(continued)*

File	Master Template	Comments
\help*_evhelp.nsf		Installed by the Enterprise Vault installation and signed by EVInstall.nsf.

EVInstall.nsf changes on a Domino 8.5 mail server

[EVInstall.nsf changes on a Domino 8.5 mail server](#) describes changes made by EVInstall.nsf.

Table 2-12

EVInstall.nsf changes on a Domino 8.5 mail server

File	Master Template	Comments
ev_mail85.ntf	EVR85Mail	This is the mail template for Domino 8.5 servers. It is a new database template; mail85.ntf still exists and any previous customizations to mail85.ntf are applied to ev_mail85.ntf. The master template name of the ev_mail85.ntf is EVR85Mail.
forms85.nsf		This is the iNotes/DWA forms database that is used by Domino 8.5 servers. For this database, the Enterprise Vault changes are inserted into the existing database instead of creating a new forms database.
forms85_x.nsf		This is the iNotes/DWA forms extension database that is used by Domino 8.5.1 (or later) servers. The Enterprise Vault changes are inserted into the existing iNotes/DWA forms extension database, if one exists. If the forms extension database does not exist, a new one is created.

EVInstall.nsf changes on a Domino 8 Enterprise Vault Domino Gateway

[Table 2-13](#) describes changes made by EVInstall.nsf.

Table 2-13 EVInstall.nsf changes on a Domino 8 Enterprise Vault Domino Gateway

File	Master Template	Comments
EVDGMail.ntf	EVDGMail	This is the template used by the temporary databases created in the EV folder on the Enterprise Vault Domino Gateway server during the item retrieval process. The master template name of EVDGMail.ntf is EVDGMail.
forms8.nsf		This is the DWA forms database that is used by Domino 8 servers. For this database, the Enterprise Vault changes are inserted into the existing database instead of creating a new forms database.
evattach.ntf		Installed by the Enterprise Vault installation. It is used to display archived attachments in a separate window when the user clicks a link in a shortcut. This file must be signed. EVInstall.nsf has an option to perform the signing.
EVOOffline.ntf		This is the template that Enterprise Vault uses to create Vault Cache databases. This file must be signed. EVInstall.nsf has an option to perform the signing.
domcfg.nsf		The Domino Web Server Configuration database (domcfg.nsf) is a database that can contain customized logon forms that will be displayed when using single sign-on. This database is created on the Enterprise Vault Domino Gateway server so that a customized logon form can be displayed for searching Domino mailbox archives.
EV\evdomino.nsf		Installed by the Enterprise Vault installation. This file must be signed. EVInstall.nsf has an option to perform the signing.
\help*_exhelp.nsf		Installed by the Enterprise Vault installation and signed by EVInstall.nsf.

EVInstall.nsf changes on a Domino 8 mail server

Table 2-14 describes changes made by EVInstall.nsf.

Table 2-14 EVInstall.nsf changes on a Domino 8 mail server

File	Master Template	Comments
ev_mail8.ntf	EVR8Mail	<p>This is the mail template for Domino 8 servers. It is a new database template; mail8.ntf still exists and any previous customizations to mail8.ntf are applied to ev_mail8.ntf.</p> <p>The master template name of the ev_mail8.ntf is EVR8Mail.</p>
forms8.nsf		<p>This is the DWA forms database that is used by Domino 8 servers. For this database, the Enterprise Vault changes are inserted into the existing database instead of creating a new forms database.</p>

EVInstall.nsf changes on a Domino 7.0.x Enterprise Vault Domino Gateway

[Table 2-15](#) describes changes made by EVInstall.nsf.

Table 2-15 EVInstall.nsf changes on a Domino 7.0.x Enterprise Vault Domino Gateway

File	Master Template	Comments
EVDGMail.ntf	EVDGMail	<p>This is the template used by the temporary databases created in the EV folder on the Enterprise Vault Domino Gateway server during the item retrieval process.</p> <p>The master template name of EVDGMail.ntf is EVDGMail.</p>
forms7.nsf		<p>This is the DWA forms database that is used by Domino 7.0 servers. For this database, the Enterprise Vault changes are inserted into the existing database instead of creating a new forms database.</p>
evattach.ntf		<p>This database is added by the Enterprise Vault installation and is then signed by EVInstall.nsf. It is used to display archived attachments in a separate window when the user clicks a link in a shortcut.</p>

Table 2-15 EVInstall.nsf changes on a Domino 7.0.x Enterprise Vault Domino Gateway *(continued)*

File	Master Template	Comments
EVOOffline.ntf		This is the template that Enterprise Vault uses to create Vault Cache databases. This file must be signed. EVInstall.nsf has an option to perform the signing.
domcfg.nsf		The Domino Web Server Configuration database (domcfg.nsf) is a database that can contain customized logon forms that will be displayed when using single sign-on. This database is created on the Enterprise Vault Domino Gateway server so that a customized logon form can be displayed for searching Domino mailbox archives.
EV\evdomino.nsf		Installed by the Enterprise Vault installation. Optionally, this file can be signed by EVInstall.nsf.
help *_evhelp.nsf		Installed by the Enterprise Vault installation and signed by EVInstall.nsf.

EVInstall.nsf changes on a Domino 7.0.x mail server

Table 2-16 describes changes made by EVInstall.nsf.

Table 2-16 EVInstall.nsf changes on a Domino 7.0.x mail server

File	Master Template	Comments
ev_mail7.ntf	EVR7Mail	<p>This is the mail template for Domino 7.0.x servers. It is a new database template; mail7.ntf still exists and any previous customizations to mail7.ntf are applied to ev_mail7.ntf.</p> <p>The master template name of the ev_mail7.ntf is EVR7Mail.</p>
ev_dwa7.ntf	EVdwa7	<p>This is the DWA mail template for Domino 7.0.x servers. It is a new database template; dwa7.ntf still exists and any previous customizations to dwa7.ntf are applied to ev_dwa7.ntf.</p> <p>The master template name of the ev_dwa7.ntf is EVdwa7, and EVdwa7 inherits its design from EVR7Mail (ev_mail7.ntf).</p>

Table 2-16 EVInstall.nsf changes on a Domino 7.0.x mail server (continued)

File	Master Template	Comments
forms7.nsf		This is the DWA forms database that is used by Domino 7.0 servers. For this database, the Enterprise Vault changes are inserted into the existing database instead of creating a new forms database.

Updating mail files with the new design after installing the Lotus Notes and DWA extensions

The final task to give users the full Enterprise Vault client functionality is to replace the design of their mail file with the appropriate Enterprise Vault mail template. The template used will depend on which mail template version users are using and whether they are using iNotes/DWA.

- On Domino 8.5 Lotus Notes and iNotes users should be using EV_Mail85.ntf.
- On Domino 8.0.x Lotus Notes and DWA users should be using EV_Mail8.ntf.
- On Domino 7.x Lotus Notes users should be using EV_Mail7.ntf, and DWA users should be using EV_DWA7.ntf.

There are two methods of replacing the design:

- To update a small number of mail files, you can click File, then Database, and then Replace Design in the Administration client.
- To update a large number of mail files, stop the mail router and then use the Convert Domino server task.

Because the Convert server task is resource intensive, you are recommended to run it out of peak hours. For a large mail server it may take some hours to convert all mail files.

To stop the mail router, type the following command in the Domino server console:

```
tell router quit
```

The simplest use of Convert is when the same mail file template is applied to all users. In the following example command, EVR7mail is applied to all users:

```
Load convert mail\*.nsf * ev_mail7.ntf
```

Take care when using the asterisk for the existingtemplatename argument, because you can inadvertently convert users to the wrong template.

To examine the full syntax of the Convert task, type the following at the Domino server console:

```
load convert -?
```

Note: To upgrade existing user-created folders in each mail file with the Enterprise Vault Lotus Notes extensions you use the `-s` and `-u` parameters of the `Convert` utility or choose 'Actions' and the 'Upgrade Folder Design' from within the mail file.

The following steps facilitate setting up subsequent new users. These changes ensure that the generic Domino archiving user automatically can access the new mail file and that the mail file is using the correct mail template:

- In the Access Control List for the Enterprise Vault Mail Template, add the generic Domino archiving user with Editor access, and 'Delete documents' and 'Create shared folders/views' permissions. When typing in the user, enclose the name in square brackets. This ensures that the user is automatically added to the ACL of any mail file that is created from the template.
- To ensure that administrators use the correct mail template when registering new users, change the default mail template in the administration preferences. To change the default mail template, do the following:
 - From the Domino Administrator client select **File**, then **Preferences**, then **Administration Preferences**.
 - Click the **Registration** tab, and then click **Mail Options**.
 - Change the mail file template to the appropriate Enterprise Vault mail template and click **OK** twice to save the preferences.

How users access Enterprise Vault Search features after installing the Lotus Notes and DWA extensions

There is an Enterprise Vault integrated search, and an Enterprise Vault browser search available in the client extensions. The integrated search requires Internet Explorer 7.0 or later. Browser search supports most modern browsers.

In both search applications, users can view and restore archived items.

Domino single sign-on (SSO) must be configured to enable access to either search application. Searching is performed using the virtual directory, `/EnterpriseVaultDomino`. This virtual directory is configured to use anonymous authentication and a special anonymous user account.

To start integrated search the user selects the option, Enterprise Vault Search, in Lotus Notes or iNotes/DWA. This option is on the **Tools** menu in Lotus Notes 7, and on the **More** menu in Lotus Notes 8. This displays the SSO logon box. The

user needs to enter their Lotus Notes user name (common name or full hierarchical name) and their Internet password. The Internet password is defined within the user's person document, and may or may not be the same as their Lotus Notes user ID password. The user must have an Internet password in order to log on to the integrated search.

There is a link to the browser search in the integrated search page. Alternatively, users can start the browser search in a browser by entering the following URL:

```
HTTP://Domino_Gateway_servername/EnterpriseVaultDomino
```

In Domino mailbox archiving, this search can only be used to search Domino mailbox archives.

In the browser search log on page, the user must enter their Lotus Notes user name (common name or full hierarchical name), their Internet password, and the Domino domain to search.

With integrated search a user can only search Domino mailbox archives in the same Domino domain. With browser search, users can search Domino mailbox archives in any Domino domain.

Identifying internal Notes mail recipients

You can specify that Enterprise Vault must perform a local address lookup for specific Notes domains. The local lookup enables Enterprise Vault to identify the Lotus Notes user name for those messages that are addressed to alternate email addresses. The local lookup results can aid searching in the Web applications and in Compliance Accelerator and Discovery Accelerator.

To specify the domains that require local address lookup you must edit the registry on the Enterprise Vault servers that run the journaling and archiving tasks.

See the *Registry Values* manual for details of the **NotesDomains** registry key.

How to edit automatic messages after installing Domino mailbox archiving

Enterprise Vault sends automatic messages to users when their mailbox is enabled for archiving.

Optionally, you can configure Enterprise Vault to send an automatic warning when a user's archive is reaching the maximum size, if you have set a limit.

Example messages are installed, but you need to customize the text for your organization.

Editing the Welcome message after installing Domino mailbox archiving

When Enterprise Vault enables a mailbox for archiving, it automatically sends a Welcome message to that mailbox. The Welcome message provides information for users on how to get help and what to expect. You must edit this message before it is sent to reflect how you have set up Enterprise Vault.

During the installation, the Welcome message is placed in a folder beneath the Enterprise Vault program folder, for example:

```
C:\Program Files (x86)\Enterprise Vault\Languages\Mailbox Messages\lang
```

where *lang* indicates the language used.

The Welcome message is in a file called `EVMessages.nsf`.

To set up the Welcome message

- 1 Decide which language version of **EVMessages.nsf** you want to use and locate the file.
- 2 Optionally, use an appropriate user ID to sign the file. The ID must have **Access to current Database** permission in the Execution Control List on the computer on which you intend to edit the file. If you have an existing ID set up for such purposes, you can use that ID.
- 3 Using a computer that has Lotus Notes installed, double-click the file **EVMessages.nsf** in Windows Explorer to edit the message.
- 4 Review the text and make any changes that you require.
- 5 Save the file.
- 6 Copy **EVMessages.nsf** to the Enterprise Vault program folder (for example `C:\Program Files (x86)\Enterprise Vault`) on every Enterprise Vault server in the site.

Enabling mailboxes for archiving after installing Domino mailbox archiving

Mailboxes that are new to Enterprise Vault are configured and enabled for archiving by the Domino Provisioning task. If you have selected the option, Automatically enable mailboxes, on the provisioning group properties, then the Domino Provisioning task will configure the mailboxes and then enable them automatically when it runs. If this option is not selected, then new mailboxes will be configured when the Domino Provisioning task runs, but you will then need to enable the mailboxes manually.

Enterprise Vault menu options do not appear in Lotus Notes until the user's mailbox has been enabled and the user has reopened their mailbox. You can therefore roll out the Enterprise Vault extensions for Lotus Notes before users' mailboxes are enabled.

When a Domino mailbox is enabled, a new archive is created for the mailbox in the vault store specified for the provisioning group. An archive has an associated account that is used for billing purposes, and can have one or more users who can access the information stored in it.

If you want to deny access to Enterprise Vault archives for certain Domino mailbox users, you can specify the users in the registry setting, `DominoProvisioningACLSyncFilters`. For details of this setting, see the *Registry Values* manual.

As part of the provisioning process, the Domino Provisioning task configures in the mail file the Enterprise Vault Domino Gateway that is to be used by the client. If the Enterprise Vault Domino Gateway and the Enterprise Vault Storage Service that manages the archive are on the same computer, then the Enterprise Vault Domino Gateway assigned will be the one that is local to the user's archive. If the Enterprise Vault Domino Gateway is not on the same computer as the Enterprise Vault Storage Service that manages the archive, then the Domino Provisioning task will select a Enterprise Vault Domino Gateway at random.

The Task Controller service and Domino Provisioning task must be started before you can enable mailboxes. The default is for tasks to start automatically when the Task Controller service starts. On a default system, the Domino Provisioning task will run once a day. On the task properties, you can schedule the task to run twice a day at specific times. You can also force a run to process new mailboxes that have been added to provisioning groups.

You can configure the Domino Provisioning task to generate reports when the task is run in both report or normal mode. The reports are created in the folder `Enterprise Vault\Reports\Domino Provisioning`. In the task properties, check that the reporting level is as you require.

