Symantec Enterprise Vault™

Setting up Exchange Server Archiving

10.0

Symantec

Symantec Enterprise Vault: Setting up Exchange Server Archiving

Last updated: 2013-06-14.

Legal Notice

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 website at the following URL:

http://support.symantec.com

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:

http://support.symantec.com

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:

http://support.symantec.com

Customer service

Customer service information is available at the following URL:

http://support.symantec.com

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

Chapter 1

About this guide

This chapter includes the following topics:

Introducing this guide

This guide describes how to set up Enterprise Vault so that you can archive items from mailboxes and public folders on Microsoft Exchange Servers.

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

- Windows Server
- Exchange Server
- SQL Server
- Message Queue Server
- 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 Documentation Library	Includes all the following documents in Windows Help (`.chm`) format so that you can search across them all. It also includes links to the guides in Acrobat (`.pdf`) format. You can access the library in several ways, including the following: ■ On the Windows **Start** menu, click **Start** > **Programs** > **Enterprise Vault** > **Documentation**. ■ In Windows Explorer, browse to the `Documentation\`*`language`* subfolder of the Enterprise Vault installation folder, and then open the `EV_Help.chm` file. ■ On the **Help** menu in the Administration Console, click **Help on Enterprise Vault**.
Introduction and Planning	Provides an overview of Enterprise Vault functionality.
Deployment Scanner	Describes how to check the prerequisite software and settings before you install Enterprise Vault.
Installing and Configuring	Provides detailed information on setting up Enterprise Vault.
Upgrade Instructions	Describes how to upgrade an existing Enterprise Vault installation to the latest version.
Setting up Exchange Server Archiving	Describes how to archive items from Microsoft Exchange user mailboxes, journal mailboxes, and public folders.
Setting up Domino Server Archiving	Describes how to archive items from Domino mail files and journal databases.
Setting up File System Archiving	Describes how to archive the files that are held on network file servers.
Setting up SharePoint Server Archiving	Describes how to archive content from Microsoft SharePoint servers.
Setting up SMTP Archiving	Describes how to archive SMTP messages from other messaging servers.
Administrator's Guide	Describes how to perform day-to-day administration, backup, and recovery procedures.

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

Document	Comments
Reporting	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.
Utilities	Describes the Enterprise Vault tools and utilities.
Registry Values	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.

Enterprise Vault training modules

The Enterprise Vault Tech Center (http://go.symantec.com/education_evtc) provides free, publicly available training modules for Enterprise Vault. Modules are added regularly and currently include the following:

- Installation
- Configuration
- Getting Started Wizard
- Preparing for Exchange 2010 Archiving
- Assigning Exchange 2007 and Exchange 2010 Permissions for Enterprise Vault
- Enterprise Vault File System Archiving

More advanced instructor-led training, virtual training, and on-demand classes are also available. For information about them, see http://go.symantec.com/education_enterprisevault.

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.

Chapter 2

Distributing Exchange Server Forms

This chapter includes the following topics:

About distributing the Microsoft Exchange forms when setting up Exchange Server archiving

If you are implementing Exchange Server archiving, Microsoft Exchange forms need to be distributed around your Microsoft Exchange Server organization. Different language versions of the forms are provided in the Enterprise Vault server kit and in the Outlook Add-In installer kit.

The forms can be distributed in the following ways:

- Allow the Outlook Add-in to store forms in each user's Personal Forms Library. This is the default method.
  See " Use of Personal Forms Libraries when setting up Exchange Server archiving" on page 22.
- Install the forms in folders in the Organizational Forms Library on the Exchange Server.
  See "About using the Organizational Forms Library when setting up Exchange Server archiving" on page 22.

Note: The Exchange forms do not affect Enterprise Vault Client for Mac OS X users.

Use of Personal Forms Libraries when setting up Exchange Server archiving

By default, the Enterprise Vault Outlook Add-In automatically deploys forms to the user's Personal Forms Library. This has the advantage of requiring no configuration by the administrator.

About using the Organizational Forms Library when setting up Exchange Server archiving

If you wish, you can install the forms in the Organizational Forms Library, rather than deploying forms to users' Personal Forms Libraries. However, this requires a certain amount of configuration effort, especially on Exchange Server 2007, which does not provide an Organizational Forms Library by default.

This section describes how to create Organizational Forms folders and install the forms. You create one folder in the Organizational Forms Library for each language version of the forms that you want to install. This section also explains that to change the deployment method you need to change a policy setting in your desktop policies.

See "Creating Organizational Forms folders when setting up Exchange Server archiving" on page 22.

See "Installing the Microsoft Exchange forms when setting up Exchange Server archiving" on page 25.

See "Updating desktop policies to change the deployment method when setting up Exchange Server archiving" on page 26.

Creating Organizational Forms folders when setting up Exchange Server archiving

On Exchange 2000 and Exchange Server 2003, you use Exchange System Manager to create folders in the Organizational Forms Library.

On Exchange Server 2007, the method used to create the Organizational Forms Library and folders has changed; you cannot use the administrative tools. The method described in this section uses the Microsoft Exchange Server MAPI editor, `MfcMapi.exe`, which you can obtain from the following page on the Microsoft website:

http://go.microsoft.com/?linkid=5684182

To create Organizational Forms folders on Exchange Server 2003 and Exchange 2000

1. Click **Start**, **Programs**, **Microsoft Exchange System Manager**.
2. Expand the **Organization (Exchange)** object.
3. Expand your **Administrative Group**.

   If this is not available, right-click your **Organization** and then select **Properties**. Then check **Display Administrative Groups** and click **OK**.
4. Expand **Folders**.
5. Right-click **Public folders** and then, on the shortcut menu, click **View System folders**. The right-hand pane displays the system folders.
6. In the left-hand pane, right-click **EFORMS REGISTRY** and then, on the shortcut menu, click **New** > **Organizational Form**. A Properties window appears.
7. Fill in the details on the Properties window.
8. Under **E-forms language**, select the language that is appropriate to the forms you are going to install and then click **OK** to return to the Exchange System Manager screen.
9. In the left-hand pane, double-click the **EFORMS REGISTRY** folder.
10. Right-click the folder you just created and then, on the shortcut menu, and click **Properties**.
11. On the properties screen, click the **Permissions** tab.
12. Click **Client Permissions**.
13. Click **Add**.
14. Click a mail-enabled, user name for the account that will be the owner of the forms. This will usually be the Enterprise Vault Service account.
15. Click the **Roles** down arrow and, in the list, click **Owner**.
16. Click **OK** to return to the Properties screen.
17. Click **OK** to close the Properties screen.
18. Close **Exchange System Manager**.

To create Organizational Forms folders on Exchange Server 2010 and Exchange Server 2007

1. Create a new Organizational forms folder, as follows:

- Open the Exchange Management Shell.
- Run the following command at the Exchange Management Shell prompt:

  ```
  New-PublicFolder -Path "\NON_IPM_SUBTREE\EFORMS REGISTRY" -Name
  "Enterprise Vault Forms (English)"
  ```

  The name given here is just an example. Repeat this command to create a folder for each language that you want to publish.

2. Check that public folders are displayed in Outlook:
   - Use an account that belongs to the Exchange Administrators Group to log on to an Enterprise Vault server that has Outlook 2003 installed.
   - Configure a new mail profile and start Outlook.
   - If the public folder store does not appear within a few seconds, you may need to wait for Exchange Server to update. Alternatively, restart the Exchange Server information store to force an update.
3. Add the PR_EFORMS_LOCALE_ID property to set language of the forms folder, as follows:
   - Start the Microsoft Exchange Server MAPI Editor (`MfcMapi.exe`).
   - On the **Session** menu, click **Logon and Display Store Table**. Log on using the Outlook profile for an account that belongs to the Exchange Administrators Group.
   - On the **MDB** menu, click **Open Public Folder Store**, and then click **OK**.
   - Expand **Public Root**, expand **NON_IPM_SUBTREE**, and then expand **EFORMS REGISTRY**.
   - Click the public folder that you created in step 1. For example, click "Enterprise Vault Forms (English)".
   - On the **Property pane** menu, click **Modify Extra Properties**.
   - Click **Add**, and then click **Select Property Tag**.
   - Click **PR_EFORMS_LOCALE_ID** in the list, and then click **OK**.
   - Click **OK** twice. A red mark is displayed next to the new **PR_EFORMS_LOCALE_ID** property.
   - Double-click **PR_EFORMS_LOCALE_ID**.
   - In the **Unsigned Decimal** box, type the locale ID you require, and then click **OK**.

     For example, type 1033 for English, or 1040 for Italian.

     To determine the locale ID for other locales, visit the following Microsoft website:

http://msdn2.microsoft.com/en-us/library/aa579489.aspx

- Select **PR_PUBLISH_IN_ADDRESS_BOOK**, right click and select **Edit Property**, clear **Boolean** and then click **OK**.
- Exit MAPI Editor.

Installing the Microsoft Exchange forms when setting up Exchange Server archiving

You can install the forms from Microsoft Outlook using a mailbox that has Owner permissions for the folder in the Organization Forms Library. Do this on the computer where you have installed the Microsoft Exchange forms from the Enterprise Vault kit, typically the Enterprise Vault server.

Note: When upgrading or reinstalling the Enterprise Vault forms, always uninstall the existing copies first, rather than installing the new forms on top of the existing copies.

Users can access the new forms when they have installed the Enterprise Vault Outlook Add-In.

To install the forms

1. On the Outlook **Tools** menu, click **Options**.
2. On the **Other** tab, click **Advanced Options**, click **Custom Forms**, and then click **Manage Forms**.
3. On the right-hand side of the dialog box, click **Set**.
4. Click **Forms Library** and select the name of your forms library. Click **OK**.
5. Click **Install**.
6. Select the **Languages\Forms** subfolder in the Enterprise Vault Program folder.
7. Select the language folder that is appropriate to the language of the forms you want to install.
8. Change the file type filter to **Form Message (*.fdm)**.
9. Double-click **EVPendingArchive.fdm** and review the displayed properties to check that this form is the Enterprise Vault Archive Pending Item form.
10. Click **OK**.
11. Repeat steps 5, 8, 9, and 10 for the following:
    - **EVPendingArchiveHTTP.fdm**: the Enterprise Vault Archive Pending Item HTTP form

- **EVPendingDelete.fdm**: the Enterprise Vault Delete Pending Item form
- **EVPendingRestore.fdm**: the Enterprise Vault Restore Pending Item form
- **EVShortcut.fdm**: the Enterprise Vault Archived Item form

12 Close the **Forms Manager** dialog box and the other open dialog boxes.

Updating desktop policies to change the deployment method when setting up Exchange Server archiving

If you are using the Organizational Forms Library to distribute the forms then when you come to set up Exchange desktop policies in the Enterprise Vault Administration Console you need to change the value of the Outlook advanced policy setting **Deploy Forms Locally** from its default value of Always.

See "Changing the default method for deploying Exchange forms in Advanced tab for desktop policy in Exchange Server archiving" on page 47.

What next?

You can now use the Enterprise Vault Administration Console to set up Exchange Server mailbox, journal or public folder archiving, as required.

Chapter 3

Setting up archiving from mailboxes

This chapter includes the following topics:

Points to note before you set up Enterprise Vault mailbox archiving

Before you enable mailboxes for Enterprise Vault archiving, take a few moments to review the requirements for the following:

- Vault store groups, vault stores, and partitions.
  See "Use of vault store groups, vault stores, and partitions with Exchange Server mailbox archiving" on page 28.
- Exchange Server database availability groups.
  See "Using Exchange Server database availability groups" on page 28.

Use of vault store groups, vault stores, and partitions with Exchange Server 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.

To control where Enterprise Vault creates new mailbox archives, you can set the default vault store at the following levels:

- Enterprise Vault server properties
- Exchange Server properties
- Provisioning Group properties

When you create a Provisioning Group, the default vault store is inherited from the Exchange Server properties. If an override vault store is not specified in the Exchange Server properties, then the vault store that is specified in the Enterprise Vault server properties is used.

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

Using Exchange Server database availability groups

Recent Exchange Server versions use database availability groups (DAGs) to provide automatic database level recovery from failures of mailbox servers or individual mailbox databases. When one database in a DAG fails, Exchange makes active another passive copy of the database on a different mailbox server.

To ensure that the mailboxes you enable for archiving are always available to Enterprise Vault, you must set up archiving for all the DAG member servers. You must also target all the DAG member servers within one Enterprise Vault site.

It is possible to add an Exchange mailbox archiving task for a server, only when it hosts an active Exchange database. Your environment might contain Exchange servers that act only as disaster recovery (DR) servers, and do not normally host active DAG member databases. These servers must be set up for Exchange server archiving because active DAG member databases can fail over to them. However, while these servers are not hosting active databases, you cannot set them up for Exchange mailbox archiving.

To set up Exchange mailbox archiving for a DR-only server

1. Fail over an active database to the DR-only server. This must be a database that contains an Enterprise Vault system mailbox.
2. Add the DR-only server as an Exchange mailbox archiving target.
3. Add an Exchange mailbox archiving task for the DR-only server.
4. Fail back the database to the original host server.

When all DAG member servers are set up for archiving, database and server failovers do not interrupt mailbox archiving.

Exchange mailbox archiving and database failovers with Exchange Server mailbox archiving

During Exchange mailbox archiving, a mailbox archiving task is associated with each mailbox server. The mailbox archiving task processes only the active copies of the mailbox databases that reside on the mailbox server. Enterprise Vault does not archive from passive database copies.

When one database in a DAG fails, Exchange makes another passive copy of the database active. The mailbox archiving task that processed the failed copy continues to process the new active copy of the database until the Enterprise Vault's provisioning task runs. When the provisioning task has run, the new active copy of the database is processed by the mailbox archiving task that is associated with the new host Exchange server.

In practice, the failed database might be restored to its initial Exchange host before the provisioning task runs and updates the list of databases that are processed by each mailbox archiving task.

You can determine which databases a mailbox archiving task is currently processing in the Administration Console, using the **Exchange Mailbox Archiving Task Properties: Targets** tab.

Defining Exchange Server mailbox archiving policies

Exchange mailbox policies define how Enterprise Vault archives target Exchange Server mailboxes. You can create different policies for different groups of mailboxes. If you wish, you can create a custom mailbox policy for each provisioning group.

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

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

1. In the Administration Console, expand your Enterprise Vault site.
2. Click **Policies** > **Exchange** > **Mailbox**.
3. Right-click **Default Exchange 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 Exchange mailbox policy

1. In the Administration Console, expand your Enterprise Vault site.
2. Click **Policies** > **Exchange** > **Mailbox**.
3. Right-click the **Mailbox** container and select **New**, **Policy** to launch the new policy wizard.

   The new policy is displayed in the right pane.
4. To adjust the policy properties, right-click the policy and select **Properties**.

To set a different policy as the default Exchange mailbox policy

1. In the Administration Console, expand your Enterprise Vault site.
2. Click **Policies** > **Exchange** > **Mailbox**.
3. In the right pane right-click the policy that you want to set as the default policy, and select **Set as Default**.

Mailbox policy settings when setting up Exchange Server archiving

This section gives an overview of the various settings available in the Exchange mailbox policy. For more information on each setting, see the online help on the mailbox policy property pages.

General tab (Exchange Server archiving mailbox policy setting)

Table 3-1 lists the settings on the General tab. These settings provide a name and description for the policy.

Table 3-1 Exchange 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 (Exchange Server archiving mailbox policy setting)

Table 3-2 lists the settings on the Archiving Rules tab. These settings control the use of age-based and mailbox storage quota-based archiving, and other archiving options.

Table 3-2 Exchange mailbox policy Archiving Rules tab settings

Setting	Description	Default value
Archiving strategy	You can choose to base archiving on one of the following: ■ Age: the age of an item ■ Quota: the percentage of the mailbox storage limit that is released ■ Age and quota: a combination of the Age and Quota options For information on configuration of archiving based on quota or age and quota, see the *Administrator's Guide*.	Archiving is based on the period of time since an item was modified. The time period is six months. Setting is locked.
Age based	The period of time to use for Age based archiving and Age and quota based archiving.	Six months.
Quota based	The percentage to use for Quota based archiving and Age and quota based archiving.	10%
Never archive items younger than	An absolute limit on the age of items that are archived.	Two weeks.

Table 3-2 Exchange mailbox policy Archiving Rules tab settings *(continued)*

Setting	Description	Default value
Start with items larger than	The size above which the Exchange Mailbox Tasks give priority to items. Items larger than this size are archived first.	Not set.
Archive only messages with attachments	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. See the *Administrator's Guide* for more details.	Not set.

Archiving Actions tab (Exchange Server archiving mailbox policy setting)

Table 3-3 describes the settings on the Archiving Actions tab. These settings control how Enterprise Vault behaves when it archives an item.

Table 3-3 Exchange mailbox policy Archiving Actions tab settings

Setting	Default value
Delete original item after archiving	Original item is deleted from mailbox after archiving. Setting is locked. This option is only available for selection if **Based on age** is selected as the archiving strategy on the **Archiving Rules** tab.
Create shortcut to archived item after archiving	After it has been archived, the item in the mailbox is replaced with a shortcut. Setting is locked.
Archive unread items	Unread items in the mailbox are not archived. Setting is locked.
Overall lock	Force users to use the policy settings for mailbox archiving. This locks the settings in the Archiving Actions section and the Archiving Strategy setting on the Archiving Rules tab.

Shortcut Content tab (Exchange Server archiving mailbox policy setting)

Table 3-4 describes the settings on the Shortcut Content tab. These settings control the size and behavior of Enterprise Vault shortcuts.

Table 3-4 Exchange 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.
Shortcut body	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. ■ 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 with Exchange Server archiving" on page 55.	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, `ShortcutText.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 with Exchange Server archiving" on page 55.

Message Classes tab (Exchange Server archiving mailbox policy setting)

The list on the Message Classes tab shows the classes of items that will be archived when the policy is applied.

Select or clear message class check boxes, as required.

If you need to edit the list of available message classes, go to the Message Classes tab of the Directory properties.

Shortcut Deletion tab (Exchange Server archiving mailbox policy setting)

Shortcut deletion does the following:

- Deletes shortcuts that are older than the age you specify on this tab.
- Deletes orphaned shortcuts. These are shortcuts to items that have been deleted, typically by a user, from an archive.

Shortcut deletion is performed by the Exchange Mailbox Archiving task. When you run the task using Run Now, you can choose a Run mode that includes shortcut processing.

Table 3-5 describes the available settings.

Table 3-5 Exchange mailbox policy Shortcut Deletion tab settings

Setting	Description	Default value
Delete shortcuts in folders	Setting this makes Enterprise Vault delete shortcuts that are older than the age you specify. This does not affect the corresponding archived items. Users can still search for the archived items. For example, you could choose to delete all shortcuts older than 12 months, but retain archived items for several years.	Not selected

Table 3-5 Exchange mailbox policy Shortcut Deletion tab settings *(continued)*

Setting	Description	Default value
Delete orphaned shortcuts	This setting makes Enterprise Vault delete shortcuts in mailboxes if the corresponding archived item has been deleted. If you use shortcuts that 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 will regain space in the Exchange Server store.	Not selected

When certain items such as calendar, task, and meeting items are archived, the original item is not replaced with a shortcut. By default, the archiving task does not delete the original items when it performs shortcut deletion. To include such items in shortcut deletion, configure the registry setting, `DeleteNonShortcutItems`. The setting is described in the *Registry Values* manual.

Moved Items tab (Exchange Server archiving mailbox policy setting)

Enterprise Vault can update the location and the retention category of archived items whose shortcuts have been moved or copied to a different folder.

The following permissions are required:

- The owner of the mailbox where the copy is made must have read permission on the archive folder where the item originated.
- If the item originated in a shared archive, the owner of the mailbox where the copy is made must have read permission on the shared archive.

If the new location is configured to use a shared archive, Enterprise Vault creates a copy of the item in that archive. It leaves a copy in the original archive even if the item's shortcut was moved, rather than copied.

The Moved Items settings control whether these updates are made.

You can choose to update the location only, or both the location and the retention category. Enterprise Vault only updates the retention category if the location is also updated.

Table 3-6 describes the available settings.

Table 3-6 Exchange mailbox policy Moved Items tab settings

Setting	Description	Default value
Update archive location for items moved in the mailbox	If you select this option, the location of items whose shortcuts have been moved or copied to a different folder is updated.	Selected
Update the Retention Category for the following items	You can select one of the following: ■ None. Do not update the retention category of moved and copied items. ■ All. Update the retention category of moved and copied items.	All
Include items with Retention Category selected by the user, set by a custom filter, or set by PST migration	If you select this option, the retention category of moved and copied items is updated regardless of how the items were archived. This option includes any item whose retention category was changed when it was archived manually, or by a custom filter, or using PST migration. If this option is not selected, the retention category is not updated on any items that were archived manually, by a custom filter, or using PST migration.	Not selected

Indexing tab (Exchange Server archiving mailbox policy setting)

Table 3-7 lists the settings on the Indexing tab. These settings control the amount of index detail that is available to users. The settings apply to the group of mailboxes to which the policy is assigned.

Table 3-7 Exchange mailbox policy Indexing tab settings

Setting	Description	Default value
Indexing Level	The required indexing level for the group of mailboxes to which the policy is assigned. The indexing level defines what users can filter on when searching for archived items. With brief indexing, only information about the item, such as the subject and author, can be searched. With full indexing you can also search on the content of each item. Brief indexes occupy approximately 4% of the space of the original data. Full indexes with a 128 character preview length occupy approximately 12% of the space of the original data. You can set a default indexing level for the entire site in site properties. You can override the site setting for particular groups of mailboxes in the mailbox policies, or for particular users in the archive properties.	Full
Preview length	This setting enables you to control the amount of text that Enterprise Vault shows in a search results list. The size of an index increases when you increase the preview length.	128 characters
Create previews of attachments	This setting makes Enterprise Vault create previews of attachment content. These previews cannot be viewed in Enterprise Vault 10.0. The size of an index increases when you enable this option.	Do not create previews

Advanced tab (Exchange Server archiving mailbox policy setting)

The Advanced tab contains various settings controlling advanced archiving behavior. As with the settings on the other tabs, you can create another policy if you require more than one version of these settings.

Table 3-8 briefly describes the available settings. Information about each advanced setting is given in the *Administrator's Guide*.

Table 3-8 Exchange mailbox policy Advanced tab settings

Setting	Description
List settings from	Controls the category of settings that are shown in the list. There is only one category: ■ Archiving General. Settings that control archiving behavior. Information about each advanced setting is given in the *Administrator's Guide*.
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 (Exchange Server archiving mailbox policy setting)

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

Defining desktop policies in Exchange Server archiving

An Exchange desktop policy defines the end user's experience when using the Enterprise Vault Outlook Add-In, OWA clients, Office Mail App, and Client for Mac OS X. It contains the settings that control the Enterprise Vault features and functionality available on the users' desktop computers. 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.

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

If you modify a desktop policy after setting up Exchange mailbox archiving, then when you have finished, synchronize the mailboxes using the button on the **Synchronization** tab in the Exchange Mailbox Archiving Task properties.

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

1. In the Administration Console, expand your Enterprise Vault site.
2. Click **Policies** > **Exchange** > **Desktop**.
3. Right-click **Default Exchange 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 Exchange desktop policy

1. In the Administration Console, expand your Enterprise Vault site.
2. Click **Policies** > **Exchange** > **Desktop**.
3. Right-click the **Desktop** container and select **New**, **Policy** to launch the new policy wizard.

   The new policy is displayed in the right pane.
4. To adjust the policy properties, right-click the policy and select **Properties**.

To set a different policy as default Exchange desktop policy

1. In the Administration Console, expand your Enterprise Vault site.
2. Click **Policies** > **Exchange** > **Desktop**.
3. In the right pane right-click the policy that you want to set as the default policy, and select **Set as Default**.

Desktop policy settings in Exchange Server archiving

This section gives an overview of the various settings available in an Exchange desktop policy. For more information on each setting, see the online help on the desktop policy property pages.

General tab (Exchange Server archiving desktop policy setting)

Table 3-9 lists the settings on the General tab. These settings provide a name and description for the policy.

Table 3-9 Exchange desktop policy General tab settings

Setting	Description	Default value
Name	A name for the policy.	None.

Table 3-9 Exchange desktop policy General tab settings *(continued)*

Setting	Description	Default value
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 (Exchange Server archiving desktop policy setting)

These options enable you to control the visibility of Enterprise Vault options and toolbar buttons in the following:

- The Enterprise Vault Outlook Add-In
- Enterprise Vault integrations with OWA clients (OWA 2010 and earlier)
- The Enterprise Vault Office Mail App
- The Enterprise Vault Client for Mac OS X

You can also control whether the Outlook and OWA Delete options delete shortcuts only or shortcuts and archived items, or whether the user decides.

Note: The Options tab refers to settings by their Outlook client names. However, each setting applies to all Enterprise Vault clients for Exchange archiving, except where noted.

Feature settings in Options tab for desktop policy in Exchange Server archiving

These settings control which options and toolbar buttons are available in the Enterprise Vault clients for Exchange archiving.

The **Enabled** check box controls whether a feature is displayed as an option, or in some cases a button.

The **On Toolbar** check box becomes available if you select the **Enabled** check box.

Note the following:

- In the Outlook 2003/2007 client, the menu options are provided on the **Tools > Enterprise Vault** menu. You can choose to make both the menu options and the toolbar buttons available.
- In the Outlook 2010/2013 client, if you check only the **Enabled** check box, the menu option appears on the **More Actions** menu on the **Enterprise Vault** tab.

If you check both the **Enabled** check box and the **On Toolbar** check box, the menu option does not appear on the **More Actions** menu. Instead, a button appears directly on the Enterprise Vault tab or, in the case of **Expiry Report**, in the Enterprise Vault Backstage view.

- In Mac OS X, the menu options are provided on the **Symantec Enterprise Vault client** menu on the menu bar.
- In OWA 2003/2007/2010 clients, the menu options are provided on the shortcut menu that appears when you right-click an item in the OWA Premium client. Buttons in the Navigation Pane provide access to Search Vaults and Archive Explorer.
- In OWA 2013, the Office Mail App provides Enterprise Vault features. For information about the Office Mail App, see *Setting up Exchange Server Archiving*.

Table 3-10 lists the Feature settings. The effect of each setting depends on which Enterprise Vault client is in use. For a more detailed description of these settings, see the Administration Console Help for the Exchange Desktop Policy: Options tab.

Table 3-10 Exchange desktop policy Options tab Feature settings

Setting	Controls users' ability to
Store in Vault	Perform manual archiving.
Restore from Vault	Use shortcuts to restore items from vaults.
Search Vault	Search archives.
Archive Explorer	Access Archive Explorer.
Delete from Vault	Delete archived items and their corresponding shortcuts.
Cancel Operation	Cancel a pending archive, pending restore, or pending delete operation.
Expiry Report (Outlook only)	Run an expiry report from Outlook.
Help	Access Enterprise Vault Help.

For the two settings **Search Vault** and **Archive Explorer** you can configure the OWA 2003/2007/2010 clients to use different values than the Outlook client, if required. To set different values for OWA 2003/2007/2010, go to the **Advanced** tab, then select the **OWA versions before 2013** category and change the values of the **Search Vaults** and **Archive Explorer** settings to the required values. If you

subsequently change the **Search Vault** or **Archive Explorer** settings on the **Options** tab, you are asked if you want to apply these revised settings to the OWA clients as well as to Outlook. If you click **No**, Enterprise Vault retains the values for the OWA clients on the **Advanced** tab.

The Cancel Operation setting is not currently supported for archive actions in the Enterprise Vault Client for Mac OS X.

Outlook Behavior settings in Options tab for desktop policy in Exchange Server archiving

The Outlook Behavior settings on the Options tab control the effect on shortcuts and archived items of the normal Delete options in the following:

- Outlook (all versions) with the Enterprise Vault Outlook Add-In installed
- OWA 2003/2007/2010

(The settings have no effect in the Enterprise Vault Client for Mac OS X, or in OWA 2013 with the Office Mail App enabled.)

Table 3-11 describes the Outlook Behavior settings.

Table 3-11 Exchange desktop policy Options tab Outlook Behavior settings

Setting	Description	Default value
Shortcut deletion	Controls what happens when the user deletes a shortcut using one of the normal Outlook or OWA Delete options; for example, by selecting a shortcut and pressing the Delete key. This setting is ignored, and only the shortcut is deleted, unless the site setting **Users can delete items from their archives** is selected. ■ Shortcut only. The shortcut is deleted. If users hold down the Shift key while they perform the deletion, the shortcut is deleted without being placed in Deleted Items. ■ Both deleted. Enterprise Vault tells the user that both the shortcut and the archived item will be deleted. If the user chooses to continue, both the shortcut and the corresponding archived item are deleted. ■ Ask user. Enterprise Vault asks the user whether to delete the shortcut and the original item, or the shortcut only.	Shortcut only

Web Applications tab (Exchange Server archiving desktop policy setting)

Table 3-12 describes the settings on the Web Applications tab. These settings control aspects of end-user web-based searching.

Table 3-12 Exchange desktop policy Web Applications tab settings

Setting	Description	Default value
Add all Enterprise Vault servers to intranet zone	Select this setting to add all Enterprise Vault servers to the user's Internet Explorer local intranet zone. The effect of this setting is that users are not prompted for their logon details when they search their archives or view or restore archived items. When you clear this setting, any existing Enterprise Vault servers remain in the user's Internet Explorer local intranet zone. No new servers are added after you clear this setting. To override this setting, use the Outlook settings **Add server to intranet zone** and **Remove server from intranet zone** on the Advanced tab in the Exchange desktop policy. ■ **Bypass local proxy server**. Select this setting to bypass the user's local proxy server. The effects of this setting are as follows: ■ It selects **Bypass proxy server for local addresses** in the Local Area Network (LAN) Settings dialog box in Internet Explorer. ■ It adds Enterprise Vault servers to the Exceptions list in the Proxy Settings dialog box in Internet Explorer. When you clear this setting, **Bypass proxy server for local addresses** is cleared. Any existing Enterprise Vault servers remain in the Exceptions list.	Selected. (Not selected if upgrading from an earlier version of Enterprise Vault.)
Show 'Browser Search' link in Integrated Search	Select this setting to display the Browser Search link to the user in Outlook. If you uncheck this setting note that the Browser Search link remains visible if the user accesses integrated search using the integrated search URL from a standalone browser.	Selected.

You cannot use the setting **Add all Enterprise Vault servers to intranet zone** if you have applied Federal Desktop Core Configuration (FDCC) group policy objects (GPO) to Windows XP and Vista computers in your organization. For instructions on how you can configure Internet Explorer for these users, see the section "Publishing Enterprise Vault server details to FDCC compliant computers" in the *Installing and Configuring* manual.

Vault Cache tab (Exchange Server archiving desktop policy setting)

Table 3-13 describes the settings on the Vault Cache tab. These settings control the availability of Vault Cache, its maximum size, and the available features. The settings include an option to make Virtual Vault available to users.

Note: In this release, the Vault Cache feature is not available to Enterprise Vault Client for Mac OS X users.

Table 3-13 Exchange desktop policy Vault Cache tab settings

Setting	Description	Default value
Make Vault Cache available for users	Select this setting to make the Vault Cache feature available in this Enterprise Vault site. If this setting is cleared, no new Vault Caches are created. Users have access to existing Vault Caches, but no new items are added. If you make Vault Cache available, additional settings enable you to choose one of the following: ■ To set up the local Vault Cache automatically for users. ■ To allow users to decide when to set up the local Vault Cache, by providing the option **Enable Vault Cache** in Outlook.	Vault Cache is not available. No new Vault Caches are created. Users have access to existing Vault Caches, but no new items are added. If you make Vault Cache available, the default is to set up Vault Cache automatically on users' computers.

Table 3-13 Exchange desktop policy Vault Cache tab settings *(continued)*

Setting	Description	Default value
Limit size of Vault Cache	Use the settings to limit the size of the Vault Cache. **Maximum use of initial free space** specifies a percentage of unused disk space. The percentage is calculated at the time the Vault Cache is created. **Maximum size** specifies a size in gigabytes. If a Vault Cache reaches the specified size, the oldest items are automatically deleted to make room for new items. **Content strategy** specifies the strategy for storage of the content of archived items in Vault Cache. The options are as follows: ■ **Do not store any items in cache**. Item headers are synchronized to Vault Cache, but the content of archived items is not stored in Vault Cache. ■ **Store all items**. Item headers are synchronized to Vault Cache and the content of archived items is stored in Vault Cache. ■ **Store only items that user opens**. Item headers are synchronized to Vault Cache, but the content of archived items is not automatically stored in Vault Cache. With this option, the content of each item that a user opens in Virtual Vault is stored in Vault Cache.	The default size limit is 10% of the unused disk space when the Vault Cache is created. The default content strategy is **Store all items**.

Table 3-13 Exchange desktop policy Vault Cache tab settings *(continued)*

Setting	Description	Default value
Features	■ The **Synchronize Vault Cache** option controls whether users can update Vault Cache manually. For Outlook 2003/2007: ■ Select **Enabled** to show the **Synchronize Vault Cache** menu option. ■ Select **On Toolbar** to show the **Synchronize Vault Cache** toolbar button. For Outlook 2010: ■ Select **Enabled** to show the **Synchronize Vault Cache** option on the **More Actions** menu. ■ Select **On Toolbar** to show the **Synchronize** button in the Vault Cache group on the Enterprise Vault tab. If you select **On Toolbar**, the **Synchronize Vault Cache** option is not shown on the **More Actions** menu. ■ **Vault Cache properties** controls whether users can access the Vault Cache Properties dialog box in Outlook. ■ **Vault Cache options** enable the user to configure the size of the local Vault Cache and the grace period after Outlook starts before checking for the files that need to be synchronized to the Vault Cache. Select **Enabled** to display the **Options** tab in the Vault Cache Properties dialog box. ■ **Vault Cache details** enable the user to see detailed information about the Vault Cache. Select **Enabled** to display the **Details** tab in the Vault Cache Properties dialog box. ■ **Make Virtual Vault available to users**. Select **Enabled** to make Virtual Vault available to Outlook users.	If you make Vault Cache available, all these features are enabled.

See "Vault Cache advanced settings" on page 87.

See "Virtual Vault advanced settings" on page 94.

Advanced tab (Exchange Server archiving desktop policy setting)

The Advanced tab provides various advanced settings for the Enterprise Vault Office Mail App, Outlook, OWA, Vault Cache, and Virtual Vault.

Table 3-14 briefly describes the available settings. As with the other settings in the policy, you can create another policy if you require more than one version of these settings.

Table 3-14 Exchange desktop policy Advanced tab settings

Setting	Description
List settings from	Controls the type of settings that are displayed in the list. Select from the following categories: ■ Office Mail App ■ Outlook ■ OWA versions before 2013 ■ Vault Cache ■ Virtual Vault The *Administrator's Guide* gives information about each advanced setting.
Reset All	Returns all the settings in the list to their default values. A confirmation prompt asks if you are sure that 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	Provides a brief description of what each setting controls.

Changing the default method for deploying Exchange forms in Advanced tab for desktop policy in Exchange Server archiving

One of the advanced settings in the Outlook category is Deploy Forms Locally. The default value of this setting is Always, which causes the Enterprise Vault forms to be deployed automatically to the user's Personal Forms Library. If you do not intend to use this method, you must change the value of this setting.

The possible values for the Deploy Forms Locally setting are as follows:

- Never: Never deploy forms locally.
- When no Org Forms: Deploy forms only when there is no Organizational Forms Library available.
- Always: Always deploy forms locally. This is the default value.

- Delete: Always delete Enterprise Vault forms from the user's Personal Forms Library.

See "About distributing the Microsoft Exchange forms when setting up Exchange Server archiving" on page 21.

Targets tab (Exchange Server archiving desktop policy setting)

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

Adding Exchange Server archiving targets

In the Administration Console you need to add the domain (Exchange Organization) and Exchange Servers that you want to archive.

Note: If you use a database availability group (DAG) in your Exchange environment, you must set up archiving for all members of the DAG.

See "Using Exchange Server database availability groups" on page 28.

Adding an Exchange server domain for archiving

Before you can add the Exchange servers that you want to archive, you must add the domains in which the Exchange servers reside.

To add a domain

1. In the left pane of the Administration Console, expand the Enterprise Vault site hierarchy until **Targets** is visible.
2. Expand **Targets**
3. Right-click **Exchange** then click **New** > **Domain**.

   The New Domain wizard starts.
4. The New Domain wizard requests the information needed to create a new domain. You need to provide the following information:
   - The name of the domain that contains the Exchange servers you want to archive.
   - Enterprise Vault automatically detects the domain's global catalog server. However, you can provide a specific global catalog server if necessary.

- Enterprise Vault automatically detects connection points for Exchange 2013 servers. However, you can provide a specific proxy server and certificate principal if necessary.

Adding an Exchange Server for archiving

You can now add your target Exchange Servers to the appropriate domain.

To add an Exchange Server

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

   The **New Exchange Server** wizard starts.
4. Work through the wizard to add the Exchange Server.

   You need the following information:

   - The name of the Exchange Server.
   - Optionally, the wizard enables you to create Exchange Server archiving tasks for user mailboxes, journal mailboxes and public folders. If you create an Exchange Mailbox task, there must also be an Exchange Provisioning task for the domain. If one does not exist, an Exchange Provisioning task for the domain is created automatically when you select the Exchange Mailbox task check box.
   - The name of the Enterprise Vault server on which you want the tasks created, if not the local computer.
   - The name of the system mailbox to be used to connect to the Exchange Server.
   - Optionally, an override default vault store that Enterprise Vault is to use when creating the archives for mailboxes on this Exchange Server.
     If you do not explicitly set the vault store for the Exchange Server, the default vault store setting is inherited from the Enterprise Vault Server properties.

Adding a Provisioning Group for Exchange Server archiving

A provisioning group enables you to apply an Exchange mailbox policy, an Exchange desktop policy and a PST migration policy to individual users or to a group of Exchange Server users.

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

You can select the mailboxes to be associated with a provisioning group using any of the following:

- Windows group
- Windows user
- Distribution Group (the Active Directory Group type, Distribution)
- Organizational Unit
- LDAP query
- Whole Exchange Server organization

Note: A mailbox must be part of a provisioning group before you can enable that mailbox for archiving.

Provisioning groups are processed, and mailboxes enabled by the Exchange Provisioning Task.

To add a Provisioning Group

1. In the left pane of the Administration Console, expand **Targets**.
2. Expand the Exchange 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 need the following information:

   - The name of the Provisioning Group.
   - The mailboxes to be included in the Provisioning Group. You can select mailboxes using any of the following: Windows group or user, Distribution Group, organizational unit , LDAP query, whole Exchange Organization.
   - The Exchange desktop, mailbox, and PST Migration policies 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.

- Optionally, an override default vault store that Enterprise Vault is to use when creating the archives for mailboxes in this Provisioning Group. If mailboxes in the Provisioning Group are automatically-enabled for archiving, the vault store will be used for any future mailboxes that are 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 Exchange Server properties. If the vault store is not specified in the Exchange Server properties, then the setting in the Enterprise Vault server properties is used.
- Whether you want Enterprise Vault 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 Exchange Mailbox Task next runs. All mailboxes created in the future will also be enabled and the associated archives automatically created.
  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.
- If auto-enabling is selected, whether to initially suspend archiving. This means that archiving of the mailbox does not start until the user enables it. This gives the users the opportunity to change archiving defaults, if required, before archiving begins.

Ordering Provisioning Groups for Exchange Server 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 reorder 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.

Adding an Exchange Provisioning task for Exchange Server archiving

An Exchange Provisioning task is required for each Exchange Server domain. This task enables mailboxes in the provisioning groups that you have created.

You can add an Exchange Provisioning task manually, as described in this section, or you can let Enterprise Vault add one automatically when you add the first Exchange Mailbox archiving task.

You are recommended to run the Exchange Provisioning task as the Vault Service account. If you want to use a different account, the account will need to be added to the Messaging Administrator role.

In addition, if you are using Exchange Server 2007, use the Exchange Management Console to assign the Exchange View-Only Administrator role to the account that the task will use. For details of how to assign the Exchange View-Only Administrator role, see the section on assigning Exchange managed folder permissions in the *Installing and Configuring* manual.

To add an Exchange Provisioning task manually

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

   The new task wizard starts.
5. Work through the wizard. You will need the following information:
   - The name of the Exchange Provisioning task
   - The name of the Exchange Server domain to be processed
6. To review the property settings for the task, double-click the task in the right-hand pane. You can modify properties such as the task schedule, the level of reporting required and whether to run the task in report mode.

   Whenever new mailboxes are added, they must be processed by the Exchange Provisioning task before they can be enabled.

Adding an Exchange Mailbox archiving task

Before you add an archiving task, ensure that the Enterprise Vault system mailbox is available. See the *Installing and Configuring* manual for instructions.

Note: If you use a database availability group (DAG) in your Exchange environment, you must set up archiving for all members of the DAG.

See "Using Exchange Server database availability groups" on page 28.

To add an Exchange Mailbox archiving task

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

   The new task wizard starts.
5. Work through the wizard. You will need the following information:
   - The name of the Exchange Server to be archived
   - The Enterprise Vault system mailbox to use

   If an Exchange Provisioning task does not exist for the domain, then one will be created automatically.

Reviewing the default settings for the Enterprise Vault site

Check the default settings that are configured in the Enterprise Vault site properties.

Site properties include the following settings. 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 and archive level. The default retention category can also be set at policy level (and at Provisioning Group level for Exchange Server mailbox archiving).

Table 3-15 Site properties

Tab	Settings
General	■ The Vault site alias and description. ■ The protocol and port to use for the Web Access application. ■ A system message for users of the Web Access application, if required. ■ The following site properties settings apply only to Exchange Server archiving: PST holding area details. ■ A note for administrators, if required.
Archive Settings	■ The default retention category. ■ Whether the retention category of moved items is always updated, or updated only when the retention period is increased or unchanged. ■ Whether users can delete items from their archives. ■ Whether items that users have deleted can be recovered. ■ The length of time for which the deleted items remain available for recovery. ■ The length of time for which to retain the transaction history for archives.
Storage Expiry	■ The schedule for running storage expiry to delete from archives any items that are older than the retention period assigned. ■ Whether expiry is based on an item's modified date or its archived date.
Site Schedule	■ The schedule for running automatic, background archiving.
Archive Usage Limit	■ If required, you can set limits on the size of archives.
Indexing	■ Indexing level: brief or full. ■ Email content that should not be indexed, such as disclaimers. ■ How long indexing subtasks are retained before they are deleted.
Advanced	■ Advanced settings that you can use to tune Enterprise Vault indexing within the Enterprise Vault site. **Note:** Do not change the Indexing settings unless your technical support provider advises you to do so.
Monitoring	■ Performance counters for monitoring Enterprise Vault.

To review the default settings for the Enterprise Vault site

1. In the Administration Console, expand the contents of the left pane until the Enterprise Vault site is visible.
2. Right-click the Enterprise Vault site and then, on the shortcut menu, click **Properties**.

   Alternatively, select the site and click the **Review Site Properties** button on the toolbar.
3. Click **Help** on any of the site properties tabs for further information.

Using customized shortcuts with Exchange Server archiving

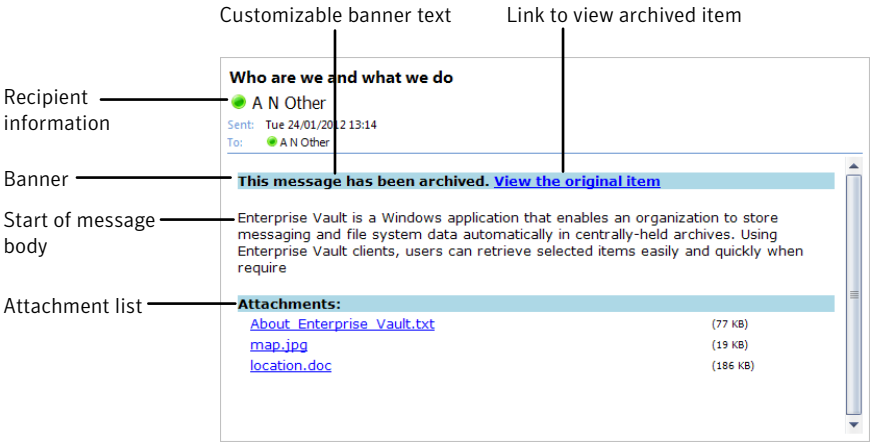
The standard Enterprise Vault shortcuts do not work well with IMAP or POP3 clients. If you have users with such clients, you can choose to use custom shortcuts. You can view these using any client that can render HTML content, such as Outlook Express.

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

- From and Subject information.
- Recipient information: To, CC, and BCC.
- A banner containing a link to the complete archived item.
- The first 1000 characters from the message body.
- Links to attachments, if there are any.

Figure 3-1 shows the structure of a default shortcut.

Figure 3-1 Structure of a shortcut



You can change the settings so that shortcuts contain as much information as you require. If you have users with IMAP, POP3 or Entourage clients, you probably want to customize shortcuts so that they contain links to archived attachments. Users can click the link to open an attachment.

Note that the changes you can 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 `ShortcutText.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 `Enterprise Vault\Languages\ShortcutText`.

Note that this file may also be used to process untitled attachments in standard shortcuts.

To define custom shortcut content

1. Locate the required language version of the `ShortcutText.txt` file (under `Enterprise Vault\Languages\ShortcutText`).
2. Open `ShortcutText.txt` with Windows Notepad and make any required changes.

   See "Layout of ShortcutText.txt for customized shortcuts with Exchange Server archiving" on page 57.
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 Restart the Exchange Server archiving tasks (for mailboxes or public folders or both) 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 **Exchange Mailbox Policy** properties.

2 Select **Customize** for the content of the shortcut body, and then specify which options you want. Click **Help** on the tab for more information.

3 Open the properties window for the Exchange mailbox archiving task and click the **Synchronization** tab.

4 Synchronize the **Archiving settings** for the required mailboxes.

Layout of ShortcutText.txt for customized shortcuts with Exchange Server archiving

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

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

You can change any of the values within the file. Remember to enclose each value in quotation marks. For example:

```
"IPM.Task=This task has been archived."
```

The sections within `ShortcutText.txt` are as follows:

`[Archived text]`

The entries in this section are displayed in the banner at the top of the shortcut.

The entry that is used for the shortcut is the one that matches the archived item's message class. For example, shortcuts to items with message class IPM.Note contain the text "This message has been archived".

Values in this section all have a space before the final quotation mark. This space separates the text from the link text.

`[Link]`	The entry in this section specifies the text in the banner that is a link to the archived item.
`[Attachment table]`	The Title entry in this section specifies the text immediately before the list of attachments. The DefaultItemTitle entry is used to label any attachments that have no title of their own.

About editing automatic messages for Exchange Server 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 for Exchange Server archiving

When Enterprise Vault enables a mailbox for archiving, it automatically sends a Welcome message to that mailbox. The Welcome message provides basic 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:

`Enterprise Vault\Languages\Mailbox Messages\`*`lang`*

where *lang* indicates the language used.

The Welcome message is in a file called `EnableMailboxMessage.msg`.