Full reporting will list the following:

- Each mailbox that is processed
- The provisioning group
- The mailbox policy assigned
- The username associated with the mailbox
- The action taken
- Details of any errors

Summary statistics about the task run are included at the end of the report.

To start the Task Controller service and Domino Provisioning task

- 1 In the left pane of the Administration Console, expand the **Enterprise Vault Servers** container.
- 2 Expand the computer to which you added the Task Controller service and then click **Services**.
- 3 In the right pane, right-click **Enterprise Vault Task Controller Service** and, on the shortcut menu, click **Start**.
- 4 In the left pane, click **Tasks** and ensure that the Domino Provisioning task has started.
- 5 The task will run automatically at the times that you have scheduled. You can also force a provisioning run by using the **Run Now** option, which is available on the **Schedule** properties page and on the menu when you right-click the task.
- 6 After the task has run, check the Domino Provisioning report.

To force the Domino Provisioning task to process mailboxes

- 1 In the left pane of the Administration Console, expand **Enterprise Vault Servers**, and then your Enterprise Vault server.
- 2 Click **Tasks**.
- 3 In the right-hand pane, right-click the Domino Provisioning task and select **Properties**.
- 4 Check that the reporting level is as you require.
- 5 In the right-hand pane, right-click the Domino Provisioning task and select **Run now**.
- 6 Select whether you want the task to run in report or normal mode. The task will then start processing the mailboxes in the provisioning groups.
- 7 After the task has run, check the Domino Provisioning report.
- 8 If you selected the option for mailboxes to be enabled for archiving automatically, they will also be enabled by the Domino Provisioning task during the run.

If you did not select the option to enable new mailboxes automatically, you must enable them manually.

To enable one or more mailboxes manually

- 1** In the Administration Console, click **Enable Mailbox** on the **Tools** menu or click the **Enable Mailboxes for Archiving** icon on the toolbar.
The **Enable Mailbox** wizard starts.
- 2** Follow the instructions, and click **Help** on any of the wizard screens for further information.
- 3** If mailboxes to be enabled are not listed as expected, check the Domino Provisioning report to ensure that they have been processed by the Domino Provisioning task.

Setting up a Vault Cache for offline users

This chapter includes the following topics:

- [About Vault Cache for Domino users](#)
- [Enabling users for Vault Cache with the Domino Desktop policy](#)
- [Disabling Vault Cache using the Domino Desktop policy](#)
- [Troubleshooting setting up Vault Cache for Domino](#)

About Vault Cache for Domino users

Vault Cache provides a local cache of archived items. Vault Cache performs the following functions:

- Gives a user instant access to archived items, even when the user is not connected to the corporate network.
- Is in addition to the normal, online archive.
- Is useful to mobile users who use laptop computers.

Additionally, Vault Cache may be useful in normal offices if you need to conserve bandwidth or improve performance. The improvement is because archived items are retrieved on the local computer.

When the Vault Cache is enabled for an archive, Enterprise Vault downloads copies of items to the Vault Cache database on the user's computer.

Enterprise Vault automatically synchronizes Vault Cache with the archive once a day. If new items have been added to the archive, copies of these are then

downloaded to Vault Cache. If there is no connection to the archive, the synchronization happens automatically the next time a connection is detected.

To minimize the number of items that need to be downloaded to the Vault Cache, items that are due to be archived soon, are automatically added to the Vault Cache. This feature is called *preemptive* copying.

When a user who is working offline opens a shortcut in Notes, the local copy in the Vault Cache database is opened.

When new items need to be downloaded to a Vault Cache database, copies of the items are gathered together and held temporarily in the Vault Cache before being downloaded to the user's Vault Cache.

Note: Vault Cache is not available for mail-in databases. Enterprise Vault ignores Administration Console Vault Cache policy settings for mail-in databases.

Enabling users for Vault Cache with the Domino Desktop policy

You can use the settings on the Vault Cache tab of the Domino Desktop policy to control behavior of the Vault Cache.

To enable users for Vault Cache

- 1 Before you start this procedure, you must have modified the mail template databases using the **Install Vault Cache** option in **EVInstall.nsf**.
See [“Installing the Lotus Notes and DWA client extensions”](#) on page 46.
- 2 If you have not already done so, grant permissions to the users who you are going to enable for Vault Cache.
See [“Granting permissions to users of Vault Cache”](#) on page 45.
- 3 Open the properties of the Domino Desktop policy and click the **Vault Cache** tab.
- 4 Select **Make Vault Cache available for users**.
- 5 Select one of the following:
 - **Automatically enable.** Select this option to enable Vault Cache automatically for all offline users.
 - **Allow users to decide.** Select this option to allow users to enable Vault Cache by selecting Enterprise Vault Cache Options from the Tools menu.
- 6 Modify the other Vault Cache settings as required.

- 7 Click **OK** to close the policy properties.
- 8 Synchronize the mailboxes. You can run the Domino Provisioning Task to synchronize the mailboxes. You can do either of the following:
 - Use **Synchronize Individual Mailboxes**, which is on the **Synchronization** tab of the provisioning task's properties. This method requires you to select the mailboxes you want to synchronize.
 - Use **Run Now**, which is on the **Schedule** tab of the provisioning task's properties. **Run Now** processes all mailboxes in the Domino domain, but may take longer because the mailboxes that are associated with other policies may also be processed.

The Vault Cache will be available to users when they create or update their local replica-based mail.

Setting permissions on the Enterprise Vault Domino Gateway when using Vault Cache

You must ensure that all users who are enabled for Vault Cache have permission to create databases on the Enterprise Vault Domino Gateway.

To set permissions on the Enterprise Vault Domino Gateway

- 1 Open the Domino server document for the Enterprise Vault Domino Gateway.
- 2 Click the **Security** tab.
- 3 Scroll down to the **Create databases & templates** setting.
- 4 Set the required value for **Create databases & templates**, as follows:
 - To allow all users to create databases on the Enterprise Vault Domino Gateway, leave **Create databases & templates** blank.
 - To restrict database creation to the users who have been enabled for Vault Cache, specify every user or group of users.
- 5 Click **Save & Close** to save your changes.

Disabling Vault Cache using the Domino Desktop policy

If you need to disable Vault Cache, you must edit the Desktop policy in the Administration Console and then replicate the local mail databases. This procedure disables Vault Cache for all users to whom the policy applies.

Note that individual users have the option to disable Vault Cache by clearing **Enable Vault Cache** in the Enterprise Vault Cache Options.

To disable Vault Cache

- 1 In the Administration Console, double-click the Domino Desktop policy to display its properties.
- 2 Click the **Vault Cache** tab.
- 3 Clear **Make Vault Cache available for users**.
- 4 Click **OK** to close the policy properties.
- 5 Run the provisioning task to apply the new policy settings.
- 6 Replicate the local mail replica databases with the mail databases on the server.

To check that Vault Cache has been disabled

- 1 Open the local mail replica database.
- 2 Click **Tools** and then **About Enterprise Vault**.
- 3 Check that Vault Cache is disabled.

Troubleshooting setting up Vault Cache for Domino

This section provides troubleshooting information for setting up Vault Cache.

Newly-enabled Vault Cache for Domino is not populated

When Vault Cache is enabled for a Notes client, the Notes agents scan the local mail replica and download messages to Vault Cache. The Notes agents are 'Process Request' and 'Trawler'. If the Notes client configuration means that these agents cannot run, Vault Cache is never populated with Notes items.

If Vault Cache is not populated, try the following

- 1 Ensure that **Enable scheduled local agents** is selected in the user preferences:
 - From the **Notes** menu, select **File**, then **Tools**, and then **User Preferences**.
 - Under **Startup Options**, select **Enable scheduled local agents**.
 - Exit, and then restart Notes.

For more information, see IBM Technote [Locally Scheduled Agents Do Not Run on Schedule](#)

- 2 Restart the Notes client.

- 3 Ensure that the database property **Disable background agents for this database** is not selected in the mail replica database:
 - **Select File**, then **Database**, then **Properties** to display the InfoBox.
 - Ensure that **Disable background agents for this database** is not selected.

For more information, see IBM Technote [Background Agents Are Not Running in a Particular Database](#)
- 4 If the problem is still not solved, try the following:
 - See IBM Technote [Troubleshooting Script for Notes Scheduled Agents \(and Agent Manager\)](#) for more troubleshooting information.
 - Set `Log_AgentManager = 1` in the `notes.ini` file to ensure that Agent Manager (amgr) events are logged to the local `log.nsf`.

Setting up Domino Journaling archiving

This chapter includes the following topics:

- [Preparation for Domino Journaling archiving](#)
- [Adding a Domino domain](#)
- [Adding a Domino server](#)
- [Assigning a vault store for Domino Journaling](#)
- [Creating a Domino Journal archive](#)
- [Adding permissions to the Domino journal archive](#)
- [Creating a Domino Journal policy](#)
- [Creating a Domino Journaling task](#)
- [Adding a Domino Journaling location](#)
- [Identifying internal Notes mail recipients](#)
- [How to configure clients when setting up Domino Journal archiving](#)

Preparation for Domino Journaling archiving

Before you proceed, ensure that you have done the following:

- Checked that software prerequisites are satisfied.
- Configured the Domino journal databases as required by Enterprise Vault.

- Prepared a Lotus Notes ID file with suitable access to the Domino domain, server and journaling location.

See the *Installing and Configuring* manual for instructions on how to perform these tasks.

Adding a Domino domain

You can now configure the target Domino domain in the Enterprise Vault Administration Console.

To add a Domino domain

- 1 In the left pane of the Administration Console, expand the **ArchivingTargets** container.
- 2 Right-click **Domino** and, on the shortcut menu, click **New** and then **Domino Domain**.

The **New Domino Domain** wizard starts.

- 3 Work through the wizard.

Adding a Domino server

Next, configure the target Domino Servers in the Enterprise Vault Administration Console.

To add a Domino server

- 1 In the left pane of the Administration Console, expand the **ArchivingTargets** container.
- 2 Expand **Domino**.
- 3 Right-click the Domino domain to which you want to add a server and on the shortcut menu, click **New** and then **Domino Server**.

The **New Domino Server** wizard starts.

- 4 Work through the wizard.

Assigning a vault store for Domino Journaling

Domino Journaling archives can be held in an existing vault store that is also used for other types of archive. Alternatively, you may want to create a new vault store for the archives. If you want to use a new vault store, create the vault store and partition before you add the Domino journaling location.

You start the New Vault Store wizard from the Administration Console. To do this from the Administration Console right-click the Vault Store container and, on the shortcut menu, click **New** and then **Vault Store**. Alternatively, click the Create new Vault Store icon on the toolbar. Follow the instructions, and click **Help** on any of the wizard screens for further information.

You will need to provide the following information:

- The name of the SQL Server.
- The location for the vault store database files.

The safety copy setting is ignored for journaling; Enterprise Vault deletes the safety copy immediately when journaling.

The name you specify for the new vault store must contain any of only the following characters:

- The letters A through Z
- Numbers 0 through 9
- Spaces

When the vault store has been created, the wizard then takes you through creating a partition.

You can view and customize the properties of vault stores, partitions and archives by right-clicking the object container in the Administration Console tree and selecting **Properties**. For information on the properties of each object, see the Administration Console online help.

Creating a Domino Journal archive

This section describes how to create a Domino Journal archive.

To create a Domino Journal archive

- 1 In the left pane of the Administration Console, expand the Site hierarchy until the **Archives** container is visible.
- 2 Expand the **Archives** container.
- 3 Right-click **Domino Journal** and, on the shortcut menu, click **New** and then **Archive**.

The **New Domino Journal Archive** wizard starts.

- 4 Work through the wizard.

Adding permissions to the Domino journal archive

You must add permissions for those users who need to be allowed access to items that have been archived from the journal mailbox.

Users can have the following different types of access to an archive:

- **Read:** users can view and retrieve items from the archive. Those who need to search items archived from the journal mailbox, such as auditors, must have at least read access to the archive.
- **Write:** this is ignored for Domino Journal archives.
- **Delete:** users can delete items from the archive.
Note that, even though you grant the delete permission here, a user cannot delete from the archive unless you also select **Users can delete items from their archives** on the **General** tab of **Site Properties**.

To add permissions to the journal archive

- 1 In the left pane of the Administration Console, expand the hierarchy until **Archives** is visible.
- 2 Expand **Archives**.
- 3 Click **Domino Journal**.
- 4 In the right pane, double-click the archive whose permission list you want to modify.
The archives properties are shown.
- 5 Click the **Permissions** tab.

Creating a Domino Journal policy

This section describes how to create a Domino Journal policy.

To create a Domino Journal policy

- 1 In the left pane of the Administration Console, expand the Site hierarchy until the **Policies** container is visible.
- 2 Expand the **Policies** container.
- 3 Right-click **Domino Journaling** and, on the shortcut menu, click **New** and then **Policy**.
The **New Domino Journaling Policy** wizard starts.
- 4 Work through the wizard.

Creating a Domino Journaling task

This section describes how to create a Domino Journaling task.

To add a Domino Journaling task

- 1 In the left pane of the Administration Console, expand the Site hierarchy until the **Enterprise Vault Servers** container is visible.
- 2 Expand the **Enterprise Vault Servers** container.
- 3 Expand the name of the server to which you want to add the Domino Journaling task.
- 4 Right-click **Tasks** and, on the shortcut menu, click **New** and then **Domino Journaling Task**.

The **New Domino Journaling Task** wizard starts.

- 5 Work through the wizard.

Adding a Domino Journaling location

By default, Enterprise Vault archives from all Domino Journaling databases that are in the subfolder and use the StdMailJournaling template. You can use a registry value to specify other templates to use.

To add a Domino Journaling location

- 1 In the left pane of the Administration Console, expand the **Archiving Targets** container.
- 2 Expand **Domino**.
- 3 Expand the Domino domain that contains the server to which you want to add a location.
- 4 Expand the Domino server to which you want to add a location and, on the shortcut menu, click **New** and then **Domino Journaling Location**.

The **New Domino Journaling Location** wizard starts.

- 5 Work through the wizard.

To specify additional journaling templates

- 1 On the Enterprise Vault server that will run the Domino Journaling task, create a new string registry value called `DominoJournalingTemplates` in the following location:


```
HKEY_LOCAL_MACHINE
  \SOFTWARE
    \KVS
      \Enterprise Vault
        \Agents
```
- 2 Give `DominoJournalingTemplates` a value that is a comma-separated list of the journaling templates that you want to use.
- 3 Restart the Domino Journaling Task to apply the new setting.