To set up the Welcome message

1. Decide which language version of **EnableMailboxMessage.msg** you want to use and locate the file.
2. Using a computer that has Microsoft Outlook installed, double-click the file **EnableMailboxMessage.msg** in Windows Explorer to edit the message.

3 Review the text and make any changes that you require. If necessary, include instructions to users about how to install the Enterprise Vault Add-Ins on their computers.

See "Setting up manual installation of the Outlook Add-In" on page 69.

4 Save the message.

5 Copy **EnableMailboxMessage.msg** to the Enterprise Vault program folder (for example `C:\Program Files (x86)\Enterprise Vault`) on every Enterprise Vault server in the site.

Editing Archive Usage Limit messages for Exchange Server archiving

You can set a maximum allowed size for users' archives on the Archive Usage Limit page of Site Properties. On the same page, you can specify if you want messages sent to users who are approaching or have reached their archive limit. For those approaching their limit, you can also define the point at which you want the message sent.

If you have selected either of the User Notification check boxes, you need to make the appropriate messages available to all the Enterprise Vault servers in the site.

During the installation the archive limit warning messages are placed in a folder beneath the Enterprise Vault Program folder:

`Enterprise Vault\Languages\Mailbox Messages\`*`lang`*

where *lang* indicates the language used.

The message files are called `ApproachingArchiveQuotaLimit.msg` and `ArchiveQuotaLimitReached.msg`.

To set up the archive limit warning messages

1 Decide which language version of the messages you want to use and locate the files, **ApproachingArchiveQuotaLimit.msg** and **ArchiveQuotaLimitReached.msg**.

2 Using a computer that has Microsoft Outlook installed, double-click the files in Windows Explorer to open the messages.

3 Review the text and make any changes that you require.

4 Save the messages.

5 Copy the two message files to the Enterprise Vault program folder (for example `C:\Program Files (x86)\Enterprise Vault`) on every Enterprise Vault server in the site.

Starting the Task Controller service and archiving task when setting up Exchange Server archiving

The Task Controller service and archiving task that you created have not yet been started. These must be started before you can enable mailboxes. The default is for archiving tasks to start automatically when the Task Controller service starts.

To start the Task Controller service and archiving 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 Exchange Mailbox archiving task has started.
5. The task will run automatically at the times that you have scheduled. You can also force an archiving 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.

Enabling mailboxes for Exchange Server archiving

Before new mailboxes can be enabled, they must be processed by the Exchange Provisioning task. On a default system, this 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.

Note: By default, Enterprise Vault processes only mailboxes that are listed in the Exchange Global Address List. If you want to archive mailboxes that are not in the Global Address List, see the section *Hidden mailboxes* in the *Administrator's Guide*.

After Exchange Server mailboxes have been processed by the Provisioning task, they need to be enabled. This can be done automatically, when the Exchange Mailbox task runs, or manually.

Enterprise Vault menu options and buttons do not appear in Outlook until the user's mailbox has been enabled and the user has restarted Outlook. You can

therefore roll out the Enterprise Vault Outlook Add-In before users' mailboxes are enabled.

When an Exchange Server 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 one or more users who can access the information stored in it.

To force the Exchange 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 Exchange Provisioning task and select **Properties**.
4. Check that the reporting level is as you require. Full reporting will list each mailbox that is processed, the provisioning group, Mailbox and PST policies assigned the username associated with the mailbox and the action taken. Summary statistics about the task run are included at the end of the report.

   You can configure the task to generate reports when the task is run in both report or normal mode.
5. In the right-hand pane, right-click the Exchange 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. If you selected the option for mailboxes to be enabled for archiving automatically, they will be enabled the next time the Exchange Mailbox task runs.

   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.

Creating shared archives for Exchange Server archiving

There may be times when you want to create extra archives that can be shared by a number of users. For example, you may want to archive all documentation concerning a particular project in the same archive.

You create the shared archive manually and then set permissions on the archive to give each of the users access to it. You can add or remove users at any time.

Note that shared archives do not contain folders.

To create an archive manually

1. Start the Enterprise Vault Administration Console.
2. In the left pane of the Administration Console, expand the Enterprise Vault site hierarchy until the **Archives** container is visible.
3. Expand the **Archives** container to display the various archive types.
4. Right-click **Shared** and then click **New > Archive**.

   The New Archive wizard starts.
5. Answer the wizard's questions to create the archive. You will be asked to provide the following information:
   - The vault store for the archive
   - Indexing service and indexing level to use
   - Billing account

To set access permissions on the shared archive

1. In the left pane, expand the Enterprise Vault site hierarchy until the **Archives** container is visible.
2. Expand the **Archives** container, and click **Shared**.
3. In the right pane, double-click the name of the archive that you want to modify.
4. Right-click the archive you want to change and then click **Properties**.
5. Modify the permissions as required.

Installing the Outlook Add-In on a server for Exchange Server archiving

There is no requirement for you to install the Enterprise Vault Outlook Add-In on an Enterprise Vault Server.

Overriding PSTDisableGrow

If the registry value PSTDisableGrow is enabled, you experience the following limitations in the use of Enterprise Vault:

- Users cannot open Enterprise Vault shortcuts in Outlook.
- The Vault Cache feature does not work because synchronization fails.
- Client-driven PST migration does not work. For information about client-driven PST migration, see the *Administrator's Guide*.

You need to perform the following actions to override PSTDisableGrow.

- For Outlook 2003 and Outlook 2007, request the appropriate Outlook hotfix from Microsoft and apply it. Note however that the hotfix may already have been applied as part of a Microsoft Update.
  - For Outlook 2003:
    http://support.microsoft.com/?kbid=953671
  - For Outlook 2007:
    http://support.microsoft.com/?kbid=953925
    This hotfix is not required if Outlook 2007 Service Pack 2 or later is installed.
- Enable the registry value PSTDisableGrowAllowAuthenticodeOverrides, which bypasses the PSTDisableGrow policy.

  You can set PSTDisableGrow in the following registry locations:
  - `HKEY_CURRENT_USER\Software\Microsoft\Office\`*`Office version`*`\Outlook\PST`. This location is the default location for PSTDisableGrow.
  - `HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\`*`Office version`*`\Outlook\PST`.

  You can only set PSTDisableGrowAllowAuthenticodeOverrides in the following registry location:
  - `HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\`*`Office version`*`\Outlook\PST`

When you enable PSTDisableGrowAllowAuthenticodeOverrides, it does not mean that users can create new PST files, or add items to existing PST files. PSTDisableGrowAllowAuthenticodeOverrides only enables the Outlook Add-In to perform these actions.

If PSTDisableGrow is enabled and PSTDisableGrowAllowAuthenticodeOverrides is not enabled, the Enterprise Vault Outlook Add-In displays a warning when it loads in Outlook.

To configure users' computers with PSTDisableGrowAllowAuthenticodeOverrides

1. Install the latest Enterprise Vault Outlook Add-In on users' computers.
2. Enable the registry value PSTDisableGrowAllowAuthenticodeOverrides in one of the following locations:
   - For Outlook 2003:
     `HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\11.0\Outlook\PST`
   - For Outlook 2007:
     `HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\PST`
   - For Outlook 2010:
     `HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\14.0\Outlook\PST`
   - For Outlook 2013:
     `HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\15.0\Outlook\PST`

   You must use one of the locations that are shown here. Note that, unlike the default PSTDisableGrow locations, these paths include the `\Policies` subkey.

   Both PSTDisableGrow and PSTDisableGrowAllowAuthenticodeOverrides must be of type **REG_DWORD**, and have a value of **1**.

Users' tasks for Exchange Server mailbox archiving

If you have set automatic enabling of mailboxes in the Provisioning Group, and you have chosen to initially suspend archiving, Outlook users must manually enable automatic archiving for their mailboxes.

Instructions on how to turn on archiving for a mailbox are given in the online Enterprise Vault help in Outlook 2003/2007 and also included in the Welcome message.

How users turn on automatic archiving for their mailbox in Outlook 2003/2007

1. Open Outlook.
2. In the folder list view, right-click the **Mailbox** and then click **Properties**.
3. Click the **Enterprise Vault** tab.
4. Clear **Suspend Enterprise Vault archiving for this mailbox**.

Chapter 4

Setting up users' desktops

This chapter includes the following topics:

About setting up users' desktops for Exchange Server archiving

Desktop policies define the end user's experience when using the Enterprise Vault Exchange clients. Setting up desktop policies is described as part of setting up mailbox archiving.

See "Defining desktop policies in Exchange Server archiving" on page 38.

Other sections cover the additional steps required to set up users' desktops to work with Enterprise Vault. The steps include distributing the Outlook Add-In and enabling its installation, enabling searching of archives using Windows Desktop Search, and ensuring Outlook is set up to synchronize forms.

Enterprise Vault Outlook Add-In for Exchange Server archiving

The Enterprise Vault Outlook Add-In is available as a Microsoft® Windows® Installer (MSI) kit. The installer kit is in the folder `Symantec Enterprise Vault\Outlook Add-In` on the Enterprise Vault distribution media.

The Exchange desktop policy Outlook advanced setting **Outlook Add-In behavior** lets you configure the Outlook Add-In to work in either of the following modes:

- Full mode. In full mode, there are no functional restrictions on the behavior of the Outlook Add-In.
- Light mode. This mode is the default. In light mode, the following restrictions apply:
  - Users have no access to the Enterprise Vault properties of folders.
  - When users archive items manually, they cannot specify the destination archive and retention category.
  - When users restore archived items, they cannot choose the destination folder. The Outlook Add-In only restores items to the folders where the shortcuts are.

For more information about the advanced setting **Outlook Add-In behavior**, see the *Administrator's Guide*.

If Outlook users access Exchange Server 2003 using RPC over HTTP, you will also need to configure Enterprise Vault access on the Exchange Server using the Enterprise Vault RPC server extensions. With Exchange Server 2007, Enterprise Vault server extensions are not required for RPC over HTTP connections.

See "About Outlook RPC over HTTP and Outlook Anywhere configurations" on page 185.

Before users have access to Enterprise Vault features from within Outlook, the Outlook Add-In must be installed on each desktop computer.

There are various ways of distributing the Outlook Add-In. For example, you can use one of the following methods:

- Deploy the MSI kit to desktop computers using a software distribution application, such as Systems Management Software (SMS) or Active Directory Group Policy.
  See "Publishing the Outlook Add-In in Active Directory for Exchange Server archiving" on page 68.
- Set up manual installation.
  See "Setting up manual installation of the Outlook Add-In" on page 69.

Enterprise Vault buttons and menu options do not appear in Outlook until the user's mailbox has been enabled and the user has restarted Outlook. You can therefore roll out the Enterprise Vault Outlook Add-In before users' mailboxes are enabled.

Enabling Windows Desktop Search plug-in for Exchange Server archiving

A plug-in for Windows Desktop Search is included in the Enterprise Vault Outlook Add-In. Using advanced settings in the Exchange Desktop policy, you can enable users to search their Vault Cache from Windows Desktop Search.

Note that Windows Desktop Search must be installed on the desktop computers before you install the Outlook Add-In.

The plug-in is not enabled by default when the Outlook Add-In is installed.

To enable Vault Cache users to search their Vault Caches

1. In the Administration Console, open the **Advanced** properties page of the Exchange Desktop policy.
2. Select **Vault Cache** settings from the drop-down list.
3. Set **WDS search auto-enable** to **Force on**.
4. On the **Synchronization** page of the Exchange Mailbox task properties, synchronize the user mailboxes.
5. When users next start Outlook, the policy changes are implemented.

   See "Configuring Windows Search for Exchange Server archiving" on page 74.

   Note that to use Windows Desktop Search to search their Vault Cache, users do not require Administrator privileges on their desktop computer.

Command line activation of Windows Desktop Search plug-in for Exchange Server archiving

The recommended way to enable Vault Cache searching is using the **WDS Search Auto-enable** setting in the Exchange Desktop Policy. Alternatively, you can enable the plug-in during installation by including the command line parameter `ACTIVATE_WDS_PLUGIN=1`. Note that this command line switch is case-sensitive.

For example, the command line for a silent install would be the following:

```
msiexec /I path_to_installer ACTIVATE_WDS_PLUGIN=1 /qn
```

where *path_to_installer* is the path to the Enterprise Vault Outlook Add-In MSI file.

See "Setting up manual installation of the Outlook Add-In" on page 69.

Publishing the Outlook Add-In in Active Directory for Exchange Server archiving

This section describes the steps to publish the Outlook Add-In using Active Directory Group Policy.

To publish in Active Directory in Windows Server 2000/2003

1. Copy the MSI file from the Enterprise Vault distribution media to the network share from which you want it to be distributed.
2. Click **Start**, **Programs**, **Administrative Tools**, **Active Directory Users and Computers**.
3. In the left pane, navigate to the Organizational Unit to which you want to make the Outlook Add-In available.
4. Right-click the Organizational Unit and, on the shortcut menu, click **Properties**.
5. Click the **Group Policy** tab.
6. Click **New**.
7. Enter a name for the new Group Policy Object, for example "EV Desktop Rollout".
8. Click **Edit**. The Group Policy window appears.
9. In the left pane, under **Computer Configuration**, expand **Software Settings**.
10. Right-click **Software installation** and, on the shortcut menu, click **New** and then **Package**.
11. Select the MSI file that you copied in step 1. In the **File name** box, ensure that the file name includes the UNC path of the file. For example:

    ```
    \\mycomputer\distribute\Symantec Enterprise Vault Outlook
    Add-in.msi
    ```

    Then click **Open**. The **Deploy Software** dialog box opens.
12. Select **Assigned** and click **OK**.

    The new package appears in the list of software installations.
13. Close the Group Policy window.

    The new package is installed when each user's computer is restarted.

To publish in Active Directory in Windows Server 2008/2012

1. Copy the MSI file from the Enterprise Vault distribution media to the network share from which you want it to be distributed.
2. In Windows, open the **Group Policy Management** administrative tool.
3. In the left pane, navigate to the Organizational Unit to which you want to make the Outlook Add-In available.
4. Right-click the Organizational Unit and, on the shortcut menu, click **Create a GPO in this domain, and Link it here**.
5. Enter a name for the Group Policy Object (GPO), for example "EV Desktop Rollout", and click **OK**.
6. Right-click the new GPO and, on the shortcut menu, click **Edit**. The Group Policy Management Editor appears.
7. In the left pane, under **Computer Configuration**, expand **Policies** and **Software Settings**.
8. Right-click **Software installation** and, on the shortcut menu, click **New** and then **Package**.
9. Select the MSI file that you copied in step 1. In the **File name** box, ensure that the file name includes the UNC path of the file. For example:

   ```
   \\mycomputer\distribute\Symantec Enterprise Vault Outlook Add-in.msi
   ```

   Then click **Open**. The **Deploy Software** dialog box opens.
10. Select **Assigned** and click **OK**.

    The new package appears in the list of software installations.
11. Close the Group Policy Management Editor.

    The new package is installed when each user's computer is restarted.

Setting up manual installation of the Outlook Add-In

The usual way to install the Outlook Add-In is to deploy the MSI package to desktop computers using a software distribution application. However , you can allow users to install the Outlook Add-In themselves. The users must have local administrator permissions to install the Outlook Add-In.

In some cases the users can launch the MSI directly, but for some users you also need to provide a `setup.exe` file. The users must run `setup.exe` to launch the MSI. The `setup.exe` file that you may need is included on the Enterprise Vault media, in the same folder as the MSI file.

You need to provide a `setup.exe` file if both of the following conditions apply:

- The operating system on the client computer is Windows Vista/7/8.
- Windows User Account Control (UAC) is turned on.

Launching the MSI with `setup.exe` ensures that the installation process is elevated before the MSI is launched. This early elevation is necessary to enable the installation to complete all of its processes. If UAC is turned on and a user tries to launch the MSI directly, the installation process displays an error message.

Note: When a user runs `setup.exe` it must be in the same folder as the MSI file.

We recommend that you make the files available to users as follows.

Making the MSI file and setup.exe available to users

1. Place the MSI file in a shared folder, together with the `setup.exe` if required.

   The files are in the following folder on the Enterprise Vault media:

   ```
   Symantec Enterprise Vault\Outlook Add-In
   ```

2. Do one of the following:

   - For a new installation of Enterprise Vault, add a link to the Welcome message from which users can access the shared folder. Edit the Welcome message to include suitable instructions. If you have provided `setup.exe`, tell users to run `setup.exe`, not the MSI file. If they download the files, tell them that the files must be in the same folder.
     See "Editing the Welcome message for Exchange Server archiving" on page 58.
   - For an upgrade installation, users do not receive the Welcome message, so inform them by another method. If you have provided `setup.exe`, tell users to run `setup.exe`, not the MSI file. If they download the files, tell them that the files must be in the same folder.

See "Enterprise Vault Outlook Add-In for Exchange Server archiving" on page 66.

Managing FilesInUse dialog boxes in a manual upgrade or an uninstall of the Outlook Add-In

The information in this section is provided so that if necessary you can advise users about which option to choose in a FilesInUse dialog box. The section also outlines how you can prevent FilesInUse dialog boxes from appearing.

When a user upgrades the Outlook Add-In manually on Windows Vista/7/8, the Windows Restart Manager may detect that one or more files are locked. In this

case, the Restart Manager displays a FilesInUse dialog box that says that the relevant application or applications should be closed. The dialog box may also appear during an uninstall of the Outlook Add-In. In a new installation of the Outlook Add-In, the dialog box is much less likely to appear, though it is still possible.

The user can choose one of the following options:

- Close the applications automatically and attempt to restart them after setup is complete. This option is the default.
- Do not close the applications, but a system restart may be required.

We recommend that users should choose the option to close and restart the applications automatically.

Table 4-1 shows the applications that users are most likely to see in the dialog box.

Table 4-1 Applications in a FilesInUse dialog box

Application name	Notes
Windows Explorer	A file is locked because Windows Explorer has loaded it to support search functionality. If the user chooses to close Windows Explorer automatically, all Explorer windows are closed. The Desktop also closes, which the user may not expect; that is, the Desktop icons and the Taskbar disappear for a short time. The installation continues and Windows Explorer is restarted.
Windows host process (Rundll32)	Windows may have used this process to load an Enterprise Vault DLL to support integration with the Indexing Options in the Windows Control Panel. If the user chooses to close the process automatically, the installation continues and the process is restarted. However, users may not recognize the process name. They may not want to close this application in case it closes Windows, and may not know which option to choose.
Outlook	We recommend that users close Outlook before they install or upgrade the Outlook Add-In, but it is not essential. The user can choose to close Outlook automatically.

If Restart Manager is disabled or Windows XP is in use, the FilesInUse dialog box may provide different options, as follows:

- Cancel the installation. This option is the default.

- Retry after the user has closed the application.
- Ignore the locked file. With this option, a system restart may be required.

We recommend that users should choose the option to ignore the locked file.

To disable the Restart Manager, you can set MSIRESTARTMANAGERCONTROL to Disable in the `msiexec` command line.

Alternatively, you can apply a transform to the MSI package to disable the Restart Manager. You can also use the transform to remove the FilesInUse dialog box from the installer.

See "Enterprise Vault Outlook Add-In for Exchange Server archiving" on page 66.

See "Setting up manual installation of the Outlook Add-In" on page 69.

Enterprise Vault Client for Mac OS X with Exchange Server archiving

The installer kit for the Enterprise Vault Client for Mac OS X is available as a disk image (`.dmg`) file. The file is located under the folder `Client for Mac OS X` on the Enterprise Vault distribution media.

There are various ways to distribute the client. For example, you can do the following:

- Send users a shortcut to the `.dmg` file.
  See "Editing the Welcome message for Exchange Server archiving" on page 58.
- Deploy the `.dmg` file to desktop computers using a software distribution application.

Setting up Kerberos authentication for the Enterprise Vault Client for Mac OS X

Note: Kerberos authentication is currently supported for use with Outlook 2011 for Mac only.

To use Kerberos authentication between the Enterprise Vault Client for Mac OS X and the Exchange and Enterprise Vault servers, you must do both of the following:

- On each Exchange server and Enterprise Vault server in your site, configure Internet Information Services (IIS) to allow Windows authentication with the

Negotiate setting enabled. This is necessary to ensure that users can log in to the Enterprise Vault Client and select the facilities on its toolbar and menu.

- Register with Active Directory a Service Principal Name (SPN) for each Enterprise Vault server and its DNS alias.

To configure IIS to allow Windows authentication with the Negotiate setting enabled

1. Open Internet Information Services (IIS) Manager.
2. In the left pane, navigate to the level that you want to manage.

   On Microsoft Exchange servers, this is the Exchange and EWS virtual directories. On Enterprise Vault servers, it is the EnterpriseVault virtual directory.
3. In **Features View**, double-click **Authentication**.
4. On the **Authentication** page, ensure that the status of **Windows Authentication** is **Enabled**.

   If the status of **Windows Authentication** is **Disabled**, select **Windows Authentication** and then click **Enable** in the **Actions** pane.
5. With **Windows Authentication** selected, click **Providers** in the **Actions** pane.
6. Ensure that the list of enabled providers includes **Negotiate**.

To register with Active Directory an SPN for each Enterprise Vault server and its DNS alias

- See the following article on the Microsoft website for guidelines on how to register the SPNs:

  http://social.technet.microsoft.com/wiki/contents/articles/717.service-principal-names-spns-setspn-syntax-setspn-exe.aspx

Forcing Outlook to synchronize forms when using Exchange Server archiving

If an Outlook user has enabled Use Cached Exchange Mode, then by default Outlook forms are not synchronized. This results in Enterprise Vault icons not being displayed for archived items.

To make Outlook synchronize forms

1. Start Outlook.
2. Open the **Send/Receive Groups** dialog box. How you do this depends on the version of Outlook:

- In Outlook 2003/2007: click **Tools > Send/Receive > Send/Receive Settings**. Then click **Define Send/Receive Groups**.
- In Outlook 2010/2013: click the **File** tab, then click **Options**, then click **Advanced**. Under **Send and receive**, click **Send/Receive**.

3. Select **All Accounts Online and Offline** and click **Edit**.
4. Select **Synchronize Forms**.
5. Exit from Outlook and then restart it.
6. Open an archived item. This automatically installs the forms.

Getting users started with Exchange Server archiving

You should ensure that users know how to install the Enterprise Vault Outlook Add-In or Client for Mac OS X, as necessary, using one of the methods described in other sections, and how to use Enterprise Vault.

JavaScript must be enabled in users' browsers.

If you want users to be able to launch Archive Explorer or archive Search in a standalone browser, you will need to tell them the URL to use. You could include this information in the Welcome message.

See "Editing the Welcome message for Exchange Server archiving" on page 58.

If you are making Microsoft Exchange Forms for Enterprise Vault available using Organizational Forms Library, ensure that the forms have been installed on all Microsoft Exchange Server computers that are being processed by Enterprise Vault.

See "About distributing the Microsoft Exchange forms when setting up Exchange Server archiving" on page 21.

See "Setting up manual installation of the Outlook Add-In" on page 69.

Configuring Windows Search for Exchange Server archiving

If you have enabled the Enterprise Vault plug-in for Windows Search, users can use Windows Search to search their local Vault Cache. Before they can do this, they need to start Outlook and the Windows Search.

They can use the following steps to check that the Vault Cache and Virtual Vault are configured in Windows Search indexing, and force Windows Search to index archived items.

To check the Windows Search options

1. Open the Indexing Options dialog box. How you open this dialog box depends on which version of Windows you use. For example:
   - In Windows XP, right-click the **Windows Search** icon in the Windows taskbar, and then click **Windows Search Options**.
   - In Windows 7, click **Start > Control Panel**. In the search box, type **indexing options**, and then click **Indexing Options**.
   - In Windows 8, hold down the the Windows logo key and press **w**. Type **index**, and then click **Indexing Options**.
2. In the **Indexing Options** dialog box, click **Modify**.
3. In the **Change selected locations** list, ensure that the entry for your Virtual Vault is selected. In addition, if the Symantec Vault Cache location appears in the list, ensure that it is selected.
4. Click **OK**.
5. Close the Indexing Options dialog box.

When your computer is idle, Windows Search updates its index to include the items in your Vault Cache.

What next?

You should now have a fully functioning Enterprise Vault system. You may find over time that you need to change some of the properties of Enterprise Vault to suit your requirements. For details about these and any other features of Enterprise Vault, refer to the online Help.

Chapter 5

Setting up Vault Cache and Virtual Vault

This chapter includes the following topics:

About Vault Cache and Virtual Vault

A Vault Cache is a local copy of a user's Enterprise Vault archive. The Vault Cache is maintained on the user's computer by the Enterprise Vault Outlook Add-In.

The main functions of Vault Cache are as follows:

- It makes Virtual Vault available to users, if you choose to enable Virtual Vault.
- It lets offline users open archived items from Enterprise Vault shortcuts.
- It lets offline users view their archives in offline Archive Explorer.

Virtual Vault integrates a view of the user's archive into the Outlook Navigation Pane. To users, a Virtual Vault looks like a mailbox or a personal folder, and it

behaves in much the same way. For example, users can open archived items and drag and drop items to and from the Virtual Vault.

Figure 5-1 shows a mailbox and a Virtual Vault in the Outlook Navigation Pane.

Figure 5-1 Example of a Virtual Vault

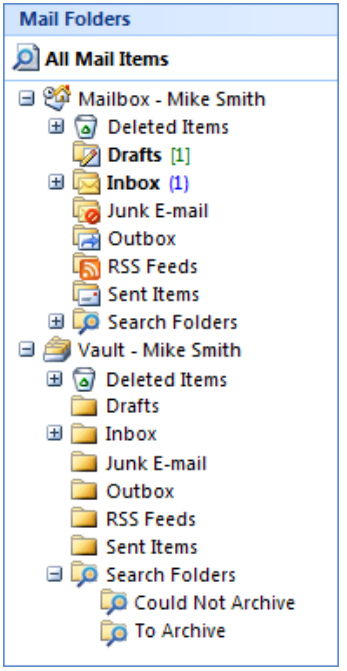
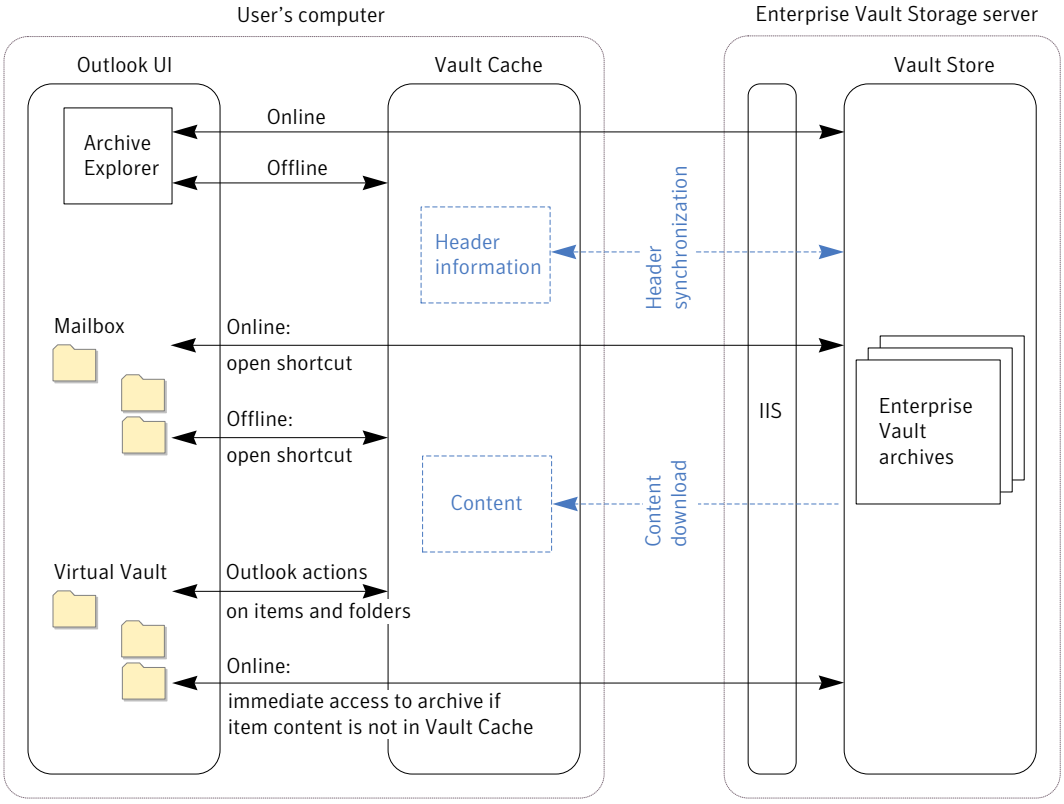


Figure 5-2 shows the relationship between Vault Cache and Virtual Vault, and Vault Cache synchronization with the online archive.

Figure 5-2 Vault Cache and Virtual Vault



The user can synchronize archives other than their primary mailbox archive to the Vault Cache, if they have the necessary permissions. Each archive that is synchronized to a Vault Cache has its own Virtual Vault, if Virtual Vault is enabled. In Virtual Vault, access to archives other than the user's primary mailbox archive is read-only.

The actions that users can perform in Virtual Vault include the following:

- View, forward, and reply to archived items
- After opening an email to send from Outlook, drag and drop items from Virtual Vault into the email to send them as attachments
- Search the Virtual Vault with Outlook Instant Search, Outlook Advanced Find, or Windows Desktop Search
- Delete items and folders

- Move items between folders, and reorganize folders
- Archive items using drag and drop
- Move items into Virtual Vault using Outlook rules

Note: The Vault Cache feature is not available to users of the Enterprise Vault Client for Mac OS X.

Vault Cache content strategy

You can specify a strategy for how the content of archived items is stored in Vault Cache. The content strategy controls whether full items or just item headers are stored locally.

The content strategy options are on the **Vault Cache** tab in the Exchange Desktop policy, and are as follows:

- **Do not store any items in cache**. Item headers are synchronized to Vault Cache, but the content of archived items is not stored in Vault Cache. If a user who is online opens an item in Virtual Vault, Enterprise Vault immediately retrieves the content from the online archive.
- **Store all items**. This option is the default. Item headers are synchronized to Vault Cache and the content of archived items is stored in Vault Cache.
- **Store only items that user opens**. Item headers are synchronized to Vault Cache. If a user who is online opens an item in Virtual Vault, or selects an item when the Reading Pane is open, Enterprise Vault immediately retrieves the content from the online archive. The content of each item that a user opens in Virtual Vault is stored in Vault Cache.

See "Show content in Reading Pane (Exchange Virtual Vault setting)" on page 100.

See "Vault Cache header synchronization and content download" on page 82.

Vault Cache synchronization

Vault Cache synchronization updates the Vault Cache with changes made to the online archive, and updates the online archive with changes made to the Vault Cache. The changes that are synchronized between Vault Cache and the online archive include create, update, and delete actions on items and folders.

Whether the Vault Cache is fully up to date with the online archive depends on when Vault Cache synchronization and the Exchange Mailbox Archiving task last ran.

After an initial synchronization when the Vault Cache is first enabled, synchronization can start in the following ways:

- The Enterprise Vault Outlook Add-In automatically performs Vault Cache synchronization once a day. If the Outlook Add-In cannot connect to Enterprise Vault, then it waits for a minimum of five minutes before it attempts to contact the server again.

  If a scheduled synchronization time is missed, the Outlook Add-In attempts a synchronization when the user next opens Outlook. The first attempt is made after the period specified in the Exchange Desktop policy, in the Vault Cache advanced setting **Pause interval**.

  For example, users may miss their scheduled Vault Cache synchronization times during a weekend, when they do not use Outlook. In this case, a large number of header synchronization requests may occur at around the same time on Monday. To avoid an excessive load on the Enterprise Vault server, an Enterprise Vault mechanism limits the number of header synchronization requests that are accepted. When this mechanism operates, scheduled synchronization succeeds for some users. Other users have to wait until their header synchronization request is processed. The mechanism is invisible to users, so they do not see any error message. Their header synchronization request is repeated, as usual, at minimum intervals of five minutes until it succeeds. When the synchronization succeeds, the daily scheduled synchronization time is reset to the time of the successful synchronization.

  Alternatively, you can use the registry setting, **OVAllowMissedMDCSyncOnStartup**, to configure the Outlook Add-In to ignore missed scheduled Vault Cache synchronizations when the user opens Outlook. If you enable this setting, a Vault Cache sychronization occurs at the next scheduled sychronization time.

- If Vault Cache synchronization is required at other times, the user can start the synchronization in Outlook. A manual synchronization does not affect the next scheduled time for automatic synchronization.

  Unlike a scheduled synchronization, a manual synchronization that fails is not retried.

- You can use the Virtual Vault advanced settings **Threshold number of items to trigger synchronization** and **Threshold total size of items to trigger synchronization** to trigger an automatic Vault Cache synchronization. The settings specify thresholds for the number and total size of pending archive items in Virtual Vault.

  These threshold settings are important if your users move or copy items from their mailboxes into Virtual Vault to archive them. When only scheduled synchronization and manual synchronization are in use, items are probably not archived until the scheduled time. Until then, moved and copied items

exist only on the user's computer. The threshold settings let you control when synchronization occurs, so you can minimize the risk of data loss.

By default, the threshold settings are not active. You can optionally set one or both of them. If you set both, the first threshold value that is reached or exceeded triggers a synchronization.

If the user suspends Vault Cache synchronization and either of these threshold settings is active, the user cannot move or copy items into Virtual Vault.

Unlike a scheduled synchronization, an automatically triggered synchronization that fails is not retried.

See "Threshold number of items to trigger synchronization (Exchange Virtual Vault setting)" on page 101.

See "Threshold total size of items to trigger synchronization (Exchange Virtual Vault setting)" on page 101.

The content download from the Enterprise Vault server to the Outlook client uses Microsoft Background Intelligent Transfer Service (BITS) technology.

For information about troubleshooting Vault Cache synchronization problems, see the appendix "Troubleshooting" in the *Administrator's Guide*. The section on Vault Cache synchronization problems includes details of how to use the Vault Cache Diagnostics web page. This web page shows the last Vault Cache synchronization attempt from each user, and for each archive that they synchronize. The reporting information that is displayed on the page is posted by client computers immediately after they attempt a synchronization, and regardless of the outcome.

See "Vault Cache initial synchronization" on page 84.

Vault Cache header synchronization and content download

Vault Cache synchronization consists of the following processes:

- Header synchronization
- Content download

Vault Cache header synchronization

Header synchronization is always part of Vault Cache synchronization. The item header contains enough information to enable the item to be represented in Virtual Vault, or in offline Archive Explorer within Outlook. It also contains information to associate the header with the content of the full item.

Where changes have occurred in the online archive, Vault Cache synchronization downloads header information from the Enterprise Vault server and applies the changes to the Vault Cache.

Note that some changes within the mailbox do not take effect in the online archive until the next run of the Mailbox Archiving task. For example, a run of the Mailbox Archiving task is required when a user moves an archived item or creates a folder in the mailbox.

Changes to the online archive may potentially require Vault Cache synchronization to include content download as well as header synchronization, for example when an item is automatically archived. However, content download may not be necessary if preemptive caching is in use.

See "Preemptive caching when using Vault Cache" on page 85.

Where changes have occurred in Virtual Vault and therefore in Vault Cache, those changes are synchronized to the online archive.

Header synchronization also synchronizes any changes that are made to the folder hierarchy, either in the online archive or in Virtual Vault. Users cannot move, delete, or rename a folder in Virtual Vault if the folder exists in the mailbox. Users must perform the actions on these folders in the mailbox, in Outlook or OWA.

Vault Cache content download

Content download is performed only when the content strategy is **Store all items**. Vault Cache synchronization downloads the content of items from the online archive to the Vault Cache. After the initial Vault Cache synchronization, content download can be minimized by preemptive caching. You can determine the age of items on which to perform preemptive caching, using the Vault Cache advanced setting **Preemptive archiving in advance**.

See "Preemptive caching when using Vault Cache" on page 85.

If the content strategy is **Store only items that user opens**, an item's content is downloaded immediately when the user opens the item. The content is then stored in Vault Cache for later use.

Vault Cache and Virtual Vault status

You can check the status and details of Vault Cache synchronization in the **Vault Cache Properties** dialog box in Outlook on the user's computer.

If you have enabled users to archive items by moving them into Virtual Vault, the users' Virtual Vaults include the following search folders:

- **Could Not Archive**. This folder lists items that Vault Cache synchronization could not archive, after the number of attempts configured in the advanced setting **Max attempts to archive an item**.

- **To Archive**. This folder lists items that the user has moved or copied into Virtual Vault and that are awaiting archiving. The folder does not include items that Vault Cache synchronization could not archive.

Vault Cache initial synchronization

When a mailbox is enabled for Vault Cache, header synchronization starts when the Vault Cache wizard finishes. Content download may also be performed, if the content strategy requires content download. If the archive contains a large number of items, content download takes much longer than header synchronization.

You can control the maximum age of items in the initial content download using the Vault Cache advanced settings **Download item age limit** and **Lock for download item age limit**.

A Virtual Vault is automatically added to a user's profile when the following criteria are met:

- The Enterprise Vault archiving task has processed all the archives that the user can access.
- The initial header synchronization has completed.
- The user has not previously removed the Virtual Vault from the profile.

If a Virtual Vault does not appear automatically in the Navigation Pane, the user can select it on the **Virtual Vault** tab in the **Vault Cache Properties** dialog box.

Control of concurrent content download requests by Vault Cache

To control the amount of system resources used by Vault Cache content downloads, you can restrict the number of content download requests that the server manages at a time. To restrict the number of content download requests, use the setting **Maximum number of concurrent updates** on the **Cache** tab of the Enterprise Vault server properties.

Enterprise Vault server cache location when using Vault Cache

If new items have been added to the online archive, copies of these items are held temporarily in a cache on the Enterprise Vault server. The items are then downloaded to the user's computer. The location of the server cache is specified on the **Cache** tab of the Enterprise Vault server properties.

Retention category changes when using Virtual Vault

In Virtual Vault, some changes may affect the retention categories of items and folders. These changes are handled as follows:

- If a user moves an item between folders with different retention categories, the item's retention category is updated. But if the original retention category prevents deletion and the destination folder's retention category allows deletion, the retention category is not updated.
- The user may move a folder that inherits its retention category into a folder with a different effective retention category. (The effective retention category is the retention category that is either inherited or assigned specifically.) In this case, the moved folder and its contents inherit the new retention category. Any subfolders and their contents that inherit the retention category are similarly updated.
- The user may move a folder with a specific retention category into a folder with a different effective retention category. In this case, the moved folder's retention category does not change.
- If the user creates a new folder in Virtual Vault, the folder inherits its parent folder's retention category.

Note: The effects of these actions on retention categories also depend on the **Update the category for moved items** settings on the Archive Settings tab in the Enterprise Vault site properties. The settings control whether the retention category of moved items is always updated, or updated only when the retention period is increased or unchanged.

Preemptive caching when using Vault Cache

To minimize downloads to the Vault Cache, the Outlook Add-In regularly searches the mailbox for any items that are due to be archived soon. It automatically adds these items to the Vault Cache. This feature is called preemptive caching.

The Vault Cache advanced setting **Offline store required** controls whether an offline store is required in Outlook for Vault Cache to be enabled. If a user does not have an OST file, Enterprise Vault cannot perform preemptive caching.

See "Offline store required (Exchange Vault Cache setting)" on page 90.

See "Preemptive archiving in advance (Exchange Vault Cache setting)" on page 91.

The Vault Cache wizard

You can choose to enable Vault Cache automatically for users' mailboxes, or allow users to enable it by running the Vault Cache wizard in Outlook.

The wizard enables Vault Cache for the user's primary mailbox only. If the user has access to other archives, those archives are listed on the **Vaults** tab in the **Vault Cache Properties** dialog box in Outlook. The additional archives are not synchronized to the Vault Cache until the user selects them in the dialog box.

Setting up Vault Cache and Virtual Vault

Before you set up Virtual Vault, see the *Virtual Vault Best Practice Guide*. It is available from:

http://www.symantec.com/docs/TECH75381

To enable Vault Cache, you select **Make Vault Cache available for users** on the **Vault Cache** tab in the Exchange Desktop policy. To enable Virtual Vault, you select **Make Virtual Vault available to users**, as well as **Make Vault Cache available for users**.

You can also do the following:

- Change the default Vault Cache settings on the **Vault Cache** tab.
- Configure Vault Cache and Virtual Vault advanced settings in the Exchange Desktop policy. You should review the advanced settings, and change them if necessary, before you synchronize the updated policy to users' mailboxes.

A Vault Cache is created for each Windows user's mailbox profile. A single user can have several Vault Caches, if the user has access to several mailbox profiles.

To set up Vault Cache and Virtual Vault in the Exchange Desktop policy

1. In the Exchange Desktop policy, on the **Vault Cache** tab, select **Make Vault Cache available for users**.
2. On the **Vault Cache** tab, select or clear other settings as required. If you want to enable Virtual Vault, select **Make Virtual Vault available to users**.

   For descriptions of the settings, click **Help** on the **Vault Cache** tab.
3. Click **Apply**.
4. On the Exchange Desktop policy **Advanced** tab, click **Vault Cache** on the **List settings from** menu and configure advanced settings for Vault Cache.

   See "Vault Cache advanced settings" on page 87.
5. Click **Apply**.
6. If you have enabled Virtual Vault, click **Virtual Vault** on the **List settings from** menu and configure advanced settings for Virtual Vault.

   See "Virtual Vault advanced settings" on page 94.

7 Click **OK**.

8 If you have disabled the expansion of PST files on users' computers by setting the registry entry PstDisableGrow, then you need to perform some additional setup tasks on users' computers.

See "Overriding PSTDisableGrow" on page 63.

Vault Cache advanced settings

The Vault Cache advanced settings let you control the behavior of Vault Cache.

Table 5-1 lists the Vault Cache advanced settings.

Table 5-1 Vault Cache advanced settings

Advanced setting	Description
Archive Explorer connection mode (Exchange Vault Cache setting)	Controls whether Archive Explorer respects the connection state when Outlook is in Cached Exchange Mode.
Download item age limit (Exchange Vault Cache setting)	Specifies the maximum age of items, in days, at which items are considered too old to be initially downloaded to the Vault Cache.
Lock for download item age limit (Exchange Vault Cache setting)	Controls whether users can change the download age limit.
Manual archive inserts (Exchange Vault Cache setting)	Controls whether an item that is manually archived is also automatically added to the Vault Cache.
Message Class exclude (Exchange Vault Cache setting)	A list of message classes that the Vault Cache never processes.
Message Class include (Exchange Vault Cache setting)	A list of message classes that the Vault Cache always processes.
Offline store required (Exchange Vault Cache setting)	Controls whether Vault Cache can be enabled when no offline store (OST) file is present.
Pause interval (Exchange Vault Cache setting)	The number of minutes to wait before Enterprise Vault starts searching for items that need to be added to the Vault Cache.
Per item sleep (Exchange Vault Cache setting)	The delay, in milliseconds, that will be used between items when updating the Vault Cache.

Table 5-1 Vault Cache advanced settings *(continued)*

Advanced setting	Description
Preemptive archiving in advance (Exchange Vault Cache setting)	The Outlook Add-In uses the **Preemptive archiving in advance** value when it determines the age of items on which to perform preemptive caching.
Root folder (Exchange Vault Cache setting)	The location in which to place Vault Caches.
Root folder search path (Exchange Vault Cache setting)	Enables you to supply a list of possible locations for the Vault Cache.
Search across all indexes (Exchange Vault Cache setting)	If offline Archive Explorer fails to find an item in its index, it can also perform a search across all indexes, which may be slow. This setting controls whether this fallback search is allowed.
Show Setup Wizard (Exchange Vault Cache setting)	Controls whether the client shows the Vault Cache setup wizard.
Synchronize archive types (Exchange Vault Cache setting)	Controls what is synchronized by Vault Cache.
WDS search auto-enable (Exchange Vault Cache setting)	Controls whether the Vault Cache search plug-in for Windows Desktop Search is automatically enabled for users.

Archive Explorer connection mode (Exchange Vault Cache setting)

Description: Controls whether Archive Explorer respects the connection state when Outlook is in Cached Exchange Mode. This setting has no effect unless Cached Exchange Mode is being used.

Supported values:

- Respect connection (default). Archive Explorer checks the Outlook connection state each time Archive Explorer starts. If a connection is available, online Archive Explorer is used; if there is no connection, offline Archive Explorer is used.
- Always offline. Offline Archive Explorer is always used.

Legacy name: ForceOfflineAEWithOutlookCacheMode

Download item age limit (Exchange Vault Cache setting)

Description	Specifies the maximum age of items, in days, at which items are considered too old to be initially downloaded to the Vault Cache. For example, if **Download item age limit** is set to 30 then items up to 30 days old are downloaded. If **Download item age limit** is set to 0 then all items are downloaded.
Supported values	■ 0. No age limit. All items are downloaded. ■ Integer. The maximum age, in days, of items that will be downloaded. All items up to this age will be downloaded.
Legacy name	OVDownloadItemAgeLimit

Lock for download item age limit (Exchange Vault Cache setting)

Description	Controls whether users can change the download age limit.
Supported values	■ On. Locked. ■ Off. Not locked.
Legacy name	OVLockDownloadItemAgeLimit

Manual archive inserts (Exchange Vault Cache setting)

Description	Controls whether an item that is manually archived is also automatically added to the Vault Cache.
Supported values	■ On (default). Automatically add manually archived items to the Vault Cache. ■ Off. Do not add to the Vault Cache.
Legacy name	OVNoManualArchiveInserts.

Message Class exclude (Exchange Vault Cache setting)

Description	A list of message classes that the Vault Cache never processes. Use semi-colons to separate the classes.
Supported values	■ Text string. A list of message classes to exclude, separated by semi-colons.
Legacy name	OVMessageClassExclude

Message Class include (Exchange Vault Cache setting)

Description	A list of message classes that the Vault Cache always processes. Use semi-colons to separate the classes.
Supported values	■ Text string. A list of message classes to include, separated by semi-colons.
Legacy name	OVMessageClassInclude

Offline store required (Exchange Vault Cache setting)

Description	Controls whether Vault Cache can be enabled when no offline store is present. Users have offline store (OST) files if Outlook Cached Exchange Mode is enabled. If a user does not have an OST file, Enterprise Vault cannot perform preemptive caching. If there is no preemptive caching, there is an increased load on Vault Cache content synchronization for newly archived items. The increased load is only a consideration if the Vault Cache content strategy is **Store all items**.
Supported values	■ Yes (default). An offline store is required for Vault Cache to be enabled. ■ No. An offline store is not required for Vault Cache to be enabled.
Legacy name	OVRequireOfflineStore

Pause interval (Exchange Vault Cache setting)

Description	The number of minutes to wait before Enterprise Vault starts searching for items that need to be added to the Vault Cache.
Supported values	■ An integer value. The default is 3 (minutes).
Legacy name	OVPauseInterval

Per item sleep (Exchange Vault Cache setting)

Description	The delay, in milliseconds, that will be used between items when updating the Vault Cache.

Supported values
- Integer. The number of milliseconds to use between items when updating the Vault Cache Default is 100 (milliseconds).

Legacy name OVPerItemSleep

Preemptive archiving in advance (Exchange Vault Cache setting)

Description The Outlook Add-In copies items from the user's Outlook `.OST` file to the Vault Cache before the items are due to be archived. The process is known as preemptive caching. Preemptive caching takes place on the user's computer. It reduces the number of items that need to be downloaded from the mailbox archive to the Vault Cache when the two are synchronized.

Preemptive caching obeys the settings in the Exchange mailbox policy's archiving rules.

The Outlook Add-In uses the **Preemptive archiving in advance** value when it determines the age of items on which to perform preemptive caching. To determine the age, it deducts the **Preemptive archiving in advance** value from the **Archive items when they are older than** value in the Exchange mailbox policy's archiving rules.

For example, you do not change **Preemptive archiving in advance** from its default value. You set the **Archive items when they are older than** mailbox policy setting to six weeks. The Outlook Add-In deducts the **Preemptive archiving in advance** default value of seven days from six weeks, and preemptively caches the items that are five weeks old or older.

Note that if you use an archiving strategy that includes quotas, it is difficult to predict the age at which items are archived. It is then usually advantageous to preemptively cache items as soon as possible. Enterprise Vault therefore uses 0 days as the age at which to perform preemptive caching if both of the following are true:

- The mailbox policy uses an archiving strategy that is based on quota or age and quota.
- You do not change the **Preemptive archiving in advance** setting from its default value.

Supported values
- An integer, specifying a number of days. The default is 7.

Legacy name OVPreemptAdvance

Root folder (Exchange Vault Cache setting)

Description	The location in which to place Vault Caches. This value is used when a user enables Vault Cache. Changing this value has no effect on existing Vault Caches.
Supported values	■ Path. A path to a folder that Enterprise Vault can create on the user's local computer. If you do not specify Root Folder, Enterprise Vault uses an Enterprise Vault subfolder in the user's Application Data folder.
Legacy name	OVRootDirectory

Root folder search path (Exchange Vault Cache setting)

Description	Enables you to supply a list of possible locations for the Vault Cache. The first such location that is valid on a user's computer is the one that will be used at the time the Vault Cache is created. This enables you to specify a list that is likely to be suitable for computers with different configurations. For example, if you specify `E:\vault;C:\vault` then the Vault Cache would be created in `E:\vault` if that was valid on the user's computer and, if it was not valid, then in `C:\vault`. If none of the locations is valid, the one specified by Root folder is used, if possible. See "Root folder (Exchange Vault Cache setting)" on page 92.
Supported values	■ A text string. A semicolon-separated list of possible locations for the Vault Cache.
Legacy name	OVRootDirectorySearchPath

Search across all indexes (Exchange Vault Cache setting)

Description	If offline Archive Explorer fails to find an item in its index, it can also perform a search across all indexes, which may be slow. This setting controls whether this fallback search is allowed.
Supported values	■ Off (default). Do not allow a search across all indexes. ■ On. Allow the fallback search.
Legacy name	EnableStoreTrawling

Show Setup Wizard (Exchange Vault Cache setting)

Description
: Controls whether the client shows the Vault Cache setup wizard.

  The setup wizard does the following:

  - Summarizes what Vault Cache does and what is about to happen.
  - Asks whether the user wants to start a download automatically after the initial scan has finished. The default is to start the download.

  If the wizard is turned off, Vault Cache waits for the amount of time that is specified in **Pause interval** and then automatically begins looking for items to download.

  See "Pause interval (Exchange Vault Cache setting)" on page 90.

Supported values
: - 0. Do not show the setup wizard.
  - 1 (default). Show the setup wizard.

Legacy name
: OVSetupWizard

Synchronize archive types (Exchange Vault Cache setting)

Description
: Controls what is synchronized by Vault Cache.

Supported values
: - Default mailbox. Synchronize the primary mailbox only.
  - All mailbox archives. Synchronize the primary mailbox archive, and any delegate mailbox archives to which the user has access.
  - All mailbox and shared archives. Synchronize the primary mailbox archive, and any delegate or shared mailbox archives to which the user has access.

Legacy name
: OVSyncArchiveTypes

WDS search auto-enable (Exchange Vault Cache setting)

Description
: Controls whether the Vault Cache search plug-in for Windows Desktop Search is automatically enabled for users.

  This plug-in, which is installed with the Outlook Add-In, enables users to search their Vault Cache using Windows Desktop Search.

Supported values
: - Force off. Disable this feature.
  - Force on. Enable this feature.
  - Keep user's setting. Retain the user's setting for this feature.

Legacy name OVWDSAutoEnable

Virtual Vault advanced settings

The Virtual Vault advanced settings let you control the behavior of Virtual Vault.

Table 5-2 shows the Virtual Vault advanced settings.

Table 5-2 Virtual Vault advanced settings

Advanced setting	Description
Max archive requests per synchronization (Exchange Virtual Vault setting)	Controls the maximum number of archive requests during a Vault Cache synchronization.
Max attempts to archive an item (Exchange Virtual Vault setting)	Specifies how many times Vault Cache tries to archive an item.
Max data archived per synchronization (Exchange Virtual Vault setting)	Controls the maximum amount of data in megabytes that can be uploaded during a Vault Cache synchronization.
Max delete requests per synchronization (Exchange Virtual Vault setting)	Controls the maximum number of delete requests during a Vault Cache synchronization. Any remaining requests are made at the next synchronization.
Max item size to archive (Exchange Virtual Vault setting)	Controls the maximum size in megabytes of an item that can be moved or copied into Virtual Vault.
Max item updates per synchronization (Exchange Virtual Vault setting)	Controls the maximum number of property change requests during a Vault Cache synchronization. Any remaining requests are made at the next synchronization.
Max total size of contentless operations (Exchange Virtual Vault setting)	Controls the maximum total size in megabytes of copy and move operations when items have no content in Vault Cache. This setting only applies to standard Outlook mail types, for example, mail items, calendar items, tasks, and contacts.
Max total size of items to archive (Exchange Virtual Vault setting)	Controls the maximum total size in megabytes of pending archive data in Vault Cache.

Table 5-2 Virtual Vault advanced settings *(continued)*

Advanced setting	Description
Show content in Reading Pane (Exchange Virtual Vault setting)	Controls whether content is shown in the Outlook Reading Pane.
Threshold number of items to trigger synchronization (Exchange Virtual Vault setting)	Specifies the total number of pending archive items in Virtual Vault that triggers automatic Vault Cache synchronization.
Threshold total size of items to trigger synchronization (Exchange Virtual Vault setting)	Specifies the total size in megabytes of pending archive items in Virtual Vault that triggers automatic Vault Cache synchronization.
Users can archive items (Exchange Virtual Vault setting)	Controls whether users can archive items manually using Virtual Vault.
Users can copy items to another store (Exchange Virtual Vault setting)	Controls whether users can copy and move items from a Virtual Vault to another message store.
Users can copy items within their archive (Exchange Virtual Vault setting)	Controls whether users can copy items within their archive.
Users can hard delete items (Exchange Virtual Vault setting)	Controls whether users can hard delete items from Virtual Vault.
Users can reorganize items (Exchange Virtual Vault setting)	Controls whether users can reorganize items in Virtual Vault.

Max archive requests per synchronization (Exchange Virtual Vault setting)

Description

Controls the maximum number of archive requests during a Vault Cache synchronization. Any remaining requests are made at the next synchronization.

When a user stores unarchived items in Virtual Vault, the archive operation does not take place until after the next Vault Cache header synchronization.

No limit or a high value can increase the time that is required to complete a Vault Cache synchronization. This effect is a consideration if the additional load affects the Enterprise Vault server.

Also, until the items that a user has stored in Virtual Vault are archived in the online archive, moved and copied items exist only on the user's computer. You can set two thresholds that trigger automatic Vault Cache synchronization based on the number or total size of pending archive items in Virtual Vault.

See "Threshold number of items to trigger synchronization (Exchange Virtual Vault setting)" on page 101.

See "Threshold total size of items to trigger synchronization (Exchange Virtual Vault setting)" on page 101.

Supported values

- An integer value. The default is 0 (no limit).

Legacy name

OVMaxItemArchivesPerSync

Max attempts to archive an item (Exchange Virtual Vault setting)

Description

Specifies how many times Enterprise Vault tries to archive an item.

The archive operation is tried this number of times before the item is listed in the Virtual Vault Search folder named Could Not Archive.

Supported values

- An integer value. The default is 3.

Legacy name

OVItemArchiveAttempts

Max data archived per synchronization (Exchange Virtual Vault setting)

Description

Controls the maximum amount of data in megabytes that can be uploaded during a Vault Cache synchronization. Any remaining data is uploaded at the next synchronization.

No limit or a high value can increase the time that is required to complete a Vault Cache synchronization. This effect is a consideration if the additional load affects the Enterprise Vault server.

Also, until the items that the user stores in Virtual Vault have been archived in the online archive, moved and copied items exist only on the user's computer. You can set two thresholds that trigger automatic Vault Cache synchronization based on the number or total size of pending archive items in Virtual Vault.

See "Threshold number of items to trigger synchronization (Exchange Virtual Vault setting)" on page 101.

See "Threshold total size of items to trigger synchronization (Exchange Virtual Vault setting)" on page 101.

The value of this setting must be greater than or equal to the value of **Max item size to archive**. If not, the value of **Max item size to archive** is used.

Supported values

- An integer value. The default is 512 (MB). The value 0 specifies no limit.

Legacy name

OVMaxToArchivePerSyncMB

Max delete requests per synchronization (Exchange Virtual Vault setting)

Description

Controls the maximum number of delete requests during a Vault Cache synchronization. Any remaining requests are made at the next synchronization.

Deletion requests use relatively few resources on the Enterprise Vault server.

Supported values

- An integer value. The default is 0 (no limit).

Legacy name

OVMaxItemDeletesPerSync

Max item size to archive (Exchange Virtual Vault setting)

Description

Controls the maximum size in megabytes of an item that can be moved or copied into Virtual Vault.

If this value is similar to the value of **Max total size of items to archive**, a full synchronization can consist of one item.

The **Max item size to archive** value may be used automatically for **Max data archived per synchronization** or **Max total size of items to archive**. It is used if the value of those settings is less than the **Max item size to archive** value.

You can set two thresholds that trigger automatic Vault Cache synchronization based on the number or total size of pending archive items in Virtual Vault.

See "Threshold number of items to trigger synchronization (Exchange Virtual Vault setting)" on page 101.

See "Threshold total size of items to trigger synchronization (Exchange Virtual Vault setting)" on page 101.

Supported values

- An integer value. The default is 256 (MB). The value 0 specifies no limit.

Legacy name

OVMaxMessageSizeToArchiveMB

Max item updates per synchronization (Exchange Virtual Vault setting)

Description

Controls the maximum number of property change requests during a Vault Cache synchronization. Any remaining requests are made at the next synchronization.

Update requests use relatively few resources on the Enterprise Vault server.

Supported values

- An integer value. The default is 0 (no limit).

Legacy name

OVMaxItemUpdatesPerSync

Max total size of contentless operations (Exchange Virtual Vault setting)

Description
Controls the maximum total size in megabytes of copy and move operations when items have no content in Vault Cache. This setting does not apply to documents that are placed directly in the mailbox. It only applies to standard Outlook mail types, for example, mail items, calendar items, tasks, and contacts.

This setting only applies when two or more items with no content are involved in the operation. Retrieval of one item is allowed regardless of its size.

Supported values
- An integer value. The default is 64 (MB). The value 0 specifies no limit.

Legacy name
VVDenyMultiContentlessOpsAboveMB

Max total size of items to archive (Exchange Virtual Vault setting)

Description
Controls the maximum total size in megabytes of pending archive data in Vault Cache.

Pending archive data consists of items that the user has moved or copied into Virtual Vault. These items are pending archive until Vault Cache synchronization has successfully uploaded and archived them.

The value of this setting must be greater than or equal to the value of **Max item size to archive**. If not, the value of **Max item size to archive** is used.

You can set two thresholds that trigger automatic Vault Cache synchronization based on the number or total size of pending archive items in Virtual Vault.

See "Threshold number of items to trigger synchronization (Exchange Virtual Vault setting)" on page 101.

See "Threshold total size of items to trigger synchronization (Exchange Virtual Vault setting)" on page 101.

Supported values
- An integer value. The default is 512 (MB). The value 0 specifies no limit.

Legacy name
OVMaxTotalToArchiveMB

Show content in Reading Pane (Exchange Virtual Vault setting)

Description	Controls whether the content of an item that is selected in Virtual Vault is shown in the Outlook Reading Pane. If the item itself is a document, it is not displayed in the Reading Pane. A message in the Reading Pane advises the user to open the item to read the item's contents.
Supported values	■ Never show content. The Reading Pane always shows only the selected item's header. A banner provides a link to open the original item. ■ When in Vault Cache (default). The Reading Pane shows the selected item's header. If the item is in Vault Cache, it also shows the content. If the content is not shown, a banner provides a link to open the original item. When the Vault Cache content strategy is **Store only items that user opens**, the effect of this value is that the Reading Pane only shows the content of previously opened items. ■ Always show content. The Reading Pane always shows the header and content of the item that is selected in Virtual Vault. **Show content in Reading Pane** can only have the value **Always show content** if the following conditions apply: ■ You have upgraded from an earlier release. ■ In the earlier release, **Show content in Reading Pane** had the value **Always show content**. **Always show content** is not available in the **Modify Setting** dialog. So if **Always show content** is the current value and you change it, you cannot go back to it.
Legacy name	VVReadingPaneContent

Threshold number of items to trigger synchronization (Exchange Virtual Vault setting)

Description

Specifies the total number of pending archive items in Virtual Vault that triggers automatic Vault Cache synchronization.

Pending archive data consists of items that the user has moved or copied into Virtual Vault. These items are pending archive until Vault Cache synchronization has successfully uploaded and archived them.

If you enable this setting, consider how it interacts with other settings, as follows:

- **Max item size to archive** and **Max total size of items to archive** can prevent the user from adding items to Virtual Vault, so that the threshold is never reached.
- **Max archive requests per synchronization** may have a value that is lower than the value of **Threshold number of items to trigger synchronization**. In this case, automatic synchronization may occur but not all the pending archive items are archived.

Supported values

- 0 (default). The threshold is inactive.
- Non-zero integer. The total number of pending archive items in Virtual Vault that triggers automatic Vault Cache synchronization.

Legacy name

VVAutoSyncItemThreshold

Threshold total size of items to trigger synchronization (Exchange Virtual Vault setting)

Description

Specifies the total size in megabytes of pending archive items in Virtual Vault that triggers automatic Vault Cache synchronization.

Pending archive data consists of items that the user has moved or copied into Virtual Vault. These items are pending archive until Vault Cache synchronization has successfully uploaded and archived them.

If you enable this setting, consider how it interacts with other settings, as follows:

- **Max item size to archive** and **Max total size of items to archive** can prevent the user from adding items to Virtual Vault, so that the threshold is never reached.
- **Max data archived per synchronization** may have a value that is lower than the value of **Threshold total size of items to trigger synchronization**. In this case, automatic synchronization may occur but not all the pending archive items are archived.

Supported values
- 0 (default). The threshold is inactive.
- Non-zero integer. The total size in megabytes of pending archive items in Virtual Vault that triggers automatic Vault Cache synchronization.

Legacy name VVAutoSyncItemsSizeThresholdMB

Users can archive items (Exchange Virtual Vault setting)

Description Controls whether users can archive items manually by adding new items to Virtual Vault using standard Outlook actions. Examples of these standard Outlook actions are drag and drop, move and copy, and Rules.

Note: No safety copies exist for these items.

If you disable this setting, users can still create folders if **Users can reorganize items** is enabled.

If you enable this setting, consider setting the thresholds that trigger automatic Vault Cache synchronization.

See "Threshold number of items to trigger synchronization (Exchange Virtual Vault setting)" on page 101.

See "Threshold total size of items to trigger synchronization (Exchange Virtual Vault setting)" on page 101.

Supported values
- Yes (default). Users can archive items manually in Virtual Vault.
- No. Users cannot archive items manually in Virtual Vault.

Legacy name VVAllowArchive

Users can copy items to another store (Exchange Virtual Vault setting)

Description Controls whether users can copy and move items from a Virtual Vault to another message store.

If users can copy or move items out of Virtual Vault and the content is available in Vault Cache, the items are retrieved from Vault Cache.

If the Vault Cache content strategy is **Do not store any items in cache**, the items are retrieved from the online archive. In this case, use the Virtual Vault advanced setting **Max total size of contentless operations** to control the maximum total size of view, copy, and move operations.

Supported values
- Yes (default). Users can copy and move items to another message store.
- No. Users cannot copy and move items to another message store.

Legacy name VVAllowInterStoreCopyAndMove

Users can copy items within their archive (Exchange Virtual Vault setting)

Description Controls whether users can copy items within their archive.

If users can copy items within their archive and the content is available in Vault Cache, the items are retrieved from Vault Cache.

If the Vault Cache content strategy is **Do not store any items in cache**, the items are retrieved from the online archive. In this case, use the Virtual Vault advanced setting **Max total size of contentless operations** to control the maximum total size of view, copy, and move operations.

If you enable this setting, consider setting the thresholds that trigger automatic Vault Cache synchronization.

See "Threshold number of items to trigger synchronization (Exchange Virtual Vault setting)" on page 101.

See "Threshold total size of items to trigger synchronization (Exchange Virtual Vault setting)" on page 101.

Supported values
- Yes. Users can copy items within their archive.
- No (default). Users cannot copy items within their archive.

Legacy name VVAllowIntraStoreCopy

Users can hard delete items (Exchange Virtual Vault setting)

Description Controls whether users can hard delete items from Virtual Vault.

For this setting to take effect, the option **Users can delete items from their archives** must be enabled on the **Archive Settings** tab in the **Site Properties** dialog box.

If you disable this setting, users can still move items to the Deleted Items folder if **Users can reorganize items** is enabled.

Supported values
- Yes (default). Users can hard delete items from Virtual Vault.
- No. Users cannot hard delete items from Virtual Vault.

Legacy name VVAllowHardDelete

Users can reorganize items (Exchange Virtual Vault setting)

Description Controls whether users can reorganize items in Virtual Vault.

This setting can enable users to move items between folders and to create, move, rename, or delete folders.

If folders still exist in the mailbox, users cannot move, rename, or delete them.

Users can hard delete only empty folders, unless **Users can hard delete items** is enabled.

Supported values
- Yes (default). Users can reorganize items in Virtual Vault.
- No. Users cannot reorganize items in Virtual Vault.

Legacy name VVAllowReOrg

Chapter 6

Setting up archiving from public folders

This chapter includes the following topics:

About archiving from public folders

Read this section to find out how to set up archiving from public folders.

In summary, the process of setting up archiving from public folders is as follows:

- Add the Exchange Server computer to your organization, create a vault store, and add a Task Controller service. You created these when setting up archiving from mailboxes.
- Create a public folder archive, if required.
- Create new retention categories, if required.

- Review the public folder policy settings.
- Add an Exchange Public Folder task.
- Add Public Folder Archiving Targets.
- Schedule the Exchange Public Folder task.

In order to set up Public Folder archiving, you must be logged in as an account that has appropriate Exchange Server permissions. The Vault Service account has the correct permissions. Alternatively, set up the account you want to use so that it has the correct permissions. See the "Additional requirements for Exchange Server archiving" section of the *Installing and Configuring* manual for instructions.

The following video demonstrates how to set up and configure archiving from public folders.

http://video.symantec.com/services/player/bcpid292374537001?bckey=AQ~~,AAAABuIiy9k~,I8Bhas-Vwr9zYL9V36WFi86fR_NoePscn&bctid=1913200705001

Note on vault store and partition when setting up archiving from public folders

A vault store and a vault store partition must exist before you enable public folders for archiving. If you want to use Enterprise Vault's optimized single instance storage, ensure that vault store groups, vault stores, and vault store partitions are correctly configured for your requirements.

See the Chapter, *Setting up storage*, in the *Installing and Configuring* manual.

If you auto-enable the target public folders for archiving, Enterprise Vault automatically creates archives for the public folders in the vault store selected for the public folder archiving target.

Creating a public folder archive

You can configure Enterprise Vault to create archives automatically using the auto-enabler. If you are not going to use the auto-enabler, then you need to create the required archives manually. You then assign the archives when configuring the public folder archiving targets. Multiple public folders can share an archive.

To create a public folder archive

1. In the left pane of the Administration Console, expand the **Archives** container.
2. Right-click **Public Folder** and then, on the shortcut menu, click **New > Archive**.

   The New Public Folder Archive wizard starts.
3. Work through the wizard. You will need to provide the following information:
   - The Enterprise Vault Indexing service computer
   - The indexing level to use for any items stored in this archive
   - The billing address

Adding a Public Folder task

This section describes the steps required to add a Public Folder task.

To add a Public Folder 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 computer to which you want to add the Public Folder task.
4. Right-click **Tasks** and then, on the shortcut menu, click **New > Public Folder** Task.

   The New Public Folder Task wizard starts.
5. Work through the wizard. You need to provide the following information:
   - The Exchange Server hosting the public folders.
   - The name for the task.
   - The Enterprise Vault system mailbox to use when connecting to Exchange Server. This can be the same system mailbox used by the Exchange Mailbox task.

About public folder policy settings

The settings that are used during public folder archiving come from the public folder policy that is being used. There is a default public folder policy, Default Exchange Public Folder Policy, which you can edit as required. Alternatively, you

can create further policies as necessary, and set a different policy as the default policy.

Exchange Public Folder policy settings

These settings fall into the following categories:

- General tab (Exchange Public Folder policy setting)
- Archiving Rules tab (Exchange Public Folder policy setting)
- Archiving Actions tab (Exchange Public Folder policy setting)
- Shortcuts tab (Exchange Public Folder policy setting)
- Message Classes tab (Exchange Public Folder policy setting)
- Advanced tab (Exchange Public Folder policy setting)
- Targets tab (Exchange Public Folder policy setting)
- Shortcut Deletion tab (Exchange Public Folder policy setting)

General tab (Exchange Public Folder policy setting)

Table 6-1 describes the settings on this tab, which you can use to override the indexing level for the target public folders.

Table 6-1 General settings

Setting	Default value
Name and Description	The name and description of the policy. These can be changed later if required.
Indexing level	Whether to use Brief or Full indexing when archiving from the target public folders. Phrase searching on content is only available with Full indexing. The indexing level can be set at site, policy and archive level. The setting on the archive will take precedence.

Archiving Rules tab (Exchange Public Folder policy setting)

Table 6-2 describes the settings on this tab, which you can use to choose between size-based archiving and quota-based archiving.

Table 6-2 Archiving Rules 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 set.
Archiving strategy	Archive items based on age of item.	Archiving is based on the period of time since an item was modified. The time period is six months. Setting is locked.
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. See the *Administrator's Guide* for more information.	Not set.

Archiving Actions tab (Exchange Public Folder policy setting)

Table 6-3 describes the settings on this tab, which you can use to control how Enterprise Vault behaves when it archives an item.

Table 6-3 Archiving Actions settings

Setting	Default value
Delete original item after archiving	Original item is deleted from public folder after archiving. Setting is locked, which forces users to use policy setting.
Create shortcut to archived item after archiving	After it has been archived, the item in the public folder is replaced with a shortcut. Setting is locked, which forces users to use policy setting.

Shortcuts tab (Exchange Public Folder policy setting)

Table 6-4 describes the settings on this tab, which you can use to control the size and behavior of Enterprise Vault shortcuts

Table 6-4 Shortcuts settings

Setting	Description	Default value
Include recipient information in shortcut	Whether to store recipient information (To: and Cc: details) in shortcuts. Shortcuts always contain the From and Subject information.	Shortcuts include recipient information.
Shortcut body	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. ■ 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.	None
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 `ShortcutText.txt` file is required if you configure customized shortcuts. You can also use this file to process standard shortcuts for untitled attachments.

See "Using customized shortcuts with Exchange Server archiving" on page 55.

Message Classes tab (Exchange Public Folder policy setting)

The list on this tab shows the classes of items that will be archived when the policy is applied. Select or clear message class check boxes, as required.

If you need to edit the list of available message classes, go to the Message Classes tab of the Directory properties.

Advanced tab (Exchange Public Folder policy setting)

The settings on this tab let you control aspects of public folder archiving, such as how to process items that the task fails to archive. For details of these settings, see the *Administrator's Guide*.

Targets tab (Exchange Public Folder policy setting)

This tab displays the archiving target public folders that will use this policy.

Shortcut Deletion tab (Exchange Public Folder policy setting)

Shortcut deletion does the following:

- Deletes shortcuts that are older than the age you specify on this page.
- Deletes orphaned shortcuts. These are shortcuts to items that have been deleted, typically by a user, from an archive.

Shortcut deletion is performed by the Exchange Public Folder task. When you run the task using Run Now, you can choose a Run mode that includes shortcut processing.

Table 6-5 Shortcut Deletion settings

Setting	Description	Default value
Delete shortcuts in folders	Setting this makes Enterprise Vault delete shortcuts that are older than the age you specify. This does not affect the corresponding archived items. Users can still search for the archived items. For example, you could choose to delete all shortcuts older than 12 months, but retain archived items for several years.	Not selected

Table 6-5 Shortcut Deletion settings *(continued)*

Setting	Description	Default value
Delete orphaned shortcuts	This setting makes Enterprise Vault delete shortcuts in public folders if the corresponding archived item has been deleted. If you use shortcuts that 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 will regain space in the Exchange Server store.	Not selected

Adding public folder archiving targets

An Exchange Public Folder task archives public folder targets. A public folder target is a single public folder hierarchy, starting from its root path and working down. You can have a few, or many Exchange Public Folder tasks, as required. Each Exchange Public Folder task can process multiple public folder targets.

The Exchange Public Folder task processes all folders beneath each target's root path, except for folders that are processed by another Exchange Public Folder task and folders that have had their Enterprise Vault properties changed to stop the folder from being archived.

You can add a public folder target with a root path that is higher up a public folder hierarchy than the root path of an existing public folder target. You cannot add one with a lower root path.

If you use Outlook to view the properties of the public folder, you can copy the folder path to the clipboard and then paste it in as the root path for the target public folder.

There are several ways to add public folders: manually or automatically.

- Manual (standard) method. You select the public folder and the archive that is to be used for it. The same archive is used for the folder and its subfolders.
- Automatic method. You add an Enterprise Vault "auto-enabler" that then enables folders that are immediately beneath the folder you specify. These folders and their subfolders are all enabled for archiving.

  By default, a separate archive is automatically created for each folder at this level.

For example, if you add an auto-enabler to `\myPublic Folder`, then new archives will be created for `\myPublic Folder\Finance` and `\myPublic Folder\Property`. No archive will be created for `\myPublic Folder\Property\Commercial` because that folder will use the same archive as its parent (`\myPublic Folder\Property`).
Alternatively, you can select an existing archive to use.
If new folders are added later, they are automatically archived too.

Manual (standard) method of adding public folder archiving targets

This section describes the manual method of adding a public folder. You select the public folder and the archive that is to be used for it. The same archive is used for the folder and its subfolders.

To add a public folder archiving target

1. In the left pane of the Administration Console, expand the hierarchy until **Targets** is visible.
2. Expand **Targets**.
3. Expand **Exchange**.
4. Expand the domain that contains the Exchange Server that hosts the folder you want to add.
5. Expand **Exchange Server**.
6. Expand the Exchange Server that has the public folder you want to add.
7. Right-click **Public Folder** and, on the shortcut menu, click **New** and then **Public Folder**.

   The **New Public Folder** wizard starts.
8. Work through the wizard. You will need to provide the following information:
   - The path to the top-level public folder to be archived
   - The Exchange Public Folder task to use
   - The Exchange Public Folder policy to assign
   - The retention category to use
   - The archive to use

Automatic method of adding public folder archiving targets

This section describes the automatic method of adding a public folder. You add an Enterprise Vault "auto-enabler" that then enables folders that are immediately

beneath the folder you specify. These folders and their subfolders are all enabled for archiving.

By default, a separate archive is automatically created for each folder at this level.

To add a public folder auto-enabler

1. In the left pane of the Administration Console, expand the hierarchy until **Targets** is visible.
2. Expand **Targets**.
3. Expand **Exchange**.
4. Expand the domain that contains the Exchange Server that hosts the folder you want to add.
5. Expand **Exchange Server**.
6. Expand the Exchange Server that has the public folder you want to add.
7. Right-click **Public Folder** and, on the shortcut menu, click **New** and then **Public Folder Auto-Enabler**.

   The **New Public Folder Auto-Enabler** wizard starts.
8. Work through the wizard. You will need to provide the following information:
   - The path to the top-level public folder to be archived.
   - Whether to archive items in the root folder. If yes, you can specify the archive to use.
   - The Exchange Public Folder policy to use.
   - The Exchange Public Folder task to use.
   - The retention category to use.
   - The vault store to create the new archives in.

Applying archiving settings to public folders

The default public folder archiving settings are set on each public folder. These are the settings that you specified on the Archiving Rules and Archiving Actions pages of Exchange Public Folder Policy properties.

Using the Enterprise Vault User Extensions for Outlook, only users with Owner access to public folders can customize these settings.

To apply archiving settings to a public folder

1. View the public folder using an Outlook client that has the Enterprise Vault User Extensions installed.
2. Right-click the public folder and click **Properties** on the shortcut menu.

   The properties for the public folder are displayed.
3. Click the **Enterprise Vault** tab.

   The Enterprise Vault property page shows the folder currently has no settings.
4. Click **Change**.

   The Change Enterprise Vault properties dialog box is displayed.
5. Select the settings you want to apply.

   Users will be able to apply custom settings to a public folder only if the settings on the **Archiving Actions** page of the public folder policy's properties are not locked.
6. Once you have finished applying settings, click **OK**.

Scheduling the Public Folder task

All Public Folder tasks run according to a schedule that you set.

Each Exchange Public Folder task can be set to run according to the following:

- The schedule, which is defined on the Site Schedule page of site properties. By default all archiving tasks run according to this schedule.
- Its own schedule, defined on the task's Schedule property page.

To modify the schedule for a single task

1. In the left pane of the Administration Console, expand the hierarchy until the **Enterprise Vault Servers** container is visible.
2. Expand the **Enterprise Vault Servers** container.
3. Expand the computer that is running the task that you want to modify.
4. Click **Tasks**.
5. In the right pane, double-click the task that you want to modify.
6. Click the **Schedule** tab.
7. Modify the schedule as required.

To modify the schedule for all archiving tasks

1. In the Administration Console, expand the contents of the scope (left) pane until the Enterprise Vault site is visible.
2. Right-click the Enterprise Vault site and select **Properties**. The site properties dialog is displayed.
3. Click the **Site Schedule** tab.
4. Modify the schedule as required.

Note on removing Public Folder targets

Be careful when removing lower-level public folder targets. When you remove a public folder target that is below another public folder target, the folders are archived to the same archives as before. In this case, if you want to prevent public folders from being archived, change the settings for the lower-level public folders so that they are not archived.

If you want to remove a public folder target, use the Administration Console to do so because this removes the marker that Enterprise Vault places on the root path folder.

For example, this is important if you are running a pilot installation of Enterprise Vault that has an Exchange Public Folder task on a computer that you later decide to remove. If you merely take away the Exchange Public Folder task computer, the marker is not removed and so you cannot add another public folder target with that root path.

Chapter 7

Setting up archiving of journaled messages

This chapter includes the following topics:

Before you start setting up archiving of journaled messages

Before an Enterprise Vault Exchange Journaling task can be configured, you must have configured the Exchange Server to direct all mail to one or many journal mailboxes.

Vault store group, vault store, and partition when archiving journaled messages

All items from a journal mailbox need to be archived. If you are configuring both Exchange journal archiving and Exchange mailbox archiving, you can take advantage of Enterprise Vault's optimized single instance storage. Ensure that vault store groups, vault stores, and vault store partitions are correctly configured for your requirements.

See the Chapter, *Setting up storage*, in the *Installing and Configuring* manual.

Creating a journal archive

This section describes how to create a Journal archive. You must have already created a journal vault store and partition before you can create a Journal archive.

To create a journal archive

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

   The **New Journal Archive** wizard starts.
4. Work through the wizard. When prompted to select a vault store, choose the one that you just created.

   You will need to provide the following information:

   - The vault store in which to create the archive
   - The required Indexing service
   - The indexing level
   - A billing account

Adding permissions to the 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 multiple 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	Users can archive items in the archive. The owner of the journal mailbox must have at least write access to the archive. This enables items to be archived from the journal mailbox.
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 **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.

Adding an Exchange Journaling task

This section describes how to add an Exchange Journaling task.

To add an Exchange Journaling task

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

   The **New Exchange Journaling Task** wizard starts.
5. Work through the wizard. You will need to provide the following information:
   - The Exchange Server hosting the journal mailbox.

- Name for the task.
- Enterprise Vault system mailbox to use when connecting to Exchange Server. This can be the same system mailbox used by the Exchange Mailbox task.

Reviewing the journaling policy settings

The settings that used during Exchange Server journal mailbox archiving come from the Exchange Journaling policy that is being used. There is a default Exchange Journaling policy that you can edit as required. Alternatively, you can create further policies as necessary, and set a different policy as the default policy.

To review the default Exchange Journaling policy settings

1. In the left pane of the Administration Console, expand the **Policies** container.
2. Expand the **Exchange** container and click **Journaling**.
3. In the right pane, double-click **Default Exchange Journaling Policy**.

   The properties of the policy appear.
4. Check the settings on the **Advanced** tab, and change them as necessary.

   You can click each setting to see a description of what it controls. The settings are described in the online help in the Administration Console and in the *Administrator's Guide*.

Adding an Exchange Server journal mailbox as a target

This section describes how to add an Exchange Server journal mailbox as an archiving target.

Note: When you have completed the configuration of Exchange Server journal archiving, Enterprise Vault directly targets the journal mailbox. For this reason, if you need to move the journal mailbox to a different Exchange server in the same Exchange organization, there is no need to reconfigure journal archiving.

To add an Exchange Server journal mailbox as a target

1. In the left pane of the Administration Console, expand **Targets**.
2. Expand the domain that contains the Exchange Server with the journal mailbox you are adding.
3. Expand **Exchange Server**.

4 Expand the Exchange Server.

5 Right-click **Journal Mailbox** and, on the shortcut menu, click **New > Journal Mailbox**.

The New Journal Mailbox wizard starts.

6 Work through the wizard. You will need to provide the following information:

- The name of the Exchange journal mailbox to archive
- The Exchange Journaling task to use
- The Exchange Journaling policy to apply
- The retention category to apply to archived items
- The archive to use

Starting the Journaling task

This section describes how to start an Exchange Journaling task.

To start the Journaling task

1 In the left pane of the Administration Console, expand the Enterprise Vault site hierarchy until **Enterprise Vault Servers** container is visible.

2 Expand the **Enterprise Vault Servers** container.

3 Expand the name of the computer that has the Exchange Journaling task you want to start.

4 Click tasks.

5 In the right pane, right-click the task and, on the shortcut menu, click **Start**.

You do not normally need to start the Exchange Journaling task in this manner: by default, the task starts automatically when the Task Controller service is started.

6 The task runs continually, archiving items immediately from the Exchange Server journal mailbox. Items are deleted from the mailbox as they are archived and no shortcuts are created.

What to do after setting up archiving of journaled messages

It is important that you monitor journal mailboxes to make sure that items are being archived promptly. For details of how to monitor the mailboxes, see the *Administrator's Guide*.

You can customize the Exchange Server journal mailbox so that items are archived to different archives and with different retention categories. See the *Administrator's Guide* for details.

Chapter 8

Envelope Journaling

This chapter includes the following topics:

About Enterprise Vault and Exchange Server journal reports

Envelope Journaling is used by Exchange Server to capture the complete recipient list of a message. The Enterprise Vault Exchange Journaling task automatically recognizes an envelope message and processes it accordingly.

Each journaled message has two parts:

- A journal report (P1 envelope message)
- The original message (P2 message)

In the body of the journal report there may be uncategorized recipients, in addition to the TO, CC and BCC recipients. This happens when there is no way of discovering the original category of such recipients; for example, when a report is sent over SMTP by Exchange Server 2007. Enterprise Vault classifies such recipients as Undisclosed recipients.

You can search for Undisclosed recipients using the Recipient field option on the advanced page of the Enterprise Vault browser search. (The search index property, RNDN, is used for Undisclosed recipients.)

Undisclosed recipients are recognized in Compliance and Discovery Accelerator searches.

The journal report is stored with the original message in the message saveset, but Enterprise Vault does not currently support the retrieval of journal reports from the archive.

This section describes how Enterprise Vault Journaling task handles the different Exchange Server journal reports.

How Enterprise Vault handles Exchange 2000 and Exchange Server 2003 journal reports

When the Enterprise Vault Journaling task receives an Exchange 2000 or Exchange Server 2003 journal report:

- The complete list of recipients is extracted from the journal report contents.
- This list is compared with recipients in the header of the attached message. Recipients found in the journal report but not the attached message header are classed as Undisclosed recipients.
- If a BCC recipient is also in the TO or CC fields and the message arrives over SMTP, then Enterprise Vault will store the recipient in the TO or CC field but not in the Undisclosed field.
- When messages are addressed to Alternate recipients and BCC recipients and sent over SMTP, these recipients will be included in the body of the journal report but not in the message header of the original message. As there is no way of discovering the original category of such recipients, Enterprise Vault will store them as Undisclosed recipients.
- When a message is redirected to an Alternate recipient (that is, forwarded to the Alternate recipient without actually being delivered to the original recipient), then the message headers will show the originally intended recipient and not the final (Alternate) recipient. Both recipients will be indexed, even though the originally intended recipient never actually received the message. This is because it is not possible to determine from the journal report that the original recipient was skipped.
- If an Alternate recipient also appears as an originally intended recipient (TO or CC), then the recipient will not be stored as an Undisclosed recipient.
- A copy of the journal report, complete with original message attached, is passed to any external filters (including the Compliance Accelerator Journaling Connector, if configured).
- The journaling task cannot archive a message from the journal mailbox if it cannot find the message body or the Message-ID, Recipients, and Sender tags in the journal report. For example, these can be stripped by antivirus applications that find suspicious messages.
- The journaling task copies any journal report that it cannot process to the folder Enterprise Vault Journaling Service/Failed To Copy.

How Enterprise Vault handles Exchange Server 2007 format journal reports

When the Enterprise Vault Journaling task receives an Exchange Server 2007 format journal report:

- The list of recipients is extracted from the journal report contents.
- This list is not compared with recipients in the header of the attached message.
- Uncategorized recipients found in the journal report body are classed as Undisclosed recipients.
  For example, recipients of messages that are sent over SMTP will be included in the recipient list in the journal report body but will not be categorized.
- A copy of the journal report, complete with original message attached, is passed to any external filters (including the Compliance Accelerator Journaling Connector, if configured).
- The journaling task cannot archive a message from the journal mailbox if it cannot find the message body or the Message-ID, Recipients, and Sender tags in the journal report. For example, these can be stripped by antivirus applications that find suspicious messages.
- The journaling task copies any journal reports that it cannot process to the folder Enterprise Vault Journaling Service/Failed To Copy.

How Enterprise Vault handles Exchange Server 2013 and 2010 format journal reports

When the Enterprise Vault Journaling task receives an Exchange Server 2013 and 2010 format journal report:

- The list of recipients is extracted from the journal report contents.
- This list is not compared with recipients in the header of the attached message.
- Uncategorized recipients found in the journal report body are classed as Undisclosed recipients.
  For example, recipients of messages that are sent over SMTP will be included in the recipient list in the journal report body but will not be categorized.
- A copy of the journal report, complete with original message attached, will be passed to any external filters (including the Compliance Accelerator Journaling Connector, if configured).
- The journaling task cannot archive a message from the journal mailbox if it cannot find the message body or the Message-ID, Recipients, and Sender tags

in the journal report. For example, these can be stripped by antivirus applications that find suspicious messages.

- The journaling task copies any journal reports that it cannot archive to the folder Enterprise Vault Journaling Service/Failed To Copy.

About support for Exchange Server 2013 and 2010 journal report decryption

If journal report decryption is configured on Exchange Server 2013 and 2010, then two messages are attached to the journal report – the original RMS-protected message and a clear text version. The advanced setting in the Enterprise Vault Exchange Journaling policy, **ClearText copies of RMS Protected items**, lets you select whether Enterprise Vault uses the clear text message or the RMS-protected message as the primary message during archiving. Note that after Enterprise Vault has archived a message, you cannot change the message version used as the primary message.

Enterprise Vault stores both versions of the message and the journal report in the message saveset. However, Enterprise Vault does not currently support the retrieval of the secondary message or the journal report from the archive.

By default, Enterprise Vault uses the clear text message as the primary message. The following action is taken when the clear text message is used as the primary message:

- The clear text message is returned in response to retrieval requests from Enterprise Vault clients and Symantec Discovery Accelerator.
- Enterprise Vault indexes the content and properties of the clear text message, and any attachments that are not encrypted.
- Standard Enterprise Vault Exchange journal filters work with clear text messages.

See the online help in the Administration Console and in the *Administrator's Guide* for a full description of this setting.

Chapter 9

Setting up the Enterprise Vault Office Mail App

This chapter includes the following topics:

About Microsoft Office Mail Apps

A Microsoft *app for Office* is a web page that is hosted inside an Office client application. In addition to the capabilities of a web page, an app for Office can interact with the Office application and with the user's content.

Microsoft *Office Mail Apps* require Exchange Server 2013. They display next to the currently selected item in Outlook 2013 and Outlook Web App (OWA) for Exchange 2013.

For detailed information about Office Mail Apps, see the Microsoft website.

About the Enterprise Vault Office Mail App

The Enterprise Vault Office Mail App provides Enterprise Vault features in the following mail clients for mailboxes that are hosted on Exchange 2013:

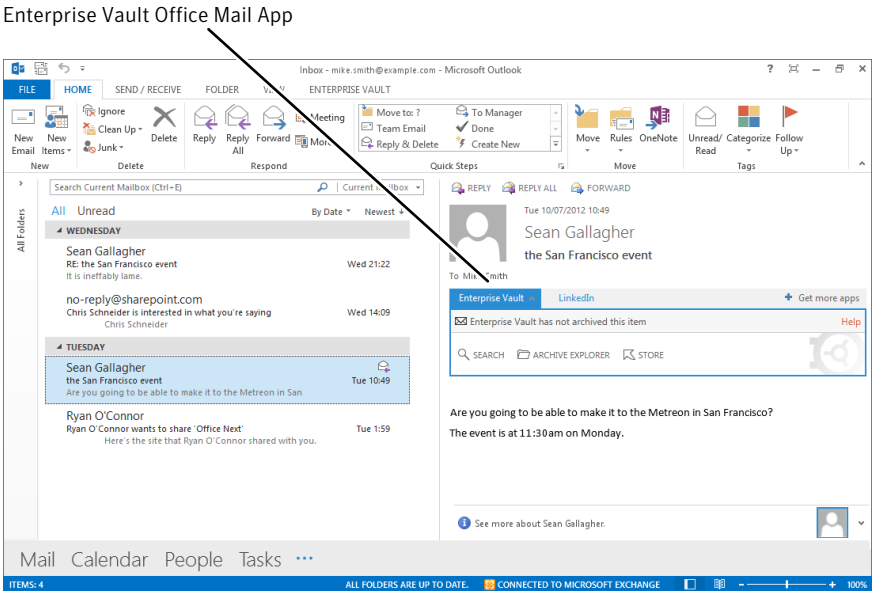
- Outlook 2013. You can enable the Office Mail App in Outlook 2013 whether or not the Outlook Add-In is installed.
- OWA 2013. The Office Mail App is the only Enterprise Vault client available for OWA 2013 users.

The Enterprise Vault Office Mail App has the following advantages over previous Enterprise Vault integrations with Exchange Server and OWA:

- There is no installation impact on Exchange servers. The Office Mail App requires deployment to users, for which we recommend that you use Microsoft PowerShell commands in the Exchange Management Shell.
  See "Deploying the Enterprise Vault Office Mail App" on page 133.
- No client installation is required to enable the Office Mail App for either Outlook or OWA.

For information about operating system support for use of the Office Mail App on tablets and phones, see the Enterprise Vault *Compatibility Charts* at http://www.symantec.com/docs/TECH38537.

The following figure shows the Office Mail App in Outlook 2013:



The following video gives a short introduction to the Office Mail App.

http://video.symantec.com/services/player/bcpid292374537001?bckey=AQ~~,AAAABuIiy9k~,I8Bhas-Vwr9zYL9V36WFi86fR_NoePscn&bctid=2098914278001

Enterprise Vault Office Mail App features

The Enterprise Vault Office Mail App provides a different set of features from the following Enterprise Vault clients:

- The Enterprise Vault Outlook Add-In
- Enterprise Vault integrations with Exchange Server 2010, OWA 2010, and earlier versions

Table 9-1 describes the differences. You may find that this information is useful in deciding whether to make the Office Mail App, the Outlook Add-In, or both available to Outlook 2013 users. The information applies to the Office Mail App in both Outlook 2013 and OWA 2013, unless it states otherwise.

Table 9-1 Differences between the Office Mail App and other Enterprise Vault clients

Features	Differences
Open, reply to, and forward from shortcut	Users cannot open, reply to, or forward an archived item directly from a shortcut. They have to view the item from the Office Mail App and then perform the action.
Actions on multiple selections of items	The Office Mail App allows actions on a single selected item, not on multiple selections.
Availability for all item types that can be archived	The Office Mail App is available only when users have selected a mail item, calendar item, or meeting request. To find an archived item of another type or one with no shortcut, users can open an Enterprise Vault search application or Archive Explorer.
Support for Outlook and OWA deletion of archived items	The Office Mail App does not support deletion of archived items using the normal Outlook or OWA Delete options; for example, by selecting a shortcut and pressing the Delete key. To perform the Delete action, users have to use the Office Mail App.
Availability for draft items	The Office Mail App is not available for draft items.
Availability for public folders	The Office Mail App is not available for items in public folders.
Enterprise Vault support in OWA Light client	The Office Mail App is only available in the OWA 2013 Premium client. The OWA 2013 Light client does not support Office Mail Apps.

The following video demonstrates how to use some of the Office Mail App features.

http://video.symantec.com/services/player/bcpid292374537001?bckey=AQ~~,AAAABuIiy9k~,I8Bhas-Vwr9zYL9V36WFi86fR_NoePscn&bctid=2098938372001

Enterprise Vault Office Mail App policy settings and options

The Enterprise Vault Office Mail App advanced setting **Availability** in the Exchange desktop policy controls the availability of the Office Mail App. You can

choose whether the Office Mail App is available for Outlook, or OWA, or both. Other advanced settings let you control some details of Office Mail App behavior.

For details of the Office Mail App advanced settings, see the *Administrator's Guide*.

The settings on the Exchange Desktop policy Options tab control the availability of the Office Mail App options, with the following exceptions:

- **Expiry Report** setting on the Options tab: the Office Mail App does not include an Expiry Report option.
- **Help** setting on the Options tab: the Office Mail App **Help** option is always available.
- **Shortcut Deletion** setting on the Options tab: this option does not apply to the Office Mail App.

For information about the settings on the Exchange Desktop policy Options tab, see the Administration Console help.

Table 9-2 describes the Enterprise Vault options that are available in the Office Mail App.