Identifying internal Notes mail recipients

You can specify that Enterprise Vault must perform a local address lookup for specific Notes domains. The local lookup enables Enterprise Vault to identify the Lotus Notes user name for those messages that are addressed to alternate email addresses. The local lookup results can aid searching in the Web applications and in Compliance Accelerator and Discovery Accelerator.

To specify the domains that require local address lookup you must edit the registry on the Enterprise Vault servers that run the journaling and archiving tasks.

See the *Registry Values* manual for details of the **NotesDomains** registry key.

How to configure clients when setting up Domino Journal archiving

A Web browser on a client computer can be used to search for archived items. An HTML preview of archived items is always available from within the search results. However, whether an alternate format of the item is available depends on the software that is installed on the user's computer.

The format that Enterprise Vault uses for the items that it sends to the client computer depends on settings in the `WebApp.ini` initialization file. This initialization file controls the behavior of the Web access application.

[Table 4-1](#) shows the requirements and corresponding `WebApp.ini` settings.

Table 4-1 WebApp.ini settings for Domino

Download format	Requirements	WebApp.ini setting
As a .HTML file that is then opened by the Web browser on the client computer.	None.	HTMLNotMSG=1
As an EML file that the client can open immediately.	Outlook Express or Outlook must be present on the user's computer.	None required

Note on using a Lotus Notes client when setting up Domino Journal archiving

You cannot use a Lotus Notes client to view archived Domino Server messages.

The Lotus Notes client installed on the Enterprise Vault server, is used by Enterprise Vault and should not be used by any other user. You cannot start this client while Enterprise Vault is running.

Configuring filtering

This chapter includes the following topics:

- [About filtering](#)
- [Configuring custom filtering](#)

About filtering

Filtering provides more granular control over how Enterprise Vault archiving tasks process items during an archiving run.

Note: It is important that you test your filtering configuration on a development server, using realistic data, before implementing it on your production servers.

Enterprise Vault provides the following filtering features:

- Custom filtering. This feature provides sophisticated filtering. You create rules that select messages by matching one or more attributes, such as email addresses, subject text, message direction or the value of certain message properties.

The rules also include instructions on how Enterprise Vault is to process a selected message. This can include archiving the message, assigning a particular retention category, storing the message in a specified archive, or deleting or marking the message.

The option to remove message attachments is not yet available when filtering Domino server messages.

By default, Enterprise Vault archives items that do not match any filter rule. You can configure filter rules so that only items that match a rule are archived. See [“About custom filtering ruleset files”](#) on page 80.

- Custom properties. This feature is an extension of custom filtering. It enables you to configure Enterprise Vault to index additional properties on messages that are selected by the custom filters. These properties may be standard properties that a default Enterprise Vault system does not index, or they may be properties added to messages by a proprietary, third party application. Custom properties also introduces the concept of "content categories" for grouping the settings that are to be applied to messages that match a rule. These settings can include the retention category to assign, the archive to use and the additional properties to index.
As the custom properties feature provides extended functionality to custom filtering, it is enabled with custom filtering, and shares the custom filtering configuration.

Configuring custom filtering

Custom filtering provides sophisticated filtering for Domino server journal archiving. For example, you may want items with a particular subject, sender or recipients to be sent to a separate archive, or you may want messages sent within the company to be given a special retention category of "Internal".

You can set up default filters that apply to all archiving tasks that are enabled for custom filtering. In addition, you can create separate custom filters for specific Domino journaling locations.

If custom properties have been added to items, you may want these properties indexed for selected items. Instructions are provided on how to extend custom filtering to use the custom properties feature.

See [“Configuring custom properties and content categories”](#) on page 105.

Table 5-1 Steps to configure custom filtering

Step	Action	More information
Step 1	Configure registry settings to enable custom filtering.	See “Configuring registry settings for Domino server journal filtering” on page 78.

Table 5-1 Steps to configure custom filtering (*continued*)

Step	Action	More information
Step 2	Create filter rules and actions in one or more XML ruleset files, as required. The ruleset files must be placed in the folder Enterprise Vault\Custom Filter Rules.	<p>See “About custom filtering ruleset files” on page 80.</p> <p>See “About the general format of ruleset files for custom filtering” on page 86.</p> <p>See “About rule actions for custom filtering” on page 89.</p> <p>See “About message attribute filters for custom filtering” on page 90.</p> <p>See “Example ruleset file for custom filtering” on page 101.</p>
Step 3	Restart the archiving tasks that have custom filtering enabled.	<p>The following message is sent to the Enterprise Vault event log when the Domino server archiving tasks start:</p> <pre>EventID = 41086 Description = External Filter The Lotus custom filter 'KVS.EnterpriseVault. LotusDomino.CustomFilter' has started.</pre> <p>The following message is sent to the Enterprise Vault event log when the Domino server archiving tasks stop:</p> <pre>EventID = 41087 Description = External Filter 'KVS.EnterpriseVault. LotusDomino.CustomFilter' stopped.</pre>

About custom filtering in distributed Enterprise Vault environments

In a distributed environment, with archiving tasks on more than one computer, the registry entries must be set up on each computer that hosts archiving tasks that are to be enabled for custom filtering. Similarly, the XML ruleset files must be copied to all computers that host archiving tasks that are enabled for custom filtering.

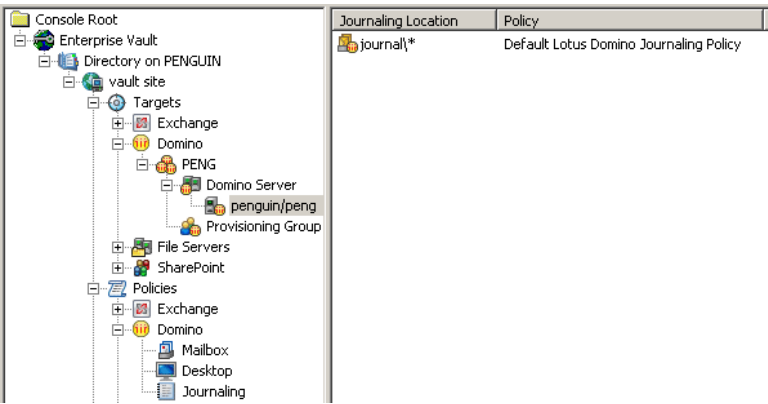
If you change the registry settings or XML files, remember to propagate the changes to each of the other computers.

Configuring registry settings for Domino server journal filtering

Each Domino journal archiving target is configured in Enterprise Vault Administration Console as a Domino "Journaling Location" during the setup process.

Figure 5-1 shows an example of a Domino journaling location that is configured in the Enterprise Vault Administration Console.

Figure 5-1 Domino journaling location in the Administration Console



In this example, the target Domino server is "penguin" in the Domino organization, "peng", and the target journaling location is the folder called "journal" in the Domino Data directory.

Configuring the registry settings that are described in this section enables custom filtering for all the Domino Journaling tasks that are hosted on the server.

By creating a named ruleset file, you can limit filtering to particular journaling locations.

See [“About custom filtering ruleset files”](#) on page 80.

To configure the registry settings for Domino server journal filtering

- 1 On the computer that hosts the Enterprise Vault Domino Journaling task, log on as the Vault Service account.
- 2 Start Regedit.
- 3 Navigate to the following location:

```
HKEY_LOCAL_MACHINE
\Software
\KVS
\Enterprise Vault
\External Filtering
\Lotus Journaling
```

If the External Filtering key does not exist, create it as follows:

- Right-click Enterprise Vault and select **New > Key**.
- Name the key External Filtering.

Similarly, if the Lotus Journaling key does not exist, create it as follows:

- Right-click External Filtering and select **New > Key**.
- Name the key Lotus Journaling.

- 4 If the Lotus Journaling key does exist, any existing filters are listed under it. Filter names must be an unbroken numbered sequence starting at 1.

If you have installed the Compliance Accelerator Journaling Connector,

```
KVS.EnterpriseVault.LotusDominoMsgHandler.dll!
KVS.EnterpriseVault.LotusDomino.CADominoFilter
```

then it must be the last in the sequence. When you add other filters, you must rename the Journaling Connector to ensure that it remains last in the sequence.

To rename the Journaling Connector setting:

- Right-click the setting name and select **Rename**.
 - Enter the new name, for example, 2.
- 5 Create a new string value for the new custom filtering setting. The name of this setting must fit into the existing number sequence. If no other journaling filters exist, set the name to 1. Give it the following value

```
KVS.EnterpriseVault.LotusDominoCustomFilter!
KVS.EnterpriseVault.LotusDomino.CustomFilter
```

- 6 Optionally, you can create a DWORD entry with the name `Override`, if it does not exist. Set its value to 0 (zero). This entry controls whether the Domino Journaling task reexamines any messages that are marked as `MARK_DO_NOT_ARCHIVE` each time it processes the Domino journaling location. If the value is 0, or the `Override` entry does not exist, then the Domino Journaling task does not reexamine the messages.

If you later change the rule action, you can temporarily set the value to 1. Setting this value forces the Domino Journaling task to reprocess any messages in the Domino journaling location.
- 7 Close Regedit.
- 8 After you have configured the required XML filter rules, restart the Domino Journaling tasks.

About custom filtering ruleset files

You create filter rules and actions in XML ruleset files. A ruleset file contains one or more rules.

Each rule contains the following:

- A set of one or more attribute filters for evaluating each item that the archiving task processes. The order of attribute filters in a rule is not significant, as all the attribute filters are evaluated.
- An action to be applied to an item that matches all the attribute filters in the rule. Examples of actions are applying a particular retention category or storing the item in a specified archive. More than one action can be applied to matching items.

Although the order of the attribute filters in a rule is not significant, the order of the rules in the ruleset file is significant. The rules are evaluated in the order in which they appear in the file. The action associated with the first matching rule is applied to the item, and no further rules are evaluated for that item. If none of the rules match the item, the default action is to archive the item.

Tip: By default items that do not match any rules are archived. If you want to archive only items that match a rule, then create a "catch-all" rule as the last rule in the ruleset file. Assign the action "MARK_DO_NOT_ARCHIVE" to this last rule. You can create a "catch-all" rule using message direction attributes, for example.

See [“Message direction filters for custom filtering”](#) on page 98.

All ruleset files must be available in the folder `Custom Filter Rules` in the main Enterprise Vault folder (for example `C:\Program Files (x86)\Enterprise`

Vault) on the computer hosting the archiving tasks that are enabled for custom filtering.

After Enterprise Vault has been installed, this folder contains the following XML files:

- `Example Filter Rules.xml` — This provides examples of filter rules.
- `ruleset schema.xdr` — This contains the XML schema for validating the XML ruleset files.
- `Example Custom Properties.xml` — This provides example entries for the `custom properties.xml` file.
See [“About the general format of Custom Properties.xml”](#) on page 108.
- `customproperties.xsd` — This contains the XML schema for validating the custom properties XML file.

When you modify a ruleset file, you must restart the associated archiving tasks to pick up the changes. In a distributed environment, you must copy the updated file to each computer with tasks enabled for custom filtering, and then restart the associated tasks on each computer.

Note: It is important to set permissions on the ruleset files to prevent unauthorized editing. For increased security, you could also enable Windows file auditing on these files.

About the default filter rules file for custom filtering

If you create a ruleset file called `Default Filter Rules.xml`, this will be used as the default ruleset file for all custom filtering.

To implement specific filtering for particular Domino journaling locations, you can create named ruleset files in addition to the default ruleset file. Each target location associated with a named ruleset file is processed according to the rules in its named ruleset file. All other custom filtering will use the rules in the default ruleset file.

If no custom filtering is to be applied other than those specified by named ruleset files, it is more efficient to omit the default ruleset file, `Default Filter Rules.xml`, and configure the `IGNORENODEFAULT` registry setting.

See [“About controlling default custom filtering behavior”](#) on page 82.

In this way, custom filtering is only applied to target locations explicitly defined by named ruleset files.

If you implement the custom properties feature, and want the same actions applied to all items that the archiving tasks process (that is, specific items are not selected for processing by matching attributes), you can omit ruleset files altogether and define a default content category in the file, `custom_properties.xml`.

Information on content categories and the `custom_properties.xml` file is provided in the following section:

See [“Configuring custom properties and content categories”](#) on page 105.

About named ruleset files for individual Domino journaling locations

To set up custom filtering for specific Domino journaling locations, you need to create a separate ruleset file for each journaling location that you want to filter. The name of each ruleset file must be `journaling_location_name.xml`.

For example, if you want to filter the Domino journaling location that is shown as "Symantec/*" in the Administration Console, you would create a ruleset file called "Symantec.xml". Any other journaling locations that are serviced by the Domino archiving tasks and which have been enabled for custom filtering, are processed using the default ruleset file, `Default Filter Rules.xml`.

If archiving tasks are enabled for custom filtering, but neither the default ruleset file nor named ruleset files exist, the archiving tasks will attempt to use a default content category, as defined in `custom_properties.xml`. If none of the above exists, an error is logged and the archiving tasks stop. You can configure archiving tasks to manage missing defaults gracefully using the `IGNORENODEFAULT` registry setting.

See [“About controlling default custom filtering behavior”](#) on page 82.

This registry setting is particularly useful if you want to restrict filtering to named mailboxes only.

About controlling default custom filtering behavior

If Enterprise Vault archiving tasks are enabled for filtering, the action they take when archiving is determined by the existence of the various configuration entities:

- XML ruleset files in the folder, `Enterprise Vault\Custom Filter Rules`
- The XML ruleset file, `Default Filter Rules.xml`
- The XML custom properties file, `Custom Properties.xml`
- Content category entries in `Custom Properties.xml`

An additional configuration option, `IGNORENODEFAULT` registry entry, can be used to alter the archiving task behavior, if some of the configuration entities are not defined.

See [“Setting `IGNORENODEFAULT` registry entry for custom filtering”](#) on page 83.

Different configurations and the resulting actions of archiving tasks for each configuration are shown in [Table 5-2](#) and [Table 5-3](#).