Table 9-2 Enterprise Vault Office Mail App options

Enterprise Vault Office Mail App options	Notes
View: view an archived item from its shortcut	The Office Mail App **View** option is always available. The Office Mail App advanced policy setting **Behavior of Mail App Bar** controls how the Office Mail App opens items. You can specify that clicking the Enterprise Vault tab in the Office Mail App bar does both of the following: ■ Shows the available options for a shortcut ■ Automatically opens the item in a new window The default is to show the Office Mail App options without automatically opening the item.
Store: archive an item manually	The Office Mail App advanced policy setting **Mode** lets you choose an Office Mail App mode. Light mode is the default. In Light mode, Enterprise Vault archives the item with the default retention category for the mailbox folder that contains the item. In Full mode, users can select a retention category when they archive an item manually.

Table 9-2 Enterprise Vault Office Mail App options *(continued)*

Enterprise Vault Office Mail App options	Notes
Restore: restore an archived item	Users can restore an archived item from its shortcut. If a user opens an archived item with the Office Mail App **View** option, the **Restore** option is not available while the item is open.
Delete: delete an archived item	As in other Enterprise Vault clients, the Office Mail App **Delete** option deletes the selected shortcut and the archived item.
Cancel: cancel an action	The Office Mail App **Cancel** option appears temporarily when an action that users can cancel is in progress.
Search: open an Enterprise Vault search application	The Office Mail App advanced policy setting **Search Application** controls which Enterprise Vault search application opens when users click **Search**. The default is Enterprise Vault Browser Search. The alternative is Enterprise Vault Integrated Search. If you specify Integrated Search, the **Search** option is hidden from OWA users in browsers other than Internet Explorer.
Archive Explorer: open Archive Explorer	The Office Mail App **Archive Explorer** option is hidden from OWA users in browsers other than Internet Explorer.

Initial configuration of HTTPS for use of the Enterprise Vault Office Mail App

The following initial configuration is required for use of the Enterprise Vault Office Mail App.

You must configure HTTPS with a suitable certificate on Enterprise Vault servers that serve the Enterprise Vault Office Mail App. Office Mail Apps must be served using Secure Sockets Layer (SSL).

We recommend that you obtain a certificate from a certification authority. Otherwise, if the certificate is from another source, a browser may display a warning and require the user to accept the certificate. Prompting for acceptance of a certificate is not available in the Office Mail App. The result is that the user sees a blank window in the Office Mail App.

You do not have to configure Enterprise Vault to use HTTPS at site level.

See the following technical note for instructions on how to request and apply an SSL certificate:

http://www.symantec.com/docs/HOWTO83452

Deploying the Enterprise Vault Office Mail App

The Enterprise Vault Office Mail App does not appear in Outlook 2013 or OWA 2013 by default. It requires deployment to users.

We recommend that you use Microsoft PowerShell commands in the Exchange Management Shell to deploy the Office Mail App.

The main methods are as follows:

- Deploy the Office Mail App for each user who is enabled for Enterprise Vault.
- Deploy the Office Mail App at organization level.

  If you consider deploying the Office Mail App at organization level, note the following:

  - All users will see the Office Mail App in Outlook 2013 and OWA 2013, including users who are not enabled for Enterprise Vault. If a user is not enabled for Enterprise Vault, a message in the Office Mail App says that it is not available.
  - The same Enterprise Vault server is used for Office Mail App requests from all users, which could affect the overall performance of that server.

The following video demonstrates how to use the PowerShell commands to deploy the Office Mail App.

http://video.symantec.com/services/player/bcpid292374537001?bckey=AQ~~,AAAABuIiy9k~,I8Bhas-Vwr9zYL9V36WFi86fR_NoePscn&bctid=2098895031001

About the PowerShell commands for Office Mail Apps

The following Microsoft PowerShell commands are available for managing Office Mail Apps:

`Get-App`	Returns information about the installed Office Mail Apps.
`New-App`	Deploys an Office Mail App.
`Remove-App`	Removes the specified Office Mail App.
`Disable-App`	Disables a specific Office Mail App for a specific user.

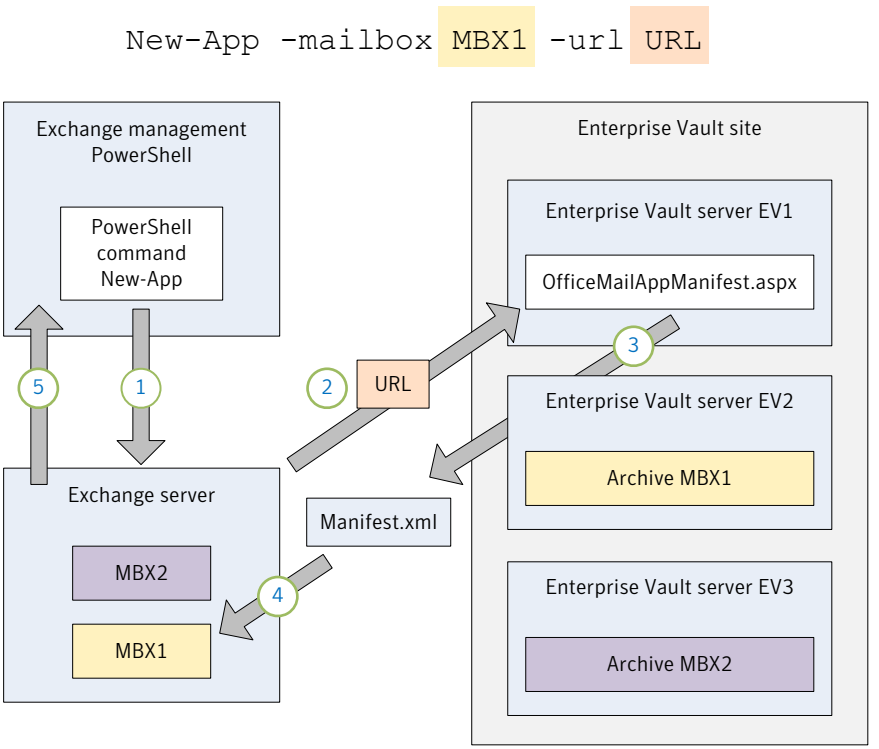
`Enable-App`	Enables an Office Mail App for a specific user.
`Set-App`	Sets configuration properties on an Office Mail App.

About deploying the Office Mail App with the New-App command

Figure 9-1 shows the process when you use the `New-App` command to deploy the Enterprise Vault Office Mail App for an individual user. A simplified representation of the command is shown at the top of the figure.

The process is similar when you deploy the Office Mail App for a whole organization. You still specify only one mailbox in the `New-App` command. This mailbox must be one whose archive is stored on the Enterprise Vault server to which you want all organization level requests to be sent. In this case the Exchange Server configures the manifest file for all the mailboxes in the organization. The result is that a single Enterprise Vault server has to serve the Office Mail App to all users.

Figure 9-1 New-App command overview



In the figure, the numbered stages are as follows:

1. You run the PowerShell command `New-App` in the Exchange Management Shell.

   The command specifies the following:

   - A mailbox (MBX1) that is enabled for archiving and that you want to enable for the Office Mail App.
   - The URL of the `OfficeMailAppManifest.aspx` page.

     The server that is specified in the URL can be any Enterprise Vault server in your site. In this example, the URL specifies a server named EV1.

     The URL for `OfficeMailAppManifest.aspx` can use the HTTP or HTTPS protocol, depending on the protocol that is enabled in IIS on the Enterprise Vault server.

2. The Exchange server sends a request to Enterprise Vault server EV1 to configure a manifest file.
3. On EV1, the `OfficeMailAppManifest.aspx` page generates a manifest file for MBX1 and sends it to the Exchange server. The manifest file contains the Office Mail App settings for MBX1. The settings include the URL from which the Office Mail App will be loaded, which in this example is on Enterprise Vault server EV2 because the MBX1 archive is stored on EV2.
4. The manifest file is associated with MBX1 on the Exchange server.
5. The `New-App` command completes.

About New-App command parameters for the Enterprise Vault Office Mail App

In the `New-App` command, you must specify the Active Directory attribute LegacyExchangeDN with the `OfficeMailAppManifest.aspx` page. You can also specify other parameters, if required. The `OfficeMailAppManifest.aspx` page supports the following query string parameters:

LegacyMbxDN	Mandatory. The Active Directory attribute LegacyExchangeDN for the user.
OfficeAppName	Optional. The name of the Office Mail App in the Office Mail App Bar. The name defaults to Enterprise Vault.
BaseURL	Optional. The URL of the `EnterpriseVault` virtual directory on the server that is to be used to load the Office Mail App. You can set this value for an external URL or a specific Enterprise Vault server if required.

The manifest file is not generated if invalid values are supplied. The typical causes are as follows:

- The mailbox is not enabled for archiving.
- The BaseURL value is not valid.

If the manifest file is not generated, the `New-App` command may return an error message of the following type:

```
The app couldn't be downloaded. Error message: The remote server
returned an error: (500) Internal Server Error.
```

The Office Mail App troubleshooting information includes an example script that returns a more detailed error message when the manifest file is not created.

See "The Enterprise Vault Office Mail App manifest file is not created" on page 149.

Deploying the Enterprise Vault Office Mail App for an individual user

To deploy the Enterprise Vault Office Mail App for an individual user, use the PowerShell command `New-App` in the Exchange Management Shell.

See "About deploying the Office Mail App with the New-App command" on page 134.

Note: You must log in to the Exchange server using an account that is assigned the management role User Options. By default, members of the "Organization Management" role group are assigned this role.

The following example shows how to use the `New-App` command to enable an individual user for the Office Mail App.

The backtick character (`) is the PowerShell line-continuation character.

```
$Mbx = get-mailbox "mailbox"

New-App -mailbox $Mbx.LegacyExchangeDN -Url `
    ("http://EV_server/EnterpriseVault/OfficeMailAppManifest.aspx?LegacyMbxDn=" +
    $Mbx.LegacyExchangeDN)
```

where:

- *mailbox* is the name of a mailbox that is enabled for archiving, and that you want to enable for the Office Mail App.
- *EV_server* is the name of any Enterprise Vault server in your site. This Enterprise Vault server is not necessarily the one that is used to load the Office

Mail App. The Enterprise Vault server that is used to load the Office Mail App is the server where the archive for the specified mailbox is located. The name of the correct Enterprise Vault server for the specified mailbox is returned within the manifest file.

Users may access the Enterprise Vault server externally, with no direct access. In this case, the manifest file must point to the URL of the server that provides external access. The same server would also be used for internal access. For example, the server may be a Microsoft Forefront Threat Management Gateway (TMG) server.

The following example shows how to use the BaseURL parameter with the `OfficeMailAppManifest.aspx` page to configure the manifest file to point to a server that provides external access.

The backtick character (`) is the PowerShell line-continuation character.

```
$Mbx = get-mailbox "mailbox"

New-App -mailbox $Mbx.LegacyExchangeDN -Url `
    ("http://EV_server/EnterpriseVault/OfficeMailAppManifest.aspx?LegacyMbxDn=" +
    $Mbx.LegacyExchangeDN + "&BaseURL=https://external_access_server/EnterpriseVault")
```

where:

- *mailbox* is the name of a mailbox that is enabled for archiving, and that you want to enable for the Office Mail App.
- *EV_server* is the name of any Enterprise Vault server in your site. This Enterprise Vault server is not necessarily the one that is used to load the Office Mail App. The Enterprise Vault server that is used to load the Office Mail App is the server that is specified in the BaseURL parameter.
- *external_access_server* is the name of the server that provides external access.

See "About configuring Threat Management Gateway 2010 for Outlook 2013 and OWA 2013" on page 217.

Deploying the Enterprise Vault Office Mail App for multiple users

The following example PowerShell script shows how to deploy the Enterprise Vault Office Mail App for multiple users. All the users must be within a single organizational unit.

A script of this type may take some time to complete for a large number of users. The speed at which the script enables users will vary from system to system, depending on the particular environment in which it is run.

Note: You must log in to the Exchange server using an account that is assigned the management role User Options. By default, members of the "Organization Management" role group are assigned this role.

The backtick character (`) is the PowerShell line-continuation character.

```
function EVDeploy([string]$evserver, [string]$ou) {
Get-Mailbox -OrganizationalUnit $ou |
  ForEach-Object {
    If (New-App -mailbox $_.LegacyExchangeDN -ErrorAction:Ignore -Url `
        ("http://" + $evserver +
"/EnterpriseVault/OfficeMailAppManifest.aspx?LegacyMbxDn=" +
$_.LegacyExchangeDN)) {
      Write-host ("Deployed to: " + $_.DisplayName);
    } Else {
      If (Get-App -mailbox $_.LegacyExchangeDN `
                  -Identity 0cc6d075-e610-4b8a-90c6-1460e6d4d710 `
                  -ErrorAction:Ignore) {
        Write-host ("Already deployed to: " + $_.DisplayName);
      } Else {
        Write-host ("Could not deploy to: " + $_.DisplayName);
      };
    };
  };
};

EVDeploy "EV_server" "org_unit"
```

where:

- *EV_server* is the name of any Enterprise Vault server in your site. This Enterprise Vault server is not necessarily the one that is used to load the Office Mail App. The Enterprise Vault server that is used to load the Office Mail App is the server where the archive for the specified mailbox is located. The name of the correct Enterprise Vault server for the specified mailbox is returned within the manifest file.
- *org_unit* is the organizational unit that contains the users for whom you want to deploy the Office Mail App.

Note: *EV_server* and *org_unit* in the final line of this script are the only variables that you need to replace.

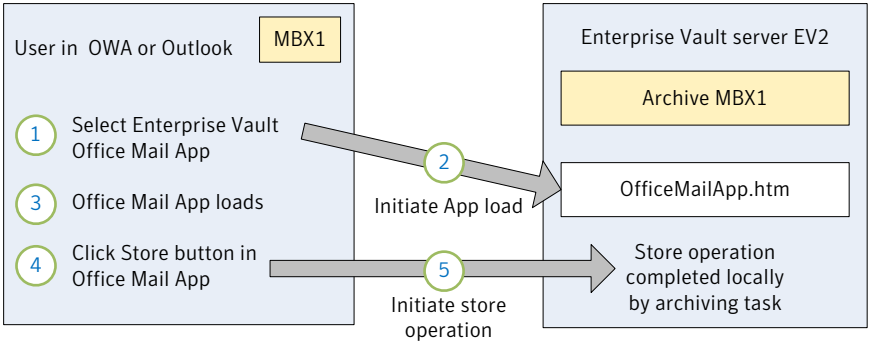
The GUID identifies the Enterprise Vault Office Mail App, and does not change.

About the Enterprise Vault Office Mail App after deployment for an individual user

Figure 9-2 shows what happens when:

- The Office Mail App has been deployed for an individual user.
- The user selects the Office Mail App and stores an item.

Figure 9-2 Office Mail App after deployment for an individual user



In the figure, the numbered stages are as follows:

1. The user of mailbox MBX1 selects the Office Mail App in OWA or Outlook.
2. A request to load the Office Mail App is sent to `OfficeMailApp.htm` on Enterprise Vault server EV2, where the archive for MBX1 is stored.
3. The Office Mail App loads.
4. The user selects an unarchived item and clicks **Store**.
5. The Office Mail App sends a request to store the item to EV2. On EV2, Enterprise Vault stores the item in the archive MBX1.

Each Enterprise Vault server only serves the Office Mail App to users whose archives are stored on that server.

Deploying the Enterprise Vault Office Mail App for an organization

In an Exchange environment where archiving is to a single Enterprise Vault installation, you may decide to deploy the Office Mail App at organization level. The advantage of deployment at organization level is that it is simpler and quicker than deployment to individual mailboxes.

However, if you consider deploying the Enterprise Vault Office Mail App at organization level, note the following:

- All users will see the Office Mail App in Outlook 2013 and OWA 2013, including users who are not enabled for Enterprise Vault. If a user is not enabled for Enterprise Vault, a message in the Office Mail App says that it is not available.
- The same Enterprise Vault server is used for Office Mail App requests from all users, which could affect the overall performance of that server.
  If this Enterprise Vault server becomes unavailable, all requests to load the Office Mail App will fail. You could mitigate this impact and other performance impacts by using a round robin DNS load-balancing solution.

To deploy the Enterprise Vault Office Mail App at organization level, use the PowerShell command `New-App` in the Exchange Management Shell.

See "About deploying the Office Mail App with the New-App command" on page 134.

Note: You must log in to the Exchange server using an account that is assigned the management roles Org Custom Apps and User Options. By default, members of the "Organization Management" role group are assigned these roles.

The following example shows how to use the `New-App` command to enable an organization for the Office Mail App.

The backtick character (`) is the PowerShell line-continuation character.

```
$Mbx = get-mailbox "mailbox"

New-App -OrganizationApp -DefaultStateForUser:enabled -Url `
    ("http://EV_server/EnterpriseVault/OfficeMailAppManifest.aspx?LegacyMbxDn=" +
    $Mbx.LegacyExchangeDN)
```

where:

- *mailbox* is the name of a mailbox that is enabled for archiving. This mailbox must be one whose archive is stored on the Enterprise Vault server to which you want all organization level requests to be sent.

- *EV_server* is the name of any Enterprise Vault server in your site.This Enterprise Vault server is not necessarily the one that is used to load the Office Mail App. The Enterprise Vault server that is used to load the Office Mail App for all users is the server where the archive for the specified mailbox is located. The name of the correct Enterprise Vault server for the specified mailbox is returned within the manifest file.

Users in the organization may access the Enterprise Vault server externally, with no direct access. In this case, the manifest file must point to the URL of the server that provides external access. The same server would also be used for internal access. For example, the server may be a Microsoft Forefront Threat Management Gateway (TMG) server.

The following example shows how to use the BaseURL parameter with the `OfficeMailAppManifest.aspx` page to configure the manifest file to point to a server that provides external access.

The backtick character (`) is the PowerShell line-continuation character.

```
$Mbx = get-mailbox "mailbox"

New-App -OrganizationApp -DefaultStateForUser:enabled -Url `
    ("http://EV_server/EnterpriseVault/OfficeMailAppManifest.aspx?LegacyMbxDn=" +
    $Mbx.LegacyExchangeDN + "&BaseURL=https://external_access_server/EnterpriseVault")
```

where:

- *mailbox* is the name of any mailbox that is enabled for archiving.
- *EV_server* is the name of any Enterprise Vault server in your site. This Enterprise Vault server is not necessarily the one that is used to load the Office Mail App. The Enterprise Vault server that is used to load the Office Mail App for all users is the server that is specified in the BaseURL parameter.
- *external_access_server* is the name of the server that provides external access.

See "About configuring Threat Management Gateway 2010 for Outlook 2013 and OWA 2013" on page 217.

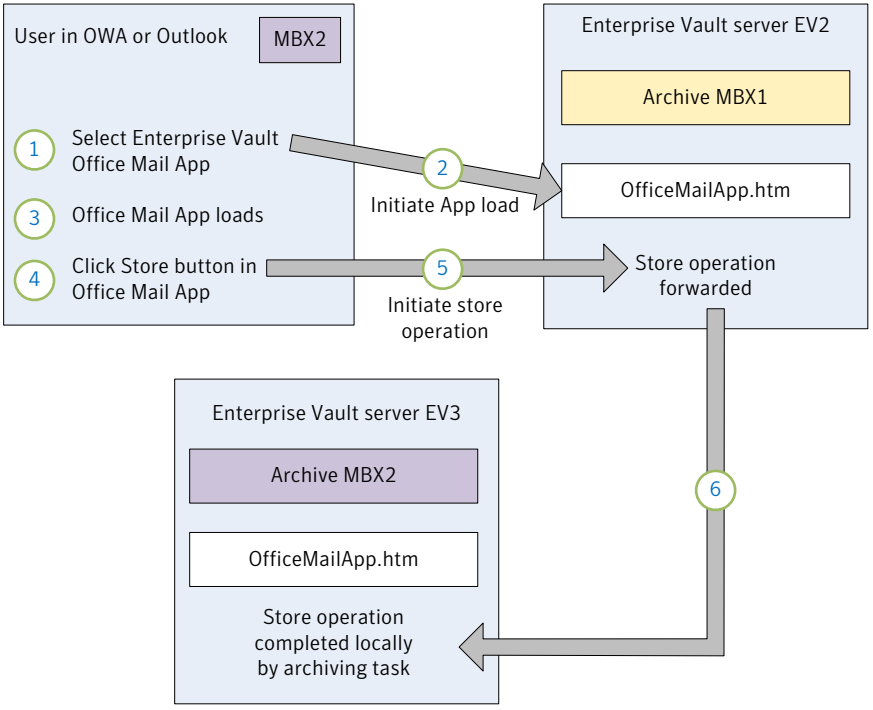
About the Enterprise Vault Office Mail App after deployment for an organization

Figure 9-3 shows what happens when:

- The Office Mail App has been deployed for an organization.

- The `New-App` command specified mailbox MBX1 and a URL on Enterprise Vault server EV1 for `OfficeMailAppManifest.aspx`.
- The user selects the Office Mail App and stores an item.

Figure 9-3 Office Mail App after deployment for an organization



In the figure, the numbered stages are as follows:

1. The user of mailbox MBX2 selects the Office Mail App in OWA or Outlook.
2. A request to load the Office Mail App is sent to `OfficeMailApp.htm` on Enterprise Vault server EV2, where the archive for MBX1 is stored.
3. The Office Mail App loads.
4. The user selects an unarchived item and clicks **Store**.
5. The Office Mail App sends a request to store the item to EV2.
6. Enterprise Vault on EV2 forwards the request to Enterprise Vault server EV3. On EV3, Enterprise Vault stores the item in the archive MBX2.

No forwarding of the request to store is required for users whose archives are on EV2.

Mailbox synchronization after upgrade to enable use of the Office Mail App

If you have upgraded Enterprise Vault and deployed the Enterprise Vault Office Mail App to existing users' mailboxes, those mailboxes must be synchronized.

Until the mailboxes are synchronized, the Office Mail App does not load fully after the user clicks the Enterprise Vault tab. It does not show any buttons, and instead displays an appropriate error message.

If the Exchange Mailbox archiving task is set to run automatically, it synchronizes mailboxes the next time it runs. If the startup type is manual, or if you want to run the task before the next scheduled time, you can optionally start the task from the Administration Console. The startup type is set on the Exchange Mailbox Task Properties: General tab in the Administration Console.

Additional requirements on Enterprise Vault Office Mail App users' computers

You should ensure that client computers meet the following additional requirements for use of the Enterprise Vault Office Mail App:

- Internet Explorer 9 or later must be installed on client computers. For the latest information on supported browsers, see the Enterprise Vault *Compatibility Charts* at http://www.symantec.com/docs/TECH38537.
- In the Internet Explorer Security settings, the Enterprise Vault server must be included in the Local intranet zone. Including the Enterprise Vault server in the Local intranet zone prevents unwanted authentication prompts to users.

  Note that installation of the Enterprise Vault Outlook Add-In automatically adds the Enterprise Vault server to Local intranet zone sites.
- This requirement applies when both of the following are true:
  - Internet Explorer 10 is installed.
  - The Exchange server and the Enterprise Vault web server are in different zones in the Internet Explorer Security settings.

  In this case, each zone must have the same **Enable Protected Mode** setting. If the **Enable Protected Mode** settings are different, the Office Mail App options Search, Archive Explorer, and Help may fail to open a browser window. This issue occurs only if the user runs the Office Mail App from OWA 2013 in Internet Explorer 10. It does not occur if the user runs the Office Mail App in Outlook 2013.

  An error message informs the user if a window fails to open.

- Users' computers must have external Internet access. They must be able to access the following URLs for the Office Mail App to load correctly:
  - https://appsforoffice.microsoft.com/lib/1.0/hosted/office.js
  - https://ajax.aspnetcdn.com/ajax/3.5/MicrosoftAjax.js

Disabling and re-enabling the Enterprise Vault Office Mail App for a device type

After deployment of the Enterprise Vault Office Mail App, it is enabled by default for computers, tablets, and phones. To disable the Office Mail App for any of these device types, you can add an entry to the `web.config` file on the Enterprise Vault server. For example, you might want to disable the Office Mail App for tablets and phones, but leave it enabled for computers.

The `web.config` file is in the `\WebApp` folder below the Enterprise Vault installation folder, for example `C:\Program Files (x86)\Enterprise Vault\WebApp`.

When you disable a device type, the Enterprise Vault tab still appears but the Office Mail App does not show the usual options. Instead, the following message is displayed:

```
The Enterprise Vault Office Mail App is not available on this device
```

To disable the Office Mail App for a device type

1. Make a copy of `web.config` and rename the copy in case you need to revert to it.
2. Open `web.config` in a text editor.

   Note: User Account Control (UAC) may prevent you from editing `web.config` in its usual location. If so, copy it from the `\WebApp` folder to a location where you can edit it.

3. If the `<appsettings>` section does not exist, add the section. The start and the end tags are `<appsettings>` and `</appsettings>`.
4. In the `<appsettings>` section, add the following line:

   ```
   <add key="key_name" value="false"/>
   ```

   where *key_name* is one of the following:

   - To disable the Office Mail App for computers: `OMAEnabledOnDesktop`.

- To disable the Office Mail App for tablets: `OMAEnabledOnTablet`.
- To disable the Office Mail App for phones: `OMAEnabledOnPhone`.

5 Save and close `web.config`.

6 If necessary, copy the edited `web.config` file back to the `\WebApp` folder.

To re-enable the Office Mail App for a device type

1 Repeat steps 1 and 2 in the procedure above.

2 In the `<appsettings>` section, do one of the following:

- Delete the line that disables the device type.
- In the relevant line, change the value `false` to `true`.

3 Repeat steps 5 and 6 in the procedure above.

Removing, disabling, and re-enabling the Enterprise Vault Office Mail App for a user or an organization

You can remove the Enterprise Vault Office Mail App for an individual user or an organization by using the PowerShell command `Remove-App`.

You can disable the Office Mail App for an individual user by using the command `Disable-App`. It is not possible to disable an Office Mail App that is installed at the organization level.

After you have disabled the Office Mail App, you can re-enable it by using the command `Enable-App`.

When you disable the Office Mail App with `Disable-App`, it does not load and the Enterprise Vault tab does not appear on the Office Mail App bar. As an alternative, you can use a separate, more easily reversible method to disable the Office Mail App for a particular device type. With this method, the Office Mail App still loads. The Enterprise Vault tab appears on the Office Mail App bar, but the usual options are not available.

See "Disabling and re-enabling the Enterprise Vault Office Mail App for a device type" on page 144.

To remove the Office Mail App for an individual user

1 Log in to the Exchange server using an account that is assigned the management role User Options. By default, members of the "Organization Management" role group are assigned this role.

2 Open the Exchange Management Shell.

3 Run a PowerShell command based on the following example:

```
Remove-App -mailbox mailbox -Identity 0cc6d075-e610-4b8a-90c6-1460e6d4d710
```

where *mailbox* is the mailbox from which you want to remove the Office Mail App.

The GUID identifies the Enterprise Vault Office Mail App, and does not change.

You are prompted to confirm the action.

4 To confirm, enter your response and press Enter.

To remove the Office Mail App for an organization

1 Log in to the Exchange server using an account that is assigned the management role User Options. By default, members of the "Organization Management" role group are assigned this role.

2 Open the Exchange Management Shell.

3 Run the following PowerShell command:

```
Remove-App -OrganizationApp -Identity 0cc6d075-e610-4b8a-90c6-1460e6d4d710
```

The GUID identifies the Enterprise Vault Office Mail App, and does not change.

You are prompted to confirm the action.

4 To confirm, enter your response and press Enter.

To disable the Office Mail App for an individual user

1 Log in to the Exchange server using an account that is assigned the management role User Options. By default, members of the "Organization Management" role group are assigned this role.

2 Open the Exchange Management Shell.

3 Run a PowerShell command based on the following example:

```
Disable-App -mailbox mailbox -Identity 0cc6d075-e610-4b8a-90c6-1460e6d4d710
```

where *mailbox* is the mailbox for which you want to disable the Office Mail App.

The GUID identifies the Enterprise Vault Office Mail App, and does not change.

You are prompted to confirm the action.

4 To confirm, enter your response and press Enter.

To re-enable the Office Mail App for an individual user

1. Log in to the Exchange server using an account that is assigned the management role User Options. By default, members of the "Organization Management" role group are assigned this role.
2. Open the Exchange Management Shell.
3. Run a PowerShell command based on the following example:

```
Enable-App -mailbox mailbox -Identity 0cc6d075-e610-4b8a-90c6-1460e6d4d710
```

   where *mailbox* is the mailbox for which you want to re-enable the Office Mail App.

   The GUID identifies the Enterprise Vault Office Mail App, and does not change.

   You are prompted to confirm the action.
4. To confirm, enter your response and press Enter.

Troubleshooting the Enterprise Vault Office Mail App

This section includes the following topics:

The following video shows how to diagnose and resolve any issues that may arise when you deploy and use the Office Mail App.

http://video.symantec.com/services/player/bcpid292374537001?bckey=AQ~~,AAAABuIiy9k~,I8Bhas-Vwr9zYL9V36WFi86fR_NoePscn&bctid=2098892410001

Enterprise Vault Office Mail App: client tracing

The Enterprise Vault Office Mail App writes to a console trace window on the client computer.

To launch the console trace in a new window

- Hold down the Ctrl key and click **Help** in the Enterprise Vault Office Mail App window.

Enterprise Vault Office Mail App: server tracing

You can use the DTrace utility to trace Office Mail App problems on the Enterprise Vault server.

Table 9-3 shows the processes to monitor with DTrace.

Table 9-3 Processes to monitor for the Office Mail App

Process	Description
`W3wp.exe`	This process hosts `.aspx` pages. Tracing this process can show errors in the `.aspx` pages.
`AgentClientBroker.exe`	When Enterprise Vault initially marks items to archive, restore, delete, or view, it uses AgentClientBroker.exe. Tracing this process can show errors in connecting to Exchange Server.
`ShoppingService.exe`	Enterprise Vault uses this process as part of its restore and view functionality.
`RetrievalTask.exe`	Enterprise Vault uses this process when it retrieves an item.
`StorageRestore.exe`	Enterprise Vault uses this process when it restores an item.
`StorageDelete.exe`	Enterprise Vault uses this process when it deletes an item.
`StorageArchive.exe`	Enterprise Vault uses this process when it archives an item.

For more information on DTrace, see the Enterprise Vault *Utilities* guide.

Checking deployment of the Enterprise Vault Office Mail App

You can find out the following information about deployment of the Enterprise Vault Office Mail App by using the PowerShell command `Get-App`:

- Whether the Office Mail App is deployed at the organization level.
- A list of the mailboxes to which the Office Mail App has been deployed individually.

To check whether the Office Mail App is deployed at the organization level

1. Log in to the Exchange server using an account that is assigned the management role User Options. By default, members of the "Organization Management" role group are assigned this role.
2. Open the Exchange Management Shell.
3. Run the following PowerShell command:

```
Get-App -OrganizationApp -Identity 0cc6d075-e610-4b8a-90c6-1460e6d4d710
```

The GUID identifies the Enterprise Vault Office Mail App, and does not change.

The command either reports that the Office Mail App is deployed, or it displays an error saying that the application identity was not found.

To list the mailboxes to which the Office Mail App has been deployed individually

1. Log in to the Exchange server using an account that is assigned the management role User Options. By default, members of the "Organization Management" role group are assigned this role.
2. Open the Exchange Management Shell.
3. Run the following PowerShell command. The backtick character (`) is the PowerShell line-continuation character.

```
Get-Mailbox |
ForEach {
  If (Get-App -mailbox $_.LegacyExchangeDN `
              -Identity 0cc6d075-e610-4b8a-90c6-1460e6d4d710 `
              -ErrorAction:Ignore | Where {$_.Type -Eq "Private"} )
     {Write-Host $_.DisplayName} }
```

The GUID identifies the Enterprise Vault Office Mail App, and does not change.

The command lists the mailbox display names of all the mailboxes to which the Office Mail App has been deployed individually.

The Enterprise Vault Office Mail App manifest file is not created

If invalid parameter values are supplied for the `OfficeMailAppManifest.aspx` page for use with the PowerShell command `New-App`, no manifest file is created. The command fails and returns an error message of the following type:

```
The app couldn't be downloaded. Error message: The remote server
returned an error: (500) Internal Server Error.
```

The typical causes of this error are as follows:

- The user is not enabled for Enterprise Vault.
- The BaseURL value is not valid.

The following example shows a script that returns a more detailed error message when the manifest file is not created for a specified individual user.

```
$Mbx = get-mailbox "mailbox"
$uri = new-object system.uri(
    "http://EV_server/EnterpriseVault/OfficeMailAppManifest.aspx?LegacyMbxDn=" +
    $Mbx.LegacyExchangeDN)
$webclient = New-Object Net.Webclient
$webClient.UseDefaultCredentials = $true
try
{
    $bytes = $webclient.DownloadData($uri)
    New-App -mailbox $Mbx.LegacyExchangeDN -FileData $bytes
}
catch [Net.WebException]
{
    [Net.HttpWebResponse] $webResponse = [Net.HttpWebResponse]$_.Exception.Response;
    Write-Warning $webResponse.StatusDescription
}
```

where:

- *mailbox* is the name of the mailbox you are trying to enable for the Office Mail App.
- *EV_server* is the name of the Enterprise Vault server.

The Enterprise Vault Office Mail App window is blank or contains an error message

The Enterprise Vault Office Mail App may appear on the Office Mail App bar, but its window is blank or it displays only an error message.

If this problem occurs, try the following steps:

- If you have more than one Enterprise Vault server, determine which Enterprise Vault server is requested when Enterprise Vault tries to load the Office Mail App, as described in the procedure below.
- Check whether you can load the following web page from the client computer:
  `https://EV_server/EnterpriseVault/OfficeMailApp.aspx`
  where *EV_server* is the name of the Enterprise Vault server from which the Office Mail App is loaded.

Navigating directly to `OfficeMailApp.aspx` can show the following:

- Whether there are certificate errors
- Whether there is a particular problem loading the web page

The Office Mail App does not initialize fully when you load it in this way.

- Check that the following URLs are accessible from the client computer:
  - https://appsforoffice.microsoft.com/lib/1.0/hosted/office.js
  - https://ajax.aspnetcdn.com/ajax/3.5/MicrosoftAjax.js

  Access to these URLs is required for the Office Mail App to load correctly. If they are not accessible, it may be because the client computer has no Internet connection, or the connection is too slow.

To determine the Enterprise Vault server with the Get-App command

1. Log in to the Exchange server using an account that is assigned the management role User Options. By default, members of the "Organization Management" role group are assigned this role.
2. Open the Exchange Management Shell.
3. If the Office Mail App is deployed to an organization, go to step 4.

   If the Office Mail App is deployed to individual users, run the following PowerShell command:

```
Get-App 0cc6d075-e610-4b8a-90c6-1460e6d4d710 -Mailbox mailbox | Format-List ManifestXML
```

   where *`mailbox`* is the mailbox you are troubleshooting.

   The GUID identifies the Enterprise Vault Office Mail App, and does not change.
4. If the Office Mail App is deployed to an organization, run the following PowerShell command:

```
Get-App 0cc6d075-e610-4b8a-90c6-1460e6d4d710 -OrganizationApp | Format-List ManifestXML
```

   The GUID identifies the Enterprise Vault Office Mail App, and does not change.
5. In the output XML, find the `<DesktopSettings>` node. The `DefaultValue` contains the Enterprise Vault server URL that is requested when Enterprise Vault tries to load the Office Mail App.

An Enterprise Vault Office Mail App action fails with an error message

When a user clicks an Enterprise Vault Office Mail App option, a problem may cause the action to fail. The Office Mail App displays an error message.

When an action fails, you can hover over the error message to see additional information.

For example, if the error message says `Failed to archive item`, one possible additional information message is as follows:

```
Enterprise Vault cannot perform the requested action because a service
is not running
```

The Office Mail App client tracing includes more detailed information.

See "Enterprise Vault Office Mail App: client tracing" on page 147.

Chapter 10

Configuring OWA access to Enterprise Vault

This chapter includes the following topics:

About Enterprise Vault functionality in OWA clients

The Enterprise Vault features that are available to OWA users depend on the version of the Exchange Server. Table 10-1 lists the features that are available to users whose mailboxes are hosted on Exchange Server 2010 and earlier.

Table 10-1 Enterprise Vault features in OWA 2010 and earlier clients

Exchange Server version	Enterprise Vault features available in OWA clients
Exchange 2000	■ View items. ■ Reply to and forward shortcuts (using standard OWA functionality). ■ Delete shortcuts (using standard OWA functionality). ■ View archived public folder items.

Table 10-1 Enterprise Vault features in OWA 2010 and earlier clients *(continued)*

Exchange Server version	Enterprise Vault features available in OWA clients
Exchange Server 2003, Exchange Server 2007, or Exchange Server 2010	■ View items using standard OWA functionality. ■ Reply to and forward shortcuts or original items (using standard OWA functionality). ■ Archive items and folders using Enterprise Vault buttons or menu options. Default archiving properties can be changed. ■ Restore items using Enterprise Vault buttons or menu options. Restore properties can be set. ■ Delete shortcuts, archived items, or both using Enterprise Vault buttons or menu options or standard OWA functionality. ■ Archive Explorer button. ■ Search archive option. (No link to Browser Search.) ■ View archived public folder items. This feature is available with Exchange Server 2003 and Exchange Server 2007 SP1 or later. In the OWA 2003 client the archived item is presented like a custom shortcut containing a link to the archived item. When the user clicks the link, the item is displayed in a browser window. With OWA 2007 or later clients, the archived item shortcut looks and behaves like a mailbox shortcut. ■ Administrator can configure Enterprise Vault functionality available in Premium and Basic clients.

For those mailboxes that are hosted on Exchange Server 2013, the Enterprise Vault Office Mail App provides Enterprise Vault features in OWA 2013 clients. These features differ slightly from the features that are available to users of older OWA clients.

See "About the Enterprise Vault Office Mail App" on page 128.

Exchange Desktop policy settings in the Enterprise Vault Administration Console let you customize Enterprise Vault functionality in OWA clients. Settings in the Options page of the Exchange Desktop policy let you choose the features to make available to users in OWA and Outlook clients. Separate lists of OWA and Outlook settings in the Advanced page of the Exchange Desktop policy let you customize how the Enterprise Vault features behave in different clients. See the *Administrator's Guide* for more details.

About OWA forms-based authentication for Enterprise Vault

With forms-based authentication, OWA users must re-enter login credentials when they start Enterprise Vault Search, Archive Explorer, or first open an archived item using Enterprise Vault View mode. This is because the request accesses a different IIS virtual directory (Exchange Server 2003) or web server (Exchange Server 2007 and later), which requires different authentication.

View mode can be set to Enterprise Vault in the OWA settings on the Advanced page of the Exchange Desktop policy. This setting controls what happens when a user clicks **Open the original item** in the banner of a custom shortcut. If OWA is set as the value of this setting, OWA renders the original item, which looks like an OWA message. If Enterprise Vault is set as the value, Enterprise Vault renders the item.

About OWA configurations for Enterprise Vault

The following figures give examples of some typical OWA environments in which Enterprise Vault can be deployed. The types of authentication supported by Enterprise Vault are also shown.

See " Exchange Server 2007/2010 OWA configurations" on page 155.

See "Exchange Server 2003/2007 mixed OWA environment" on page 158.

See " Exchange Server 2000/2003 OWA with front-end and back-end servers" on page 160.

See "Exchange Server 2000/2003 OWA without front-end server" on page 162.

See "Clustered OWA configurations" on page 163.

See "Configurations for demonstrating Enterprise Vault with OWA" on page 165.

Exchange Server 2007/2010 OWA configurations

The following example configurations show simple Exchange Server 2007 and 2010 OWA environments.

Figure 10-1 Exchange Server 2007 OWA configuration

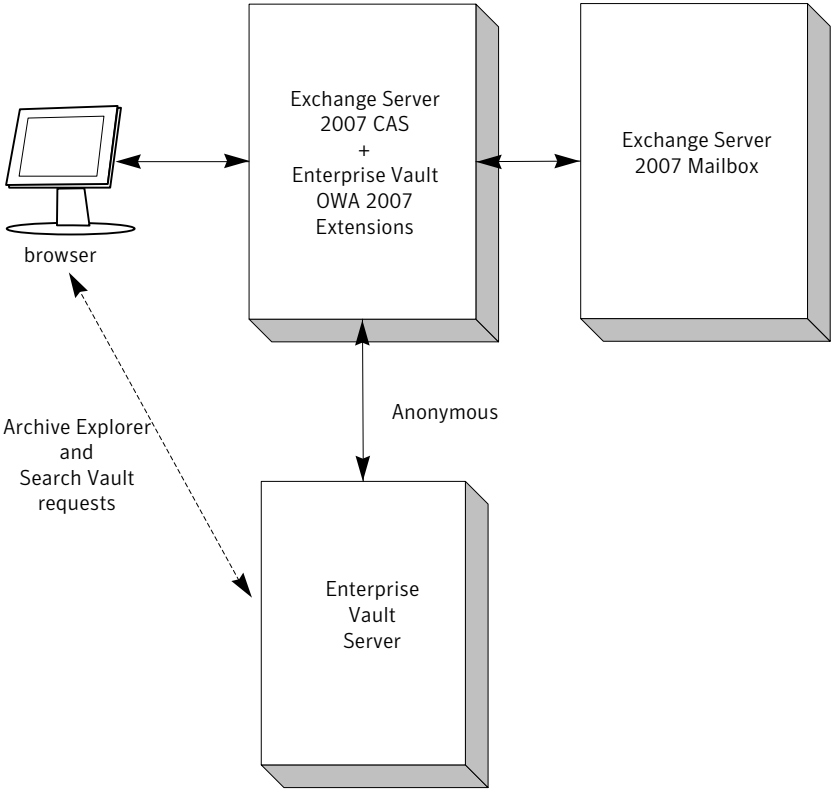
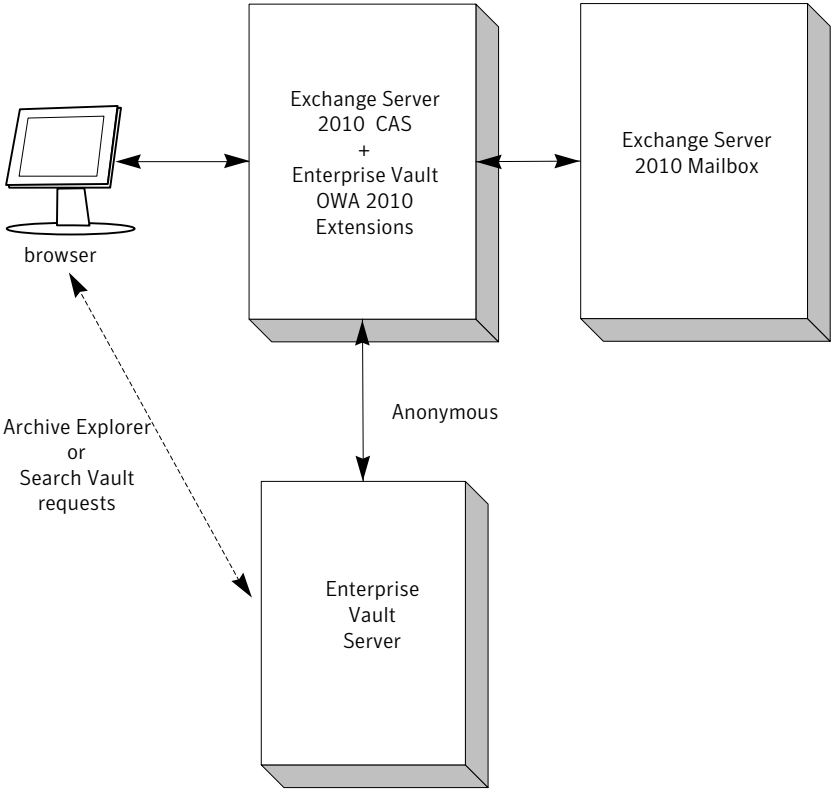


Figure 10-2 Exchange Server 2010 OWA configuration



In these configurations Enterprise Vault OWA 2007 or 2010 Extensions are installed on the Exchange CAS computer. Typically, the Exchange Mailbox server would be on a separate computer, but it could be co-located with the Exchange CAS.

With Exchange Server 2007, if the mailboxes are located on a server which is separate from the CAS computer, and users are authenticated to OWA using Integrated Windows Authentication (IWA), then it is necessary to configure constrained delegation. Configuring constrained delegation requires a domain functional level of Windows Server 2003 or later.

When a user starts Archive Explorer or an archive search from the OWA client, the client will always try to connect directly to the Enterprise Vault web server on the Enterprise Vault server.

Additional configuration is required if OWA 2007 clients access the Exchange 2007 CAS through an Exchange Server 2010 CAS. The additional steps are documented in the following technical note on the Symantec Support website:

http://www.symantec.com/docs/TECH125053

If OWA 2010 clients need access to archived items in public folders on Exchange Server 2007, then you need to perform additional configuration steps. The configuration steps are described in the following technical note on the Symantec Support website:

http://www.symantec.com/docs/TECH135624.

If clients connect to the Exchange CAS computer using Microsoft ISA Server, then the Enterprise Vault web server URL must be published by the ISA Server in addition to the Exchange CAS URL.

The Exchange CAS connects to the Enterprise Vault server using anonymous authentication. On the Enterprise Vault server, the Data Access account is configured to manage the anonymous connections.

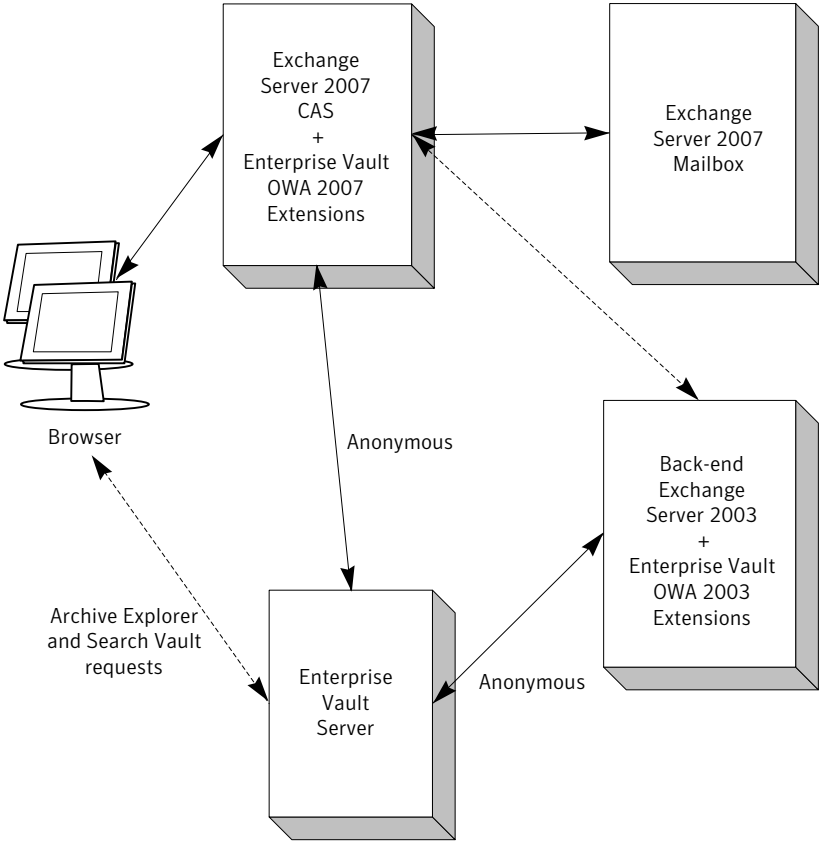
See "Configuring Enterprise Vault for anonymous connections" on page 168.

Exchange Server 2003/2007 mixed OWA environment

The following configuration shows a possible Exchange Server 2007 and 2003 mixed OWA environment. OWA 2007 clients access the Exchange 2007 Mailbox server through the Exchange 2007 CAS. OWA 2003 clients access the Exchange Server 2003 back-end server through the Exchange 2007 CAS.

This mixed configuration may exist while Exchange Servers are gradually being upgraded.

Figure 10-3 Mixed Exchange Server 2003/2007 OWA configuration



In this configuration, the Enterprise Vault OWA 2003 Back-End Extensions are installed on Exchange Server 2003 and Enterprise Vault OWA 2007 Extensions are installed on the Exchange 2007 CAS computer. OWA 2003 users access their mailbox using a URL such as https://*cas_server*/exchange, rather than http://*cas_server*/owa. This is because Enterprise Vault extensions on the Exchange 2007 CAS computer do not process requests from OWA 2003 clients. Instead, these requests are just passed to the appropriate Exchange Server 2003 back-end server.

If an OWA 2003 client accesses a mailbox on Exchange Server 2003 through the Exchange 2007 CAS, then any Archive Explorer or archive search requests will always attempt to access the Enterprise Vault server directly (irrespective of the value of OWA setting, Client Connection, in the Exchange Desktop policy).

If OWA 2007 clients need access to archived items in public folders on Exchange Server 2003, then you need to perform additional configuration steps. The configuration steps are described in the following technical note on the Symantec Support website:

http://www.symantec.com/docs/TECH66761

If clients connect through a Microsoft ISA Server, then you will need to publish to clients the OWA site on the Exchange 2007 CAS and the Enterprise Vault web server URL.

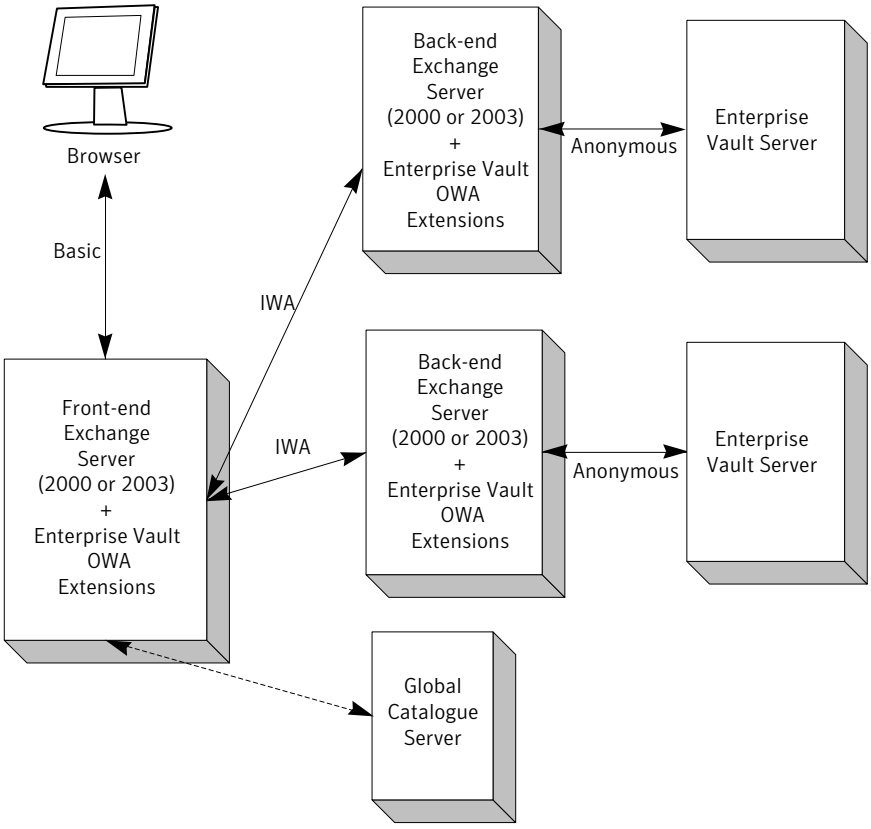
The Exchange Server 2003 back-end server and the Exchange 2007 CAS connect to the Enterprise Vault server using anonymous authentication. On the Enterprise Vault server, the Data Access account is configured to manage the anonymous connections.

See "Configuring Enterprise Vault for anonymous connections" on page 168.

Exchange Server 2000/2003 OWA with front-end and back-end servers

In the following example configuration there is one Exchange Server configured as a front-end server and two Exchange Servers configured as back-end servers.

Figure 10-4 Front-end/back-end Exchange Server 2000/2003 OWA configuration



OWA client browser sessions connect to the front-end Exchange Server.

Enterprise Vault OWA 2000 or 2003 Extensions are installed on all front-end and back-end Exchange Servers.

If the front-end Exchange Server is running Exchange Server 2003 and the back-end Exchange Server is running Exchange 2000, clients will only have the Enterprise Vault functionality available with OWA 2000 Extensions, in the same way as OWA functionality will be limited.

In configurations with front-end Exchange Servers it is advisable to check that Enterprise Vault works correctly when users are connected to the back-end Exchange Servers. When OWA works correctly in this configuration, then you can add the Enterprise Vault OWA Extensions to the front-end Exchange Servers. If Enterprise Vault does not work correctly when the OWA clients are connected to the front-end Exchange Server, then the problem lies in the front-end server.

Typically, users connect to the front-end server using basic authentication wrapped in an SSL connection. Integrated Windows Authentication (IWA) is used for the connection between Exchange Servers and anonymous authentication is used for the connection between the back-end Exchange Server and the Enterprise Vault server. On the Enterprise Vault server, the Data Access account is configured to manage the anonymous connections.

See "Configuring Enterprise Vault for anonymous connections" on page 168.

An Enterprise Vault Exchange Desktop policy setting (Client connection) can be used to enable OWA 2003 clients to connect directly to the Enterprise Vault server when users start Archive Explorer or an archive search from their OWA client.

If your environment is configured as follows, then the Exchange Server 2003 front-end server and the Enterprise Vault web server URL must be published to clients:

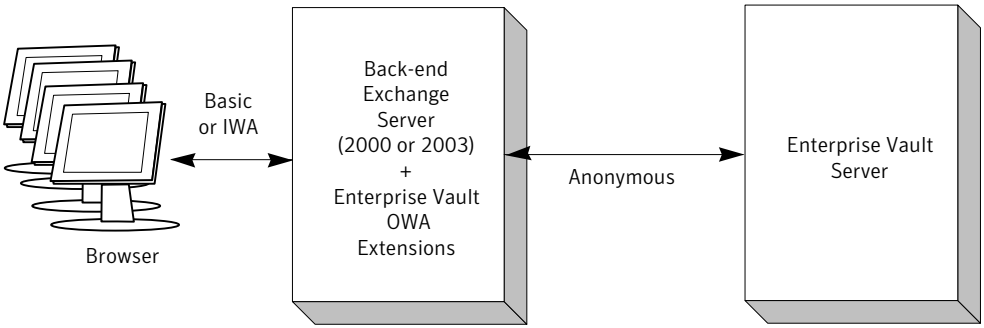
- Clients connect to the Exchange Server 2003 front-end server through an ISA Server.
- Direct connections are configured for Archive Explorer and archive search.

If direct connections are not configured (which is the default for Exchange Server 2003 OWA), then only the Exchange Server 2003 front-end server needs to be published.

Exchange Server 2000/2003 OWA without front-end server

In the following example configuration there are no front-end Exchange Servers.

Figure 10-5 Back-end only Exchange Server 2000/2003 OWA configuration



Instead, users connect to an Exchange Server that is configured as a back-end Exchange Server. This configuration can provide more security. You can force users to use IWA authentication instead of basic authentication when the clients connect to the Exchange Servers. Anonymous authentication is used for the

connection between the Exchange Server and the Enterprise Vault server. The Data Access account is configured to manage the anonymous connections.

See "Configuring Enterprise Vault for anonymous connections" on page 168.

Connecting OWA clients directly to the back-end Exchange Server is a good way to troubleshoot problems with Enterprise Vault in the OWA clients. This test is also useful after you have upgraded the Enterprise Vault OWA Extensions, or made changes to OWA files on the Exchange Server.

As in previous configurations, an Enterprise Vault Exchange Desktop policy setting can be used to enable OWA 2003 clients to connect directly to the Enterprise Vault server. Direct connections are used when users start Archive Explorer or an archive search from their OWA client.

If your environment is configured as follows, then the Exchange Server 2003 back-end server and the Enterprise Vault web server URL must be published to clients:

- Clients connect to the Exchange Server 2003 back-end server through an ISA Server.
- Direct connections are configured for Archive Explorer and archive search.

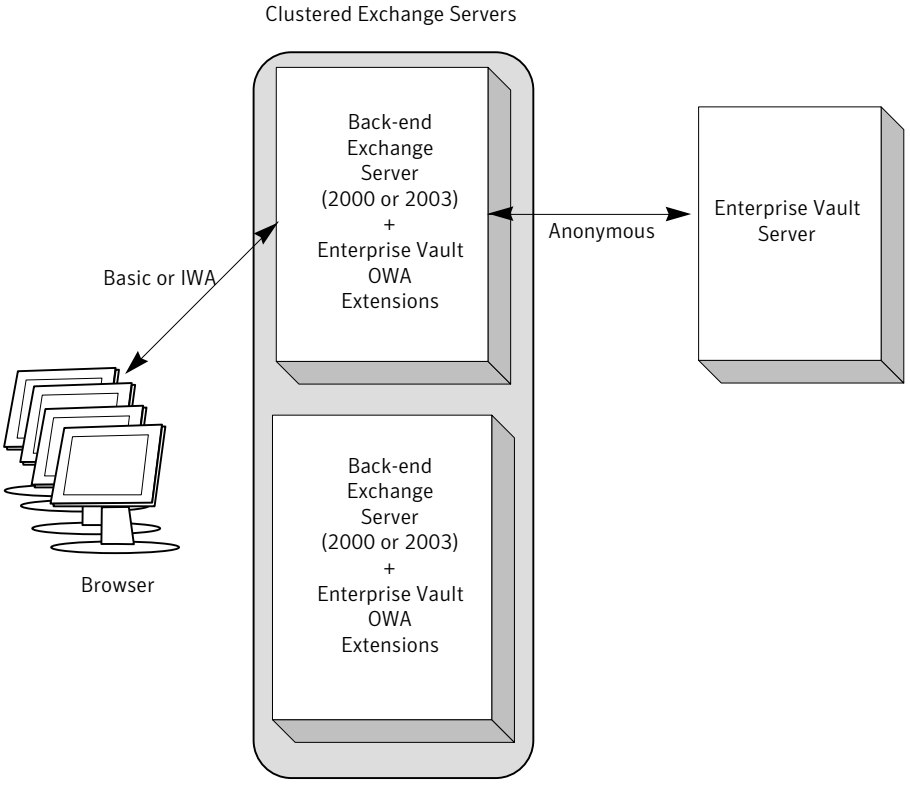
If direct connections are not configured (which is the default for Exchange Server 2003 OWA), then only the Exchange Server 2003 back-end server needs to be published.

Clustered OWA configurations

Figure 10-6 gives an example of an active/passive cluster of Exchange Servers.

The following clustering examples relate only to Exchange Server 2000 and 2003 OWA configurations. In an Exchange Server 2007 or 2010 OWA environment, the Mailbox server can be clustered, but the CAS server cannot. As it is the CAS server that contacts the Enterprise Vault server, the Enterprise Vault configuration is unaffected when Exchange Server 2007 or 2010 Mailbox servers are clustered.

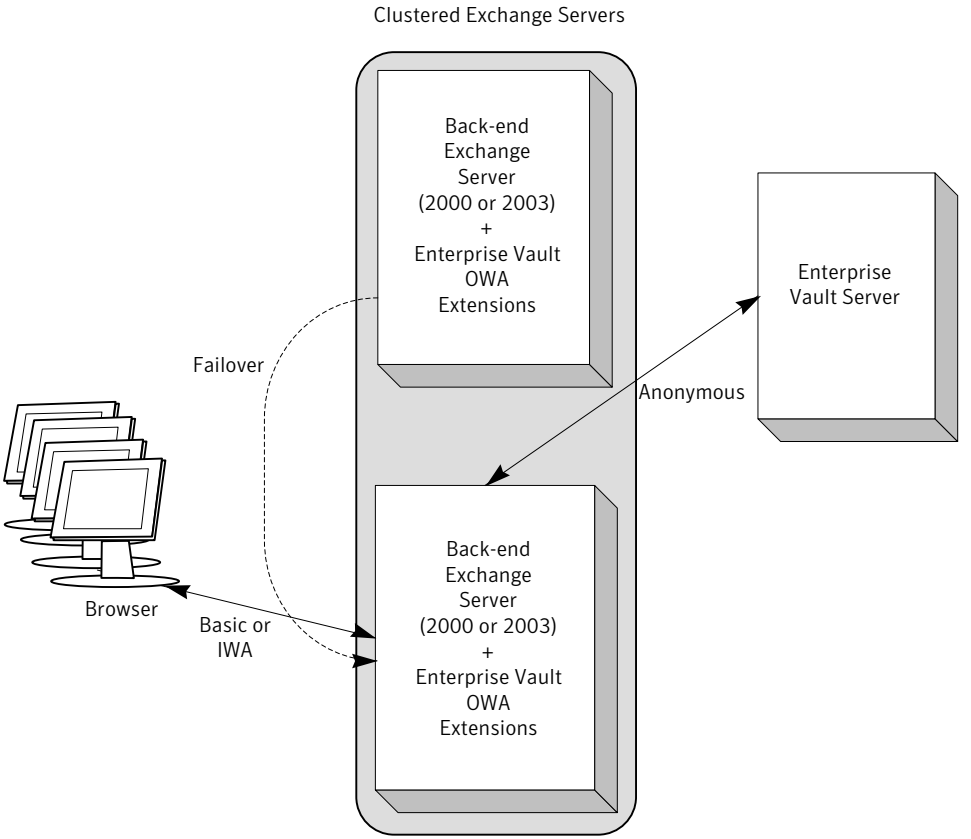
Figure 10-6 Clustered Exchange Server 2000/2003 OWA example



In this configuration, Enterprise Vault OWA 2000 or 2003 Extensions must be installed and configured on both Exchange Servers in the cluster. Enterprise Vault automatically adds the necessary cluster addresses to its configuration files when you configure the OWA Extensions. There could also be a front-end Exchange Server, but this would not normally be included in a cluster configuration.

When one Exchange Server in the cluster fails over to the other, connections to the Enterprise Vault servers are established automatically; users can continue to access items in their Enterprise Vault archives.

Figure 10-7 Configuration after failover



Configurations for demonstrating Enterprise Vault with OWA

If you are setting up an Enterprise Vault environment to demonstrate or pilot Exchange Server 2000 or 2003 OWA access to Enterprise Vault archives, the Enterprise Vault server and Exchange Server can be installed on one computer. Installing Exchange Server 2007 or 2010 on the Enterprise Vault server is supported but not recommended.

See "Configuring a demonstration system for use with Enterprise Vault OWA 2003 Extensions" on page 184.

Which OWA Extensions to install for use with Enterprise Vault

To provide OWA access to Enterprise Vault for Exchange Server 2007 or 2010 mailboxes, Enterprise Vault OWA Extensions need to be installed on all Exchange Server 2007 and 2010 CAS computers.

To provide OWA access to Enterprise Vault for Exchange 2000 or Exchange Server 2003 mailboxes, Enterprise Vault OWA Extensions need to be installed on all front-end and back-end OWA Exchange Servers.

When you install the Enterprise Vault OWA Extensions on your Exchange Servers, ensure that you install the same Enterprise Vault release version of the extensions on all the Exchange Servers. All the Exchange Servers on which you install the extensions should be at the same Exchange Server service pack and hotfix level.

As Enterprise Vault OWA 2003 Extensions modify OWA control files on Exchange Server 2003, the version of these files must be one that is supported by Enterprise Vault. The supported versions of OWA control files are listed in *Exchange Server OWA control file versions* in the Enterprise Vault Compatibility Charts. Before you install an Exchange Server hotfix that changes the OWA control file version, check in the Compatibility Charts that the version is supported by Enterprise Vault.

The Enterprise Vault Extensions for Exchange Server 2003 servers are also needed to support Enterprise Vault access from Outlook clients working in RPC over HTTP mode. With Exchange Server 2007 and Exchange Server 2010, no Enterprise Vault extensions are required to support Enterprise Vault access from Outlook Anywhere clients.

Note that the Enterprise Vault buttons are not available in OWA clients when using Exchange 2000, which means that you can only view archived items with these extensions. To be able to archive, restore and delete archived items from your OWA client and have integrated access to Archive Explorer and search archive features, you need to use OWA on Exchange Server 2003 or later.

Instructions of how to uninstall the Enterprise Vault OWA Extensions are given in the following technical note on the Symantec Support website:

http://www.symantec.com/docs/TECH77119

Configuring Enterprise Vault access for OWA users

Before starting the tasks described in this section, it is important to check that your Exchange Servers and Enterprise Vault servers meet with the prerequisites described in "Prerequisites for OWA" in *Installing and Configuring*.

There are a number of tasks that you need to complete before installing the Enterprise Vault OWA Extensions. There may also be post-installation steps required, depending on your OWA environment. This section provides details of the preparation, installation and post-installation tasks required to enable Enterprise Vault access for OWA users.

The required steps can be summarized as follows:

- On Enterprise Vault servers, configure the Data Access account to accept anonymous connections from Exchange 2007 or 2010 CAS servers, and any Exchange 2000 or Exchange Server 2003 back-end servers.
- If required, configure OWA settings in the Exchange Desktop Policy in the Enterprise Vault Administration Console to change the Enterprise Vault functionality available in OWA clients.
- For OWA 2003 and OWA 2000, prepare the `EVServers.txt` file on an Enterprise Vault server. This file enables the installation program to add entries to the proxy bypass list.
  You populate the file using the script, `MakeEVServersTxt.wsf`.
  See "Preparing proxy bypass list entries for OWA 2000 and OWA 2003 Extensions" on page 173.
  If you are installing the OWA Extensions remotely using, for example, Active Directory, then the `EVServers.txt` file needs to be copied to the file share containing the installation files. If you are installing the OWA Extensions interactively on each server, then `EVServers.txt` needs to be copied to each Exchange Server 2003 and Exchange 2000 back-end server.
- On Exchange Server 2003 and Exchange 2000 servers, run the installation program to install and automatically configure the Enterprise Vault OWA Extensions.
- On Exchange 2007 CAS server computers, install the Enterprise Vault OWA 2007 Extensions. (You can install the 64-bit or 32-bit version, depending on the mode of your Exchange Server.)
- Depending on the arrangement of CAS and Mailbox servers in your Exchange Server 2007 environment, you may need to perform some additional configuration steps to enable access.
- On Exchange 2010 CAS server computers, install the Enterprise Vault OWA 2010 Extensions.
- If your Exchange Server 2010 environment includes CAS proxy servers, then you need to perform additional configuration steps.
  See "Additional configuration steps for Exchange Server 2010 CAS proxying for use with OWA" on page 183.

- When Archive Explorer or archive search is started in an OWA 2007 or 2010 client, the client will attempt to access the Enterprise Vault server directly. If you are using a firewall or ISA Server, you need to ensure that both the Exchange CAS server and Enterprise Vault server web server URL are published to clients.
  For details of how to configure different URLs for internal and external access to Enterprise Vault, see the following technical note on the Symantec Support website: http://www.symantec.com/docs/TECH63250.
- If OWA 2007 clients need access to archived items in public folders on Exchange Server 2003, you need to perform additional configuration steps. The configuration steps are described in the following technical note on the Symantec Support website:
  http://www.symantec.com/docs/TECH66761
- If OWA 2010 clients need access to archived items in public folders on Exchange Server 2007, you need to perform additional configuration steps. The configuration steps are described in the following technical note on the Symantec Support website:
  http://www.symantec.com/docs/TECH135624

If you have problems with installing Enterprise Vault OWA Extensions, or when accessing archived items using OWA, see the following technical note on the Symantec Support website: http://www.symantec.com/docs/TECH69113. This technical note gives detailed troubleshooting information for Enterprise Vault OWA Extensions.

Configuring Enterprise Vault for anonymous connections

To prepare Enterprise Vault servers for anonymous connections from Exchange 2007 or 2010 CAS servers, or Exchange 2000 or Exchange Server 2003 back-end servers, perform the following steps as described in this section:

- Ensure that IIS Roles and Feature Delegation rights are configured as described in the section, "Prerequisites for OWA" *Installing and Configuring*.
- On each Enterprise Vault server that may receive connection requests from OWA servers, create an `ExchangeServers.txt` file in the Enterprise Vault installation folder. This file contains a list of the IP addresses for all the Exchange CAS servers, and any Exchange 2000 or Exchange Server 2003 back-end servers, that will connect to the Enterprise Vault server.
  Additional entries are needed if you are configuring this file for clustered Exchange Virtual Server configurations.
  See "About configuring OWA and RPC Extensions in clustered configurations" on page 203.

- Create or select a domain account to be used for anonymous connections from Exchange Servers to the Enterprise Vault server. This is the Data Access account, which is also used for anonymous connections to the Domino Mailbox Archiving web application. The steps required to configure the Data Access account for OWA Extensions and Domino Mailbox Archiving are different. To configure the account for OWA, you run a command line script. To configure the Data Access account for Domino Mailbox Archiving, you specify the account on the **Data Access Account** tab of Directory properties.
  If you are configuring both Enterprise Vault OWA Extensions and Domino Mailbox Archiving, it is important to use the same account as the Data Access account for both features.
- On each Enterprise Vault server on which you have created an `ExchangeServers.txt` file, run the script, `owauser.wsf`, to configure the Data Access account
- Synchronize mailboxes and restart the Enterprise Vault Admin service.

To create the ExchangeServers.txt file

1. Open Notepad.
2. Type the IP address of each Exchange CAS server, and Exchange 2000 server or Exchange Server 2003 back-end server that will connect to the Enterprise Vault server, one entry per line.

   Addresses can be in either IPv4 or IPv6 format. IPv6 addresses must be in the form **fdfa:9c37:5267:d2e3:a192:b168:cc80:d204**.
3. Save the file as `ExchangeServers.txt` in the Enterprise Vault installation folder (for example `C:\Program Files (x86)\Enterprise Vault`). When you save the file, select ANSI, Unicode, or Unicode big endian encoding.
4. Close Notepad.

To configure the Data Access account for OWA

1. Create or select a domain account to be used for anonymous connections to the Enterprise Vault server. This is the Data Access account. The account should be a basic domain account; a local machine account cannot be used. The account should not belong to any administrator group, such as Administrators or Account Operators.

   If you are configuring both Enterprise Vault OWA Extensions and Domino Mailbox Archiving, it is important to use the same account as the Data Access account for both features. If you have already set up Domino Mailbox Archiving, note the details of the account specified on the **Data Access Account** tab of Directory properties in the Administration Console. Configure this account for OWA as described in this section.

2. Log on to the Enterprise Vault server as the Vault Service account.

3. Open a Command Prompt window with administrator privileges.

4. Navigate to the Enterprise Vault installation folder.

5. Enter the command line that is appropriate to your system. If you have OWA on both Exchange Server 2000 and Exchange Server 2003 in your organization, use the command line for OWA on Exchange Server 2003.

   - Command line for OWA on Exchange Server 2010, 2007 and 2003:
     `cscript owauser.wsf /domain:`*`domain`* `/user:`*`username`*
     `/password:`*`password`*
   - Command line for OWA on Exchange Server 2000 :
     `cscript owauser.wsf /domain:`*`domain`* `/user:`*`username`*
     `/password:`*`password`* `/exch2000`

   The file `owauser.wsf` is installed in the Enterprise Vault installation folder.

   For *domain*, give the domain of the Data Access account.

   For *username*, give the username of the Data Access account.

   For *password*, give the password of the Data Access account.

   To display help for the `cscript` command, type

   ```
   cscript owauser.wsf /?
   ```

6 The progress of the script execution is displayed in the command prompt window.

The configuration changes made by the script are described in the following technical note on the Symantec Support website:

http://www.symantec.com/docs/TECH69113

When the configuration script finishes, you are prompted to restart the Enterprise Vault Admin service and synchronize mailboxes.

7 If there are multiple Enterprise Vault servers in your environment, logon to each server on which you created an `ExchangeServers.txt` file, and run the script, `owauser.wsf`, using the instructions given in this section.

If you add another Exchange CAS server, or an Exchange 2000 or Exchange Server 2003 back-end server to your environment at a later date, add the IP address of the server to the `ExchangeServers.txt` file on the Enterprise Vault server to which the Exchange Server will connect, and then rerun the `owauser.wsf` script.

Restart the Admin Service and synchronize mailboxes for OWA configuration

To complete the configuration, you need to restart the Enterprise Vault Admin service and synchronize mailboxes. Restarting the Admin service ensures that Enterprise Vault authentication knows the identity of the Data Access account. Synchronizing the mailboxes updates the client hidden message with the URL to be used by the OWA extensions when connecting to Enterprise Vault.

To restart the Admin Service

1 In Control Panel, select Services.

2 Right-click **Enterprise Vault Admin Service** and select **Restart**.

Enterprise Vault services and tasks will restart.

3 Close the Services console.

To synchronize mailboxes

1 Start the Enterprise Vault Administration Console.

2 Expand the Enterprise Vault **Directory** container and then your site. Expand **Enterprise Vault Servers** and select the required Enterprise Vault server. Expand this container. Expand **Tasks**.

3 In the right hand pane, double-click the **Exchange Mailbox Archiving** task for the Exchange Server, to display the properties window for the task.

4. Select the **Synchronization** tab. Make sure **All mailboxes** and **Mailbox properties and permissions** are selected.
5. Click **Synchronize**.
6. Click **OK** to close the properties window.
7. Close the Enterprise Vault Administration Console.

Configuring Enterprise Vault Exchange Desktop Policy for OWA

If required, you can customize the Enterprise Vault functionality that you want available in OWA 2003 and later clients.

You can customize OWA clients using the OWA settings on the Advanced page of the Exchange Desktop policy properties. For more information on these settings, see the *Enterprise Vault Administrator's Guide*.

If you change any settings in the Exchange Desktop policy, then you will need to synchronize the mailboxes.

See "To synchronize mailboxes" on page 171.

To configure direct access to the Enterprise Vault server from OWA 2003 clients

1. In the Enterprise Vault Administration Console, expand the site. Click **Policies**, then **Exchange**, and then **Desktop**.
2. Double-click the policy that you want to change to display the policy properties.
3. Click the **Advanced** tab.
4. In the drop-down box beside **List settings from:** select **OWA**.
5. Double-click the **Client connection** setting.
6. Select **Direct** in the drop-down box and click **OK** to close the dialog.
7. If required, you can also modify other OWA settings to restrict the functionality available in the OWA 2003 clients.
8. Click **OK** to close the properties dialog.
9. The new values will be set when the mailboxes are synchronized.
10. If clients connect to the Exchange Server through an ISA Server, you will need to publish the Enterprise Vault web server URL in addition to the Exchange Server.

Preparing proxy bypass list entries for OWA 2000 and OWA 2003 Extensions

Before installing the Enterprise Vault OWA 2000 or 2003 Extensions on the Exchange Servers, you need to prepare the file `EVServers.txt`. This file provides the installation program with the entries to add to the proxy bypass list. You populate the file on an Enterprise Vault server using the script, `MakeEVServersTxt.wsf`, and then make it available to the Exchange Server administrator who installs the Enterprise Vault OWA Extensions.

To prepare EVServers.txt

1. Log on to any Enterprise Vault server, using an account that has any Enterprise Vault administrator permissions.
2. Start Windows Explorer and navigate to the Enterprise Vault installation folder (for example `C:\Program Files (x86)\Enterprise Vault`). Open the appropriate OWA Extensions subfolder for the Extensions that you want to install: `OWA 2003 Extensions` subfolder or `OWA 2000 Extensions` subfolder.
3. Double-click `MakeEVServersTxt.wsf`.

   This script populates the file, `EVServers.txt`, with the entries that the installation program will add to the proxy bypass list.
4. If you are installing the OWA Extensions remotely using, for example, Active Directory, then copy the `EVServers.txt` file to the file share containing the installation files.

   If you are installing the OWA Extensions interactively on each server, then copy `EVServers.txt` to each Exchange Server 2003 and Exchange 2000 back-end server.

Installing the OWA Extensions on Exchange 2000 and Exchange Server 2003

Before you install the Enterprise Vault OWA Extensions, ensure that you have completed the prerequisite tasks.

See "Configuring Enterprise Vault access for OWA users" on page 166.

On the Enterprise Vault release media, the Enterprise Vault OWA 2000 Extensions installation program is located in the folder `Symantec Enterprise Vault\OWA Extensions\OWA 2000 Extensions`.

The Enterprise Vault OWA 2003 Extensions installation program is located in the folder `Symantec Enterprise Vault\OWA Extensions\OWA 2003 Extensions`.

You run the OWA Extensions installation program on the front-end Exchange Servers first, and then on the back-end Exchange Servers.

The instructions given in this section describe a typical, interactive installation, which you initiate by double-clicking the `.msi` file. Alternatively, the OWA Extensions can be deployed silently using an MSI command line, or using an Active Directory Group Policy Object (GPO) to install to a particular Organizational Unit (OU).

See "To perform a silent installation using the MSI command line" on page 175.

See "To perform an installation using an Active Directory Group Policy Object (GPO)" on page 175.

If you have problems with installing Enterprise Vault OWA Extensions, see the following technical note on the Symantec Support website:

http://www.symantec.com/docs/TECH69113

This technical note gives detailed troubleshooting information for Enterprise Vault OWA Extensions.

To run the OWA Extensions installation program

1. Log in to your Exchange Server computer as the account used to install Exchange Server.
2. Obtain the appropriate installation file (`Symantec Enterprise Vault OWA 2000 Extensions.msi` for Exchange 2000 or `Symantec Enterprise Vault OWA 2003 Extensions.msi` for Exchange Server 2003), together with the `EVServers.txt` file. You can copy the files to the Exchange Server computer or run them from a shared folder, as required.
3. Double-click the appropriate `.msi` file.
4. Follow the instructions on your screen.
5. When you install OWA 2000 Extensions, you are given the option to view the Enterprise Vault installation log files at the end of the installation program. The log files are created in the installation folder for the OWA Extensions (for example, `C:\Program Files (x86)\Enterprise Vault\OWA`).

   When you install OWA 2003 Extensions, you are not given an option to view log files. If the installation of the OWA 2003 Extensions fails, a message is reported in the event log, and also at the end of the installation program. The message in the installation program gives the location of the Enterprise Vault installation log files.

To perform a silent installation using the MSI command line

1 Enter the following MSI command line:

```
msiexec.exe /i <path to .msi file> /qn
```

This will install with no graphical interface or notification messages to the user who is running the command.

Specifying the parameter, `/qb`, instead of `/qn`, displays a progress bar with a cancel button.

2 Any installation messages will appear in the log files.

For more information on Windows Installer, see:

http://msdn.microsoft.com/en-us/library/aa372866.aspx

To perform an installation using an Active Directory Group Policy Object (GPO)

1 Create a new Group Policy Object (GPO) for the OU:

- Open the OU properties dialog box.
- Select the **Group Policy** tab, and click **New**.

2 Click **Edit**, and add software packages:

- Select either **User** or **Computer Configuration**.
- Select **Software Settings** > **Software Installations**.
- To add an `.msi` package, right click and select **New** > **Package**.

Installing Enterprise Vault OWA 2007 Extensions

Before you install the Enterprise Vault OWA Extensions, ensure that you have completed the prerequisite tasks.

See "Configuring Enterprise Vault access for OWA users" on page 166.

Enterprise Vault OWA 2007 Extensions are located in the folder, `Symantec Enterprise Vault\OWA Extensions\OWA 2007 Extensions` on the Enterprise Vault release media.

There is a ReadMeFirst file in the `Symantec Enterprise Vault` folder. Before you install the extensions, ensure that you check this file for details of any last-minute changes.

Two versions of the Enterprise Vault OWA 2007 Extensions are available:

- `Symantec Enterprise Vault OWA 2007 Extensions x64.msi`, for Exchange Server 2007 in 64-bit mode

- `Symantec Enterprise Vault OWA 2007 Extensions x86.msi`, for Exchange Server 2007 in 32-bit mode

Follow the instructions in this section to install the extensions interactively. Alternatively, the OWA Extensions can be deployed silently using an MSI command line, or using an Active Directory Group Policy Object (GPO) to install to a particular Organizational Unit (OU).

To enable logging for the installation process, either set up the logging policy for Windows installer on the server, or run the installer using the `msiexec` command line and include the logging option:

`/l*v log_filename`

See "To perform a silent installation using the MSI command line" on page 175.

See "To perform an installation using an Active Directory Group Policy Object (GPO)" on page 175.

If you have problems with installing Enterprise Vault OWA Extensions, see the following technical note on the Symantec Support website:

http://www.symantec.com/docs/TECH69113

This technical note gives detailed troubleshooting information for Enterprise Vault OWA Extensions.

To install Enterprise Vault OWA 2007 Extensions

1. Copy the appropriate OWA 2007 Extensions MSI file to the Exchange 2007 CAS computer.
2. Double-click the MSI file to start the installation wizard.
3. Follow the installation instructions.
4. Repeat the installation on each Exchange 2007 CAS computer.

Additional configuration steps on Exchange Server 2007 CAS computers for use with OWA

In an Exchange Server 2007 CAS and Mailbox environment, you may need to configure access between CAS servers, or between CAS and Mailbox servers. Table 10-2 shows the additional steps required for different Exchange Server 2007 configurations.

Table 10-2 Configuration required for different Exchange Server 2007 CAS configurations

CAS configuration	Forms-Based Authentication	Integrated Windows Authentication	Basic Authentication
CAS with Mailbox role	No extra configuration required	No extra configuration required	No extra configuration required
CAS to Mailbox server	No extra configuration required	See "Setting up constrained delegation for use with OWA" on page 180.	No extra configuration required
CAS with Mailbox role to Mailbox server	See "Configuration for Mailbox Role on both CAS server and remote servers for use with OWA" on page 178.	See "Configuration for Mailbox Role on both CAS server and remote servers for use with OWA" on page 178. and See "Setting up constrained delegation for use with OWA" on page 180.	See "Configuration for Mailbox Role on both CAS server and remote servers for use with OWA" on page 178.
CAS to CAS with Mailbox role	Not applicable	See "Additional configuration for linked mailboxes for use with OWA" on page 181.	Not applicable
CAS to CAS to Mailbox server	Not applicable	See "Setting up constrained delegation for use with OWA" on page 180. and See "Additional configuration for linked mailboxes for use with OWA" on page 181.	Not applicable

Table 10-2 Configuration required for different Exchange Server 2007 CAS configurations *(continued)*

CAS configuration	Forms-Based Authentication	Integrated Windows Authentication	Basic Authentication
CAS to CAS with Mailbox role to Mailbox server	Not applicable	See "Configuration for Mailbox Role on both CAS server and remote servers for use with OWA" on page 178. and See "Setting up constrained delegation for use with OWA" on page 180. and See "Additional configuration for linked mailboxes for use with OWA" on page 181.	Not applicable

Configuration for Mailbox Role on both CAS server and remote servers for use with OWA

If you have an environment that includes Exchange 2007 Mailbox Role installed on the Exchange 2007 CAS server computer and also remote Exchange 2007 Mailbox servers, you need to perform additional configuration as described in this section. The steps differ depending on whether you want the Exchange 2007 CAS server to connect to remote Exchange 2007 Mailbox servers using HTTPS or HTTP.

The configuration includes adding settings to the configuration file, *Exchange installation path*\ClientAccess\Owa\Web.Config, on the Exchange 2007 CAS server.

Table 10-3 shows the relevant settings that you can add to this file. These should be added to the **AppSettings** section of the file using the following format:

```
<add key="setting" value="value"/>
```

Note that entries in this file are case sensitive.

Table 10-3 Web.Config settings

Setting	Default Value	Notes
EnterpriseVault_WebDAVRequestProtocol	https	The protocol used by the Exchange 2007 CAS server when making WebDav requests.
EnterpriseVault_WebDAVRequestHost	Value set to "localhost" at installation. Also, if you repair the extensions in Add or Remove Programs, the value is reset to “localhost”. If the setting is not specified, then the name of the Mailbox server for the mailbox being accessed is used.	The target server for WebDav requests. If the setting is not specified (that is, the name of the Mailbox server for the mailbox is used), then either the protocol must be set to http, or a certificate must be installed on each Mailbox server.
EnterpriseVault_ WebDAVRequestVirtualDirectory	exchange	The virtual directory used by the Exchange 2007 CAS server when making WebDav requests.

To connect to remote Exchange 2007 Mailbox servers using HTTPS

1. Open the `web.config` file (*`Exchange installation path`*`\ClientAccess\Owa\Web.Config`) in a text editor.
2. Delete or comment out the following entry:

```
<add key="EnterpriseVault_WebDAVRequestHost" value="localhost"/>
```

3. Save and close the file.
4. Install a certificate for IIS on each of the remote Exchange 2007 Mailbox servers.

To connect to remote Exchange 2007 Mailbox servers using HTTP

1. Open the `web.config` file (*`Exchange installation path`*`\ClientAccess\Owa\Web.Config`) in a text editor.
2. Delete or comment out the following entry:

```
<add key="EnterpriseVault_WebDAVRequestHost" value="localhost"/>
```

3. Add the following entry:

```
<add key="EnterpriseVault_WebDAVRequestProtocol" value="http"/>
```

4. Save and close the file.

   You do not need to install a certificate for IIS on the remote Exchange 2007 Mailbox servers.

Setting up constrained delegation for use with OWA

It is necessary to configure constrained delegation for use with the Enterprise Vault OWA 2007 Extensions if the mailbox being accessed is located on a server which is separate from the CAS computer, and users are authenticated to OWA using Integrated Windows Authentication (IWA).

Note that IWA is a requirement to support Client Access Server (CAS) proxying. For information on CAS proxying, see http://msexchangeteam.com/archive/2007/09/04/446918.aspx

Configuring constrained delegation requires a domain functional level of Windows Server 2003 or later. For more information about domain functional levels, see "Domain and forest functionality" in the Help and Support Center for Windows Server 2003.

For each CAS configured for IWA, perform the following steps:

1. Using Active Directory **Users and Computers**, locate the CAS computer account.
2. Right-click the computer object, and click **Properties**.
3. Click the **Delegation** tab.
4. On the **Delegation** page, click **Trust this computer for delegation to specified services only**.
5. Click **Use any authentication protocol**.
6. Click **Add**, and then **Users or Computers**.

7 In the box, **Enter the object names to select**, type the name of an Exchange Server 2007 computer which has mailbox role installed and will be accessed through this CAS.

If the Mailbox role is clustered, be sure to use the Clustered Mailbox Server name instead of the node name.

8 Click **Check Names**, and then **OK**.

9 In the **Available services** list, click **http**, and then **OK**.

10 Repeat steps 6 to 9 to add additional Exchange Server 2007 Mailbox computers that will be accessed through this CAS.

For constrained delegation to work properly, Exchange Server 2007 computers with Mailbox roles must have IWA enabled on the `/Exchange` virtual directory.

Additional configuration for linked mailboxes for use with OWA

When implementing CAS proxying in a Resource Forest topology, you need to perform the following, additional configuration steps to enable OWA users to access linked mailboxes using Integrated Windows Access (IWA):

- Ensure that the account used by the Enterprise Vault Exchange Mailbox archiving task is in the Resource Forest. Typically the task runs as the Vault Service account.
- If calls are to be made from a user in a different forest from the one in which Exchange Server is installed, then you must ensure that a bi-directional Forest trust is configured.

Note: This is not the same as a bi-directional external trust, which is a trusted domain object (TDO). A trusted domain object does not contain the required forest trust information to manage authentication requests to the remote forest.

For more information on this requirement, see the following technical note on the Symantec Support website, http://www.symantec.com/docs/TECH62946.

- Using Exchange Management Shell, run the following command line to give the Enterprise Vault Exchange Mailbox task account the required access rights on the linked mailbox:

```
Add-ADPermission -Identity LinkedMailboxName
-User MailboxTaskAccount -AccessRights ExtendedRight
-ExtendedRights "Send As"
```

For example,

```
Add-MailboxPermission -Identity "Service Requests"
-User vsa -AccessRights ExtendedRight -ExtendedRights "Send As"
```

To set the permission on many mailboxes, you can use the Get-Mailbox cmdlet in a PowerShell pipeline.

- On the CAS Servers associated with each user who will access the linked mailbox, edit the OWA configuration file, `Web.Config`, as follows:
  - Take a backup copy of the file,
    Exchange installation folder\ClientAccess\Owa\Web.Config
    and then open the file for editing.
  - Add the following entry to the **AppSettings** section of the file:

    ```
    <add key="EnterpriseVault_VaultServiceAccountUPN"
    value="MailboxTaskAccountUPN">
    ```

    For example,

    ```
    <add key="EnterpriseVault_VaultServiceAccountUPN"
    value="vsa@domain.com">
    ```

    Note that the value given must be the User Principal Name (UPN) for the Exchange Mailbox task account, and this account must be in the Resource Forest.
    Entries in this file are case sensitive.

Installing Enterprise Vault OWA 2010 Extensions

Before you install the Enterprise Vault OWA Extensions, ensure that you have completed the prerequisite tasks.

See "Configuring Enterprise Vault access for OWA users" on page 166.

Enterprise Vault OWA 2010 Extensions are located in the folder, `Symantec Enterprise Vault\OWA Extensions\OWA 2010 Extensions` on the Enterprise Vault release media.

A ReadMeFirst file is located in the `Symantec Enterprise Vault` folder. Before you install the extensions, ensure that you check this file for details of any last-minute changes.

Follow the instructions in this section to install the extensions interactively. Alternatively, the OWA Extensions can be deployed silently using an MSI command line, or using an Active Directory Group Policy Object (GPO) to install to a particular Organizational Unit (OU).

To enable logging for the installation process, either set up the logging policy for Windows Installer on the server, or run the installer using the `msiexec` command line and include the logging option:

```
/l*v log_filename
```

See "To perform a silent installation using the MSI command line" on page 175.

See "To perform an installation using an Active Directory Group Policy Object (GPO)" on page 175.

If you have problems with installing Enterprise Vault OWA Extensions, see the following technical note on the Symantec Support website: http://www.symantec.com/docs/TECH69113. This technical note gives detailed troubleshooting information for Enterprise Vault OWA Extensions.

To install Enterprise Vault OWA 2010 Extensions

1. Copy the appropriate OWA 2010 Extensions MSI file to the Exchange 2010 CAS computer.
2. Double-click the MSI file to start the installation wizard.
3. Follow the installation instructions.
4. Repeat the installation on each Exchange 2010 CAS computer.

Additional configuration steps for Exchange Server 2010 CAS proxying for use with OWA

If CAS proxying is configured in an Exchange Server 2010 environment, you need to perform additional configuration steps to allow the CAS proxy servers to use Exchange Web Services impersonation.

Configuring Exchange Web Services impersonation on CAS proxy servers

1. Create a new security group that contains only the Exchange Server 2010 CAS computers that act as proxy servers.
2. Log on to an Exchange Server 2010 computer using an account that is assigned the "Role Management" role. By default, members of the "Organization Management" role group are assigned this role.
3. Using Exchange Management Shell, run the following command line:

   ```
   New-ManagementRoleAssignment -Name:role assignment name
   -Role:ApplicationImpersonation -SecurityGroup:security group name
   ```

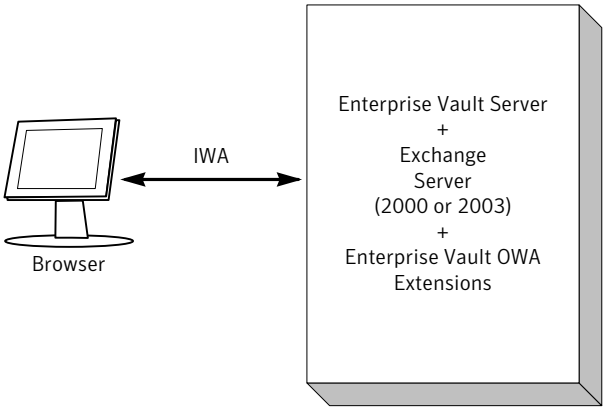
   role assignment name can be a name of your choice.

   security group name is the name of the security group you created for the proxy Exchange 2010 CAS servers.

Configuring a demonstration system for use with Enterprise Vault OWA 2003 Extensions

If you are setting up an Enterprise Vault environment to demonstrate or pilot Enterprise Vault OWA 2003 Extensions, the Enterprise Vault server and Exchange Server are typically installed on one computer, as shown in Figure 10-8.

Figure 10-8 Typical demonstration configuration



In this example, you would install and configure the Enterprise Vault OWA Extensions for a back-end Exchange Server.

Chapter 11

Configuring access to Enterprise Vault from Outlook RPC over HTTP clients

This chapter includes the following topics:

About Outlook RPC over HTTP and Outlook Anywhere configurations

This section provides overview information about access to Enterprise Vault from Outlook RPC over HTTP clients and Outlook Anywhere clients. References are provided to other sections where you can find more detailed instructions on configuration tasks.

With Outlook 2003 and later, users can access mailboxes using remote procedure call (RPC) over HTTP. With this protocol, MAPI is used to tunnel Outlook RPC requests inside an HTTP session. Using RPC over HTTP remote Outlook users can connect to Exchange Server mailboxes without the requirement for OWA or a virtual private network (VPN) connection.

In an Exchange Server 2007 or 2010 environment, when Outlook is configured to use RPC over HTTP, the feature is called Outlook Anywhere.

With RPC over HTTP enabled, the Enterprise Vault Outlook Add-In can perform the following actions:

- View archived items.
- Archive items manually.
- Restore archived items.
- Delete archived items.
- Search archives using Integrated Search. (Browser Search link is not available.)
- Use Archive Explorer.
- Use Vault Cache.
- Perform client-side PST migrations.