Setting `IGNORENODEFAULT` registry entry for custom filtering

If the appropriate registry keys are configured to enable custom filtering and properties for archiving tasks, then certain configuration entities are required to define the default actions of the archiving tasks. For example, if specific targets are to be archived using particular filter rules, then a named XML ruleset file must exist for each of the archiving targets for custom filtering, and a `Default Filter Rules.xml` file must also exist to provide filtering rules for the other archiving targets serviced by the archiving tasks. If this file does not exist, then the archiving tasks will stop and an error reported in the event log.

Alternatively, if the `Default Filter Rules.xml` file does not exist, but you configure the `IGNORENODEFAULT` registry entry, the archiving tasks ignore the fact that the file is missing and use the default archiving task policy settings when archiving all targets that do not have a named ruleset file.

The `IGNORENODEFAULT` registry entry also enables you to restrict custom filtering to target archiving targets with named ruleset files only. (If the `Default Filter Rules.xml` file exists, it is used as the default by all archiving tasks enabled for custom filtering.)

Similarly, to apply custom property indexing to specific target archiving locations, you would typically require the following configuration entities:

- A `Custom Properties.xml` file with entries defining the custom properties to index and an associated content category.
- A separate, named ruleset file for each of the archiving targets requiring custom property indexing.
- In `Custom Properties.xml`, a default content category to use for all messages archived from other locations that are not covered by the named ruleset files.

However, if you want to restrict custom filtering and custom property indexing to the named targets, it is more efficient to omit setting the default content category in `Custom Properties.xml` and set the `IGNORENODEFAULT` registry entry. In this way, custom property indexing is applied only to locations explicitly defined by named ruleset files.

To set the IGNORENODEFAULT registry entry for custom filtering

- 1 Log in as the Enterprise Vault Service account on the computer running the archiving tasks enabled for custom properties and filters.
- 2 Start Regedit.
- 3 Navigate to the following location:

```
HKEY_LOCAL_MACHINE
\Software
\KVS
\Enterprise Vault
\External Filtering
\Lotus Journaling
```

- 4 Right-click the `Lotus Journaling` key and select `New,Key`.
- 5 Name the new key `KVS.EnterpriseVault.LotusDomino.CustomFilter`.
- 6 Right-click `KVS.EnterpriseVault.LotusDomino.CustomFilter` and create a new DWORD called `IGNORENODEFAULT`.
- 7 Set the value to `1` to ignore missing default files or settings.
This key will apply to all Domino Journaling tasks on the computer.
- 8 Close Regedit.
- 9 Restart the associated archiving tasks.

In a distributed environment, where you have archiving tasks running on more than one computer, you will need to perform these steps on each computer running archiving tasks that have been enabled for custom filtering and properties.

Summary of default behavior for custom filtering

[Table 5-2](#) shows ten different configurations for custom filtering and properties.

The resulting actions taken by archiving tasks in each case are described in [Table 5-3](#).

In all cases it is assumed that the appropriate registry settings have been configured to enable the archiving task for custom filtering. The following configuration entities are considered:

- **Named XML ruleset files in the folder**, `Enterprise Vault\Custom Filter Rules`. In the example cases shown, `John Doe.xml` and `Sam Cole.xml` are named ruleset files for the mailboxes John Doe and Sam Cole respectively.

The examples in this section show named ruleset files for Exchange Server mailboxes. For Domino Server Archiving, named ruleset files can be created for specific Domino server journaling locations.

See [“About custom filtering ruleset files”](#) on page 80.

- The default ruleset file for all types of archiving, `Enterprise Vault\Custom Filter Rules\Default Filter Rules.xml`.
- The custom properties file, `Enterprise Vault\Custom Filter Rules\Custom Properties.xml`, with custom properties defined for indexing.
- Content category entries in the `Custom Properties.xml` file.
- The registry setting, `IGNORENODEFAULT`, with a value of 1.

Table 5-2 Example custom filter and custom property configurations

Case	Custom properties file exists	Default content category defined	Named ruleset file exists: John Doe.xml	Named ruleset file exists: Sam Cole.xml	Default ruleset file exists	IGNORENODEFAULT set
1	No	No	No	No	No	No
2	No	No	No	No	No	Yes
3	No	No	Yes	No	No	No
4	No	No	Yes	No	No	Yes
5	No	No	Yes	No	Yes	No
6	No	No	Yes	No	Yes	Yes
7	Yes	No	No	Yes	No	No
8	Yes	No	No	Yes	No	Yes
9	Yes	Yes	No	Yes	No	No
10	Yes	Yes	No	Yes	No	Yes

Table 5-3 Resulting actions for example configurations

Case	Resulting action
1	An error is written to the event log and the archiving task stops, because custom filtering is enabled but there is no ruleset file or custom property file.
2	Missing defaults are ignored and both mailboxes are archived according to the default mailbox policy.

Table 5-3 Resulting actions for example configurations (*continued*)

Case	Resulting action
3	An error is reported for Sam Cole's mailbox and the archiving task stops, because no default ruleset file or custom properties file exists.
4	John Doe's mailbox is archived according to rules in <code>John Doe.xml</code> and Sam Cole's mailbox is archived according to the default mailbox policy. Missing defaults are ignored.
5	John Doe's mailbox is archived according to rules in <code>John Doe.xml</code> and Sam Cole's mailbox is archived according to the rules in <code>Default Filter Rules.xml</code> . No custom properties are indexed. Content categories cannot be used.
6	As for case 5. The fact that <code>IGNORENODEFAULT</code> is set makes no difference.
7	An error is reported for John Doe's mailbox and the archiving task stops, because there is no applicable named ruleset file or default ruleset file or custom property file.
8	John Doe's mailbox is archived according to rules in the default mailbox policy. Sam Cole's mailbox is archived according to the rules in <code>Sam Cole.xml</code> .
9	All messages are archived from John Doe's mailbox and custom properties indexed. Messages are archived from Sam Cole's mailbox according to the rules in <code>Sam Cole.xml</code> .
10	As for case 9. The fact that <code>IGNORENODEFAULT</code> is set makes no difference.

About the general format of ruleset files for custom filtering

This section describes the required overall format of the XML ruleset files.

All ruleset files must be located in the `Custom Filter Rules` folder, in the main Enterprise Vault folder (for example `C:\Program Files (x86)\Enterprise Vault`) on the computer hosting the archiving tasks that are enabled for custom filtering.

Ruleset files have the following general format:

```
<?xml version="1.0"?>
<RULE_SET xmlns="x-schema:ruleset schema.xdr">

  <RULE [NAME="rule_name"] [ACTION="match_action"]
    [CONTENTCATEGORY="content_category"]
    [RETENTION="retention_category"]
```

```
[ARCHIVEID="archiveid"]>

<message_attribute [attribute_value_operators]>
  <attribute_value>
    [<attribute_value>]
  </message_attribute>

[<message_attribute>... </message_attribute>]

</RULE>

[<RULE> ... </RULE>]
</RULE_SET>
```

The ruleset can contain one or more rules. Naming a rule (NAME="rule_name") is optional. It is advisable to include it for documentation purposes and to distinguish the rule in trace output.

Each rule contains one or more message attribute filters for evaluating messages. Attachment filtering is not currently available with Domino server filtering.

[Table 5-4](#) shows the message attributes that you can use to select messages.

Table 5-4 Message attributes for custom filtering

Message attribute	More information
Author	See “Message author and recipients filters for custom filtering” on page 91.
Recipients	See “Message author and recipients filters for custom filtering” on page 91.
Direction	See “Message direction filters for custom filtering” on page 98.
Subject text	See “Message subject filters for custom filtering” on page 100.

Matching against attribute values is case-insensitive. All message attribute filters in a rule will be applied to a message, so the order of message attribute filters in a rule is not significant. A message matches a rule when it matches all the message attribute filters contained in that rule. When a message matches a rule, the action specified by ACTION= is applied to the message.

Each rule has a message action associated with it. ACTION="match_action" defines the action to be applied to the message when it matches a rule. For example, an

action could be to mark the item as evaluated but not archive it (ACTION="MARK_DO_NOT_ARCHIVE"). If the action is to archive the item, additional actions can be specified, such as assigning a specific retention category (RETENTION="*retention_category*") or storing the item in a particular archive (ARCHIVEID="*archive_ID*"). If no action is specified, it defaults to "ARCHIVE_ITEM".

The preferred way to specify how messages that match a rule are to be archived is to assign a content category. A content category is a group of settings that are to be applied to an archived item. This can include a retention category, an archive ID and a list of the additional properties that are to be indexed by Enterprise Vault. You define content categories in the file `custom_properties.xml`.

See “[About content categories](#)” on page 112.

Note: Each rule in the ruleset file will be evaluated in the order in which it appears in the file and only the first matching rule will be executed. For this reason, it is important to put the highest priority rules first.

About validating XML ruleset files for custom filtering

Archiving tasks that are enabled for custom filtering validate ruleset XML against the schema, `ruleset_schema.xdr`, when they start archiving items. If any of the XML is invalid, the tasks stop and you must correct any errors before restarting them.

To avoid disrupting tasks because of syntactic errors, it is a good idea to validate your XML file before it is accessed by the tasks. You could use a third party tool, such as the graphical XML Editor in Liquid XML Studio:

<http://www.liquid-technologies.com/XMLStudio/Free-Xml-Editor.aspx>

When using the tool, specify the namespace as:

```
x-schema:ruleset schema.xdr
```

The schema file, `ruleset_schema.xdr`, is shipped in the Custom Filter Rules folder. The schema must be referenced at the start of any ruleset files as follows:

```
<?xml version="1.0"?>
<RULE_SET xmlns="x-schema:ruleset schema.xdr">
```

If the file contains non-ANSI characters, ensure the correct encoding is set on the first line and save the file using the appropriate encoding.

Note: All the XML tags and predefined values shown in upper case in this document are case-sensitive and must be entered as upper case in the ruleset file. Values entered should also be treated as case-sensitive.

About rule actions for custom filtering

The following actions can be applied to messages that match a rule filter:

- ACTION="ARCHIVE_ITEM" – Archive the message. This is the default action if you do not include the ACTION= clause or a message does not match any of the rules.
With this action you can have additional actions: assigning a retention category (RETENTION="*retention_category*") to the item, sending the item to a specific archive (ARCHIVEID="*archive_ID*") and assigning a particular content category. See [“Assigning a retention category for custom filtering”](#) on page 90. See [“Specifying an archive for custom filtering”](#) on page 90.
- ACTION="MARK_DO_NOT_ARCHIVE" – Do not archive the message; leave it in the original location.

Note: Messages marked as MARK_DO_NOT_ARCHIVE remain in the original location. If you are applying filtering to the Domino journaling location, this action should only be used for a small number of messages, as leaving lots of messages may affect journaling performance.

If you later change the rule action, you can temporarily set the Override registry value to 1 to force the task to reprocess marked items.

See [“Configuring registry settings for Domino server journal filtering”](#) on page 78.

- ACTION="HARD_DELETE" – Do not archive the message; delete it immediately without moving it to the wastebasket.

Note: If the Compliance Accelerator Journaling Connector is being used to capture a required percentage of all Domino Server journaled messages, do not configure a custom journal filter that deletes selected messages; this will compromise the accuracy of the Compliance Accelerator monitoring policy, because any deleted messages are not available for capture by the Journaling Connector.

Assigning a retention category for custom filtering

The `RETENTION="retention_category"` option is only applicable if the rule action is `ACTION="ARCHIVE_ITEM"`.

Retention_category is the name of an existing retention category defined in Enterprise Vault. A different retention category may be specified for different rules.

The extract below shows how the option might be specified in the ruleset file. In this example, any messages that satisfy the message attribute filters will be archived and given the retention category, Legal:

```
<RULE NAME="Example rule2" ACTION="ARCHIVE_ITEM"
  RETENTION="Legal">
  <message attribute filters>
</RULE>
```

Specifying an archive for custom filtering

The `ARCHIVEID="<archive_ID>"` option is only applicable if the rule action is `ACTION="ARCHIVE_ITEM"`. *Archive_ID* identifies an existing, enabled archive.

You can define a different archive for different rules. If you do not specify an archive, the default archive for the mail file is used.

The extract below shows how the option might be specified in the ruleset file. In this example, any messages that satisfy the message attribute filters will be stored in the archive specified:

```
<RULE NAME="Example rule" ACTION="ARCHIVE_ITEM"
  ARCHIVEID="15165263832890493848568161647.server1.local">
  <message attribute filters>
</RULE>
```

To find the ID of the required archive

- 1 Right-click the archive in the Enterprise Vault Administration Console.
- 2 Select **Properties**. The archive ID is displayed on the **Advanced** page of **Properties**.

About message attribute filters for custom filtering

Each rule can contain one or more message attribute filters. Each message attribute filter defines an attribute in the message to evaluate. To match a rule, a message must satisfy all the message attribute filters included in the rule. That is to say,

there is an implicit AND between all message attributes included in a rule. The order of the attributes within a rule is not significant.

Message attributes are defined in a rule using the following general format:

```
<RULE NAME="rule_name" ...>

    <message_attribute [attribute_value_operators]>
        <attribute_value>
            [<attribute_value>]
        </message_attribute>

    [<message_attribute>... </message_attribute>]
</RULE>
```

message_attribute defines a message attribute to match. This can be AUTHOR, RECIPIENTS, DIRECTION or SUBJECTS.

attribute_value defines the message attribute value(s) to match. For each attribute there may be one or more values.

attribute_value_operators are special operator options that enable you to define how values for an attribute are to be applied. The operators INCLUDES= and ALLOWOTHERS= are particularly useful if you want to define negative and positive matches when filtering on AUTHOR, RECIPIENTS and SUBJECTS.

See [“About creating complex filters using the INCLUDES and ALLOWOTHERS operators”](#) on page 94.

Attribute value operators are not available when filtering on message DIRECTION.

Message author and recipients filters for custom filtering

To match message sender ("From" address) and recipient addresses ("To", "cc", "Bcc" and "Undisclosed" addresses), you can use the message attributes <AUTHOR></AUTHOR> and <RECIPIENTS></RECIPIENTS>; in the ruleset file outline, message attributes are shown as:

```
<message_attribute> ...</message_attribute>
```

You can specify the actual addresses to match as SMTP email addresses, display names or SMTP domains using the following XML elements (these are represented by the *<attribute_value>* lines in the ruleset file outline):

- <EA>name@domain</EA>

This form can be used to specify SMTP addresses. The value specified must be the complete SMTP email address; if the value specified here is only part of an address, the message will not match. Wildcard characters cannot be used.