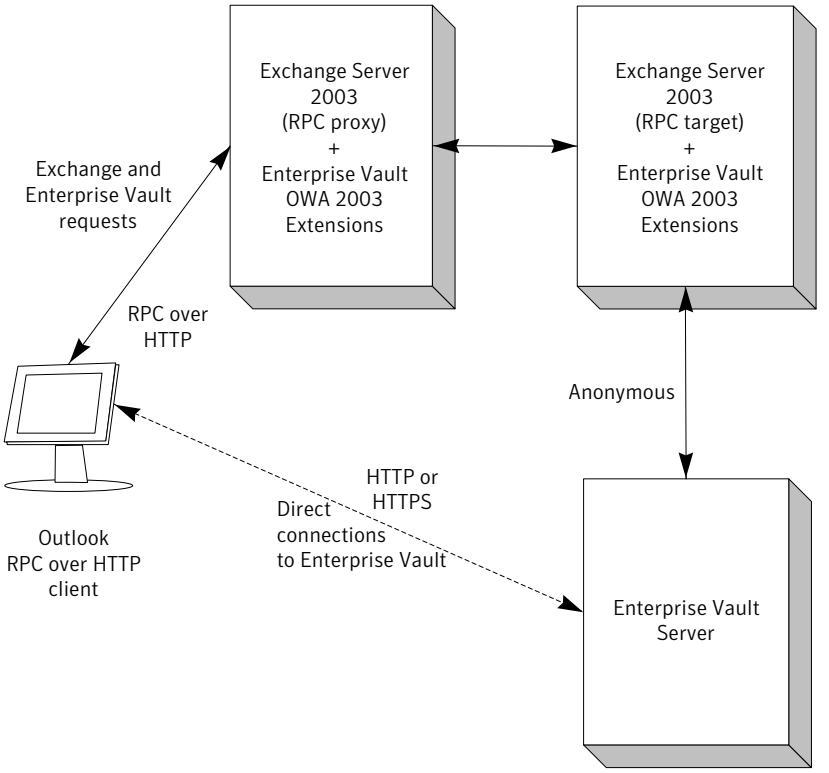
About RPC over HTTP client and Exchange Server 2003 configurations

In an Exchange Server 2003 environment, front-end Exchange RPC servers are called RPC proxy servers, and back-end Exchange Servers are called RPC target servers.

To support Outlook RPC over HTTP client connections to Enterprise Vault, you need to install the Enterprise Vault RPC 2003 Extensions on your Exchange Server 2003 RPC proxy and target computers.

You can enable Enterprise Vault support for both OWA and Outlook RPC over HTTP client connections. Follow the instructions for configuring the Enterprise Vault OWA Extensions first. You can then work through this chapter to complete the configuration that is required for Outlook RPC over HTTP client connections.

Figure 11-1 Example Outlook RPC over HTTP client and Exchange Server 2003 configuration



In Figure 11-1 Outlook is configured for RPC over HTTP, and the Enterprise Vault Outlook Add-In is enabled for RPC over HTTP connections.

RPC over HTTP settings in the Enterprise Vault Exchange Desktop policy let you configure how the client sends requests to Enterprise Vault:

- The default Enterprise Vault Exchange Desktop policy settings assume that clients send requests to Enterprise Vault through Exchange RPC proxy and target servers.

  To support this configuration, the Enterprise Vault RPC 2003 Extensions must be installed on both the RPC proxy and target servers.

  The client connects to the Exchange RPC proxy server. You can set the URL to use in the Enterprise Vault Exchange Desktop policy. If a URL is not specified in the Enterprise Vault policy, then the client uses the proxy URL configured for RPC over HTTP in the Outlook profile.

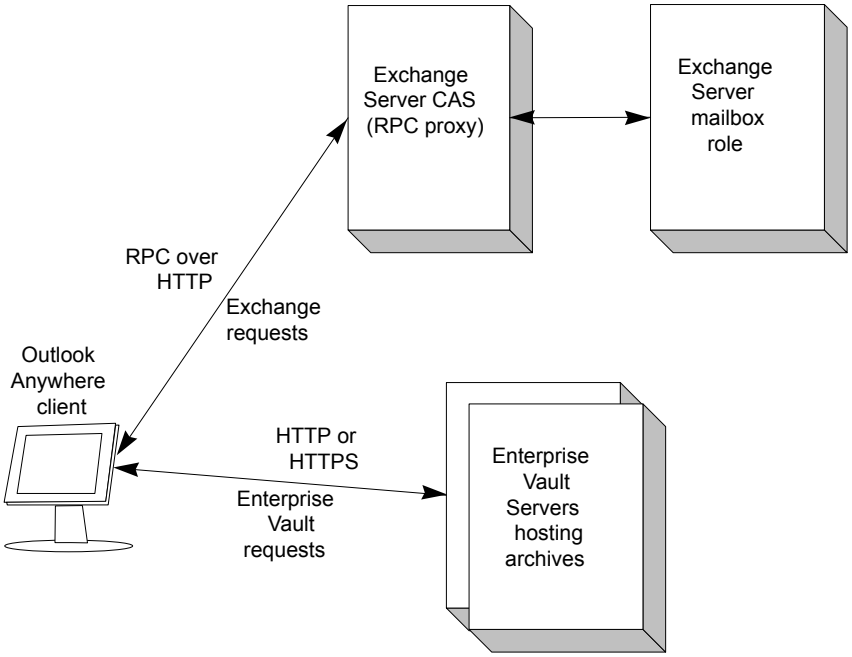
- Alternatively, you can configure the Enterprise Vault Outlook Add-In to connect directly to the Enterprise Vault server. With direct connections, all the Enterprise Vault servers that host the archives must be accessible to the internal and external clients.
  Note that the Enterprise Vault RPC 2003 Extensions are not required to support direct connections to the Enterprise Vault server from Outlook RPC over HTTP clients.

See "Configuring Exchange Server 2003 RPC over HTTP client access to Enterprise Vault" on page 191.

About Exchange Server Outlook Anywhere configurations

With Outlook Anywhere, the Enterprise Vault Outlook Add-In contacts an Enterprise Vault server directly. The Enterprise Vault client does not route requests to Enterprise Vault using an Exchange Server 2007 or 2010 CAS computer. The Enterprise Vault OWA Extensions are not required on your Exchange Server to support Enterprise Vault access from Outlook Anywhere clients.

Figure 11-2 Example Outlook Anywhere and Exchange Server configuration



In Figure 11-2 Outlook is configured for Outlook Anywhere, and the Enterprise Vault Outlook Add-In is enabled for RPC over HTTP connections.

The Enterprise Vault client contacts Enterprise Vault as follows:

- By default, the client first attempts to contact the default Enterprise Vault server that hosts the archive.
- If that is unavailable, the client uses the RPC over HTTP proxy URL configured in the Enterprise Vault Exchange Desktop policy.
- If no URL is specified in the Enterprise Vault policy, then the client uses the Exchange proxy URL configured in the Outlook profile.

With direct connections, all the Enterprise Vault servers that host the archives must be accessible to the internal and external clients. If you do not want to publish multiple Enterprise Vault servers to external clients, then you can use an Enterprise Vault server as a proxy server. A client connects to the Enterprise Vault proxy server, and the proxy server forwards the requests to the Enterprise Vault server that hosts the archive.

See "About Enterprise Vault proxy server configurations for access to Outlook RPC over HTTP clients" on page 189.

See "Configuring Outlook Anywhere client access to Enterprise Vault" on page 195.

About Enterprise Vault proxy server configurations for access to Outlook RPC over HTTP clients

Optionally, you can use an Enterprise Vault server as a proxy server for Enterprise Vault requests from the Enterprise Vault Outlook Add-In when Outlook Anywhere is configured. The Enterprise Vault proxy server forwards Enterprise Vault requests to the Enterprise Vault server that hosts the archive. In environments with multiple Enterprise Vault sites, a separate Enterprise Vault proxy server is required for each site.

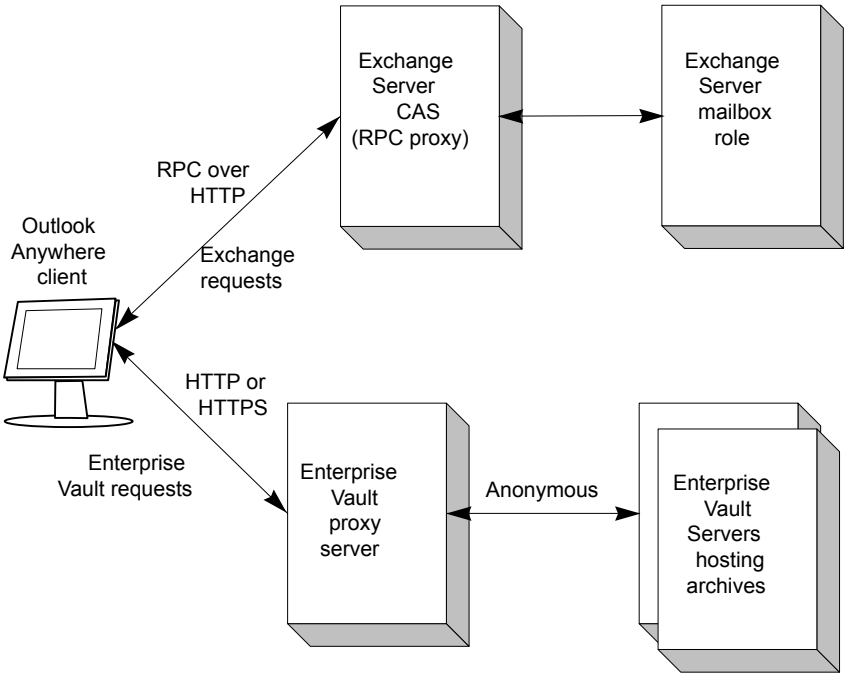
An Enterprise Vault proxy server is useful in the following situations:

- If you do not want to publish multiple Enterprise Vault servers to external users.
- If you want to publish separate URLs for external and internal Enterprise Vault users.

Note that an Enterprise Vault proxy server can only be used to manage connections from Outlook Anywhere clients. It cannot be used for other types of connections, such as OWA.

The figure, Figure 11-3, illustrates an Enterprise Vault proxy server in an Outlook Anywhere configuration. The Enterprise Vault server that is used as a proxy server can also host archives, if required. Alternatively, you can set up a minimal Enterprise Vault server to be used as a proxy server only.

Figure 11-3 Example Outlook Anywhere configuration using an Enterprise Vault proxy server



Settings in the Enterprise Vault Exchange Desktop policy let you configure the behavior of the Enterprise Vault Outlook Add-In when Outlook is configured to use RPC over HTTP.

The Enterprise Vault client contacts Enterprise Vault as follows:

- The Enterprise Vault client first attempts to connect to the default Enterprise Vault server that hosts the archive.
- If the client cannot contact the server, then the client uses the URL that you specify for the Enterprise Vault Exchange Desktop policy setting, **RPC over HTTP proxy URL**.
  This logic enables users to connect directly to the Enterprise Vault server that hosts the archive when they are in the office. When they are away from the office, the Enterprise Vault client connects to the Enterprise Vault proxy server.
- If no URL is specified in the Enterprise Vault policy, then the client uses the Exchange proxy URL configured in the Outlook profile.

The Enterprise Vault proxy server connects to the Enterprise Vault server that hosts the archive using anonymous connections. For this reason you must

configure support for anonymous connections on each Enterprise Vault server that the proxy server contacts.

In an Enterprise Vault cluster you need to configure each node in the cluster for anonymous connections.

Similarly, in building blocks configurations you may need to configure support for anonymous connections on the proxy server computer. This configuration is required for Virtual Vault users if a Storage Service can fail over to the Enterprise Vault proxy server computer.

Instructions for setting up an Enterprise Vault proxy server, and configuring support for anonymous connections are given in the following section:

See "Setting up an Enterprise Vault proxy server to manage connections from Outlook Anywhere clients" on page 196.

Configuring Exchange Server 2003 RPC over HTTP client access to Enterprise Vault

This section describes the steps to configure Enterprise Vault access from Outlook clients using RPC over HTTP in an Exchange Server 2003 environment.

To configure Enterprise Vault in an Exchange Server 2003 environment

1. If the RPC target Exchange Servers are in a clustered environment, ensure that you are familiar with the additional configuration requirements before you install the Enterprise Vault extensions.

   See "About configuring OWA and RPC Extensions in clustered configurations" on page 203.

2. Check that prerequisite tasks are completed.

   See "Prerequisite tasks to configure Enterprise Vault access from Outlook clients using RPC over HTTP in an Exchange Server 2003 environment" on page 192.

3. On Enterprise Vault servers, configure the server to accept anonymous connections from Exchange RPC target servers (back-end Exchange Server 2003). This step is the same as for OWA access.

   See "Configuring Enterprise Vault for anonymous connections" on page 168.

4 On an Enterprise Vault server, configure RPC over HTTP settings in the Exchange Desktop policy in the Enterprise Vault Administration Console. These settings enable and customize Enterprise Vault functionality in the Enterprise Vault Outlook Add-In when Outlook is configured to use RPC over HTTP.

   See "Configuring RPC over HTTP settings in Enterprise Vault Exchange Desktop policy" on page 200.

5 On an Enterprise Vault server, populate the `EVServers.txt` file, and make it available to each RPC target server (back-end Exchange Server 2003).

   See "To prepare EVServers.txt" on page 193.

6 On each Exchange RPC proxy server, and each Exchange RPC target server, run the installation program to install and automatically configure the Enterprise Vault OWA and RPC Extensions.

   See "Installing the Enterprise Vault OWA and RPC Extensions on Exchange Server 2003" on page 192.

Prerequisite tasks to configure Enterprise Vault access from Outlook clients using RPC over HTTP in an Exchange Server 2003 environment

The instructions for configuring access to Enterprise Vault assume that you have already completed the following tasks:

- Configured your Exchange environment and Outlook profiles for RPC over HTTP for Outlook.
- If you plan to use an Enterprise Vault proxy server, then you may want to configure SSL for client connections on that server also.
- Configured your Enterprise Vault server to archive Exchange Server mailboxes, public folders, or both.
- Installed the Enterprise Vault Outlook Add-In on the desktop computers.

Installing the Enterprise Vault OWA and RPC Extensions on Exchange Server 2003

Ensure that you have completed the required steps before installing the Enterprise Vault Extensions.

See "Configuring Exchange Server 2003 RPC over HTTP client access to Enterprise Vault" on page 191.

Before you run the Enterprise Vault Extensions installation program on the Exchange Server, you populate an `EVServers.txt` file on an Enterprise Vault

server, as described in this section, and then copy the file to the same folder as the MSI installation file. The Exchange Server administrator who installs the Enterprise Vault Extensions must have access to both files.

You run the Enterprise Vault Extensions installation program on the RPC proxy servers first, and then on the RPC target servers.

The instructions that are given in this section describe a typical, interactive installation, which you initiate by double-clicking the `.msi` file. Alternatively, you can deploy the Enterprise Vault Extensions silently using an MSI command line, or an Active Directory group policy object (GPO). You can use this method to install to a particular organizational unit (OU).

See "To perform a silent installation using the MSI command line" on page 194.

See "To perform an installation using an Active Directory group policy object (GPO)" on page 194.

To prepare EVServers.txt

1. Log on to any Enterprise Vault server, using an account that has any Enterprise Vault administrator permissions.
2. Start Windows Explorer and navigate to the `OWA 2003 Extensions` subfolder of the Enterprise Vault installation folder (for example `C:\Program Files (x86)\Enterprise Vault\OWA`).
3. Double-click `MakeEVServersTxt.wsf`.
4. If you install the Enterprise Vault Extensions remotely, then the `EVServers.txt` file needs to be copied to the same location as the MSI installation file. If you install the Enterprise Vault Extensions interactively on each server, then `EVServers.txt` and the MSI installation file need to be available to each RPC target server (back-end Exchange Server 2003).

To install the Enterprise Vault Extensions on an RPC proxy server

1. Log on to your Exchange Server computer.
2. Obtain the installation file, `Symantec Enterprise Vault OWA 2003 Extensions.msi`. You can copy the file to the Exchange Server computer or run it from a shared folder, as required.
3. Double-click the `.msi` file.
4. Follow the instructions on your screen.
5. If the installation fails, a message is reported at the end of the installation program, and also in the event log. The message in the installation program gives the location of the Enterprise Vault installation log files.

To install the Enterprise Vault Extensions on an RPC target server

1. Log on to your Exchange Server computer.
2. Obtain the installation file, `Symantec Enterprise Vault OWA 2003 Extensions.msi`, together with the `EVServers.txt` file. You can copy the files to the Exchange Server computer or run them from a shared folder, as required.
3. Ensure that the Exchange Server is running and that the website that is associated with the Exchange Server has an `ExAdmin` virtual directory created.
4. To install and configure both RPC and OWA, double-click the `.msi` file.

   To install and configure RPC only (without OWA), type and enter the command line:

   ```
   msiexec.exe /i <path to .msi file> RPCEXTENSIONS=1
   ```

5. Follow the instructions on your screen.
6. If the installation fails, a message is reported at the end of the installation program, and also in the event log. The message in the installation program gives the location of the Enterprise Vault installation log files.

To perform a silent installation using the MSI command line

1. Enter the following MSI command line:

   ```
   msiexec.exe /i <path to .msi file> RPCEXTENSIONS=1 /qn
   ```

   This command installs and configures RPC only, with no graphical interface or notification messages to the user who is running the command.

   Specifying the parameter, `/qb`, displays a progress bar with a cancel option.
2. Any installation messages appear in the log files.

   For more information on Windows Installer, see

   http://msdn.microsoft.com/en-us/library/aa372866.aspx

To perform an installation using an Active Directory group policy object (GPO)

1. Create a new group policy object (GPO) for the OU:
   - Open the OU properties dialog.
   - Select the **Group Policy** tab, and click **New**.
2. Click **Edit**, and add software packages:
   - Select either **User** or **Computer Configuration**.
   - Select **Software Settings**>**Software Installations**.

- To add an `.msi` package, right-click and select **New>Package**.

Configuring Outlook Anywhere client access to Enterprise Vault

This section describes the configuration steps required to enable Outlook Anywhere client access to Enterprise Vault servers.

To configure Enterprise Vault in an Outlook Anywhere environment

1. Check that prerequisite tasks on Exchange Servers and client computers are completed.

   See "Prerequisite tasks for configuring Outlook Anywhere access to Enterprise Vault" on page 195.

2. If you plan to use an Enterprise Vault proxy server, then prepare the proxy server and any Enterprise Vault servers that it contacts.

   See "Setting up an Enterprise Vault proxy server to manage connections from Outlook Anywhere clients" on page 196.

3. On an Enterprise Vault server, configure RPC over HTTP settings in the Exchange Desktop policy to enable and customize Enterprise Vault functionality in the Enterprise Vault Outlook Add-In.

   See "Configuring RPC over HTTP settings in Enterprise Vault Exchange Desktop policy" on page 200.

Prerequisite tasks for configuring Outlook Anywhere access to Enterprise Vault

The instructions for configuring Outlook Anywhere access to Enterprise Vault assume that you have already completed the following tasks:

- Configured your Exchange environment and Outlook profiles for Outlook Anywhere.
- Configured your Enterprise Vault server to archive Exchange Server mailboxes.
- Installed Enterprise Vault the Outlook Add-In on the desktop computers.

Setting up an Enterprise Vault proxy server to manage connections from Outlook Anywhere clients

This section describes what you need to do if you want to use an Enterprise Vault proxy server to manage connections from Outlook Anywhere clients. These task include:

- Configuring the Enterprise Vault proxy server to manage connections from Outlook Anywhere clients
  See "Configuring the Enterprise Vault proxy server to manage connections from Outlook Anywhere clients" on page 196.
- Configuring Enterprise Vault servers for anonymous connections from the Enterprise Vault proxy server
  See "Configuring Enterprise Vault servers for anonymous connections from the Enterprise Vault proxy server" on page 197.

See "About Enterprise Vault proxy server configurations for access to Outlook RPC over HTTP clients" on page 189.

Configuring the Enterprise Vault proxy server to manage connections from Outlook Anywhere clients

If there are multiple Enterprise Vault sites, separate Enterprise Vault proxy servers are required for each site.

The Enterprise Vault server that is used as a proxy server can also host archives, if required. Alternatively, you can set up a minimal Enterprise Vault server to be used as a proxy server.

At minimum the proxy server must have the following Enterprise Vault components installed and configured:

- Admin Service.
- Directory service.
- Shopping service.
- Task Controller service.
- Web Access application.

Clients use basic or integrated windows authentication (IWA) authentication to connect to the Enterprise Vault proxy server. If required, you can configure SSL on the Enterprise Vault proxy server to secure the client connections.

See "Customizing security for the Enterprise Vault Web Access application" in the *Installing and Configuring* manual.

If the Enterprise Vault proxy server does not host archives, then it does not require any additional configuration to support Enterprise Vault requests.

The Enterprise Vault proxy server uses anonymous connections when it connects to the Enterprise Vault servers that host archives. Detailed instructions are provided on how to configure the Enterprise Vault servers to support anonymous connections.

See "Configuring Enterprise Vault servers for anonymous connections from the Enterprise Vault proxy server" on page 197.

If the Enterprise Vault proxy server hosts archives, then you also need to configure the proxy server for anonymous connections.

In a clustered Enterprise Vault environment, you need to configure each node in the cluster for anonymous connections.

Configuring Enterprise Vault servers for anonymous connections from the Enterprise Vault proxy server

The instructions in this section are similar to the instructions for configuring Enterprise Vault servers for anonymous connections from OWA Exchange Servers. To support anonymous connections from an Enterprise Vault proxy server, you run the same script, `owauser.wsf`, but provide the details of connecting Enterprise Vault proxy servers instead of Exchange Servers.

To prepare Enterprise Vault servers for anonymous connections from an Enterprise Vault proxy server

1. Ensure that IIS Roles and Feature Delegation rights are configured as described in the section, "Prerequisites for OWA" in *Installing and Configuring*.
2. On each Enterprise Vault server that may receive anonymous connections from Enterprise Vault proxy servers, create an `ExchangeServers.txt` file as described in this section. This file contains a list of the IP addresses for all the Enterprise Vault proxy servers that connect to the Enterprise Vault server.
3. On each Enterprise Vault server on which you have created an `ExchangeServers.txt` file, run the script, `owauser.wsf`, as described in this section. This script configures the Data Access account for anonymous connections.
4. Restart the Enterprise Vault Admin Service .
5. Synchronize mailboxes.

To create the `ExchangeServers.txt` file

1. Open Notepad.
2. Type the IP address of each Enterprise Vault proxy server that connects to the Enterprise Vault server, one entry per line.

   Addresses can be in either IPv4 or IPv6 format. IPv6 addresses must be in the form **fdfa:9c37:5267:d2e3:a192:b168:cc80:d204**.
3. Save the file as `ExchangeServers.txt` in the Enterprise Vault installation folder (for example `C:\Program Files (x86)\Enterprise Vault`). When you save the file, select ANSI, Unicode, or Unicode big endian encoding.
4. Close Notepad.

To configure the Data Access account for Outlook RPC over HTTP client connections

1. If you have already configured Enterprise Vault for OWA or Domino Server Archiving, then an account already exists for managing anonymous connections. This account is the Data Access account. If the account already exists, you must use the same account for anonymous connections from Enterprise Vault proxy servers.

   For Domino Mailbox Archiving, the details of the Data Access account are specified on the **Data Access Account** tab of Directory properties in the Administration Console.

   If the Data Access account does not exist, then create an account for this purpose. The account should be a basic domain account; a local machine account cannot be used. The account should not belong to any administrator group, such as Administrators or Account Operators.
2. Use the Vault Service account to log on to the Enterprise Vault server that receives anonymous connections from the Enterprise Vault proxy server.
3. Open a Command Prompt window with administrator privileges.
4. Navigate to the Enterprise Vault installation folder.

5 Enter the following command line:

```
cscript owauser.wsf /domain:domain /user:username
/password:password
```

The file `owauser.wsf` is installed in the Enterprise Vault installation folder.

For *domain*, give the domain of the Data Access account.

For *username*, give the user name of the Data Access account.

For *password*, give the password of the Data Access account.

To display help for the `cscript` command, type

```
cscript owauser.wsf /?
```

6 The progress of the script execution is displayed in the command prompt window.

The configuration changes made by the script are described in the following technical note on the Symantec Support website:

http://www.symantec.com/docs/TECH69113

When the configuration script finishes, you are prompted to restart the Enterprise Vault Admin service and synchronize mailboxes.

Restart the Admin service using the Services console.

Use the Enterprise Vault Administration Console to synchronize mailboxes. In the **Exchange Mailbox Archiving** task properties, select the **Synchronization** tab. Synchronize **Mailbox properties and permissions** for all mailboxes.

Restarting the Admin service ensures that Enterprise Vault authentication knows the identity of the Data Access account. Synchronizing the mailboxes updates the client hidden message with the URL to use when connecting to the Enterprise Vault proxy server.

7 If there are multiple Enterprise Vault servers in your environment, logon to each server on which you created an `ExchangeServers.txt` file. Run the script, `owauser.wsf`, using the instructions that are given in this section.

If you add another Enterprise Vault proxy server to your environment at a later date, first add the IP address of the server to the `ExchangeServers.txt` file. Then you rerun the `owauser.wsf` script.

Configuring RPC over HTTP settings in Enterprise Vault Exchange Desktop policy

RPC over HTTP settings in the Enterprise Vault Exchange Desktop policy enable access to Enterprise Vault, and let you customize the Enterprise Vault functionality in Outlook RPC over HTTP clients.

To modify RPC over HTTP Exchange Desktop policy settings

1. In the left pane of the Administration Console, expand the **Policies** container until **Exchange Desktop** policies are visible.
2. In the right-hand pane, double-click the name of the policy you want to edit.

   The policy's properties are displayed.
3. Click the **Advanced** tab.
4. Next to **List settings from**, select **Outlook**.
5. Edit the following settings as required.

   Double-click a setting to edit it, or click it once to select it and then click **Modify**.

   - **RPC over HTTP restrictions**. By default Outlook RPC over HTTP client access is disabled for mailboxes that are hosted on Exchange Server 2010 or earlier versions (**Disable Outlook Add-In**). Configure the functionality that is required in Outlook by selecting one of the other values:

None	All Enterprise Vault client functionality is available.
Disable Outlook Add-In	Enterprise Vault functionality is not available in Outlook RPC over HTTP clients. This is the default value. Exchange Server 2013 only allows connections that use RPC over HTTP. If the default value is selected, all Enterprise Vault Outlook Add-In functionality is available for mailboxes that are hosted on Exchange Server 2013.
Disable Vault Cache	Vault Cache is disabled.
Disable PST Import	Client-side PST migration is disabled. Note that currently you cannot use client-side PST migration to migrate any files that reside on mapped network drives when using an Outlook client in RPC over HTTP mode.
Disable Vault Cache and PST Import	Vault Cache and client-side PST migration are disabled.

- **RPC over HTTP connection**. This setting controls how the Enterprise Vault Outlook Add-In connects to the Enterprise Vault server that hosts the archive. The value for this setting can be **Use proxy** or **Direct**. The options have the following effect.
  - In an Exchange Server 2003 environment. With the default value, **Use proxy**, the client routes all Enterprise Vault requests to the Enterprise Vault server using the Exchange RPC proxy server.
    If the value is **Direct**, then the client attempts to connect directly to the default Enterprise Vault server.
    When the user requests an Enterprise Vault operation, the client first attempts to contact the default Enterprise Vault server. If the connection cannot be made, and **RPC over HTTP connection** is set to **Use proxy**, then the URL configured for **RPC over HTTP Proxy URL** is used.
  - In an Exchange Server 2007 or 2010 environment. With the default value, **Use proxy**, the client routes all Enterprise Vault requests to the Enterprise Vault server using the Enterprise Vault proxy server for the site in which the client is located. The URL for the site proxy server must be specified in the **RPC over HTTP Proxy URL** setting.
    When the user requests an Enterprise Vault operation, the client first attempts to contact the default Enterprise Vault server. If the connection cannot be made, and **RPC over HTTP connection** is set to **Use proxy**, then the URL configured for **RPC over HTTP Proxy URL** is used.
    If the value is **Direct**, then the client attempts to connect directly to the default Enterprise Vault server.

  The value can be set to **Direct** even if you have an ISA Server configured. In this situation you must publish on the ISA Server the URLs of all the Enterprise Vault servers that host the archives.
- **RPC over HTTP Proxy URL**. This setting enables you to specify an alternative URL for the Enterprise Vault server. Enterprise Vault Outlook Add-In uses the URL when Outlook is configured to use RPC over HTTP, and **RPC over HTTP connection** is set to **Use proxy**.
  - In an Exchange Server 2003 environment. By default, clients connect to the virtual directory, **EnterpriseVaultProxy**, on the Exchange RPC proxy server.
  - In an Exchange Server 2007 or 2010 environment. If **RPC over HTTP connection** is set to **Use proxy**, the clients connect to the URL specified in this setting. In a multiple site environment, specify the URL of the Enterprise Vault proxy server for the site in which the client is located.

If you change the name of the virtual directory, then you can use this setting to specify the alternative URL. For example, if you change the virtual directory name to **EVProxy**, then you use the **RPC over HTTP Proxy URL** setting to specify the URL:

`HTTP://Web_server/EVProxy`

6 The settings are applied to mailboxes during the next synchronization run of the Exchange Mailbox task. If you want to apply the changes before the next synchronization, run **Synchronize**, which is on the **Synchronization** tab of the Exchange Mailbox task's properties.

Chapter 12

Configuring OWA and RPC Extensions in clustered configurations

This chapter includes the following topics:

About configuring OWA and RPC Extensions in clustered configurations

Enterprise Vault OWA Extensions for OWA 2000, and OWA and RPC Extensions for OWA 2003, are supported in configurations where the back-end Exchange Servers are configured in clusters that are managed by Windows Server Failover

Clustering or Veritas Cluster Server (VCS). Front-end Exchange Servers typically use load balancing, not clustering.

This section provides additional information on installing the Enterprise Vault OWA and RPC 2000 and 2003 Extensions on clustered back-end Exchange Servers. We recommend that you read the information given here before installing and configuring the extensions on the individual Exchange Servers.

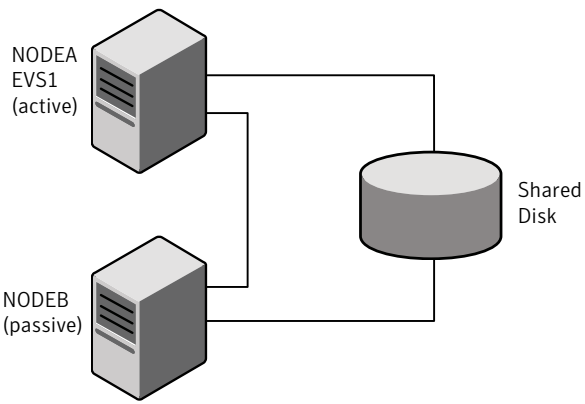
As the Enterprise Vault OWA 2007 and 2010 Extensions are installed on Exchange CAS servers, which typically use load balancing, not clustering, the information in this section does not apply to Enterprise Vault OWA 2007 or 2010 Extensions.

Supported cluster configurations for OWA and RPC Extensions

Exchange Servers in active/passive and N+1 configurations are supported. Active/active configurations are also possible, but not recommended by Microsoft.

Figure 12-1 illustrates an example basic active/passive Exchange Server cluster configuration.

Figure 12-1 Active/passive configuration

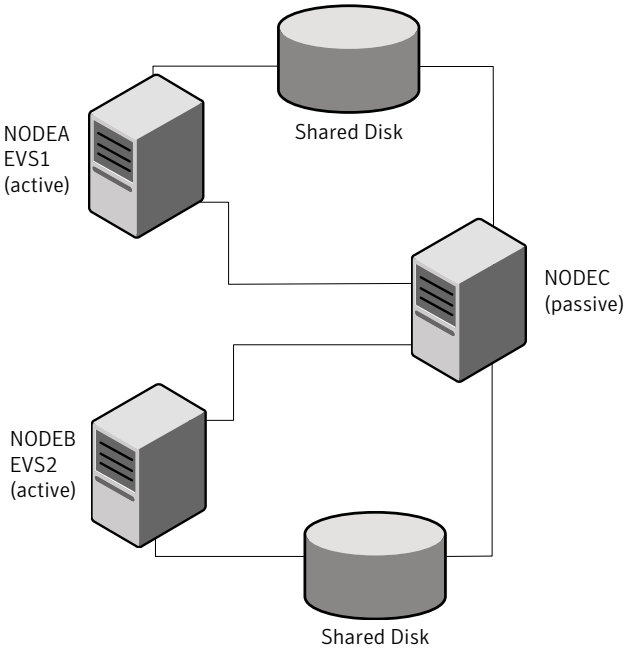


There is one Exchange Virtual Server, called EVS1, which can run on either node. As it is currently running on NODEA, this is the active node. If a problem occurs on this node, EVS1 will failover to NODEB, which then becomes the active node. Mailbox and public folder information stores and registered forms are held on the shared disks. The configuration information for the Exchange Virtual Server is held in Active Directory. In a basic active/passive configuration, there is one standby node for each active node.

N+1 clusters are similar to active/passive configurations in that there is a standby (passive) node to which applications on an active node can failover. However, in an N+1 configuration, the passive node is standby for multiple active nodes.

In Figure 12-2, NODEC is the standby node for NODEA and NODEB.

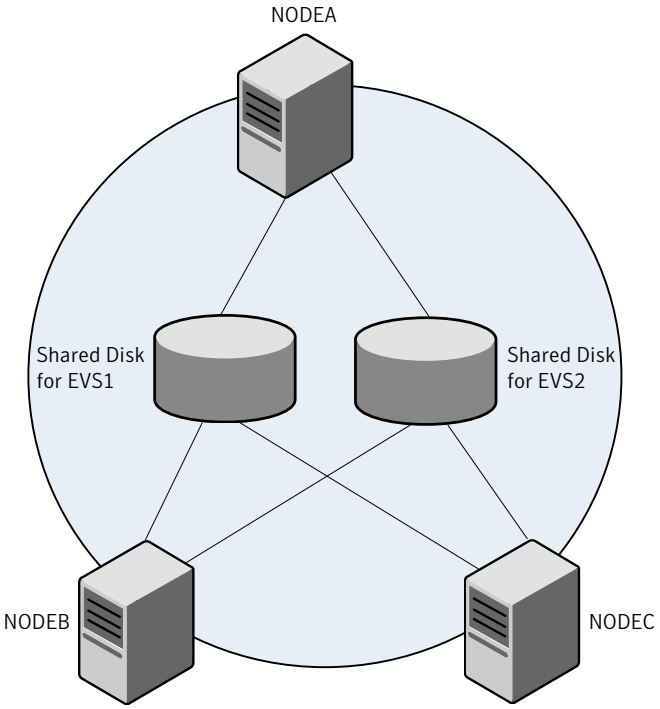
Figure 12-2 N+1 configuration



The Exchange Virtual Server, EVS1, can run on either NODEA or NODEC. The Exchange Virtual Server, EVS2, can run on either NODEB or NODEC.

Figure 12-3 illustrates an alternative N+1 configuration, in which any of the nodes can act as standby for either of the Exchange Virtual Servers.

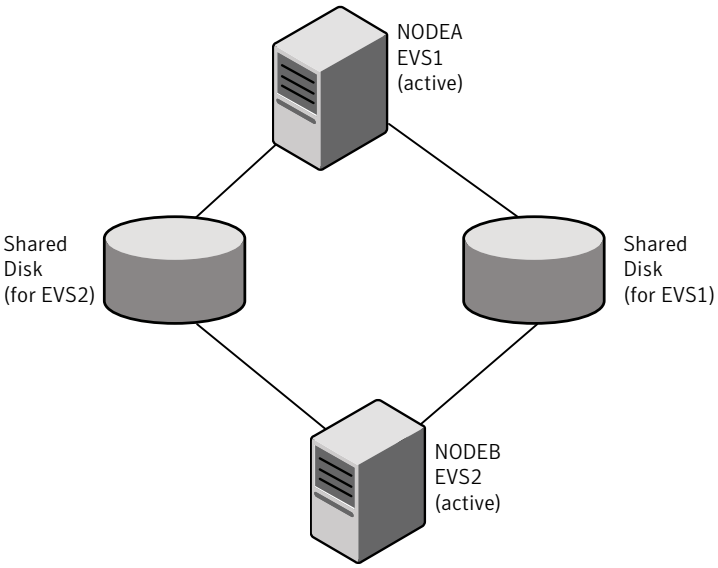
Figure 12-3 Alternative N+1 configuration



Each of the Exchange Virtual Servers, EVS1 and EVS2, can run on NODEA, NODEB or NODEC.

Figure 12-4 illustrates an active/active configuration.

Figure 12-4 Active/active configuration



Note that Microsoft does not recommend active/active configurations.

In these configurations there are no passive standby nodes; if the Exchange Virtual Server, EVS1, fails over, then both Exchange Virtual Servers will be running on NODEB, which could cause performance issues.

When configuring Enterprise Vault OWA and RPC Extensions for clustered environments, the extensions must be installed and configured on each node on which the Exchange Virtual Server can run.

Additional information on installing the extensions in active/passive and active/active clustered environments is given in the following sections.

OWA: Configuring Enterprise Vault Extensions in active/passive Windows Server failover clusters

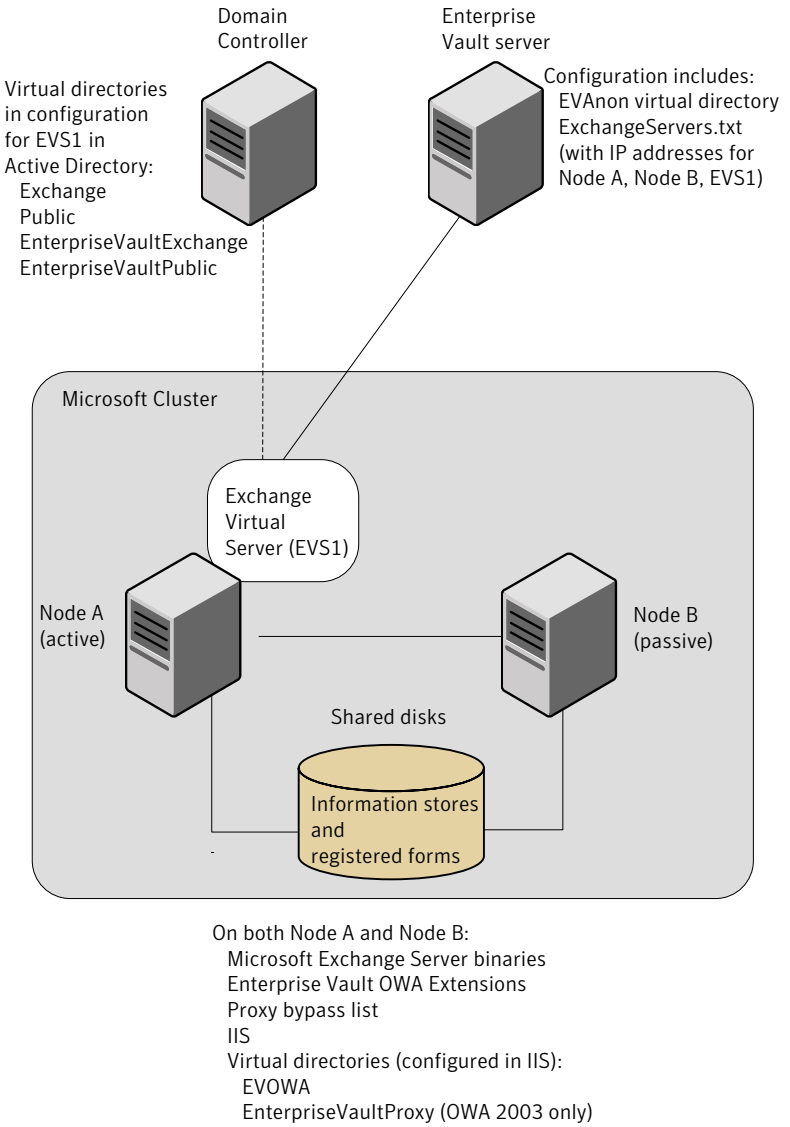
Enterprise Vault OWA Extensions are supported on clustered back-end, Exchange 2000 or Exchange Server 2003 Virtual Servers.

In active/passive Exchange Virtual Server cluster configurations, you must install the Enterprise Vault OWA 2000 or OWA 2003 Extensions on both active and passive nodes; you can install them on either an active or passive node first. Detailed instructions on how to install and configure the OWA Extensions are given in the following sections:

See "Configuring Enterprise Vault access for OWA users" on page 166.

Figure 12-5 shows the location of the various virtual directories and configuration data used by the Enterprise Vault OWA 2003 and OWA 2000 Extensions.

Figure 12-5 Detail of OWA 2003 and OWA 2000 Extensions configuration



Configuring the OWA Extensions on the active node first

If you install and configure the OWA Extensions on the active node first, running the Enterprise Vault OWA configuration wizard will do the following:

- Register forms for the OWA Extensions against the Exchange Virtual Server mailbox and public information stores.
- Create in Active Directory the following Exchange Server virtual directories for the back-end Exchange Virtual Server:
  - EnterpriseVaultExchange
  - EnterpriseVaultPublic
- Create the following IIS virtual directories on the active node computer:
  - EntepriseVaultProxy (on OWA 2003 only)
  - EVOWA
- Populate the Proxy bypass list on the active node computer from the file, `Enterprise Vault\OWA\EVServers.txt`.

If you examine the log file, `Enterprise Vault\OWA\BackEnd200`*n*`Setup.wsf.log`, after the configuration wizard has run, you will see the lines detailing the mailbox and public folder forms registration.

Configuring the OWA Extensions on the passive node first

If you install and configure the OWA Extensions on the passive node first, running the Enterprise Vault OWA configuration wizard will do the following:

- Create in Active Directory the following Exchange Server virtual directories for the back-end Exchange Virtual Server:
  - EnterpriseVaultExchange
  - EnterpriseVaultPublic
- Create the following IIS virtual directories on the passive node computer:
  - EntepriseVaultProxy (on OWA 2003 only)
  - EVOWA
- Populate the Proxy bypass list on the passive node computer from the file, `Enterprise Vault\OWA\EVServers.txt`.

Note that forms registration is only performed when you run the Enterprise Vault OWA configuration wizard on the active node. If you examine the log file,

`Enterprise Vault\OWA\BackEnd200n`Setup.wsf.log, after the configuration wizard has run on the passive node, you will not see any forms registration lines.

Configuring the OWA Extensions on the associated active or passive node

When you install and configure the OWA Extensions on the active or passive node associated with the node that you have already configured, warning messages in the log file will indicate that the EnterpriseVaultPublic and EnterpriseVaultExchange virtual directories already exist. As these virtual directories were created when you configured the OWA Extensions on the first node, you can ignore these warning messages.

Creating ExchangeServers.txt on the Enterprise Vault server when configuring OWA Extensions

When you configure an Enterprise Vault server to support OWA access, you create the `ExchangeServers.txt` file before you run the `owauser.wsf` script to configure the Data Access account.

`ExchangeServers.txt` holds the IP addresses of all the back-end Exchange Servers that will contact the Enterprise Vault server. When configuring this file for clustered Exchange Virtual Server configurations, the file must include all the IP addresses of the Exchange Virtual Servers that will access the Enterprise Vault server, and all the IP addresses of the physical computers (nodes) on which the Exchange Virtual Servers can run. Save `ExchangeServers.txt` with ANSI, Unicode, or Unicode big endian encoding.

OWA: Enterprise Vault Extensions in an active/active Windows Server failover cluster

Although Enterprise Vault OWA 2000 or OWA 2003 Extensions are supported in active/active clustered Exchange Virtual Server configurations, such configurations are not recommended by Microsoft and should be avoided, wherever possible.

In an active/active configuration, it does not matter which node you install the Enterprise Vault OWA Extensions on first.

Running the Enterprise Vault OWA configuration wizard on the first active node will perform the following tasks:

- Register the Enterprise Vault OWA forms against the mailbox and public stores in the Exchange Virtual Server.
- Create in Active Directory the following Exchange Server virtual directories for the back-end Exchange Virtual Server:
  - EnterpriseVaultExchange
  - EnterpriseVaultPublic
- Create the following IIS virtual directories on the active node computer:
  - EntepriseVaultProxy (on OWA 2003 only)
  - EVOWA
- Populate the Proxy bypass list on the active node computer from the file, `Enterprise Vault\OWA\EVServers.txt`.

If you examine the log file, `Enterprise Vault\OWA\BackEnd200`*n*`Setup.wsf.log`, after the configuration wizard has run, you will see the lines detailing the mailbox and public folder forms registration.

When you then run the Enterprise Vault OWA configuration wizard on the other active node, it performs the following tasks for the Virtual Exchange Server associated with that node:

- Registers the Enterprise Vault OWA forms against the mailbox and public stores in the Exchange Virtual Server.
- Create in Active Directory the following Exchange Server virtual directories for the back-end Exchange Virtual Server:
  - EnterpriseVaultExchange
  - EnterpriseVaultPublic
- Create the following IIS virtual directories on the active node computer:
  - EntepriseVaultProxy (on OWA 2003 only)
  - EVOWA
- Populate the Proxy bypass list on the active node computer from the file, `Enterprise Vault\OWA\EVServers.txt`.

When you install and configure the OWA Extensions on the second active node in the cluster, warning messages in the log file will indicate that the EnterpriseVaultPublic and EnterpriseVaultExchange virtual directories already exist. As these virtual directories were created when you configured the OWA Extensions on the first node, you can ignore these warning messages.

RPC over HTTP: Configuring Enterprise Vault Extensions in active/passive Windows Server failover clusters

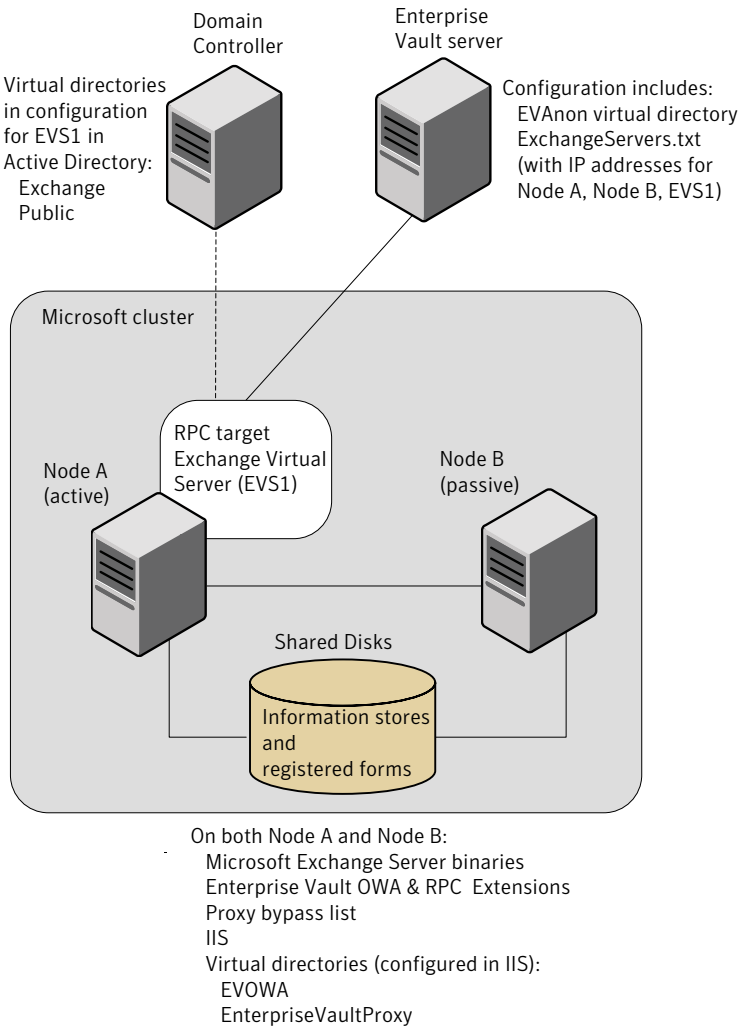
Enterprise Vault RPC Extensions are supported on clustered RPC target Exchange Virtual Servers (Exchange Server 2003).

In active/passive Exchange Virtual Server cluster configurations, you must install the Exchange 2003 Back-end Extensions (OWA & RPC) on both active and passive nodes; you can install them on either an active or passive node first.

See "About Outlook RPC over HTTP and Outlook Anywhere configurations" on page 185.

Figure 12-6 shows the location of the various virtual directories and configuration data used by the extensions.

Figure 12-6 RPC extensions configuration



Configuring RPC on the active node first

If you install and configure the extensions on the active node first, running the Enterprise Vault RPC configuration wizard will do the following:

- Create the following IIS virtual directories on the active node computer:
  - EntepriseVaultProxy
  - EVOWA

- Populate the Proxy bypass list on the active node computer from the file, `Enterprise Vault\OWA\EVServers.txt`.

Examine the log file, `\OWA\BackEnd2003Setup.wsf.log`, for any errors.

Configuring RPC on the passive node first

If you install and configure the RPC Extensions on the passive node first, running the Enterprise Vault RPC configuration wizard will do the following:

- Create the following IIS virtual directories on the passive node computer:
  - `EnterpriseVaultProxy`
  - `EVOWA`
- Populate the Proxy bypass list on the passive node computer from the file, `Enterprise Vault\OWA\EVServers.txt`.

Examine the log file, `\OWA\FrontEnd2003Setup.wsf.log`, for any errors.

Creating ExchangeServers.txt on the Enterprise Vault server when configuring RPC

When you configure an Enterprise Vault server to support Outlook RPC over HTTP client access, you create the `ExchangeServers.txt` file, before you run the `owauser.wsf` script to configure the Data Access account.

`ExchangeServers.txt` holds the IP addresses of all the Exchange RPC target Servers that will contact the Enterprise Vault server. When configuring this file for clustered Exchange Virtual Server configurations, the file must include all the IP addresses of the Exchange Virtual Servers that will access the Enterprise Vault server, and all the IP addresses of the physical computers (nodes) on which the Exchange Virtual Servers can run. Save `ExchangeServers.txt` with ANSI, Unicode, or Unicode big endian encoding.

RPC over HTTP: Configuring Enterprise Vault Extensions in an active/active Windows Server failover cluster

Although Enterprise Vault RPC Extensions are supported in active/active clustered Exchange Virtual Server configurations, such configurations are not recommended by Microsoft and should be avoided, wherever possible.

In an active/active configuration, it does not matter which node you install the Enterprise Vault Extensions on first.

Running the Enterprise Vault RPC configuration wizard on the first active node will perform the following tasks:

- Create the following IIS virtual directories on the active node computer:
  - EnterpriseVaultProxy
  - EVOWA
- Populate the Proxy bypass list on the active node computer from the file, `Enterprise Vault\OWA\EVServers.txt`.

Examine the log file, `Enterprise Vault\OWA\BackEnd200`*n*`Setup.wsf.log`, for any errors.

When you then run the Enterprise Vault RPC configuration wizard on the other active node, it performs the following tasks for the Virtual Exchange Server associated with that node:

- Create the following IIS virtual directories on the active node computer:
  - EnterpriseVaultProxy
  - EVOWA
- Populate the Proxy bypass list on the active node computer from the file, `Enterprise Vault\OWA\EVServers.txt`.

Configuring Enterprise Vault OWA and RPC Extensions on VCS

Enterprise Vault services can be installed on VCS. It is also possible to install the Enterprise Vault OWA and RPC Extensions on a back-end Exchange Server that has been installed on VCS.

To install and configure the Enterprise Vault OWA and RPC Extensions

1. Install the appropriate Enterprise Vault OWA and RPC Extensions on all nodes that could host the Exchange Virtual Server.
2. Run the appropriate Enterprise Vault configuration wizard for the extensions on each Exchange Virtual Server node, while it is the active node.

   This means that you must run the configuration wizard on the active node, fail over the Exchange Virtual Server to the passive node, and then run the configuration wizard on that node. Repeat this process for all nodes that could host the Exchange Virtual Server.
3. On the Enterprise Vault server, the `ExchangeServers.txt` file must include all the IP addresses of the Exchange Virtual Servers that will access the Enterprise Vault server, and all the IP addresses of the physical computers (nodes) on which the Exchange Virtual Servers can run.

Chapter 13

Using firewall software for external access to OWA and Outlook

This chapter includes the following topics:

About configuring Threat Management Gateway 2010 for Outlook 2013 and OWA 2013

Microsoft Forefront Threat Management Gateway 2010 (Forefront TMG 2010) can be used to create an external secure access point to Exchange servers. You can then make OWA, Outlook, and Enterprise Vault available on the Internet using web publishing rules.

See the following technical note for instructions on how to configure Forefront TMG 2010 for access to Enterprise Vault from OWA 2013 and Outlook 2013:

http://www.symantec.com/docs/TECH199448

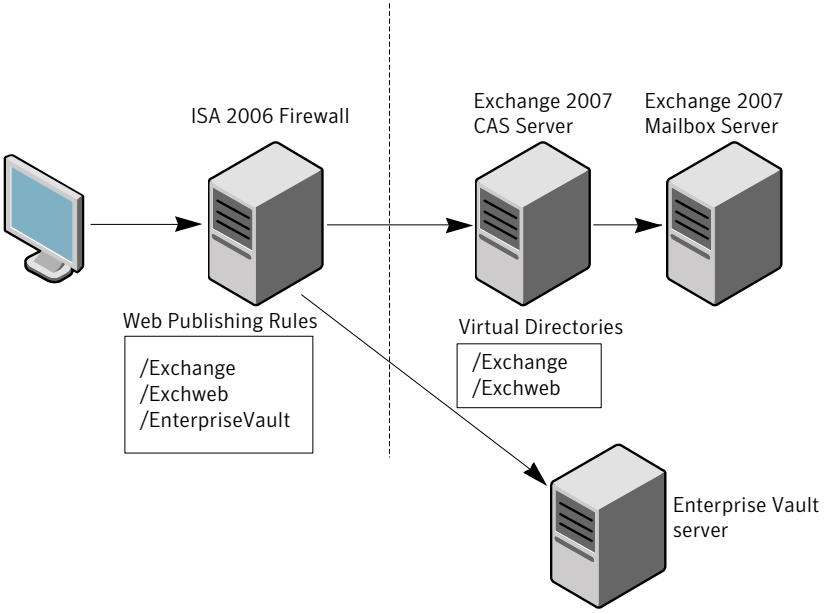
Configuring ISA Server 2006 for OWA 2007 or 2010 access to Enterprise Vault

Microsoft ISA Server 2006 can be used to secure OWA access to Exchange Server 2007 or 2010 by using web publishing rules to make the Exchange OWA website available on the Internet.

As OWA clients connect directly to Enterprise Vault for Archive Explorer and archive search client requests, you need to configure your ISA Server to ensure that clients can access Enterprise Vault. In addition to publishing the OWA website, you also need to publish to clients the Enterprise Vault web server URL.

Figure 13-1 shows how ISA Server 2006 can provide access to Enterprise Vault.

Figure 13-1 Access to Enterprise Vault using ISA Server 2006



See the following technical note for detailed instructions on how to configure ISA Server 2006 for access to Enterprise Vault from OWA clients:

http://www.symantec.com/docs/TECH61472

About configuring ISA Server 2006 for Outlook Anywhere client access to Enterprise Vault

Microsoft ISA Server 2006 can be used to secure Outlook Anywhere client access to Exchange 2007 or 2010 CAS computers by using web publishing rules to make RPC servers available on the Internet.

As Outlook Anywhere clients connect directly to Enterprise Vault, you need to configure your ISA Server to ensure that clients can access Enterprise Vault.

See the following technical note for detailed instructions on how to configure ISA Server 2006 for access to Enterprise Vault when using Outlook Anywhere clients:

http://www.symantec.com/docs/TECH61472

About configuring ISA Server 2006 for OWA 2003 and Outlook 2003 using RPC over HTTP

Microsoft ISA Server 2006 can be used to secure access to Exchange Server 2003 servers by using web publishing rules to make front-end servers for OWA, or RPC proxy servers, available on the Internet.

Using Enterprise Vault policy settings, you can configure direct connections to Enterprise Vault from Outlook 2003 in RPC over HTTP mode. Similarly, you can configure OWA clients to connect directly to Enterprise Vault for Archive Explorer and archive search client requests. If you configure direct connections to Enterprise Vault, then you need to configure your ISA Server to ensure that clients can access Enterprise Vault.

See the following technical note for detailed instructions on how to configure ISA Server 2006 for access to Enterprise Vault when using direct connections from OWA 2003 clients, and Outlook 2003 in RPC over HTTP mode:

http://www.symantec.com/docs/TECH53239

Chapter 14

Configuring Mobile Search access to Enterprise Vault

This chapter includes the following topics:

About Mobile Search

Symantec Enterprise Vault Mobile Search is a web-based application. It lets you use a web browser on a mobile device to search for and view Microsoft Exchange Server emails that Enterprise Vault has archived.

Mobile Search can search archives on single or multiple Enterprise Vault servers in an Enterprise Vault site. Mobile Search can be installed with or without BlackBerry Enterprise Server.

Mobile Search is deployed as a web application using Microsoft Internet Information Services (IIS). It accesses the IIS web server using HTTPS.

Mobile Search accepts valid connection requests from most common mobile devices without the need for any device-specific configuration. The available mobile device models and ranges change continually, so we do not specify a list of supported devices.

You can optionally add a device to the Mobile Search configuration file. However, you only need to add a device if you want to specify maximum column widths for the search results on that particular device. Mobile Search provides configurable default maximum column widths that are suitable for most devices.

See "Setting column widths on the search results page in Mobile Search" on page 234.

In the event of an issue with support of a specific device type, contact your normal support provider.

Documentation for Mobile Search end users

Mobile Search Getting Started (`Mobile_Search_Getting_Started.pdf`) is a short guide for Mobile Search end users. It describes how to log on and how to search for and view archived emails.

The guide is on the Enterprise Vault release media in the folder `\Symantec Enterprise Vault\Mobile Search\Documentation\`*`language`*.

Mobile Search deployment

You can only use Mobile Search with a single-site configuration of Enterprise Vault. An Enterprise Vault site comprises one or more Enterprise Vault servers that are configured to archive items from specified target servers.

Note the following:

- Mobile Search requires access to the domain controller and Enterprise Vault server(s). We recommend that in a production environment you should deploy it on the intranet behind a firewall. Mobile Search should be made available on the Internet through a reverse proxy server in the DMZ. However, a reverse proxy server in the DMZ is not mandatory, and Mobile Search can be installed without it.
- We recommend that in a production environment you should install Mobile Search on a separate server from Enterprise Vault and certain other applications.
  See "Prerequisites for Enterprise Vault Mobile Search in a production environment" on page 223.

Prerequisites for Enterprise Vault Mobile Search

This section includes the following topics:

Prerequisites for Enterprise Vault Mobile Search in a production environment

In a production environment, we recommend that you install Mobile Search on a computer that does not have any of the following applications installed:

- Enterprise Vault server
- Microsoft SQL Server
- Microsoft Exchange Server (the target system for Enterprise Vault archiving)
- BlackBerry Enterprise Server

Mobile Search can be installed on the same computer as these applications for pilot or demonstration purposes.

Hardware requirements for the Enterprise Vault Mobile Search server

Table 14-1 lists recommended minimum requirements for the Mobile Search server in a production environment.

Table 14-1 Mobile Search server hardware

Item	Recommended minimum
Number of CPUs	Two
Processor	Intel Xeon 1.86 GHz
RAM	2 GB
Free disk space on installation volume	100 MB

The minimum RAM requirement is particularly important if users perform large, simultaneous archive searches.

Windows Server 2003 requirements for Enterprise Vault Mobile Search

You can install Mobile Search on Microsoft Windows Server 2003 SP2.

The computer must be part of a Windows domain.

Install Windows Server 2003 SP2 with the following options and components:

- NTFS file system
- Microsoft .NET Framework 2.0
- Microsoft Internet Information Services (IIS)

Additionally, you must ensure that ASP.NET is allowed in IIS Web Service Extensions.

If you are installing Mobile Search on a 64-bit version of Windows Server 2003, you need to switch to the 32-bit version of ASP.NET 2.0. To do this, see the following article in the Microsoft Knowledge Base:

http://support.microsoft.com/?kbid=894435

Windows Server 2008 requirements for Enterprise Vault Mobile Search

You can install Mobile Search on Microsoft Windows Server 2008.

The computer must be part of a Windows domain.

Install Windows Server 2008 with the following options and components:

- NTFS file system
- Microsoft .NET Framework 2.0
- Microsoft Internet Information Services (IIS)

Additionally, you must ensure that ASP.NET is allowed in IIS Web Service Extensions.

For IIS 7.0 on a Mobile Search web server, we recommend that you add certain role service components to the web server role.

Table 14-2 lists the role service components that we recommend.

Table 14-2 Recommended role service components for the web server role

Role service	Recommended components
Common HTTP features	Static Content Default Document Directory Browsing HTTP Errors
Application Development	ASP.NET .NET Extensibility ISAPI Extension ISAPI Filters
Health and Diagnostics	HTTP Logging Request Monitor
Security	Basic Authentication Request Filtering
Performance	Static Content Compression
Management Tools	IIS Management Console

Enterprise Vault API Runtime required for Enterprise Vault Mobile Search

The API Runtime is located on the Enterprise Vault release media in the following folder:

```
\Symantec Enterprise Vault\API Runtime
```

Note the following:

- We recommend that you run Mobile Search on a server that is separate from the Enterprise Vault server. You must install the Enterprise Vault API Runtime before installing Mobile Search.
- You must ensure that the API Runtime version and the Enterprise Vault server version are the same. We recommend the use of version 10.0 or later of the API Runtime and Enterprise Vault server with Mobile Search. However, version 9.0/9.0.*n* of the API Runtime and Enterprise Vault server are also supported with Mobile Search.

Carrying out preinstallation tasks for Enterprise Vault Mobile Search

Before installing Mobile Search, you must perform the following tasks:

- Verify that Enterprise Vault is configured and all the services are running. Also, ensure that the DNS alias of the first Enterprise Vault server is accessible from the servers on which you plan to install Mobile Search.
- Obtain a digital certificate from a certification authority such as VeriSign for setting up HTTPS.
- In a configuration providing direct access to the Mobile Search web server from the Internet, do the following:
  - Verify that the firewall or firewalls are configured to allow HTTPS access to the servers on which you plan to install Mobile Search.
  - Configure any reverse proxy server that is installed in the DMZ.

About installing Enterprise Vault Mobile Search

This section describes how to install the Mobile Search server software, how to verify installation, and how to uninstall Mobile Search.

No client installation is required on the mobile device.

Installing Mobile Search

Perform the following steps to install Mobile Search.

To install Mobile Search

1. Ensure that IIS is running.
2. Log on as a local administrator.
3. On the Enterprise Vault release media, in the folder `\Symantec Enterprise Vault\Mobile Search`, double-click `Symantec Enterprise Vault Mobile Search.msi`.
4. On the License Agreement page, read the license agreement. To accept it, check **I accept the terms in the License Agreement** and click **Next**.
5. On the IIS Authentication Scheme page, select one of the following authentication methods:
   - **Use Logon Screen**. Choose this option to present users with a Log On page that requests their user name, password, and domain.

- **Use Basic Authentication**. Choose this option to present users with a browser prompt that requests their user name and password.

6 On the Configuration Information page, specify the following:

- The installation drive and folder. The folder name must be shorter than 150 characters.
- The Vault server alias. This is the DNS alias of the first Enterprise Vault server. The installer verifies the existence of the specified computer. The installer assumes that the Directory service is already installed and running on this computer.

  Click **Next**.

7 On the Ready to install page, click **Install**.

8 Click **Finish**.

Verifying Mobile Search installation

You must verify the installation before making Mobile Search available to users.

To verify Mobile Search installation

1 Open a web browser on any computer in the same domain as Mobile Search.

2 In the **Address** field, enter the Mobile Search URL.

For example, enter **https://*server*/mobilesearch**, where *server* is the Mobile Search server.

3 Click **Go** or press **Enter**.

In a deployment providing direct access to the Mobile Search web server from the Internet, the Mobile Search Log On page is displayed. In a deployment with BlackBerry Enterprise Server, the web browser prompts you for authentication.

4 Enter the details of a user who has access to at least one vault.

5 Click **Log On** or **OK**, depending on whether you view the Log On page or the web browser prompt.

If your authentication is valid, you see the Mobile Search search page.

6 Perform a search to verify that Mobile Search can return search results.

7 Click an email in the search results.

8 Do one of the following:

- If you see the contents of the email, close the web browser. You have verified installation of Mobile Search.

- If you see an error message, you need to troubleshoot the application. See "Mobile Search application problems" on page 236.

Uninstalling Mobile Search

You can uninstall Mobile Search using either the installer program `Symantec Enterprise Vault Mobile Search.msi`, or the Windows Add or Remove Programs applet.

The installation folder is removed, together with all the files that the installer copied. If you created a new file or folder in the folder manually, then the installation folder and the new file or folder are not removed. However, all other files that were installed are removed.

Uninstalling Mobile Search does not uninstall or remove the Enterprise Vault API Runtime, or any other system DLLs that were installed.

To uninstall Mobile Search using the installation program

1. Log on to the computer as a local administrator.
2. On the Enterprise Vault release media, in the folder `\Symantec Enterprise Vault\Mobile Search`, double-click `Symantec Enterprise Vault Mobile Search.msi`.
3. On the Upgrade, repair or remove setup page, select **Remove**.
4. On the next page, click **Remove**.
5. Click **Finish** to close the installer.

To uninstall Mobile Search using the Windows applet

1. Open the Windows Control Panel.
2. Select **Add or Remove Programs**.
3. In the list of programs, select **Enterprise Vault Mobile Search**.
4. Click **Remove**. You are prompted to confirm that you want to remove Mobile Search.
5. Click **Yes**.

About configuring Enterprise Vault Mobile Search

Mobile Search configuration settings are stored in the file `Web.Config`, which is in the root installation folder. To change the settings, edit `Web.Config` in a text editor.

Entries in `Web.Config` are case-sensitive, with one exception: the value that you add for a user agent string is not case-sensitive.

See "Adding a mobile device type to Mobile Search" on page 229.

When you save `Web.Config`, IIS ends all active Mobile Search sessions, with the following results:

- Users in a deployment that provides direct access to the Mobile Search web server from the Internet are returned to the Log On page.
- Users in a deployment with BlackBerry Enterprise Server are returned to the search page after an automatic logon.

We recommend that you modify `Web.Config` when there are no active user sessions.

Configuring the Mobile Search application

You can optionally configure the following features of the Mobile Search application:

- The specific mobile device types that Mobile Search recognizes
- How data is cached in the Mobile Search server's memory
- The time in minutes after which an ASP.NET session expires

Adding a mobile device type to Mobile Search

In a new installation of Mobile Search, some mobile device types are already included in the `<DeviceSpecificSettings>` section in `Web.Config`.

Mobile Search also accepts valid connections from mobile device types that are not included in `Web.Config`. You only need to add a new device if you want to specify the maximum widths of the two columns on the search results page. If the device is not included in `Web.Config`, Mobile Search uses the default maximum column width settings.

You add a mobile device type by specifying its user agent string in Web.Config. To add one particular mobile device type, enter its complete user agent string. To add a range of mobile device types, enter a partial user agent string that identifies all of them.

See "To add a mobile device type" on page 230.

To find the user agent string, connect to the Mobile Search server from the device and view the Mobile Search client information.

See "To find the user agent string of a mobile device" on page 230.

For example, suppose that your organization uses mobile devices that are named NewMobile 9100, 9300, 9500, and 9700. Each connection request includes a user agent string that starts with one of the following:

```
NewMobile9100/...
NewMobile9300/...
NewMobile9500/...
NewMobile9700/...
```

To configure all these mobile device types and any others in the 9000 range, enter the partial user agent string **NewMobile9** in `Web.Config`. Mobile Search matches the string from the left, so the partial user agent string must be common to the start of each string.

Mobile Search reads through the device definitions until it finds a match with the user agent string in a connection request. If you add a specific entry for the NewMobile 9300, place that entry before the generic entry (NewMobile9) for the rest of the range.

To find the user agent string of a mobile device

1. On the mobile device, open the web browser.
2. Go to the following URL:

   `https://`*`server`*`/mobilesearch/ClientInfo.aspx`

   where *server* is the Mobile Search server.
3. On the read-only page that is displayed, find the entry named **User Agent String**.

To add a mobile device type

1. In `Web.Config`, find the `<DeviceSpecificSettings>` section.
2. Add an entry in `<DeviceSpecificSettings>` in the following format:

   ```
   <add DeviceName="device_name" ua="user_agent_string"
   col1_width="maximum_number_of_characters"
   col2_width="maximum_number_of_characters"></add>
   ```

   where:

   - *device_name* is any name that you choose to identify this entry in `Web.Config`.
   - *user_agent_string* is a full user agent string or a partial user agent string. This value is not case-sensitive.

- *maximum_number_of_characters* is a value between 10 and 100 that specifies the maximum column width in characters on the search results page.

3 Save and close `Web.Config`.

Configuring how data is cached in Mobile Search

The caching settings control how data is cached in the Mobile Search server's memory to reduce response time to the user.

The caching settings have a direct effect on the amount of data that is cached for each user who is logged on to Mobile Search. If you change these settings, consider the available RAM and processing capacity on the Mobile Search server.

Table 14-3 describes the caching settings.

Table 14-3 Mobile Search caching settings

Setting	Default	Description
`PageSize`	20	The number of search results that are displayed on each page. Valid range: 1 to 100. If all users have devices with a large vertical layout, increase this value based on the device's screen height.
`PageContentSize`	15	The maximum size in kilobytes for the contents of one page of an email or an attachment. Above this size, pagination occurs and formatting is removed. Valid range: 1 to 5120. Default: 15 If your mobile devices can support more data per page, increase the PageContentSize value accordingly. By increasing the value you are more likely to retain the original formatting. If your mobile devices support less data per page, reduce the PageContentSize value. Reducing the value may introduce paging and lose formatting but does mean that the devices can handle the data efficiently.
`SearchResultsCacheSize`	5	The number of search result pages that are cached in the session memory for each user. Valid range: 1 to 100. SearchResultsCacheSize multiplied by PageSize gives the number of search results that are cached for each user. By default, 100 search results are cached for each user.

Table 14-3 Mobile Search caching settings *(continued)*

Setting	Default	Description
`ContentsPageCacheWindow`	6	The number of content pages that are cached in the session memory for each user. Valid range: 1 to 100. ContentsPageCacheWindow multiplied by PageContentSize gives the size in kilobytes of email or attachment data that is cached for each user. By default, 90 KB is cached.

To configure the caching settings

1. In `Web.Config`, find the `<appSettings>` section.
2. In the `<appSettings>` section, find the following lines:

   ```
   <add key="PageSize" value="number"></add>
   <add key="PageContentSize" value="size_in_kilobytes"></add>
   <add key="SearchResultsCacheSize" value="number"></add>
   <add key="ContentsPageCacheWindow" value="number"></add>
   ```

3. In each line, replace the current value with the value you require.
4. Save and close `Web.Config`.

Setting the session timeout in Mobile Search

You can specify the time in minutes after which an ASP.NET session expires.

The default is 15 minutes, and the valid range is the range that IIS supports.

To set the session timeout

1. In `Web.Config`, find the `<sessionState>` setting.
2. In the `<sessionState>` setting, find the following attribute:

   ```
   timeout="number_of_minutes"
   ```

3. Replace the current session timeout value with the value you require.
4. Save and close `Web.Config`.

Configuring the Mobile Search user interface

You can optionally configure the following features of the Mobile Search client in the web browser on the mobile device:

- The language in which the client features appear
- The maximum widths of the columns on the search results page
- The date format

Configuring Mobile Search language support

When a mobile device requests a connection, Mobile Search tries to match the language that the device requests to one of the languages it supports. If Mobile Search recognizes the language, the client features appear in that language in the web browser on the mobile device. If Mobile Search does not recognize the language or no language request is sent, the client features appear in the default language.

Most mobile devices send a language request. Mobile Search usually recognizes the request, so no special configuration is required. If there is a problem, you can do one or both of the following:

- View the language request string that the mobile device sends, and change the language configuration on the mobile device if necessary.
  See "Unexpected language on mobile device with Mobile Search" on page 238.
- Change the Mobile Search default language in the configuration file `Web.Config`.

Table 14-4 shows the possible default language values and the languages they represent.

Table 14-4 Default language values

Value	Language
en (the default)	English
da	Danish
de	German
es	Spanish
fr	French
hu	Hungarian
it	Italian
ja	Japanese
ko	Korean
nl	Dutch

Table 14-4 Default language values *(continued)*

Value	Language
pl	Polish
pt-br	Brazilian Portuguese
ru	Russian
sv	Swedish
zh-cn	Simplified Chinese
zh-tw	Traditional Chinese

If you enter any other value, a message is added to the event log and the default (en) is used.

To configure the default language

1. In `Web.Config`, find the `<appSettings>` section.
2. In the `<appSettings>` section, find the following line:

   `<add key="Language" value="default_language_value"></add>`
3. Replace the current default language value with the value you require. This value is case-sensitive.
4. Save and close `Web.Config`.

Setting column widths on the search results page in Mobile Search

Mobile Search renders the search results page in a device-specific way. The maximum widths of the two columns on the search results page are set on the basis of the device's user agent string.

To specify the maximum column widths for a particular mobile device type, you must add the device's user agent string to `Web.Config`.

See "Adding a mobile device type to Mobile Search" on page 229.

Mobile Search may not recognize the user agent string that it receives from a mobile device. In this case it uses the default maximum column widths that are specified in the Mobile Search configuration file `Web.Config`.

Table 14-5 describes the default maximum column width settings.

Table 14-5 Default maximum column widths

Setting	Default	Description
`Column1DefWidth`	20	Default maximum width in characters of column 1 on the search results page. Valid range: 10 to 100.
`Column2DefWidth`	30	Default maximum width in characters of column 2 on the search results page. Valid range: 10 to 100.

To set the default maximum column widths

1. In `Web.Config`, find the `<appSettings>` section.
2. In the `<appSettings>` section, find the following lines:

```
<add key="Column1DefWidth"
value="maximum_number_of_characters"></add>

<add key="Column2DefWidth"
value="maximum_number_of_characters"></add>
```

3. In each line, replace the current value for the maximum number of characters with the value you require.
4. Save and close `Web.Config`.

Setting the date format for Mobile Search

You can set the date format that Mobile Search uses in the search results and on mail contents pages.

The possible values are as follows:

- DD/MM/YYYY (day/month/year). This format is the default.
- MM/DD/YYYY
- YYYY/MM/DD

To set the Mobile Search date format

1. In `Web.Config`, find the `<appSettings>` section.
2. In the `<appSettings>` section, find the following line:

```
<add key="DateFormat" value="date_format"></add>
```

3 Replace the current value for the date format with the value you require. This value is case-sensitive.

4 Save and close `Web.Config`.

Mobile Search troubleshooting

This section includes the following topics:

Mobile Search installation problems

Mobile Search installation completes only if there is no error. If the Mobile Search installer exits without any error message, then you need to analyze the installer log.

You can create an installer log using the standard Windows Installer, msiexec. Execute the command at the command prompt, after ensuring that the path for msiexec is defined.

To create an installer log containing all available information

- At the command prompt, enter the following command exactly as shown, including the double quotation marks around the file name `Symantec Enterprise Vault Mobile Search.msi`:

  msiexec /I "Symantec Enterprise Vault Mobile Search.msi" /l*v logfile.txt

Mobile Search application problems

Problems with the Mobile Search application can cause error messages in the browser when users try to access the application, or when they use it.

Enterprise Vault API Runtime missing with Mobile Search

If an Enterprise Vault API Runtime is missing, users see the following message:

```
Could not load file or assembly 'KVS.EnterpriseVault.Interop.
EVContentManagementAPI, Version=version, Culture=neutral,
PublicKeyToken=26c5e2ccf2b9267c' or one of its dependencies.
The system cannot find the file specified.
```

If users see this message, check that the correct version of the API Runtime is installed. The API Runtime version and the Enterprise Vault server version must be the same.

Enterprise Vault Directory service problems with Mobile Search

If there is a problem with the Enterprise Vault Directory service, users may see one of the following messages:

- `Enterprise Vault is not running.`
- `Invalid Value configured for Enterprise Vault directory DNS alias. Please contact system administrator.`
- `An internal failure occurred. Internal Error: '<0x154>'`

If users see one of these messages, ensure the following:

- You can ping the Enterprise Vault server that is specified in the Mobile Search configuration file `Web.Config` from all Mobile Search servers. The Enterprise Vault server is specified in the `value` attribute for the setting `DNSDirectoryAlias` in the `<appSettings>` section.
- The value that is specified in the `value` attribute identifies a server that runs the Enterprise Vault Directory service.
- The Enterprise Vault Directory service is running.

Logon Failure with Mobile Search

If a user sees the error message `Logon Failure`, check that the user's credentials are correct.

If the credentials are correct, ensure that the Active Directory Server can be accessed from the Mobile Search hardware server. To perform this check, ping the Active Directory Server and ensure that it is in the correct Windows domain.

Page not found with Mobile Search

If users see the error message `Page not found` when they try to log on to Mobile Search, the likely cause is one of the following:

- The user has entered the wrong URL.
- A valid SSL certificate is not configured on the Default Web Site.
- ASP.NET is prohibited under Web Service Extensions in IIS.

Access Denied with Mobile Search

If a user sees the error message `Access Denied`, check that the user has access permissions to the requested item in Enterprise Vault. Check whether the user can access the item using Enterprise Vault search.

Unexpected language on mobile device with Mobile Search

If the Mobile Search client features appear in an unexpected language, you may need to do one or both of the following:

- Check the language request that the mobile device sends to Mobile Search, and if necessary change the language request.
  The language request is a string of one or more language codes that are specified on the mobile device.
  Mobile Search examines only the first language code in the language request. Mobile Search tries to match the exact language code to one of the languages it supports. If it does not find an exact match, it tries variations of the language code. For example, if the code is `en-us`, Mobile Search removes `-us` and matches the request to English (`en`).
- Change the Mobile Search default language.
  If Mobile Search does not recognize the language request, it uses the default language that is specified in `Web.Config` on the Mobile Search server. You may need to set the default language to one that is suitable for your mobile device users.

To check the language request from a mobile device

1. On the mobile device, open the web browser.
2. Go to the following URL:

   `https://`*`server`*`/mobilesearch/ClientInfo.aspx`

   where *server* is the Mobile Search server.
3. On the read-only page that is displayed, find the entry named **HTTP Accept Language**. This entry shows the language request string.

To change the default language on the Mobile Search server

- Change the `Language` setting in the Mobile Search configuration file `Web.Config`.

  See "Configuring Mobile Search language support" on page 233.

Web page formatting problems with Mobile Search

If Mobile Search users report web page formatting problems, it may be necessary to enable HTML table support on the device. The actions that are required are device-specific.

Using DTrace to aid troubleshooting with Mobile Search

Mobile Search uses the standard Enterprise Vault logging mechanism.

The errors and warnings are logged in the Windows Event Viewer.

All the system logs can be seen and saved using the standard DTrace utility that is shipped with the Enterprise Vault API Runtime and Enterprise Vault server.

Chapter 15

Configuring filtering

This chapter includes the following topics:

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:

- Selective journaling. This feature provides simple filtering of Exchange Server journaled messages. You can configure the Exchange Journaling task to call the selective journaling external filter that decides whether to archive or delete an item. To select messages, you set up filtering rules to match the To, CC, and From fields. If a message matches any of these rules it is archived, otherwise it is deleted.

  If you enable selective journaling on an Enterprise Vault server, it is enabled for all Exchange Journaling tasks that are hosted on that computer.
- Group journaling. This feature enables the Exchange Journaling task to mark selected messages, in order to reduce the scope of subsequent searches. This can be particularly useful where there is a high volume of journaled email and

you want to be able to identify messages sent between particular groups of users.

- 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, deleting attachments of a specified type or size, or deleting or marking the message.
  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 258.
- 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.

About journal filters with Envelope Journaling

All methods of filtering journal mailboxes support Microsoft Exchange Server Envelope Journaling. This feature ensures that target addresses in all BCC, Undisclosed and Alternate Recipient fields are captured.

See "About Enterprise Vault and Exchange Server journal reports" on page 123.

If you have journal filtering enabled and intend enabling Envelope Journaling, we recommend that you test your existing filters and check the results before enabling Envelope Journaling on your production Exchange Server.

Before enabling Envelope Journaling, you will need to make changes to any proprietary journal filters that modify the selected message, so that the journal report or the original message are accessed, as required.

See "Exchange Filtering API" in the *Application Programmer's Guide* for more information.

Configuring selective journaling

Table 15-1 describes the steps required to configure selective journaling. Repeat the steps on each Enterprise Vault server that hosts an Enterprise Vault Exchange Journaling task.

Table 15-1 Steps to configure selective journaling

Step	Action	More information
Step 1	Set up Exchange Journal archiving.	For detailed instructions see the chapter "Setting up archiving of journaled messages" in this manual.
Step 2	Create a filtering rules file. The same filtering rules file will be used by all Exchange Journaling tasks that are hosted on the computer.	See "Creating the selective journaling rules file" on page 243.
Step 3	Add the selective journaling registry settings for the Exchange Journaling task.	See "Adding selective journaling registry settings" on page 245.
Step 4	Restart the Exchange Journaling task.	See "Starting the Journaling task" on page 121.

Creating the selective journaling rules file

This section describes how to create a file of journaling filtering rules.

To set up the filtering rules file

1. Log on to the Exchange Journaling task computer as the Vault Service account.
2. Use Notepad to create a file called `SelectiveJournal_config.dat` in the Enterprise Vault installation folder (for example `C:\Program Files (x86)\Enterprise Vault`).
3. In the file, specify the rules that you want the filter to use to select journaled messages for archiving.

   See "Selective journaling filter rules" on page 244.
4. Save the file as a Unicode file.

Selective journaling filter rules

Each line of the rules file takes the following format:

keyword:*value*

Table 15-2 describes the keywords and values that you can enter in the file.

Table 15-2 List of selective journaling keywords for rules

Keyword	Description	Value
cont	Archive all items that have been sent to addresses that contain the specified text.	A text string. For example: cont:flashads The string can be part of an SMTP address.
distlist	Archive all items that have been sent to anyone who is on the specified distribution list. Note that selective journaling does not support Dynamic Distribution Groups.	The legacyExchangeDN of the distribution list. For example: distlist:/o=acme/ou=finance/cn=recipients/cn=allfinance
ends	Archive all items that have been sent to addresses that end with the specified text.	A text string. For example: ends:example.com The string can be part of an SMTP address.
exact	Archive all items that have been sent to the specified email address.	The SMTP email address of the recipient. For example: exact:smith@example.com
recip	Archive all items that have been sent to the specified recipient. The recipient can be a user account or a distribution list.	The legacyExchangeDN of the recipient user account or distribution list. For example: recip:/o=acme/ou=developer/cn=recipients/cn=smithj
starts	Archive all items that have been sent to addresses that start with the specified text.	A text string. For example: starts:john The string can be part of an SMTP address.

Note: You can view the legacyExchangeDN property using ADSIEdit.msc or a similar Active Directory tool.

Employees and resources in an organization may have several SMTP addresses in addition to an internal, Exchange Server address. If you want to capture all

email to a recipient in your organization use either the **recip** or **distlist** keyword with the address specified using the legacyExchangeDN. For example:

```
recip:/o=acme/ou=first administrative
group/cn=recipients/cn=John Doe
```

Alternatively, specify a distribution list that the recipient is a member of. For example,

```
distlist:/o=acme/ou=first administrative
group/cn=recipients/cn=Sales
```

Using the **recip** or **distlist** keyword will capture email to any of the recipient's SMTP addresses and also internal email to their Exchange Server address. In this situation, the keywords, **exact**, **starts**, **ends**, and **cont** are not appropriate, as they may not capture external inbound email to all the addresses that the recipient may have.

You can use the keywords, **exact**, **starts**, **ends**, and **cont** to capture email to and from domains or SMTP addresses that are external to your organization. For example, you could use **ends:acme.com** to capture all communication to and from the external domain, acme.com.

Adding selective journaling registry settings

This section describes how to configure the registry settings that enable selective journaling.

To add the selective journaling registry settings

1. Log on to the Journaling task computer as the Vault Service account.
2. Run regedit and navigate to the following location:

```
HKEY_LOCAL_MACHINE
\Software
 \Wow6432Node
  \KVS
   \Enterprise Vault
    \External Filtering
     \Journaling
```

   Add the `External Filtering` key under `Enterprise Vault`, and the `Journaling` key under `External Filtering`, if they do not exist.

3 In `Journaling`, create a new STRING value with the name `1` and set its value to `SelectiveJournal.SJFilter`.

By default, items that are not archived are sent to the Deleted Items folder in the journal mailbox.

If you want items to be deleted immediately, without going to the Deleted Items folder, add the DWORD, `HardDeleteItems`, to the following location and give it a value of `1`:

```
HKEY_LOCAL_MACHINE
\Software
 \Wow6432Node
  \KVS
   \Enterprise Vault
    \Agents
     \SelectiveJournal
```

Add the `SelectiveJournal` key, if it does not exist.

4 To apply your changes, stop and restart all Journaling tasks on the server. You need to do this whenever you make a change to the rules file or if you modify the registry values.

Managing invalid distribution lists with selective journaling

You can set the following registry entry to control what the Exchange Journaling task does if a distribution list is invalid.

To manage invalid distribution lists

1. Log on to the Journaling task computer as the Vault Service account.
2. Run regedit and navigate to the following location:

```
HKEY_LOCAL_MACHINE
\Software
 \Wow6432Node
  \KVS
   \Enterprise Vault
    \Agents
```

3. Create a new DWORD value with the name `ActionForInvalidDL` and set its value to one of the following:

0	(Default) If a distribution list is invalid, continue to process the remainder of the recipient list.
1	If a distribution list is invalid, stop processing the recipient list.
2	If a distribution list is invalid, treat this as a match and archive the message.
3	If a distribution list is invalid, leave the message in the journaling mailbox and report an error event in the Event Log.

Configuring group journaling

Group journaling stamps a message with a specific retention category if it was sent between two identified groups. The scope of subsequent searches can be substantially reduced by including the retention category in the search criteria.

You can also specify that only a sample of messages with the retention category are to be archived. The percentage is specified in the configuration (minimum of 0.1%; 1 in every 1000).

If you enable group journaling on an Enterprise Vault server, it will be enabled for all Exchange Journaling tasks that are hosted on that computer.

Table 15-3 describes the steps required to configure group journaling. Repeat the steps on each Enterprise Vault server that hosts an Enterprise Vault Exchange Journaling task.

Table 15-3 Steps to configure group journaling

Step	Action	More information
Step 1	Set up Exchange Journal archiving.	For detailed instructions see the chapter "Setting up archiving of journaled messages" in this manual.
Step 2	Create a rules file. This file specifies the addresses to match, the retention category to assign and the sample size. The same rules file will be used by all Exchange Journaling tasks that are hosted on the computer.	See "Creating the group journaling rules file" on page 248.
Step 3	If it does not exist, create the retention category to be assigned to matched messages.	See the *Administrator's Guide* for instructions on how to do this.
Step 4	Check the distribution lists.	On the Exchange Server, ensure that the distribution lists exist and are populated with the required users. Note that group journaling does not support Dynamic Distribution Groups.
Step 3	On the Enterprise Vault Exchange Journaling task computer, add the group journaling registry settings.	See "Adding group journaling registry settings" on page 250.
Step 4	Restart all Exchange Journaling tasks on the computer, and test your configuration.	See "Starting the Journaling task" on page 121. See "Testing group journaling settings" on page 250.

Creating the group journaling rules file

This section describes how to create the group journaling rules file. The same rules file will be used by all Exchange Journaling tasks that are hosted on the computer.

To create the group journaling rules file

1. Log on to the Exchange Journaling task computer as the Vault Service account.
2. Use Notepad to create a file called `SJGroupFilter.dat` in the Enterprise Vault installation folder (for example `C:\Program Files (x86)\Enterprise Vault`).

3 In the file, specify the rules that you want the filter to use to select journaled messages for archiving.

See "Group journaling filter rules" on page 249.

4 Save the file as a Unicode file.

Group journaling filter rules

Each line of the rules file takes the following format:

`<keyword>:<value>`

Table 15-4 shows the keywords and values that you can enter in the file.

Table 15-4 List of Group Journaling keywords for rules

Keyword	Description	Value
retcat	The retention category to assign to matching messages. The file must contain a retention category line and the retention category must exist.	Retention category name. For example: retcat:Flagged
sample	The percentage sample rate of matching messages to be archived. If this line is missing, the sample rate defaults to 100%.	Integer (without % sign). For example: sample:25
userset	Used to define the groups of user addresses to be matched. The rules file must contain two userset lines; one for each group. Each line defines a distribution list containing the addresses of group members. The specified distribution lists must not be empty. Note that group journaliing does not support Dynamic Distribution Groups.	legacyExchangeDN of the distribution list. For example: userset:/o=acme/ou=research/cn=recipients/cn=groupa

Note: You can view the legacyExchangeDN property using ADSIEdit.msc or a similar Active Directory tool.

Using the following example rules file, 25% of the messages sent by members of one distribution list to members of the other distribution list will be assigned the retention category, `Flagged`.

```
userset:/o=acme/ou=research/cn=recipients/cn=groupa
userset:/o=acme/ou=research/cn=recipients/cn=groupb
retcat:Flagged
sample:25
```

Adding group journaling registry settings

This section describes how to configure the registry settings for group journaling.

To add the group journaling registry settings

1. Log on to the Journaling task computer as the Vault Service account.
2. Run regedit and navigate to the following location:

   ```
   HKEY_LOCAL_MACHINE
   \Software
    \Wow6432Node
     \KVS
      \Enterprise Vault
       \External Filtering
        \Journaling
   ```

   Add the `External Filtering` and `Journaling` keys, if they do not exist.
3. Create a new STRING value called `1` and set its value to `SelectiveJournal.SJGroupFilter`.
4. Restart all Enterprise Vault Exchange Journaling tasks on the computer.

Testing group journaling settings

This section describes how to test the group journaling settings.

To test the group journaling settings

1. Send a message from a user in one of the specified distribution lists to a user in the other distribution list.
2. Wait for Enterprise Vault to archive the message, and then search for it using the **Retention Category** field on the **Advanced** page of the Enterprise Vault browser search. (For the **Advanced** page, the URL should end with `Search.asp?Advanced`.)

   The message should have the group journaling retention category assigned.

3 Now repeat the test only in reverse; send a message from a user in the second distribution list to a user in the first distribution list.

   Again, the message should have the group journaling retention category assigned.

4 Next, send a message from a user in the first distribution list to someone who is not in the second distribution list.

   The message should be archived with the retention category specified in the default Exchange journal policy.

5 Send a message from a user in the second distribution list to someone not in the first distribution list.

   Again, the message should be archived with the retention category specified in the default Exchange journal policy.

Configuring custom filtering

Selective and group journaling provide very limited filtering capabilities and are only available with Exchange Server journal mailbox archiving; the same filtering is applied to all journal mailboxes serviced by the Exchange Journaling tasks configured on the Enterprise Vault server computer. Custom filtering provides more sophisticated filtering for all types of Exchange Server archiving (user and journal mailbox and public folder). 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 public folder archiving, or specific user or journal mailboxes.

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 294.

Table 15-5 Steps to configure custom filtering

Step	Action	More information
Step 1	Configure registry settings to enable custom filtering for the required archiving tasks.	See "Configuring registry settings for Exchange Server journal custom filtering" on page 253. See "Configuring registry settings for Exchange Server mailbox custom filtering" on page 255. See "Configuring registry settings for Exchange Server public folder custom filtering" on page 257.
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`.	See "About custom filtering ruleset files" on page 258. See "About the general format of ruleset files for custom filtering" on page 265. See "About rule actions for custom filtering" on page 268. See "About message attribute filters for custom filtering" on page 271. See "Attachment attribute filters for custom filtering" on page 284. See "Example ruleset file for custom filtering" on page 290.

Step 3	Restart the archiving tasks that have custom filtering enabled.	The following message is sent to the Enterprise Vault event log when the Exchange Server archiving tasks start:
		`EventID = 45329`
		`Description = External Filter 'EnterpriseVault.CustomFilter' initialising...`
		The following message is sent to the Enterprise Vault event log when the Exchange Server archiving tasks stop:
		`EventID = 45330`
		`Description = External Filter 'EnterpriseVault.CustomFilter' stopped.`

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 Exchange Server journal custom filtering

Configuring the registry settings described in this section will enable custom filtering for all the Exchange Journaling tasks hosted on the server.

By creating a named ruleset file you can limit filtering to particular journal mailboxes.

See "About custom filtering ruleset files" on page 258.

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

To configure the registry settings for Exchange Server journal custom filtering

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

```
HKEY_LOCAL_MACHINE
\Software
 \Wow6432Node
  \KVS
   \Enterprise Vault
    \External Filtering
     \Journaling
```

If the `External Filtering` key does not exist, create it by performing the following steps in the order listed:

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

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

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

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

If the Compliance Accelerator Journaling Connector is installed (`KVS.Accelerator.PlugIn.Filter`), it must be the last in the sequence, so you will need to rename it before creating the new custom filtering setting. For example, if the Journaling Connector is currently named `1`, rename this setting as `2` and create the new custom filtering setting with the name `1`.

To rename the Journaling Connector setting, do as follows:

- 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 value `EnterpriseVault.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 Exchange Journaling task reexamines any messages that are marked as MARK_DO_NOT_ARCHIVE each time it processes the journal mailbox. If the value is 0, or the `Override` entry does not exist, then the Exchange 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 Exchange Journaling task to reprocess any messages in the journal mailbox.

7 If it does not exist, create a DWORD value called `MoveOnFilterFailure` and set its value to `1`.

This entry controls whether the Exchange Journaling task moves messages to the folder `Failed External Filter` when an unhandled error occurs in the external filter. This folder is automatically created when required in the journal mailbox.

If the `MoveOnFilterFailure` registry entry does not exist then, when an unhandled error occurs in the external filter, the Exchange Journaling task moves the associated messages to the `Enterprise Vault Journaling Service\Invalid Journal Report` folder in the journal mailbox.

8 Close Regedit.

9 After you have configured the required XML filter rules, restart the Exchange Journaling tasks.

See "About custom filtering ruleset files" on page 258.

Configuring registry settings for Exchange Server mailbox custom filtering

Configuring the registry settings described in this section will enable custom filtering for all the Exchange Mailbox tasks hosted on the server.

By creating named ruleset files, you can limit filtering to particular mailboxes.

See "About custom filtering ruleset files" on page 258.