If the character '&' is included in an SMTP address, the character must be replaced with

`&`;

as '&' is a special character in XML. For example, the SMTP address `admin&finance@ourcompany.com` should be specified in the XML file as:

`admin&finance@ourcompany.com`

■ **<DISPN>display name</DISPN>**

This form can be used to specify display names. As with the SMTP address, the value must be the full display name, without wildcard characters. As display names can take many different forms, it is advisable to include a filter for the associated SMTP address.

An example display name for Domino server messages is:

`<DISPN>Kevin Smith/exampleorg</DISPN>`

To match all required messages, ensure that you include all possible variations for a display name. If Organizational Units are included in display names, these must also be specified. For example,

`<DISPN>Kevin Smith/Sales/exampleorg</DISPN>`

■ **<DOMAIN>exampledomain.com</DOMAIN>**

This form can be used to specify SMTP domains. The value specified can be the full domain or a subdomain. For example, if the following domain value is specified:

`<DOMAIN>ourcompany.com</DOMAIN>`

The following addresses will match:

- `john.doe@ourcompany.com`
- `jack.doe@hq.ourcompany.com`
- `jane.doe@uk.hq.ourcompany.com`

but the following address will not match:

- `john.doe@hqourcompany.com`

■ **<DL>distribution list name</DL>**

Use this form when you want to match messages that have been sent to any members of the specified distribution list or group. For example, if a rule contains the following line:

```
<DL>ALL SALES</DL>
```

Then messages sent to any member of the distribution list or group called ALL SALES will match, irrespective of whether the member's name is shown as the Display Name or SMTP address on the message.

See [“About distribution lists in attribute values with custom filtering”](#) on page 93.

Note: Matching attribute values is case-insensitive.

The following example shows how you can specify a simple rule to archive and set the retention category "Legal" on any messages sent from anyone in the domain, ourcompany.com, with legal@ourcompany.com or the Lotus Notes user, Greg Court, in the recipient list:

```
<RULE ... ACTION='ARCHIVE_ITEM' RETENTION='legal'>
  <AUTHOR>
    <DOMAIN>ourcompany.com</DOMAIN>
  </AUTHOR>
  <RECIPIENTS>
    <EA>legal@ourcompany.com</EA>
    <DISPN>Greg Court/ourorg</DISPN>
  </RECIPIENTS>
</RULE>
```

The attribute value operators, INCLUDES= and ALLOWOTHERS=, enable you to define complex filters.

See [“About creating complex filters using the INCLUDES and ALLOWOTHERS operators”](#) on page 94.

About distribution lists in attribute values with custom filtering

If you want to match all messages sent to members of a particular Domino group, then use the <DL> </DL> message attribute. For example,

```
<RECIPIENTS>
  <DL>ALL SALES</DL>
</RECIPIENTS>
```

would match any message sent to any member of the group, ALL SALES.

For this matching to work, ensure that expansion of groups is enabled in the Administration Console (in the "Archiving General" settings on the "Advanced" tab of the Domino journal policy).

You can specify distribution lists and groups using the <EA>, <DISPN> and <DOMAIN> message attributes. However, only messages with the specified string will match; no attempt is made to compare message recipients with individual members in the specified distribution list.

For example, the members of an Domino group called ALL SALES are:

- john.doe@ourcompany.com
- ken.brookes@ourcompany.com
- len.scott@ourcompany.com

In the ruleset file, the following message attribute filter is specified in a rule:

```
<RECIPIENTS>  
  <DISPN>ALL SALES</DISPN>  
</RECIPIENTS>
```

If a message has the display name ALL SALES in the recipient list, the message will satisfy the attribute filter above. If the message does not have the display name ALL SALES in the recipient list, it will not match the attribute filter, even if the recipient list does include the email address of a member of the distribution list.

About creating complex filters using the INCLUDES and ALLOWOTHERS operators

You can create more complex filters by specifying several values for AUTHOR or RECIPIENTS message attributes and using the operators, INCLUDES= and ALLOWOTHERS= to define how the attribute values are to be matched.

INCLUDES= can have the following values:

- INCLUDES="NONE" means match messages that do not include the values specified for the attribute
- INCLUDES="ANY" means match messages that include one or more of the values specified for the attribute
- INCLUDES="ALL" means match messages that include all of the values specified for the attribute

If the INCLUDES= operator is not specified, INCLUDES="ANY" is assumed.

ALLOWOTHERS= can have the following values:

- ALLOWOTHERS="N" means match messages that include only the values specified in the filter and no others
- ALLOWOTHERS="Y" means that matched messages can include attribute values other than those listed in the filter can be included

If the ALLOWOTHERS= operator is not specified, ALLOWOTHERS="Y" is assumed.

In the following example, messages will match the rule if they have all three of the listed email addresses (INCLUDES="ALL"), and only these addresses (ALLOWOTHERS="N"), in the recipient list:

```
<RULE ... >
  <RECIPIENTS INCLUDES="ALL" ALLOWOTHERS="N">
    <EA>john.doe@ourcompany.com</EA>
    <EA>ken.brookes@ourcompany.com</EA>
    <EA>len.scott@ourcompany.com</EA>
  </RECIPIENTS>
</RULE>
```

In the next example, messages will match the rule if they have any of the listed email addresses (INCLUDES="ANY") but nothing else (ALLOWOTHERS="N"):

```
<RULE ... >
  <RECIPIENTS INCLUDES="ANY" ALLOWOTHERS="N">
    <EA>john.doe@ourcompany.com</EA>
    <EA>ken.brookes@ourcompany.com</EA>
    <EA>len.scott@ourcompany.com</EA>
  </RECIPIENTS>
</RULE>
```

In the next example, messages will match the rule if they do not include any of the listed email addresses in the recipient list (INCLUDES="NONE"). Matched messages can have other addresses in the recipient list (ALLOWOTHERS="Y"):

```
<RULE ... >
  <RECIPIENTS INCLUDES="NONE" ALLOWOTHERS="Y">
    <EA>john.doe@ourcompany.com</EA>
    <EA>ken.brookes@ourcompany.com</EA>
    <EA>len.scott@ourcompany.com</EA>
  </RECIPIENTS>
</RULE>
```

If you want to specify both positive and negative matches within a single rule, you can have multiple message attribute entries and use INCLUDES="NONE" or INCLUDES="ALL", as appropriate. For example:

```
<RULE ... >
  <RECIPIENTS INCLUDES="NONE">
    <EA>john.doe@ourcompany.com</EA>
    <EA>len.scott@ourcompany.com</EA>
  </RECIPIENTS>
```

```
<RECIPIENTS> INCLUDES="ALL">
  <EA>Ken.Brookes@ourcompany.com</EA>
  <EA>robert.hill@ourcompany.com</EA>
</RECIPIENTS>
</RULE>
```

In the above example, messages will match if they do not include john.doe@ourcompany.com or len.scott@ourcompany.com in the recipient list:

```
<RECIPIENTS INCLUDES="NONE" ...</RECIPIENTS>
```

but do include both ken.brookes@ourcompany.com and robert.hill@ourcompany.com

```
<RECIPIENTS INCLUDES="ALL" ... </RECIPIENTS>
```

By using different combinations of INCLUDES= and ALLOWOTHERS= values, you can set fairly complex filters.

Table 5-5 shows filter results for different messages when different combinations of values are set for the operators, INCLUDES= and ALLOWOTHERS=, in the following example filter:

```
<RULE ... ACTION="ARCHIVE_ITEM">
  <RECIPIENTS INCLUDES="NONE|ANY|ALL"
    ALLOWOTHERS="N|Y">
    <EA>Ann@example.com</EA>
    <EA>Bill@example.com</EA>
  </RECIPIENTS>
</RULE>
```

Ann@example.com and Bill@example.com are the recipient addresses to match.

Table 5-5 Effect of using different operator value combinations

Operator values set	Msg 1: recipient is Ann	Msg 2: recipients are Ann & Bill	Msg 3: recipients are Ann, Bill & Colin	Msg 4: recipients are Bill & Colin	Msg 5: recipient is Colin
INCLUDES="NONE" + ALLOWOTHERS="Y"	no match	no match	no match	no match	match
INCLUDES="NONE" + ALLOWOTHERS="N"	no match	no match	no match	no match	no match
INCLUDES="ANY" + ALLOWOTHERS="Y"	match	match	match	match	no match

Table 5-5 Effect of using different operator value combinations (*continued*)

Operator values set	Msg 1: recipient is Ann	Msg 2: recipients are Ann & Bill	Msg 3: recipients are Ann, Bill & Colin	Msg 4: recipients are Bill & Colin	Msg 5: recipient is Colin
INCLUDES="ANY" + ALLOWOTHERS="N"	match	match	no match	no match	no match
INCLUDES="ALL" + ALLOWOTHERS="Y"	no match	match	match	no match	no match
INCLUDES="ALL" + ALLOWOTHERS="N"	no match	match	no match	no match	no match

In the table, the main column headings show the recipients in five different test messages. (For brevity, the recipients are called Ann, Bill, and Colin in the column headings.)

The first column shows different combinations of values set for the INCLUDES= and ALLOWOTHERS= operators.

"no match" means that, if the operator combination shown in the left column is set, a message sent to the recipients shown in the column heading would not satisfy the filter rule and would not be archived (that is, the rule action is not applied).

"match" means that, if the operator combination shown in the left column is set, a message sent to the recipients shown in the column heading would satisfy the filter rule and be archived.

[Figure 5-2](#) and [Figure 5-3](#) illustrate what happens in two of the scenarios in [Table 5-5](#).

Figure 5-2

Msg 1 with INCLUDES="NONE" and ALLOWOTHERS="N"

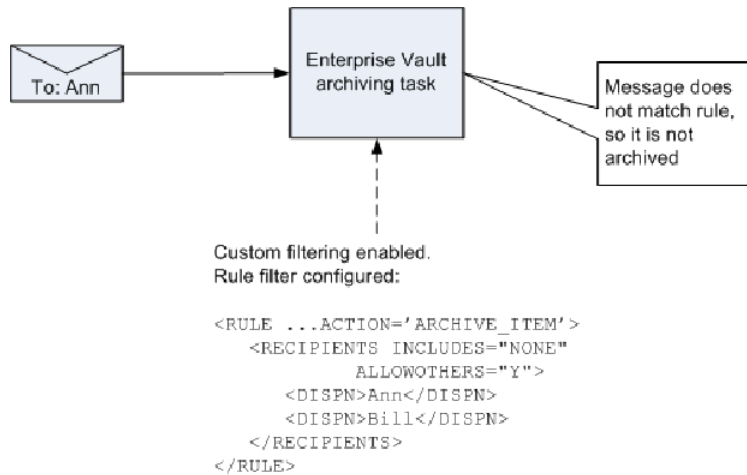
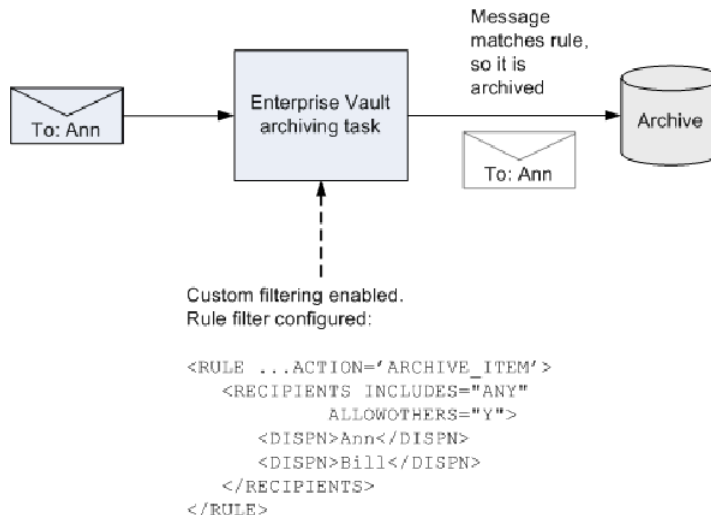


Figure 5-3

Msg 1 with INCLUDES="ANY" and ALLOWOTHERS="Y"



Message direction filters for custom filtering

The `<DIRECTION></DIRECTION>` message attribute enables you to match messages based on the direction of the message, in relation to the organization, without needing to specify the author or recipient details in the rule. Message

direction can be internal to the organization, outbound from the organization or inbound to the organization.

One or more of the following values can be specified in the `<DIRECTION></DIRECTION>` message attribute:

- `INTERNAL="Y"` means match the message if it is from an internal address to an internal address. The message must not include any external addresses in the recipient list.
- `OUTBOUND="Y"` means match the message if it is from an internal address to an external address. The message must include at least one external address in the recipient list.
- `INBOUND="Y"` means match the message if it is from an external address to an internal address. The message must include at least one internal address in the recipient list.

If the value is not specified, it defaults to "N". For any messages to match, at least one value must be set to "Y".

The following example rule will archive and set the retention category "Internal", on messages from one internal address to another internal address only. Note that a message from one internal address to another internal address that also has an external address in the recipient list will be treated as external:

```
<RULE NAME="Internal only" RETENTION="Internal" >
  <DIRECTION INTERNAL="Y" OUTBOUND="N" INBOUND="N"/>
</RULE>
```

The following example rule will archive and set the retention category "External", on messages sent to or received from addresses outside the organization:

```
<RULE NAME="External" RETENTION="External" >
  <DIRECTION OUTBOUND="Y" INBOUND="Y"/>
</RULE>
```

If you want only items that match the rules to be archived, the following example rule can be added to the end of the file as a "catch-all" rule:

```
<RULE NAME="Do not archive anything else" ACTION="MARK_DO_NOT_ARCHIVE">
<DIRECTION INBOUND="Y" OUTBOUND="Y" INTERNAL="Y"/> </RULE>
```

For each item that is evaluated using this example rule, one of the direction attributes will always have the value "Y". Therefore items that do not match any other rule in the file will match this rule. The associated action means that the matching items are not archived.

About defining which addresses are internal with custom filtering

You can specify internal domains using the InternalSMTPDomains registry key.

To add domains using the registry key, do the following on each computer with an Enterprise Vault Journaling task

- 1 Start Regedit and navigate to the following location:

```
HKEY_LOCAL_MACHINE
\Software
\KVS
\Enterprise Vault
\Agents
```

- 2 Create a new String Value called InternalSMTPDomains.
- 3 Modify the key and in the Value Data field enter the required domains as a semicolon delimited string. For example, setting this string to the following means that addresses such as jld@eng.uk.ourcompanyinc.com and kv@hq.ourcompany.parentcorp.com will also be treated as internal:

"ourcompanyplc.com;ourcompanyinc.com;ourcompany.parentcorp.com"

Message subject filters for custom filtering

The <SUBJECTS></SUBJECTS> message attribute enables you to match messages on the subject text of the message. Within a <SUBJECTS> attribute, values to match can be defined as follows:

- Match any message with a subject that is exactly the same as the specified string:

```
<SUBJ MATCH="EXACT">string</SUBJ>
```

- Match any message with a subject that contains the specified string:

```
<SUBJ MATCH="CONTAINS">string</SUBJ>
```

- Match any message with a subject that starts with the specified string:

```
<SUBJ MATCH="STARTS">string</SUBJ>
```

- Match any message with a subject that ends with the specified string:

```
<SUBJ MATCH="ENDS">string</SUBJ>
```

Matching against attribute values is case-insensitive. Wildcards cannot be used.

In the following example, messages that have a subject of exactly "Welcome New Employee" or starts with "Salary Summary for" or ends with "Message Notification" will be deleted without being archived:

```
<RULE NAME="Delete" ACTION="HARD_DELETE">
  <SUBJECTS>
    <SUBJ MATCH="EXACT">Welcome New Employee</SUBJ>
    <SUBJ MATCH="STARTS">Salary Summary for</SUBJ>
    <SUBJ MATCH="ENDS">Message Notification</SUBJ>
  </SUBJECTS>
</RULE>
```

The INCLUDES="NONE" operator can be used to match messages with a subject that does not include particular strings. For example, the following rule will match messages that do not have any of the specified values in the message subject:

```
<RULE ... >
  <SUBJECTS INCLUDES="NONE">
    <SUBJ MATCH="EXACT">Welcome New Employee</SUBJ>
    <SUBJ MATCH="STARTS">Salary Summary for</SUBJ>
    <SUBJ MATCH="ENDS">Message Notification</SUBJ>
  </SUBJECTS>
</RULE>
```

Example ruleset file for custom filtering

The following shows the supplied example ruleset file, Default Filter Rules.xml (a renamed copy of Example Filter Rules.xml). If the registry keys have been set to enable custom filtering, this file will be used for filtering any archiving targets that do not have a named ruleset file.

Note: The options used in Example Rules 3 and 11 are currently not available for Domino Server archiving.

```
<?xml version="1.0"?>
<RULE_SET xmlns="x-schema:ruleset schema.xdr">

  <!-- Example Rule 1: This rule will exclude any email from archiving
  if it originates from someone in the Employee Benefits distribution
  list.-->

  <RULE NAME="Benefits correspondence" ACTION="MARK_DO_NOT_ARCHIVE">
```

```

    <AUTHOR>
        <DISPN>HR Employee Benefits</DISPN>
    </AUTHOR>
</RULE>

<!--Example Rule 2: This rule will exclude any email from archiving
if it is sent to someone in the Employee Benefits distribution list.
-->
<RULE NAME="Benefits correspondence" ACTION="MARK_DO_NOT_ARCHIVE">
    <RECIPIENTS>
        <DISPN>HR Employee Benefits</DISPN>
    </RECIPIENTS>

</RULE>

<!--Example Rule 3: (Available for Exchange Server archiving only)
This rule will move email to the wastebasket if it comes
from any of the sources listed, and is about any of the
subjects listed.-->
<RULE NAME="Newsletters" ACTION="MOVE_DELETED_ITEMS">
    <AUTHOR INCLUDES="ANY">
        <EA>icweek@ucg.com</EA>
        <EA>WebDirect@ACLI.com</EA>
        <DOMAIN>limra.com</DOMAIN>
    </AUTHOR>
    <SUBJECTS INCLUDES="ANY">
        <SUBJ MATCH="STARTS">Society SmartBrief</SUBJ>
        <SUBJ MATCH="EXACT">TaxFacts ENews</SUBJ>
    </SUBJECTS>

</RULE>

<!--Example Rule 4: Delete mail from known junk-mail sources,
(and others), if it contains certain common spam subjects -->
<RULE NAME="Junk Mail" ACTION="HARD_DELETE">
    <AUTHOR INCLUDES="ANY" ALLOWOTHERS="Y">
        <DOMAIN>indiatimes.com</DOMAIN>
        <DOMAIN>websavings-usa.net</DOMAIN>
    </AUTHOR>
    <SUBJECTS INCLUDES="ANY">
        <SUBJ MATCH="CONTAINS">enlargement</SUBJ>
        <SUBJ MATCH="CONTAINS">weight loss</SUBJ>
    </SUBJECTS>
    <SUBJECTS INCLUDES="ALL">

```

```

    <SUBJ MATCH="CONTAINS">debt</SUBJ>
    <SUBJ MATCH="CONTAINS">consolidate</SUBJ>
    <SUBJ MATCH="CONTAINS">loan</SUBJ>
  </SUBJECTS>
</RULE>

```

<!--Example Rule 5: Take default action (ARCHIVE_ITEM) if the subject matches the composite rule:
Must start with "MEMO", contain "INTERNAL"
and end in "OurCompany"
e.g. "MEMO : Contains information internal to OurCompany"
would match, but "MEMO : do not distribute" would not match.
Also allocates the message to a content category "Memoranda"-->

```

<RULE NAME="Internal Memo" CONTENTCATEGORY="Memoranda">
  <SUBJECTS INCLUDES="ALL">
    <SUBJ MATCH="STARTS">Memo</SUBJ>
    <SUBJ MATCH="CONTAINS">Internal</SUBJ>
    <SUBJ MATCH="ENDS">OurCompany</SUBJ>
  </SUBJECTS>
</RULE>

```

<!--Example Rule 6: Take default action (ARCHIVE_ITEM) on any email from management members included here. Email from management will be categorized under "ManagementMail" and retained as "Important"-->

```

<RULE NAME="Management" CONTENTCATEGORY="ManagementMail"
RETENTION="Important">
  <AUTHOR INCLUDES="ANY">
    <EA>mike.senior@management.com</EA>
    <EA>jon.little@management.com</EA>
    <EA>jill.taylor@management.com</EA>
  </AUTHOR>
</RULE>

```

<!--Example Rule 7: Take default action (ARCHIVE_ITEM) if an email is addressed to any of the managers AND NO ONE ELSE
The message will be archived in a special archive reserved only for this kind of email - specified by the ARCHIVEID-->

```

<RULE NAME="Sent to Management ONLY"
  ARCHIVEID="16611B008A3F65749BC4118182E0021461110000evsite.
  ourcompany.com ">

```

```

        <RECIPIENTS INCLUDES="ANY" ALLOWOTHERS="N">
            <EA>mike.senior@management.com</EA>
            <EA>jon.little@management.com</EA>
            <EA>jill.taylor@management.com</EA>
        </RECIPIENTS>
    </RULE>

<!--Example Rule 8: Do not archive mail that was sent to someone
outside OurCompany -->

<RULE NAME="External Recipient" ACTION="MARK_DO_NOT_ARCHIVE">
    <RECIPIENTS INCLUDES="NONE">
        <DOMAIN>OurCompany.com</DOMAIN>
    </RECIPIENTS>
</RULE>

<!--Example Rule 9: Archive and give the existing Retention
Category, Internal, to any email that was sent only to employees
in OurCompany.-->

<RULE NAME="Internal Recipient" ACTION="ARCHIVE_ITEM"
RETENTION="Internal">
    <DIRECTION INTERNAL="Y"/>
</RULE>

<!--Example Rule 10: Use a special retention category for mail
addressed to any members of the specified DL. -->
<RULE NAME="On the VIP list" RETENTION="VeryImportant">
    <RECIPIENTS>
        <DL>TheVIPs</DL>
    </RECIPIENTS>
</RULE>

<!--Example Rule 11: (Available for Exchange Server archiving only)
Delete MP3 attachments before archiving -->
<RULE NAME="DeleteMP3s" ATTACHMENT_ACTION="REMOVE">
    <FILES>
        <FILE FILENAME="*.MP3"/>
    </FILES>
</RULE>

<!--Example Rule 12: (This example is specific to Exchange
Server archiving, but filtering on document properties is

```



```
also available for Domino Server archiving).  
Match against named MAPI properties defined in  
Custom Properties.xml -->  
<RULE NAME="Category Match" ACTION="ARCHIVE_ITEM">  
  <NAMEDPROP TAG="CaseAuthor" INCLUDES="ANY">  
    <PROP VALUE="Engineering"/>  
    <PROP VALUE="Support"/>  
  </NAMEDPROP>  
  <NAMEDPROP TAG="CaseStatus" INCLUDES="ANY">  
    <PROP VALUE="Open"/>  
    <PROP VALUE="Pending"/>  
  </NAMEDPROP>  
</RULE>  
</RULE_SET>
```

Configuring custom properties and content categories

Custom properties is an extension to custom filtering. It enables you to configure Enterprise Vault to index additional properties on messages that are selected by the custom filters. These properties may be standard properties that a default Enterprise Vault system does not index, or they may be properties added to messages by a proprietary, third party application.

Read this section to find out:

- How to include in Enterprise Vault indexes additional properties on an item, for example, properties that have been added to messages by third-party applications.
- How to configure the browser search to enable users to search on these indexed properties.
- How to configure content categories.

The custom properties feature is an extension to custom filtering that enables Enterprise Vault to access and index additional Domino server properties, that have been added to messages by a third-party application, when archiving items.

Content categories are groups of settings to be applied to messages as they are archived. Settings can include a retention category to be applied, an archive to be used and particular message properties to be indexed. You can configure Enterprise Vault to apply a content category on all messages archived by particular archiving tasks. Alternatively, by using custom filtering together with custom properties, you can configure Enterprise Vault to apply a content category on selected messages only.

You define custom properties and content categories in the XML file, `Custom Properties.xml`, which must be located in the folder `Enterprise Vault\Custom Filter Rules`. Additional entries in this file enable you to make the indexed properties available to other applications, for example, the Enterprise Vault browser search. Users can then include the custom properties in archive search criteria. An example of the custom properties file, `Example Custom Properties.xml`, is installed in the `Custom Filter Rules` folder.

An API is available to enable third-party applications to access the custom properties.

If you have special filtering requirements for your archiving system, Symantec Corporation can supply the appropriate custom filters.

Table 5-6 Steps to configure custom properties or content categories

Step	Action	More information
Step 1	Ensure that the custom filtering registry settings for the required archiving tasks are configured. These need to be set, even if you want to implement custom properties or content categories, without filtering.	See “Configuring registry settings for Domino server journal filtering” on page 78.

Table 5-6 Steps to configure custom properties or content categories
(continued)

Step	Action	More information
Step 2	Create the XML file, <code>Custom Properties.xml</code> . Place this file in the folder <code>Enterprise Vault\Custom Filter Rules</code> .	<p>See “About the general format of Custom Properties.xml” on page 108.</p> <p>The entries in <code>Custom Properties.xml</code> enable you to do the following:</p> <ul style="list-style-type: none"> ■ Index custom properties on messages. ■ Define required content categories. ■ Display custom properties and content categories in Web search applications, so that users can include them in search criteria. <p>To configure Enterprise Vault to index specific custom properties on all messages, without performing any filtering, create a <code>Custom Properties.xml</code> file but no ruleset file. The <code>Custom Properties.xml</code> file must include definitions of the custom properties and a default content category. The default content category will be applied to all messages and defines which properties Enterprise Vault is to index. This behavior can be altered using the <code>IGNORENODEFAULT</code> registry setting.</p> <p>See “About controlling default custom filtering behavior” on page 82.</p>
Step 3	If you want to index the properties on selected messages or apply content categories to selected messages, create the required filter rules and actions in XML ruleset files. These are held in one or more XML ruleset files, which must also be placed in the folder, <code>Enterprise Vault\Custom Filter Rules</code> .	See “Configuring custom filtering” on page 76.
Step 4	Restart the archiving tasks that have custom properties and filters enabled.	

About the general format of Custom Properties.xml

For Enterprise Vault to access and index additional properties on Domino server messages, the properties must be defined in the file `Custom Properties.xml`, which you create in the `Enterprise Vault\Custom Filter Rules` folder on the computer running the archiving tasks enabled for custom filtering. The installed file, `Enterprise Vault\Custom Filter Rules\Example Custom Properties.xml` provides an example of this file.

The file has the following sections:

- `<CONTENTCATEGORIES></CONTENTCATEGORIES>` This section defines available content categories. A content category is a group of settings that will be applied to an item when it is archived. This can include custom properties to index.
See [“About content categories”](#) on page 112.
- `<CUSTOMPROPERTIES></CUSTOMPROPERTIES>` This section defines the additional message properties that are to be available to Enterprise Vault.
See [“Defining additional Domino message properties in custom properties”](#) on page 110.
- `<PRESENTATION></PRESENTATION>` This section defines how the content categories and custom properties are displayed to users in external applications, such as the Enterprise Vault Web Access application browser search.
See [“Defining how custom properties are presented in third party applications”](#) on page 115.

Note: The order of these sections is significant.

The following outline shows the general format of the file:

```
<?xml version="1.0"?>
<CUSTOMPROPERTYMETADATA xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance"
    xsi:noNamespaceSchemaLocation="customproperties.xsd">
<!-- 1. DEFINITION OF CONTENT CATEGORIES AVAILABLE -->
    <CONTENTCATEGORIES>
        <CONTENTCATEGORY> ... </CONTENTCATEGORY>
        [<CONTENTCATEGORY> ... </CONTENTCATEGORY>]
    </CONTENTCATEGORIES>

<!-- 2. DEFINITION OF CUSTOM PROPERTIES AVAILABLE -->
    <CUSTOMPROPERTIES>
        <NAMESPACE> ... </NAMESPACE>
```

```

    [<NAMESPACE> ... </NAMESPACE>]
  </CUSTOMPROPERTIES>

<!-- 3. DEFINITION OF PRESENTATION PROPERTIES AVAILABLE -->
<PRESENTATION>
  <APPLICATION>
    <FIELDGROUPS>
      <FIELDGROUP> ... </FIELDGROUP>
      [<FIELDGROUP> ... </FIELDGROUP>]
    </FIELDGROUPS>
    <AVAILABLECATEGORIES>
      <AVAILABLECATEGORY> ... </AVAILABLECATEGORY>
      [<AVAILABLECATEGORY> ... </AVAILABLECATEGORY>]
    </AVAILABLECATEGORIES>
  </APPLICATION>
  [<APPLICATION> ... </APPLICATION>]
</PRESENTATION>

```

A summary description of all mandatory and optional elements and attributes in the file is provided in the following section:

See [Table 5-7](#) on page 120.

Whenever you modify the file, you must restart the associated archiving tasks. In a distributed environment, you must copy the updated file to each computer with tasks enabled for custom properties, and then restart the associated tasks on each computer.

If the browser search is being used to search for custom properties, then the Enterprise Vault Application Pool in IIS Manager must also be restarted.

About validating Custom Properties.xml

When Enterprise Vault is installed, `customproperties.xsd` is placed in the Custom Filter Rules folder. This is the XML schema for validating Custom Properties.xml.

The schema file must be referenced in the CUSTOMPROPERTYMETADATA entry at the start of the Custom Properties.xml file, as follows:

```

<?xml version="1.0"?>
<CUSTOMPROPERTYMETADATA xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="customproperties.xsd">

```

If the file contains non-ANSI characters, ensure the correct encoding is set on the first line and save the file using the appropriate encoding.

The XML is validated when the associated task starts processing messages. If anything is invalid, the task stops and you must correct any errors before restarting the task.

To avoid disrupting tasks because of syntactic errors, it is a good idea to validate your XML file before it is accessed by the tasks. You could use a third party tool, such as the graphical XML Editor in Liquid XML Studio:

<http://www.liquid-technologies.com/XmlStudio/Free-Xml-Editor.aspx>

When using the tool, specify the namespace as:

```
x-schema:customproperties.xsd
```

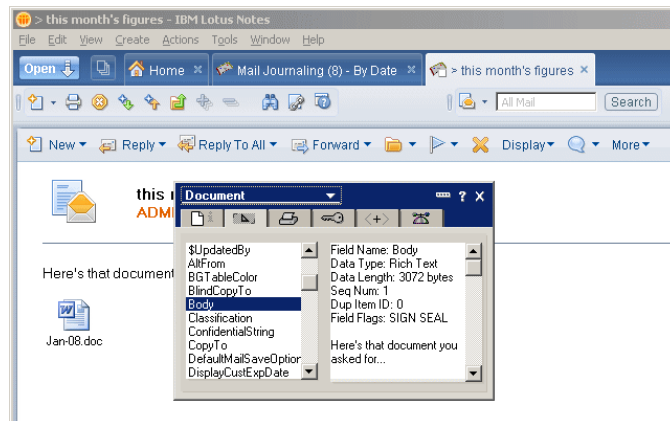
Note: All the XML tags and predefined values shown in upper case in this document are case-sensitive and must be entered as upper case in the file. Values entered should also be treated as case-sensitive.

Defining additional Domino message properties in custom properties

To include custom Domino message properties in Enterprise Vault indexes, you define the required properties in `Custom Properties.xml`.

In the Lotus Notes client, you can view Domino properties on a message as shown in [Figure 5-4](#).

Figure 5-4 Viewing Domino message properties



To view Domino message properties

- 1 Open the message in the Lotus Notes client, then right-click the message.
- 2 Select **Document Properties** in the menu.
- 3 Select the **Fields** tab in the dialog that is displayed.

The property names are listed in the left-hand pane. When you select a property in the left-hand pane, details of that property are displayed in the right-hand pane.

To make Domino message properties available to Enterprise Vault, you define them in the <CUSTOMPROPERTIES> section of `Custom Properties.xml`. The properties defined in this section can then be referenced in the content category and presentation sections.

The properties are grouped using the <NAMESPACE> element. Typically, properties accessed by a particular application are defined in the same namespace.

This outline of the custom properties section shows how Domino properties are defined:

```
<!-- 2. DEFINITION OF CUSTOM PROPERTIES AVAILABLE -->

<CUSTOMPROPERTIES>
  <NAMESPACE TYPE="LOTUS">
    <PROPERTY NAME="Domino_prop_name" LOTUSTYPE="Domino_data_type"
TAG="EV_prop_name" />
    [<PROPERTY ... />]
  </NAMESPACE>
</CUSTOMPROPERTIES>
```

The TYPE="LOTUS" identifies the property as a Domino property.

Within each <NAMESPACE> element, the properties are defined in <PROPERTY> elements using NAME and TAG attributes, as follows:

- In NAME="Domino_prop_name", the value is the property name displayed in the Lotus Notes document properties. The value must exactly match the value displayed in the Lotus Notes client.
- LOTUSTYPE="Domino_data_type" identifies the property data type. The following types are supported: "TEXT", "NUMBER", "TIME". Enterprise Vault indexes "NUMBER" properties as integers.
- TAG identifies the property within Enterprise Vault. It can contain only alphanumeric characters (A-Z a-z 0-9); spaces and underscore characters are not permitted. The value assigned to the property TAG must be unique within

the XML file; although you can cross refer to the property using the TAG value, the same value cannot be used to identify any other entities in the file.

About content categories

In the `<CONTENTCATEGORIES>` section of `Custom Properties.xml`, you define the content categories that you want to apply to filtered messages.

A content category defines a group of settings that are to be applied to an item when it is archived.

The settings can include the following:

- The retention category to assign to the item
- The destination archive
- A list of the additional message properties that Enterprise Vault is to index

There can be more than one content category defined in the `<CONTENTCATEGORIES>` element.

In ruleset files, the actions associated with a rule can include assigning a particular content category to messages that satisfy the rule. The content category definition in `Custom Properties.xml` provides the default settings for the content category. Some of these can be overridden for particular rules.

See [“About assigning content categories in rules when configuring custom properties”](#) on page 114.

The following example shows entries for a content category called Litigation:

```
<!-- 1. DEFINITION OF CONTENT CATEGORIES AVAILABLE -->

<CONTENTCATEGORIES DEFAULT="Litigation">
  <CONTENTCATEGORY NAME="Litigation" RETENTIONCATEGORY="Litigation"
    ARCHIVEID="15165263832890493848568161647.server1.local">
    <INDEXEDPROPERTIES RETRIEVE="Y">
      <PROPERTY TAG="CaseAuthor"/>
      <PROPERTY TAG="CaseStatus"/>
    </INDEXEDPROPERTIES>
  </CONTENTCATEGORY>
</CONTENTCATEGORIES>
```

- `<CONTENTCATEGORIES></CONTENTCATEGORIES>` defines the content category section in the file.
- The `DEFAULT` attribute specifies the content category to be used as the default. This default applies to all types of archiving enabled for custom filtering.

This attribute is optional, if custom filtering is used, but mandatory if there are no ruleset files (unless the registry setting IGNORENODEFAULT is configured).

If filters are configured in ruleset files and a default content category is specified, any item that does not match any rules will be archived according to the settings in the default content category. If no default content category is specified, then a content category will only be applied to an item if specified by a matching rule in a filter ruleset file.

If no applicable ruleset files exist, then you must specify a default content category using the DEFAULT attribute in the <CONTENTCATEGORIES> element in `Custom Properties.xml`. The settings in the content category are then applied to all messages archived (unless the registry setting IGNORENODEFAULT is configured).

The actions of archiving tasks are determined by combinations of ruleset files, custom properties, content categories and the registry setting IGNORENODEFAULT.

- The <CONTENTCATEGORY> element defines a particular content category. There must be at least one content category defined.
- The content category NAME is used to identify this content category in the presentation section of the file, rules in custom filter ruleset files and external subsystems, such as the Enterprise Vault Indexing service. The name must have at least five characters, which can include alphanumeric characters only (A-Z a-z 0-9); space and underscore characters are not permitted.
If the content category is included in the presentation section of the file, it will be possible to search on the content category name in order to find all items archived using this particular content category.
- RETENTIONCATEGORY is optional and enables you to assign a retention category to each item archived using this content category. The retention category must already exist in Enterprise Vault.
- ARCHIVEID is optional and enables you to specify a destination archive for the item. The archive must exist and be enabled. To find the ID of an archive, display the archive properties in the administration console and click the "Advanced" tab.
- The <INDEXEDPROPERTIES> element is mandatory and groups the additional properties that Enterprise Vault is to index.
- The RETRIEVE attribute (optional) determines whether or not the defined properties should be returned with archive search results. By default, the properties are not displayed with search results (RETRIEVE="N").
- A <PROPERTY> element is required for each additional property to be indexed.

- The TAG value must match the associated Enterprise Vault TAG value specified in the custom properties section.

See [“Defining additional Domino message properties in custom properties”](#) on page 110.

About assigning content categories in rules when configuring custom properties

When using custom properties, the preferred way to specify the actions to be taken for messages that match a filter rule is to assign a content category in the rule, in the ruleset file. You define the default settings included in a content category in the content categories section of `Custom Properties.xml`.

In the ruleset file, you assign a content category as follows:

```
<RULE NAME="Example rule" ACTION="ARCHIVE_ITEM"
  CONTENTCATEGORY="content_category_name">
  <message attribute filters>
</RULE>
```

The value of `"content_category_name"` is the name of the required content category as specified in `Custom Properties.xml`.

In the ruleset file, content categories can only be assigned when `ACTION="ARCHIVE_ITEM"`.

Overriding default content category settings

A rule can assign a content category and override some of the default content category settings. For example, if you have a content category that defines all the custom properties to index, a retention category and a destination archive, different rules can assign the content category but override values for the archive or retention category, as required.

For example, if a content category called `Litigation` is defined in `Custom Properties.xml` as follows:

```
<CONTENTCATEGORY NAME="Litigation" RETENTIONCATEGORY="Litigation"
  ARCHIVEID="15165263832890493848568161647.server1.local">
  <INDEXEDPROPERTIES RETRIEVE="Y">
    <PROPERTY TAG="AUTHOR01"/>
    <PROPERTY TAG="CASESTATUS"/>
  </INDEXEDPROPERTIES>
</CONTENTCATEGORY>
```

It can be referenced in a ruleset file as follows:

```
<RULE NAME="Example rule1" ACTION="ARCHIVE_ITEM"
  CONTENTCATEGORY="Litigation">
  <message attribute filters>
</RULE>
<RULE NAME="Example rule2" ACTION="ARCHIVE_ITEM"
  CONTENTCATEGORY="Litigation"
  ARCHIVEID="1516526383289049384890493848.server2.local">
  <message attribute filters>
</RULE>
```

Additional properties defined in the content category will be indexed with both rules. The second rule uses the same content category, but items that match this rule will be stored in a different archive.

Note: Before you alter an existing configuration, make sure that you understand what default behavior has been configured for each type of archiving. Check the DEFAULT content category attribute in `Custom Properties.xml` and the IGNORENODEFAULT registry setting.

See [“About controlling default custom filtering behavior”](#) on page 82.

Defining how custom properties are presented in third party applications

The presentation section of the file, `<PRESENTATION>`, defines how available content categories and custom properties are presented to external applications, such as an archive search engine.

Separating the presentation of properties from the underlying property definitions enables flexible mapping of custom property details onto a user interface. This also facilitates the support of multiple languages.

To access the custom property information in the `Custom Properties.xml` file, external applications must use the custom filter and property API.

See the *Enterprise Vault Application Programmer's Guide*.

Entries in the presentation section define the following:

- Custom properties available for displaying by the named application
- How properties are to be grouped and displayed in the application
- Content categories available to the application
- How each content category should be displayed in the application

Presentation information can be defined for each application that will require access to custom properties in archived items.

Here is an example of a presentation section (partially completed) that shows how to define how custom properties are displayed in the Enterprise Vault browser search application:

```
<!-- 3. DEFINITION OF PRESENTATION PROPERTIES AVAILABLE -->

<PRESENTATION>
  <APPLICATION NAME="search.asp" LOCALE="1033">
    <FIELDGROUPS>
      <FIELDGROUP LABEL="Case Properties">
        <FIELD TAG="CaseAuthor" LABEL="Author" CATEGORY="Litigation">
        </FIELD>
        <FIELD TAG="CaseStatus" LABEL="Status" CATEGORY="Litigation">
        </FIELD>
      </FIELDGROUP>
      <FIELDGROUP LABEL="Client Properties">
        <FIELD TAG="Client" LABEL="Client Name" CATEGORY="ClientAction">
        </FIELD>
        <FIELD TAG="Topic" LABEL="Message Topic" CATEGORY="ClientAction">
        </FIELD>
      </FIELDGROUP>
    </FIELDGROUPS>

    <AVAILABLECATEGORIES>
      <AVAILABLECATEGORY CONTENTCATEGORY="Litigation" LABEL="Litigation">
      </AVAILABLECATEGORY>
      <AVAILABLECATEGORY CONTENTCATEGORY="ClientAction" LABEL="Client Action">
      </AVAILABLECATEGORY>
    </AVAILABLECATEGORIES>
  </APPLICATION>

  <APPLICATION NAME="mysearch.asp" LOCALE="1041">
    <FIELDGROUPS>
      <FIELDGROUP LABEL="...">
        <FIELD TAG="CaseAuthor" LABEL="..." CATEGORY="Litigation"></FIELD>
        <FIELD TAG="CaseStatus" LABEL="..." CATEGORY="Litigation"></FIELD>
      </FIELDGROUP>
      <FIELDGROUP LABEL="...">
        <FIELD TAG="Client" LABEL="..." CATEGORY="ClientAction"></FIELD>
        <FIELD TAG="Topic" LABEL="..." CATEGORY="ClientAction">
        </FIELD>
      </FIELD>
    </FIELD>
  </FIELD>
</FIELD>
```

```

</FIELDGROUP>
</FIELDGROUPS>
<AVAILABLECATEGORIES>
  <AVAILABLECATEGORY CONTENTCATEGORY="Litigation" LABEL="...">
</AVAILABLECATEGORY>
  <AVAILABLECATEGORY CONTENTCATEGORY="ClientAction" LABEL="...">
</AVAILABLECATEGORY>
</AVAILABLECATEGORIES>
</APPLICATION>
</PRESENTATION>

```

The example shows entries for two applications – the US English (locale "1033") version of the Enterprise Vault browser search and a Japanese (locale "1041") version of a proprietary application. In this particular case, the same elements and attributes have been specified for both applications, but the LABEL values for the second application (omitted in the example) would be in Japanese.

Note the following:

- The properties available to each application are grouped using the <APPLICATION> element.
- The NAME attribute identifies the application.
- The value of the LOCALE attribute is defined by the calling application. The Enterprise Vault browser search uses the standard Microsoft Locale ID for the language that the application will use: 1033 represents US English. The second application in the example, `mysearch.asp`, also uses the Microsoft Locale ID; 1041 represents Japanese.

In the Web search page, custom properties are displayed in groups defined by their content category; that is, when a particular content category is selected, the custom properties with that content category are displayed.

Note the following:

- The <FIELDGROUPS> element is used to define all the groups of custom properties to be displayed.
- Each group is defined in a <FIELDGROUP> element. The LABEL attribute gives the title that will be displayed in the application for the group of properties. The value of the LABEL attribute must be unique in the application.
- <FIELD> elements define each property to be displayed in the group. The value of the TAG attribute identifies the property to be displayed. The value specified here must match the associated TAG value of the property in the <CUSTOMPROPERTIES> section of the file.

The value of the CATEGORY attribute identifies the content category with which this property is to be associated. When the user selects this content category in the search criteria, a box for this property will be displayed. The value specified for CATEGORY must match the associated NAME for the content category in the content category section of the file. Also, CATEGORY must be one defined in the <AVAILABLECATEGORIES> element.

TAG must be unique in the <FIELDGROUP> and the TAG/CATEGORY combination must be unique within the <APPLICATION> element.

LABEL defines the name that you want displayed in the user interface for the custom property.

- <AVAILABLECATEGORIES> groups the content categories that are to be available for selection in the application. Each content category is defined using the <AVAILABLECATEGORY> element; the value of the CONTENTCATEGORY attribute must match the name of the content category specified in the content category section of the file. The LABEL attribute defines the name you want displayed for the content category in the user interface.

Displaying custom properties in the browser search

The Enterprise Vault browser search application uses the custom filter and properties API to access custom properties defined in the `Custom Properties.xml` file.

This section shows how the example presentation section entries would be displayed in the US English version of this application.

[Figure 5-5](#) shows the Enterprise Vault browser search with the example custom properties and content categories displayed.

Figure 5-5 Example presentation properties displayed in the browser search page

Vault	<All Vaults> ▼	
Subject	contains any of ▼	<input type="text"/>
Author	contains any of ▼	user2 <input type="text"/>
Content	contains any of ▼	<input type="text"/>
Recipient	contains any of ▼	<input type="text"/>
Date	From: <input type="text"/>	To: <input type="text"/>
Expired Date	From: <input type="text"/>	To: <input type="text"/>
File Extension	<input type="text"/>	
Retention Category	<input type="text"/> ▼	
Folders	<input type="text"/>	<input type="button" value="Browse..."/>
Content Category	Litigation ▼	
Case Properties	Author:	<input type="text"/>
	Status:	<input type="text"/>
Client Properties	Client Name:	<input type="text"/>
	Message Topic:	<input type="text"/>
Results	Items: 10 ▼	Details: Full ▼

The **Content Category** dropdown box shows the content categories available to be used in searches. These were defined using the <AVAILABLECATEGORIES> element. You can change the content categories listed in the dropdown box, but you cannot change or hide the label, **Content Category**.

Selecting a content category in the box and clicking **Search** will return all items that were archived with the selected content category.

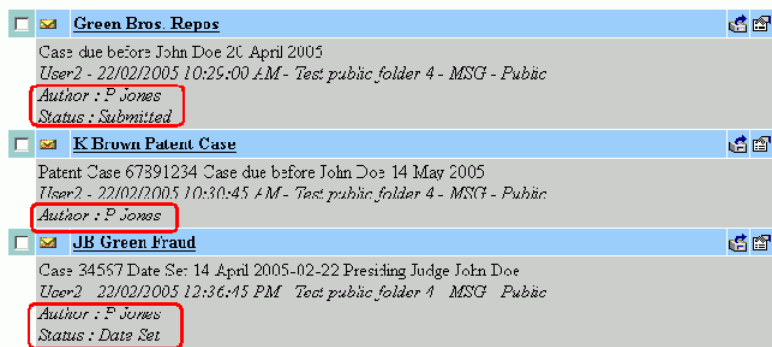
The **Case Properties** and **Client Properties** sections display each group of custom properties (FIELDGROUP) associated with the selected content category. Entering a value for a custom property and clicking **Search** will search the custom property index entry of archived items.

To see the additional property details in the search results, **Details** must be set to **Full**.

If the user selects a different content category, the custom properties available will change.

As RETRIEVE="Y" was set in the definition of the **Litigation** content category, and **Details** was set to **Full** on the Search page, custom properties in search result items will be displayed at the end of the list of normal message attributes.

Figure 5-6 Custom properties displayed in search results



Note the following on displaying custom properties in browser search:

- You must include the LOCALE attribute.
- If custom properties are to be used in the Enterprise Vault browser search, Internet Explorer security settings must allow cookies for the Enterprise Vault server site.
- When changes are made to the custom property configuration, you need to restart the Enterprise Vault Application Pool in IIS Manager.
- If the contents of the Custom Properties.xml file is changed, searches may return different results. For example, if an item is indexed using one content category and the properties included in the content category are changed, the custom properties returned by subsequent searches will be different. To ensure you can still search on the original properties, leave the original content category and create a new one.

Summary of custom property elements and attributes

Table 5-7 summarizes all elements and attributes in Custom Properties.xml.

The value in the **Mandatory** column assumes that the IGNORENODEFAULT registry setting is not used.

Table 5-7 XML elements and attributes in the Custom Properties.xml file

Element	Attribute	Mandatory	Description
CONTENTCATEGORIES		Yes	Defines the content category section of the file.

Table 5-7 XML elements and attributes in the Custom Properties.xml file
(continued)

Element	Attribute	Mandatory	Description
	DEFAULT=	No	Value is the name of the content category to be used as default. Required if custom properties in all items are to be indexed.
CONTENTCATEGORY		Yes	Defines a group of settings that are to be assigned to an archived item.
	NAME=	Yes	Value is a unique name to identify category to ruleset and presentation interface.
	RETENTIONCATEGORY=	No	Value is a retention category to be assigned to the archived item. retention category must exist in Enterprise Vault.
	ARCHIVEID=	No	Value is the ID of the archive to store the item in. Value can be found in the properties of the archive in the Enterprise Vault Administration Console.
INDEXEDPROPERTIES		Yes	Defines a set of additional properties in the content category.
	RETRIEVE=	No	Value is "Y" or "N". Indicates whether or not properties in this set should appear in the search results. Default is "N".
PROPERTY		Yes	Defines an additional property to index for items that are assigned this content category.
	TAG=	Yes	Value is the Enterprise Vault TAG of the property.
CUSTOMPROPERTIES		Yes	Defines the custom property section of the file.
NAMESPACE		Yes	Defines a NAMESPACE that contains a group of custom properties.

Table 5-7 XML elements and attributes in the Custom Properties.xml file
(continued)

Element	Attribute	Mandatory	Description
PROPERTY	TYPE=	Yes	Value is the type of property: "LOTUS".
		Yes	Defines a custom property.
	NAME=	Yes	Value is the identity of the property as displayed in message properties in the Lotus Notes client. Value must be unique in NAMESPACE.
	LOTUSTYPE=	Yes	Value is the Domino property data type: "TEXT", "NUMBER" or "TIME".
PRESENTATION	TAG=	Yes	TAG identifies the property within Enterprise Vault. It can contain only alphanumeric characters (A-Z a-z 0-9); spaces and underscore characters are not permitted. The value must be unique within the XML file. TAG value is the property name that will be stored in the index.
		Yes	Defines the presentation property section of the file.
APPLICATION		Yes	Defines a group of fields for use by a named application.
	NAME=	Yes	Value is the name of the application that will use the fields in this definition.
	LOCALE=	Yes	The value depends on what the calling application requires to define the language. The Enterprise Vault browser search uses standard Microsoft Locale ID number that the application will run under. (Currently only "1033", US English, is supported for displaying custom properties in the browser search.)

Table 5-7 XML elements and attributes in the Custom Properties.xml file
(continued)

Element	Attribute	Mandatory	Description
FIELDGROUPS		Yes	Define the field groups available to the application.
FIELDGROUP		Yes	A logical grouping of fields for the presentation interface.
	LABEL=	No	Value will be presented to the application for this field group. The label must be unique within the application.
FIELD		Yes	Defines a field that will reference a custom property.
	LABEL=	Yes	Value will be displayed on the application user interface to represent this custom property.
	CATEGORY=	Yes	Value is the name of a content category listed in AVAILABLECATEGORIES for the application.
	TAG=	Yes	Value is the TAG of a custom property. The tag must be unique in the FIELDGROUP.
AVAILABLECATEGORIES		Yes	Define which content categories are available to the application.
AVAILABLECATEGORY		Yes	Defines a content category.
	LABEL=	Yes	Value defines how the content category is to appear in the user interface.
	CONTENTCATEGORY=	Yes	Value is the NAME of the required content category as specified in the Content Category section of the file.

Index

A

- Advanced desktop policy settings
 - Domino archiving 35
- Advanced mailbox policy settings
 - Domino mailbox archiving 28

C

- Content categories
 - introduction 76
- Custom filtering
 - ALLOWOTHERS operator 94
 - assigning archive 90
 - assigning retention category 90
 - configuring 76
 - default rules 81
 - Domino registry settings 78
 - filtering messages 91
 - filtering on DLs 92–93
 - filtering on message direction 98
 - filtering on message subject 100
 - format of ruleset files 86
 - INCLUDES operator 94
 - introduction 75
 - named ruleset files 82
 - rule actions 89
 - ruleset file example 101
 - ruleset file schema 81
 - ruleset file security 81
 - ruleset files 80
- Custom properties
 - introduction 76, 105
 - supported properties 105
- Custom properties.xml
 - schema 81
- Customized filters 106

D

- Desktop policies
 - Domino mailbox archiving 32

- Domino archives
 - restricting access 58
- Domino Gateway
 - permissions for Vault Cache 63
- Domino Journaling 67
 - adding a domain 68
 - adding a server 68
 - adding permissions to the journal archive 70
 - assigning a vault store 68
 - configuring clients 72
 - creating a task 71
 - creating a vault store 69
 - creating an archive 69
 - Lotus Notes client 73
 - preparation for archiving 67
 - set up policy 70
- Domino Journaling Archiving 67
- Domino journaling location 78
 - ruleset file name 82
- Domino mailbox archiving
 - adding a domain 22
 - adding a Domino mail server 22
 - Advanced tab desktop policy settings 35
 - Advanced tab mailbox policy settings 28
 - Archiving Actions tab mailbox policy settings 25
 - Archiving Rules tab mailbox policy settings 24
 - archiving user account 45
 - configuring 21
 - customized shortcuts 29
 - desktop policies 32
 - disabling Vault Cache 63
 - domino forms 21
 - Domino Gateway server account 45
 - Domino Mailbox task 36
 - Domino Provisioning task 36
 - enabling mailbox manually 60
 - enabling mailboxes for archiving 57
 - enabling Vault Cache 62
 - EVInstall.nsf 42, 44–45, 48
 - EVInstall.nsf changes on a Domino 7.0.x
 - Enterprise Vault Domino Gateway 52

Domino mailbox archiving (*continued*)

- EVInstall.nsf changes on a Domino 7.0.x mail server 53
 - EVInstall.nsf changes on a Domino 8 Enterprise Vault Domino Gateway 50
 - EVInstall.nsf changes on a Domino 8 mail server 51
 - EVInstall.nsf changes on a Domino 8.5 Enterprise Vault Domino Gateway 48
 - EVInstall.nsf changes on a Domino 8.5 mail server 50
 - Execution Control List permissions 44
 - force Domino Provisioning task to process mailboxes 59
 - Forms tab mailbox policy settings 27
 - General tab desktop policy settings 33
 - General tab mailbox policy settings 24
 - installing client templates 40
 - installing Lotus Notes and DWA extensions 46
 - Lotus Notes and DWA 40
 - LotusShortcutText.txt 30
 - mailbox policies 24
 - Options tab desktop policy settings 33
 - ordering provisioning group 40
 - preparation 18
 - search features for Lotus Notes and DWA extensions 55
 - server configuration 18
 - setting up 15
 - Shortcut Content tab mailbox policy settings 26
 - Shortcut Deletion tab mailbox policy settings 27
 - Site settings 37
 - start Task Controller and Domino Provisioning task 59
 - Targets tab desktop policy settings 35
 - Targets tab mailbox policy settings 29
 - troubleshooting Vault Cache 64
 - updating mail files for Lotus Notes and DWA extensions 54
 - Vault Cache 45
 - Vault Cache tab desktop policy settings 34
 - vault store group, vault store, and partition 20
 - web connections 19
 - welcome message 57
- Domino retention folders 31
 - Domino retention plan 31
 - XML file 31
 - Domino users
 - Vault Cache 61

DominoHubServers 23

E

- Enabling Domino mailbox
 - manually 60
- Enabling mailbox
 - wizard 59
- EVDominoRetentionPlans.exe 31
- EVMessages.nsf 57

F

- Filtering
 - Custom filtering 75

I

- Internal addresses
 - Defining 100
- InternalSMTPDomains 100

M

- Mailbox
 - enabling manually 60
- Mailbox policies
 - Domino mailbox archiving 24
- Message classes 27

N

- Notes mail recipients
 - identifying internal 56, 72
- NotesDomains registry key
 - to identify internal mail recipients 56, 72

R

- Retention folders, Domino 31
- Retention plan, Domino 31
- Ruleset file schema 88

S

- Site Settings
 - reviewing 37

V

- Vault Cache
 - disabling with Domino Desktop policy 63
 - Domino users 61
 - enabling with Domino Desktop policy 62

- Vault Cache *(continued)*
 - troubleshooting for Domino 64
- Vault Store
 - name
 - valid characters 69

W

- Welcome message
 - editing 57
 - location of 57
- Wizards
 - Enable Domino mailboxes for archiving 60

X

- XML file
 - for Domino retention plan 31