To configure the registry settings for Exchange Server mailbox custom filtering

1 On the computer that hosts the Enterprise Vault Exchange Mailbox task, log on as the Vault Service account.

2 Start Regedit.

3 Navigate to the following location:

```
HKEY_LOCAL_MACHINE
\Software
 \Wow6432Node
  \KVS
   \Enterprise Vault
    \External Filtering
```

If the `External Filtering` key does not exist, create it by performing the following steps in the order listed:

- Right-click `Enterprise Vault` and select **New > Key**.

- Name the key `External Filtering`.

4 Create a `Mailbox` key as follows:

- Right-click `External Filtering` and select **New > Key**.
- Name the key `Mailbox`.

5 Create a new string entry called `1` for the new custom filtering entry.

6 Right-click the new entry and select **Modify**. Give it the value:

```
EnterpriseVault.CustomFilter
```

7 Optionally, you can create a new DWORD entry with the name `Override`, and set its value to `0` (zero). By changing the value of this entry you can control whether the Exchange Mailbox task applies the custom filtering rules during archiving:

- `0` (zero) — The Exchange Mailbox task applies the custom filtering rules to all messages.
- `1` — The Exchange Mailbox task does not apply the custom filtering rules.

If the `Override` entry does not exist, then the task applies the custom filtering rules to all messages.

8 If it does not exist, create a DWORD entry called `MoveOnFilterFailure` and set its value to `1`.

This entry controls whether the Exchange Mailbox task moves messages to the folder `Failed External Filter` when an unhandled error occurs in the external filter. This folder is automatically created when required in the user mailbox.

If the `MoveOnFilterFailure` registry entry does not exist then, when an unhandled error occurs in the external filter, the Exchange Mailbox task does not move the associated messages. The task tries to process the messages during each archiving run.

9 Close Regedit.

10 After you have configured the required XML filter rules, restart the Exchange Mailbox tasks.

Configuring registry settings for Exchange Server public folder custom filtering

Configuring the registry settings described in this section will enable custom filtering for all the Exchange Public Folder tasks hosted on the server. You can create a public folder ruleset file to apply specific rules to public folder archiving.

Unlike mailbox filtering, you cannot use named ruleset files to configure filtering for particular public folders.

To configure the registry settings for Exchange Server public folder custom filtering

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

   ```
   HKEY_LOCAL_MACHINE
   \Software
    \Wow6432Node
     \KVS
      \Enterprise Vault
       \External Filtering
   ```

   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`.

4. Create a `PublicFolder` key as follows:

   - Right-click `External Filtering` and select **New > Key**.
   - Name the key `PublicFolder`.

5. Create a new string value called `1` for the new custom filtering entry.
6. Right-click the new entry and select **Modify**. Give it the value:

   ```
   EnterpriseVault.CustomFilter
   ```

7. Optionally, you can create a new DWORD entry with the name `Override`, and set its value to `0` (zero). By changing the value of this entry you can control whether the Exchange Public Folder task applies the custom filtering rules during archiving:

   - `0` (zero) — The Exchange Public Folder task applies the custom filtering rules to all messages.

- `1` — The Exchange Public Folder task does not apply the custom filtering rules.

If the `Override` entry does not exist, then the task applies the custom filtering rules to all messages.

8 Close Regedit.

9 After you have configured the required XML filter rules, restart the Exchange Public Folder tasks.

See "About custom filtering ruleset files" on page 258.

About custom filtering ruleset files

Custom filter rules and actions are defined in XML ruleset files. Each ruleset file contains one or more rules with associated actions.

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, 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.

An item may be a message or an attachment. If a message has an attachment, the message is evaluated first, and then the attachment is evaluated.

By default items that do not match any rules are archived by the mailbox archiving task or the journal archiving task. If you want to archive only items that match a rule, you can create a catch-all rule as the last rule in the ruleset file. Assign the action "MARK_DO_NOT_ARCHIVE" to this last rule.

While developing and testing your filter, we strongly advise that you assign the action "MARK_DO_NOT_ARCHIVE" to your rules. Check that the rules are applied exactly as you expect before changing them to the actions that you want to use in your production environment.

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 297.
- customproperties.xsd — This contains the XML schema for validating the custom properties XML file.

When you create ruleset files or modify existing ruleset files, you must restart the associated archiving tasks before the changes take effect. 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: If you create rules to match names that contain special characters, you must save the XML ruleset files with Unicode encoding.

About the default filter rules file for custom filtering

Default filters and actions are defined in a ruleset file called Default Filter Rules.xml.

To implement specific filtering for public folders or particular mailboxes, 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 you choose not to use Default Filter Rules.xml, you must configure the IGNORENODEFAULT registry value.

See "About controlling default custom filtering behavior" on page 261.

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 294.

About named ruleset files for individual Exchange Server mailboxes

To set up custom filtering for an individual Exchange Server user or journal mailbox, you need to create a separate ruleset file for each mailbox you want to filter. The name of each ruleset file must be *`mailbox_owner`*`.xml`.

The mailbox owner will typically be the same as the account Display Name, but could be different if you have changed the mailbox owner name, for some reason.

For example, if you want to filter John Doe's mailbox, and John Doe is the mailbox owner name, you would create a ruleset file called "John Doe.xml". To apply filtering to a journal mailbox with the mailbox owner name "Journal US1", you would create a ruleset file called "Journal US1.xml". Any other mailboxes that do not have a named ruleset file and are serviced by the archiving tasks 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 261.

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

Note: If custom filtering is enabled for all Exchange Server mailbox archiving and you want to apply different rules to Exchange Server user and journal mailboxes, you could create a named ruleset file for the Exchange Server journal mailbox and configure the default ruleset file for filtering all user mailboxes. This would avoid having to create a large number of named ruleset files.

About the named ruleset file for public folders

To set up specific filtering for Exchange Server public folders, you need to create a separate ruleset file called `Public Folder Rules.xml`. This will be used by all Exchange Public Folder tasks hosted on the Enterprise Vault server computer. If `Public Folder Rules.xml` does not exist, the default ruleset file, `Default Filter Rules.xml`, will be used. If neither of these files exist, but a default content category is defined in `custom properties.xml`, items will be archived according to the settings in the default content category.

See "Configuring custom properties and content categories" on page 294.

If none of the above exists—`Public Folder Rules.xml`, `Default Filter Rules.xml` or a default content category—an error will be logged and the archiving tasks will stop, unless you have configured the IGNORENODEFAULT registry setting.

You can configure archiving tasks to manage missing defaults gracefully using the IGNORENODEFAULT registry setting.

About controlling default custom filtering behavior

If Enterprise Vault archiving tasks are enabled for filtering, the actions 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 261.

Different configurations and the resulting actions of archiving tasks for each configuration are shown in Table 15-6 and Table 15-7.

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
 \Wow6432Node
  \KVS
   \Enterprise Vault
    \External Filtering
     \Journaling|Mailbox|PublicFolder
```

4 Right-click the required archiving key (`Journaling`, `Mailbox` or `PublicFolder`) and select `New`,`Key`.

5 Name the new key `EnterpriseVault.CustomFilter`.

6 Right-click `EnterpriseVault.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 tasks for the selected type of archiving.

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 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 15-6 shows ten different configurations for custom filtering and properties.

The resulting actions taken by archiving tasks in each case are described in Table 15-7.

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. Remember that named ruleset files can also be created for Exchange Server public folders or specific Exchange Server journal mailboxes.
See "About custom filtering ruleset files" on page 258.
- 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 15-6 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 15-7 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.
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 `John Doe.xml` 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 `John Doe.xml` and Sam Cole's mailbox is archived according to the rules in `Default Filter Rules.xml`. No custom properties are indexed. Content categories cannot be used.
6	As for case 5. The fact that IGNORENODEFAULT is set makes no difference.

Table 15-7 Resulting actions for example configurations *(continued)*

Case	Resulting action
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 Sam Cole.xml.
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 `Sam Cole.xml`.
10	As for case 9. The fact that IGNORENODEFAULT 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"]
   [ATTACHMENT_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>]

     [<attachment_attributes> [attribute_value_operator]>
       <attachment_attribute_values>
```

```
        [<attachment_attribute_values>]
      </attachment_attributes>]

      [<attachment_attributes>... </attachment_attributes>]

 </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. A rule may also contain attachment attribute filters for evaluating attachments to messages.

Table 15-8 shows the message attributes that you can use to select messages.

Table 15-8 Message attributes for custom filtering

Message attribute	More information
Author	See "Message author and recipients filters for custom filtering" on page 272.
Recipients	See "Message author and recipients filters for custom filtering" on page 272.
Direction	See "Message direction filters for custom filtering" on page 280.
Subject text	See "Message subject filters for custom filtering" on page 282.
Named MAPI properties	See "About MAPI named properties filters for custom filtering" on page 283.

Table 15-9 shows the attachment attributes that you can use to select specific files attached to messages.

Table 15-9 Attachment attributes for custom filtering

Attachment attribute	More information
File name	See "Attachment attribute filters for custom filtering" on page 284.

Table 15-9 Attachment attributes for custom filtering *(continued)*

Attachment attribute	More information
File size	See "Attachment attribute filters for custom filtering" on page 284.

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.

If the message attributes satisfy a rule, any attachments are then evaluated using attachment attributes. When an attachment matches a rule, the action specified by ATTACHMENT_ACTION= is applied to the attachment.

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 301.

If attachments to messages are to be evaluated, a rule must have an attachment action associated with it; ATTACHMENT_ACTION="*match_action*". If an attachment action is specified, an attachment attribute element (<FILES> element) must also be present in the rule. This defines the file names or file size (or both) to use when matching attachments. If attachments match the specified attachment filter, the attachment action is performed. Attachments to nested messages are also processed by the filter.

Note: For messages (and then attachments), 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 270.
  See “Specifying an archive for custom filtering” on page 270.
- 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 journal mailbox, 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. The Override registry value is described in the sections describing how to configure custom filtering registry settings for archiving tasks:

- See "Configuring registry settings for Exchange Server journal custom filtering" on page 253.
- See "Configuring registry settings for Exchange Server mailbox custom filtering" on page 255.
- See "Configuring registry settings for Exchange Server public folder custom filtering" on page 257.

- ACTION="MOVE_DELETED_ITEMS" — Do not archive the message; move it to the Deleted Items folder.
  This action cannot be used with public folder filtering; if this action is configured, an error will be logged and the tasks will stop.
- ACTION="HARD_DELETE" — Do not archive the message; delete it immediately without moving it to the Deleted Items folder. This action is not recommended for Exchange Server public folder filtering.

Note: If the Compliance Accelerator Journaling Connector is being used to capture a required percentage of all Exchange 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.

The following actions can be applied to message attachments that match an attachment filter:

- ATTACHMENT_ACTION="REMOVE" — If a file attached to a message matches the name or size specified in the attachment attribute filter, delete it.
- ATTACHMENT_ACTION="REPLACE" — If a file attached to a message matches the name or size specified in the attachment attribute filter, replace it with a file called `Deleted Attachments.txt`, which lists the attachments that have been deleted.

See "About the Deleted Attachments.txt file for custom filtering" on page 271.

If the message has nested messages with attachments, the action will be applied to all nested message attachments.

If the action applied to a message is "HARD_DELETE", no attempt is made to evaluate any files attached to the message.

The extract below shows how a rule name, message action and attachment action might be specified in the ruleset file. In this example, any messages that satisfy the message attribute filters will be archived in the default archive. Also, any Exchange Server messages attachments that match the attachment filter will be deleted and replaced with a file called `Deleted Attachments.txt`:

```
<RULE NAME="Archive Rule 1" ACTION="ARCHIVE_ITEM"
    ATTACHMENT_ACTION="REPLACE">
  <message attribute filters>
  <attachment attribute filter>
</RULE>
```

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 mailbox or public folder 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="151652638328904938485681616 47.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 the Deleted Attachments.txt file for custom filtering

If the attachment action is "REPLACE", users will see a file called `Deleted Attachments.txt` attached to messages that have had attachments deleted by the filter. When they open this file, it contains a list of the files that have been deleted.

The contents of this file are taken from the file, `CF_Replace_Attachment.txt`, in the Enterprise Vault directory (for example, `C:\Program Files (x86)\Enterprise Vault`). If required, you can modify the text of this file. For example, you may want to localize the descriptive text.

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 275.

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>
```

Note: Matching attribute values is case-insensitive.

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 ampersand character (&) is included in an SMTP address, the character must be replaced with

  ```
  &amp;
  ```

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

  ```
  admin&amp;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 Exchange Server messages is

```
<DISPN>John Doe</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.

  Note: Custom filtering cannot match against distribution lists that are hidden from the Exchange 2013 and Exchange 2010 Global Address List.

  See "About distribution lists in attribute values with custom filtering" on page 274.

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 275.

Note the following:

- There are situations where messages may not have an SMTP address; for example, messages imported into a mailbox from a PST file and Exchange Server addresses set up for internal messaging only. For this reason you may want to include both the display name and the email address in a rule (provided you are not using the INCLUDES="ALL" operator).
- Be aware that display names do not have to be unique; an external sender, for example, could have the same display name as an internal sender.
- If changes to your Microsoft Exchange Server Global Address List (or Global Address Catalog in Active Directory) affect users or distribution lists included in custom filters, you may have to update your custom filter rules accordingly. For example, if you are filtering on the display name of a distribution list and then change the display name, you will need to update the appropriate ruleset file entry.
- Changes made to the Microsoft Exchange Server Global Address List will not become effective until the next scheduled GAL update. If, for example, a user's address has been changed to their married name, and you have set up a filter that includes the new address as AUTHOR, there may be a delay before messages are matched.
- To ensure that Bcc and Undisclosed recipients are available when filtering on the Exchange Server journal mailbox, Envelope Journaling must be enabled on your Microsoft Exchange Server.

About distribution lists in attribute values with custom filtering

If you want to match all messages sent to members of a particular Exchange Server distribution list, 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 distribution list, ALL SALES.

For this matching to work, ensure that expansion of distribution lists is enabled in the Administration Console (in the "Archiving General" settings on the "Advanced" tab of the Exchange journal policy). Also, the distribution list must not be included in the Agents registry setting, `BlacklistedDLs`.

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 Exchange Server distribution list 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 15-10 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 15-10 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
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.)

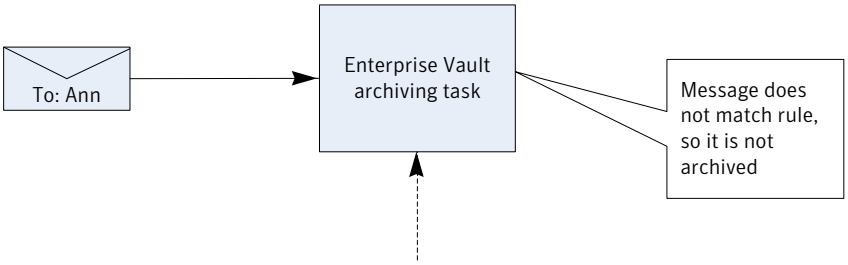
The first column shows different combinations of values set for the INCLUDES= and ALLOWOTHERS= operators.

"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 15-1 and Figure 15-2 illustrate what happens in two of the scenarios in Table 15-10.

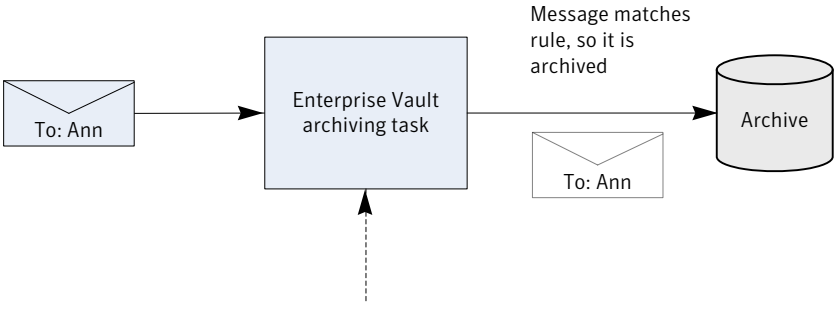
Figure 15-1 Msg 1 with INCLUDES="NONE" and ALLOWOTHERS="N"



Custom filtering enabled.
Rule filter configured:

```
<RULE ...ACTION="ARCHIVE_ITEM">
    <RECIPIENTS INCLUDES="NONE"
                ALLOWOTHERS="N">
        <DISPN>Ann</DISPN>
        <DISPN>Bill</DISPN>
    </RECIPIENTS>
</RULE>
```

Figure 15-2 Msg 1 with INCLUDES="ANY" and ALLOWOTHERS="Y"



Custom filtering enabled.
Rule filter configured:

```
<RULE ...ACTION="ARCHIVE_ITEM">
    <RECIPIENTS INCLUDES="ANY"
                ALLOWOTHERS="Y">
        <DISPN>Ann</DISPN>
        <DISPN>Bill</DISPN>
    </RECIPIENTS>
</RULE>
```

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

To determine whether addresses are internal or external addresses, Enterprise Vault uses the SMTP address domains listed for the system mailbox account associated with the Enterprise Vault Journaling task. You can see the email addresses associated with a mailbox in Active Directory.

For example, if the following SMTP addresses are listed for the system mailbox:

- VaultAdmin@ourcompanyplc.com
- VaultAdmin@ourcompanyinc.com

then any of the following addresses will be recognized as internal:

- *@ourcompanyplc.com
- *@[*.]ourcompanyplc.com
- *@ourcompanyinc.com
- *@[*.]ourcompanyinc.com

where [*.] means the string can be repeated, as in john.doe@sales.emea.ourcompanyplc.com.

Any other addresses are treated as external.

With Exchange Server filtering, addresses from local Microsoft Exchange Servers are also regarded as internal. (These addresses include the MAPI attribute, PR_SENDER_ADDRTYPE.)

For Exchange Server users, you can change the email addresses associated with a mailbox in Active Directory.

Alternatively, you can specify additional 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
 \Wow6432Node
  \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>
```

About MAPI named properties filters for custom filtering

The <NAMEDPROP> </NAMEDPROP> message attribute enables you to select Exchange Server messages for processing depending on the value assigned to specific MAPI named properties. Named properties can be single-valued or multi-valued.

The custom properties feature is used to define the required properties, so that they are indexed by Enterprise Vault. Users can then search archived messages for those with a particular value set for the named property.

Instructions are provided on how to define named properties.

See "Defining additional MAPI properties in custom properties" on page 299.

A named property filter takes the following general format:

```
<NAMEDPROP TAG="EV_tag_name" INCLUDES="operator_value">
  <PROP VALUE="value" />
  [<PROP VALUE="value" />]
</NAMEDPROP>
```

The value of the TAG attribute is the name by which Enterprise Vault knows the property. This is the TAG value set in the `Custom Properties.xml` file.

The operator value can be "ANY", "NONE" or "ALL".

Each <PROP> line defines a specific value for the property that custom filtering is to use when evaluating messages.

For example, a third party application adds a multi-valued, named MAPI property called "Location" to messages. This property identifies the department and location of the sender or recipient. The property is identified in the `Custom Properties.xml` file and given the Enterprise Vault tag name, "Loc". The following example shows a filter that would match messages that have the value "Pittsburgh" or "Finance" set for the "Location" property. Any messages that match are archived with the retention category, "Confidential".

```
<!--Example: Archive items that have Pittsburgh or Finance as values
 for the Location property -->
<RULE NAME="Location rule" ACTION="ARCHIVE_ITEM"
  RETENTION="Confidential">
  <NAMEDPROP TAG="Loc" INCLUDES="ANY">
    <PROP VALUE="Pittsburgh" />
    <PROP VALUE="Finance" />
  </NAMEDPROP>
</RULE>
```

Searches could be performed for messages that have specific values set for that named property.

Instructions are provided on how to create and implement an example custom filter that uses named MAPI properties. The example custom filter assigns a different retention category to messages of a particular message class.

See “Custom properties example” on page 313.

For more information on named properties, see the following Microsoft article:

http://msdn.microsoft.com/en-us/library/office/cc765864.aspx

Attachment attribute filters for custom filtering

To enable you to delete certain attachments before archiving messages, a rule can contain attachment attribute filters which define which attachment files to select.

The following example XML shows how you can include one or more attachment attribute filters in a rule:

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

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

    <FILES INCLUDES="ANY|ALL|NONE">
        <FILE FILENAME="filename" SIZE_GREATER_THAN_KB="integer" />
        <FILE ... />
        ...
    </FILES>

    <FILES INCLUDES="ANY|ALL|NONE">
        <FILE ... />
        ...
    </FILES>

</RULE>
```

The <FILES> tag defines an attachment filter.

If you specify an attachment action (ATTACHMENT_ACTION=), then you need to include at least one attachment filter (using the <FILES> tag). For an attachment to match a rule (and the attachment action applied), the attachment must satisfy all attachment filters specified in the rule. The order of attachment filters in a rule is not significant.

The INCLUDES= operator enables you to define how the following attribute lines are to be applied, when evaluating each attachment.

An attachment filter contains one or more <FILE> elements, that define the attributes to match. Each <FILE> element contains one or both of the following attributes:

- FILENAME="*filename*"
  <filename> is all or part of the file name to match. Wildcards can be included in the file name. You can use this attribute to filter files with specific text strings in the name or extension, for example, "`*.AVI`".
  When selecting files using the file extension, custom filtering only evaluates the file name; it does not check the type of the file contents. If files that would normally be deleted by a filter are given a different extension, they will not be deleted by the filter.
  Also, files contained in compressed files, such as .ZIP files, are not evaluated.
- SIZE_GREATER_THAN_KB="*integer*"
  This enables you to configure the filter to remove attachments over a certain size.

Where file name and size are specified in a <FILE> element, both must be satisfied for an attachment to match. For example, if an attachment is to match the following line, it must have an extension of .MP3 and be larger than 1 MB:

```
<FILE FILENAME="*.MP3" SIZE_GREATER_THAN_KB="1000" />
```

If you specify multiple <FILE> elements to use in evaluating attachment files, each one will be applied. For an attachment to match the rule, it must match each <FILE> element.

To define how the <FILE> lines are to be applied, when evaluating each attachment, use the INCLUDES= operator:

- INCLUDES="ANY" means that the attachment matches if it has the attributes specified in at least one of the <FILE> lines. This is the default action if the operator is not specified.
- INCLUDES="ALL" means that the attachment matches only if it has the attributes specified in all the <FILE> lines.
- INCLUDES="NONE" means that the attachment matches if it does not include any of the attributes specified in the <FILE> lines.

In the following example, an attachment will match the filter if all the following are true:

- The file is an MP3 file larger than 2MB
- The file name includes the text, "enlarge", and the file is larger than 1 MB
- The file has the extension, MPG
- The file is larger than 12 MB

```
<FILES INCLUDES="ANY">
  <FILE FILENAME="*.MP3" SIZE_GREATER_THAN_KB="2000" />
  <FILE FILENAME="*enlarge*.*" SIZE_GREATER_THAN_KB="1000" />
  <FILE FILENAME="*.MPG" />
  <FILE SIZE_GREATER_THAN_KB="12000" />
</FILES>
```

The following example shows how multiple attachment filters can be used to exclude certain attachments from deletion:

```
<RULE NAME="Filter attachments rule" ... ATTACHMENT_ACTION="REMOVE">

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

   <FILES INCLUDES="NONE">
       <FILE FILENAME="signature.jpg" />
   </FILES>

   <FILES INCLUDES="ANY">
       <FILE SIZE_GREATER_THAN_KB="5000" />
```

```
    </FILES>

</RULE>
```

With these attachment filters, attachments will be deleted if they do not have the filename, `signature.jpg`, and are larger than 5 MB.

How message and attachment filters are applied for custom filtering

This section describes the order in which message and attachment evaluation is applied when filtering Exchange Server messages.

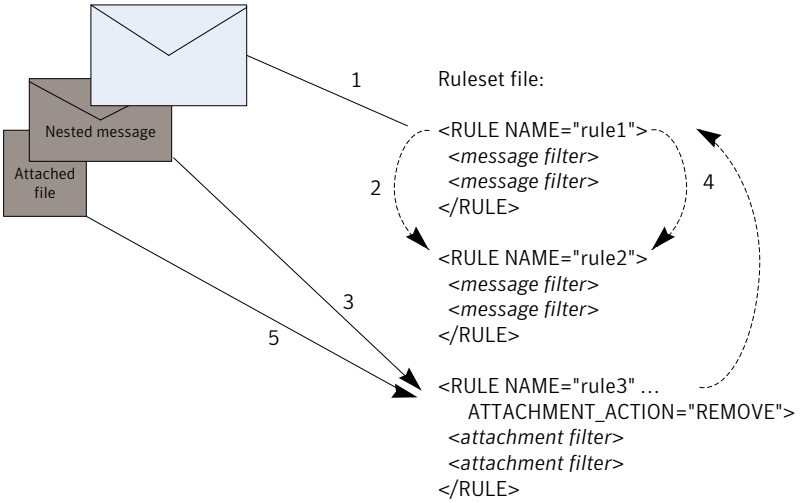
When custom filters processes messages, the following general points are observed:

- Messages and attachments are evaluated separately. Messages are evaluated first against rules in the ruleset file, and then attachments are evaluated against any rules that contain an attachment action.

  If an attachment is a message, the message is evaluated using message filters in rules (with attachment action set) and then any attachments to the nested message are evaluated using attachment filters in rules.
- When evaluating a message, only the first rule in the ruleset file that matches the message is applied. Similarly, when evaluating attachments, only the first rule that matches is applied to the attachment. For this reason the order of rules in a ruleset file is significant.
- The rule action (and attachment action) are only applied to a message (or attachment) that satisfies all the filters in the rule.
- The default action for both messages and attachments is to archive the item. This means that messages and attachments that do not match any rules will be archived.

Figure 15-3 shows how custom filtering processes a message with attachments.

Figure 15-3 Processing attachments



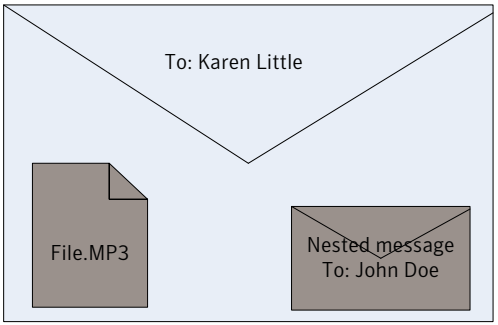
The message illustrated has a nested message attached and that message has a file attached. The simple ruleset file has two rules that contain message filters and one rule that contains attachment filters, as follows:

- The top-level message is evaluated using the first message rule, rule1.
- If that rule does match, then the rule ACTION is applied to the message. If the rule does not match, then rule2 is tried.
- (If the message ACTION is HARD_DELETE", no further evaluation is done.) As there is a rule with ATTACHMENT_ACTION, and the message has an attachment, the message attachment is evaluated using the attachment filters in rule3.
- Custom filters recognizes that the attachment is a message, so the message is evaluated against message filters in any rules with ATTACHMENT_ACTION set. In this example, only rule3 has ATTACHMENT_ACTION set and it does not have any message filters, so the message will not match the rule. Items that do not match filter rules are archived (the default action).
- The attachment to the nested message is then evaluated using the attachment filters in rule3. If the attachment matches the attachment filters then the ATTACHMENT_ACTION is applied to the attachment.

Message filters and attachment filters can be combined in a single rule to select attachments to particular messages.

Figure 15-4 shows an example message to the recipient, Karen Little, that has an MP3 file attached and also a message attached (a nested message).

Figure 15-4 Example message with attachments



Message with one attached file, File.MP3, which is 10 MB, and a nested message

The message may also have attachments.

The following example ruleset file contains a single rule to be applied to this message. The overall effect of this rule is to delete certain attachments in Exchange Server messages to recipients other than Gill Smith or John Doe. Attachments in messages to Gill Smith or John Doe are not deleted. Attachments with the following attributes will be deleted:

- MP3 attachments larger than 2 MB
- JPG attachments larger than 1 MB
- MPG files larger than 5 MB

```
<?xml version="1.0" encoding="UTF-8"?>
<RULE_SET xmlns="x-schema:ruleset schema.xdr">

<!--Disallowed attachment rule: This rule will delete the specified
attachments for all recipients except Gill Smith and John Doe.-->

<RULE NAME="Disallowed attachments (except directors)"
   ATTACHMENT_ACTION="REMOVE" >
  <RECIPIENTS INCLUDES="NONE" ALLOWOTHERS="N">
    <EA>Gill.Smith@example.com</EA>
    <EA>John.Doe@example.com</EA>
  </RECIPIENTS>
  <FILES INCLUDES="ANY">
    <FILE FILENAME="*.MP3" SIZE_GREATER_THAN_KB="2000" />
    <FILE FILENAME="*.JPG" SIZE_GREATER_THAN_KB="1000" />
    <FILE FILENAME="*.MPG" SIZE_GREATER_THAN_KB="5000" />
```

```
  </FILES>
</RULE>
```

Assuming the appropriate archiving task has custom filtering enabled, the filters in this ruleset will be applied to the example message, as follows:

- First apply the message attribute filter (the <RECIPIENTS> element) to the top-level message.
- The recipient is not Gill Smith or John Doe, so the message attribute filter matches.
- As the message matches the rule, it will be archived (ACTION=).
- Is there a rule that contains ATTACHMENT_ACTION? Yes. This means that any attachments to the message must be evaluated using <FILES> attachment filters.
- Does the attachment file name and file size match any of the <FILE> attribute lines in the rule? Yes, the attached file matches the first <FILE> line. This means that the attachment matches the rule, so delete the attachment, as specified in the ATTACHMENT_ACTION.
- Does the message have another attachment? Yes, there is an attached message. Custom filtering recognizes that the attachment is a message and evaluates the message using the message attribute filter (the <RECIPIENTS> element).
- As the nested message is to John Doe, the <RECIPIENTS> filter is not satisfied. The message is therefore archived together with its attachments.

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.

```
<?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: (Available for Exchange Server archiving only)
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 message properties when archiving items. The properties can be Exchange Server MAPI properties that have been added to messages by a third-party application, as follows:

- Standard MAPI properties that are not currently indexed by Enterprise Vault
- Custom MAPI properties
- Named MAPI properties

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.

See "Custom properties example" on page 313.

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 15-11 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 Exchange Server journal custom filtering" on page 253. See "Configuring registry settings for Exchange Server mailbox custom filtering" on page 255. See "Configuring registry settings for Exchange Server public folder custom filtering" on page 257.

Table 15-11 Steps to configure custom properties or content categories *(continued)*

Step	Action	More information
Step 2	Create the XML file, `Custom Properties.xml`. Place this file in the folder `Enterprise Vault\Custom Filter Rules`.	See "About the general format of Custom Properties.xml" on page 297. The entries in `Custom Properties.xml` enable you to do the following: ■ 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. To configure Enterprise Vault to index specific custom properties on all messages, without performing any filtering, create a `Custom Properties.xml` file but no ruleset file. The `Custom Properties.xml` 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 IGNORENODEFAULT registry setting. See "About controlling default custom filtering behavior" on page 261.
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, `Enterprise Vault\Custom Filter Rules`.	See "Configuring custom filtering" on page 251.
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 custom or standard MAPI properties on Exchange 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 301.
- <CUSTOMPROPERTIES></CUSTOMPROPERTIES> This section defines the additional message properties that are to be available to Enterprise Vault.
  See "Defining additional MAPI properties in custom properties" on page 299.
- <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 305.

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 15-12 on page 310.

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 MAPI properties in custom properties

In the <CUSTOMPROPERTIES> section of `Custom Properties.xml`, you define the additional MAPI properties that you want Enterprise Vault to evaluate or index.

Before MAPI properties can be defined in `Custom Properties.xml`, they must be defined in the MAPI subsystem. Currently, the Enterprise Vault custom properties feature supports only STRING and DOUBLE properties. Enterprise Vault supports single or multi-valued properties.

In MAPI, properties are grouped by NAMESPACE. Typically, properties accessed by a particular application are defined in the same namespace. Each namespace is identified by a GUID. Each property is defined by its STRING ID and namespace GUID.

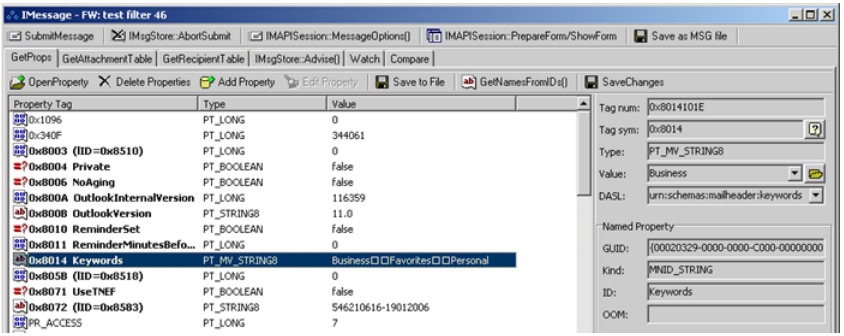
For each property that you want to include, you will need the following details from the property definition in the MAPI subsystem:

- If the property is a standard MAPI property, the hexadecimal MAPI property tag. You can specify just the Identifier part of the 32-bit hexadecimal MAPI property tag (bits 16 to 31), or the Identifier part (bits 16 to 31) plus the Property type part (bits 0 to 15). For example, if the MAPI Property tag for a standard property is 0x0070001E, the Enterprise Vault NAME value could be specified as either 0x0070001E or 0x0070.
- If the property is a custom property, the GUID of the property's namespace.
- If the property is a custom property, the property's STRING ID. If the property is a named property, the ID will be a name.

You can use third party MAPI tools, such as OutlookSpy, to view the MAPI properties associated with mailbox items.

Figure 15-5 shows how MAPI properties on a message are displayed in OutlookSpy.

Figure 15-5 Viewing MAPI properties



The selected property is the named property, "Keywords". This multi-valued property holds the Outlook categories assigned to the message. Details of the selected property are displayed on the right-hand side of the window.

Note that the "Keywords" property is only used here as an example of a named MAPI property. You do not need to add it as a custom property, because it is already indexed in a default Enterprise Vault system.

To make MAPI 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.

Here is an example showing how properties can be defined:

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

<CUSTOMPROPERTIES>
  <NAMESPACE TYPE="MAPI"
GUID="{DA6007CD-01AA-408f-B7D3-6DA958A09583}">
    <PROPERTY NAME="Author1" TAG="CaseAuthor"/>
    <PROPERTY NAME="Status1" TAG="CaseStatus"/>
  </NAMESPACE>
  <NAMESPACE TYPE="MAPI" GUID="{EF1A0001-01AA-408f-B7D3-6DA958A09583}">
    <PROPERTY NAME="Author2" TAG="Client"/>
  </NAMESPACE>

  <NAMESPACE TYPE="MAPI">
```

```
    <PROPERTY NAME="0x0070" TAG="Topic"/>
    </PROPERTY>
    <PROPERTY NAME="0x1035" TAG="MsgID"/>
    </PROPERTY>
  </NAMESPACE>
</CUSTOMPROPERTIES>
```

In this example there are three NAMESPACES. The first two define custom MAPI properties, so the GUID of the NAMESPACE is required. As the properties defined in the third NAMESPACE are standard MAPI properties, no GUID is required.

The value of the TYPE attribute identifies the property type; in this example, the properties are MAPI properties.

Within each NAMESPACE the properties are defined in PROPERTY elements using NAME and TAG values, as follows:

- If the property is a custom named MAPI property, NAME is the STRING ID defined in the MAPI subsystem. The value is case-sensitive and must match exactly the value in the MAPI subsystem.

  If the property is a standard MAPI property, NAME is either the Identifier part (bits 16 to 31) of the hexadecimal MAPI tag, or the Identifier part (bits 16 to 31) plus the Property type part (bits 0 to 15).
- TAG identifies the property within Enterprise Vault. It can contain only alphanumeric characters (A-Z, a-z, or 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.

  If you want to select messages by matching the values of specific properties, you need to create a <NAMEDPROP> filter in the appropriate XML ruleset file and specify the TAG value defined here.

  See "About MAPI named properties filters for custom filtering" on page 283.

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 303.

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="151652638328904938485681616 47.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 MAPI properties in custom properties" on page 299.

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="151652638328904938485681616 47.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="151652638328904938489049384 8.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 261.

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>
  </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.

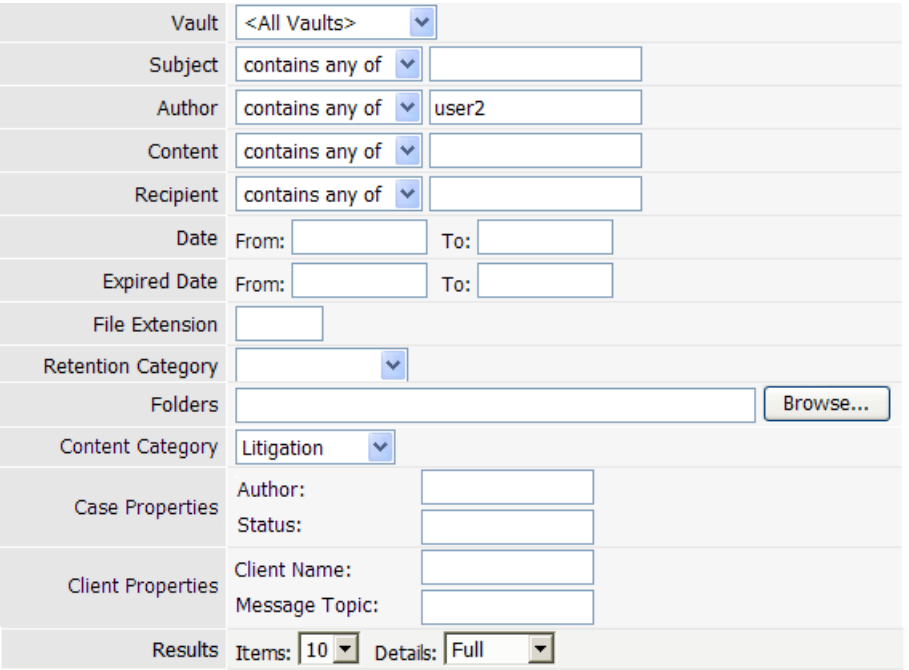
Displaying custom properties in the browser search

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 15-6 shows the Enterprise Vault browser search with the example custom properties and content categories displayed.

Figure 15-6 Example presentation properties displayed in the browser search page



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 15-7 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 15-12 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 15-12 XML elements and attributes in the Custom Properties.xml file

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

Table 15-12 XML elements and attributes in the Custom Properties.xml file *(continued)*

Element	Attribute	Mandatory	Description
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.
	TYPE=	Yes	Value is the type of property: "MAPI".
	GUID=	Yes	MAPI properties only. Value is identity of NAMESPACE to external applications.
PROPERTY		Yes	Defines a custom property.
	NAME=	Yes	If the property is a custom MAPI property, value is the STRING ID defined in the MAPI subsystem. The value is case-sensitive and must match exactly the value in the MAPI subsystem. If the property is a standard MAPI property, value is either the Identifier part of the 32-bit hexadecimal MAPI property tag (bits 16 to 31), or the Identifier part (bits 16 to 31) plus the Property type part (bits 0 to 15). Value must be unique in NAMESPACE.

Table 15-12 XML elements and attributes in the Custom Properties.xml file *(continued)*

Element	Attribute	Mandatory	Description
	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.
PRESENTATION		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.)
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.

Table 15-12 XML elements and attributes in the Custom Properties.xml file *(continued)*

Element	Attribute	Mandatory	Description
	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.

Custom properties example

This section provides an example custom filter for Exchange Server mailbox archiving. The example custom filter assigns a different retention category (180Days) to calendar items (Exchange message class, IPM.Appointment).

To implement the example custom filter

1. Create the ruleset file, `Default Filter Rules.xml`.

   See "Example ruleset file for configuring custom properties" on page 314.

2. Create the custom properties file, `Custom Properties.xml`.

   See "Example custom properties file" on page 315.

3. Configure the registry settings to enable Exchange Server mailbox filtering.

   See "Configuring registry settings for Exchange Server mailbox custom filtering" on page 255.

4 Set Dtrace logging for the archiving task (`set ArchiveTask v`).

For instructions on how to configure Dtrace logging, see the *Utilities* guide.

5 Test the custom filter.

See "Testing the example custom filter for configuring custom properties" on page 316.

6 Check the Dtrace log entries.

See "DTrace log entries for the example custom filter when configuring custom properties" on page 318.

Example ruleset file for configuring custom properties

The following example `Default Filter Rules.xml` file shows the filter rule required. This file must be located in the folder, `Custom Filter Rules`, in the Enterprise Vault installation folder (for example `C:\Program Files (x86)\Enterprise Vault\Custom Filter Rules`).

```
<?xml version="1.0"?>
<RULE_SET xmlns="x-schema:ruleset schema.xdr">
    <RULE NAME="MBX DIFF_RET_CAT" ACTION="ARCHIVE_ITEM"
        CONTENTCATEGORY="MsgClassTest" RETENTION="180Day">
        <NAMEDPROP TAG="MSGCLASS" INCLUDES="ANY">
            <PROP VALUE="IPM.Appointment" />
        </NAMEDPROP>
    </RULE>
</RULE_SET>
```

Settings in the file are used as follows:

- NAME="MBX DIFF_RET_CAT". This setting assigns a name to the rule. If Dtrace logging is enabled for the Exchange Mailbox task, the rule name is displayed when items are evaluated using this rule.
- ACTION="ARCHIVE_ITEM" CONTENTCATEGORY="MsgClassTest" RETENTION="180Day". Items that match the rule are processed as follows:
  - The items are archived.
  - The settings that are defined in the content category, MsgClassTest, are applied to the items. (The content category is defined in the file, `Custom Properties.xml`).
  - The existing retention category, 180Day, is applied to the items.
- The <NAMEDPROP> element defines the message property and value to use when evaluating items using this rule.

TAG="MSGCLASS" is the Enterprise Vault label for the property. This label is assigned to the associated MAPI property in `Custom Properties.xml`.
INCLUDES="ANY". Any item with the property value shown matches the rule.
<PROP VALUE="IPM.Appointment" />. When an item has a MSGCLASS property with the value`IPM.Appointment`, then that item matches the rule.

Example custom properties file

The content category, MsgClassTest, and the property, MSGCLASS, are defined in the following example `Custom Properties.xml` file. This file also defines how the content category and property are presented in the specified application. `Custom Properties.xml` must be located in the folder, `Custom Filter Rules`, in the Enterprise Vault installation folder.

```
<?xml version="1.0"?>
<CUSTOMPROPERTYMETADATA xmlns:xsi="http://www.w3.org/2001/
  XMLSchema-instance" xsi:noNamespaceSchemaLocation=
  "customproperties.xsd">
  <CONTENTCATEGORIES DEFAULT="MsgClassTest">
    <CONTENTCATEGORY NAME="MsgClassTest">
      <INDEXEDPROPERTIES>
        <PROPERTY TAG="MSGCLASS"/>
      </INDEXEDPROPERTIES>
    </CONTENTCATEGORY>
  </CONTENTCATEGORIES>
  <CUSTOMPROPERTIES>
    <NAMESPACE TYPE="MAPI">
      <PROPERTY TAG="MSGCLASS" NAME="0x001A" />
    </NAMESPACE>
  </CUSTOMPROPERTIES>
  <PRESENTATION>
    <APPLICATION NAME="search.asp" LOCALE="1033">
      <FIELDGROUPS>
        <FIELDGROUP LABEL="Content Category">
          <FIELD TAG="MSGCLASS" LABEL="Message Class"
                 CATEGORY="MsgClassTest"/>
        </FIELDGROUP>
      </FIELDGROUPS>
      <AVAILABLECATEGORIES>
        <AVAILABLECATEGORY CONTENTCATEGORY="MsgClassTest"
                           LABEL="Message Class Test"/>
      </AVAILABLECATEGORIES>
    </APPLICATION>
```

```
  </PRESENTATION>
</CUSTOMPROPERTYMETADATA>
```

Settings in the file are used as follows:

- The <CONTENTCATEGORY> element defines the content category, MsgClassTest.
  In the <INDEXEDPROPERTIES> element, the <PROPERTY> element specifies that the MSGCLASS property is to be indexed when the content category is applied to an item.
- In the <PROPERTY> part of the <CUSTOMPROPERTIES> element, the standard MAPI property (NAME="0x001A") is mapped to the Enterprise Vault property tag (TAG="MSGCLASS").
  0x001A is the Identifier part (bits 16 to 31) of the hexadecimal MAPI tag for the message class property.
- The <PRESENTATION> element defines how the message class property is displayed in the application specified in the <APPLICATION> element. In this example, NAME="search.asp" identifies the Enterprise Vault browser search. The language for this application (LOCALE) is US English.
  In the context of the browser search application, <FIELDGROUPS> identifies the new search criteria to be added to the search page. As the new property is to be listed under its associated content category, <FIELDGROUP LABEL="Content Category"> identifies the top level search criteria label. The properties to be listed when a particular content category is selected are identified by the <FIELD> settings. The <AVAILABLECATEGORIES> element identifies the content categories that can be selected. In this example, there is only one content category, which has only one property.
  See Figure 15-8 on page 318.

Testing the example custom filter for configuring custom properties

We recommend that you test the custom filter on a development system; not on your production Enterprise Vault server.

Before testing the custom filter, do the following:

- Configure the registry settings to enable Exchange Server mailbox filtering.
  See "Configuring registry settings for Exchange Server mailbox custom filtering" on page 255.
- In the Enterprise Vault Administration Console, configure an Exchange Mailbox policy to archive new items immediately.
  Click the **Message Classes** tab, and ensure that **IPM.Appointment*** is selected.
  Check that the policy is assigned to the appropriate provisioning group.

- In the Enterprise Vault Administration Console, create a new retention category called 180Day.
- Restart the Exchange Mailbox task in the Enterprise VaultAdministration Console, to apply the policy change and the changes in the ruleset file, `Default Filter Rules.xml`.
- Restart the IIS Admin service on the Enterprise Vault server, to apply the changes in the `Custom Properties.xml` file to the browser search page.

To test the custom filter

1. Start Outlook and log in as the test user. Create a calendar appointment that occurred in the past. Ensure the appointment is not a recurring appointment, and does not have a reminder set.
2. Enable DTrace to trace the Exchange Mailbox task (`set ArchiveTask v`).

   For instructions on how to configure DTrace logging, see the *Utilities* guide.
3. Run the Exchange Mailbox task to archive the new items, and then wait for a few minutes.
4. Check the entries in the DTrace log.

   See "DTrace log entries for the example custom filter when configuring custom properties" on page 318.
5. Use Enterprise Vault browser search to search for the appointment in the test user's archive.

   The search criteria page now includes a **Content Category** field, as shown in Figure 15-8. You can search for the appointment that matched the filter rule by typing **IPM.Appointment** in the **Message Class** box. Search results show the item that matched the custom filter rule.

   Alternatively, in the **Retention Category** drop-down list select the **180Day** retention category. Again, search results show the appointment that matched the custom filter rule, as this item was archived with the 180Day retention category.

   See Figure 15-9 on page 318.

   The following additional steps are required to display the custom property in the search results:

   - Add the attribute RETRIEVE="Y" to the <INDEXEDPROPERTIES> element in the content category definition in `Custom Properties.xml`.
   - In the browser search page, set **Details** to **Full**.

   See "About content categories" on page 301.

Figure 15-8 Content category added to browser search criteria

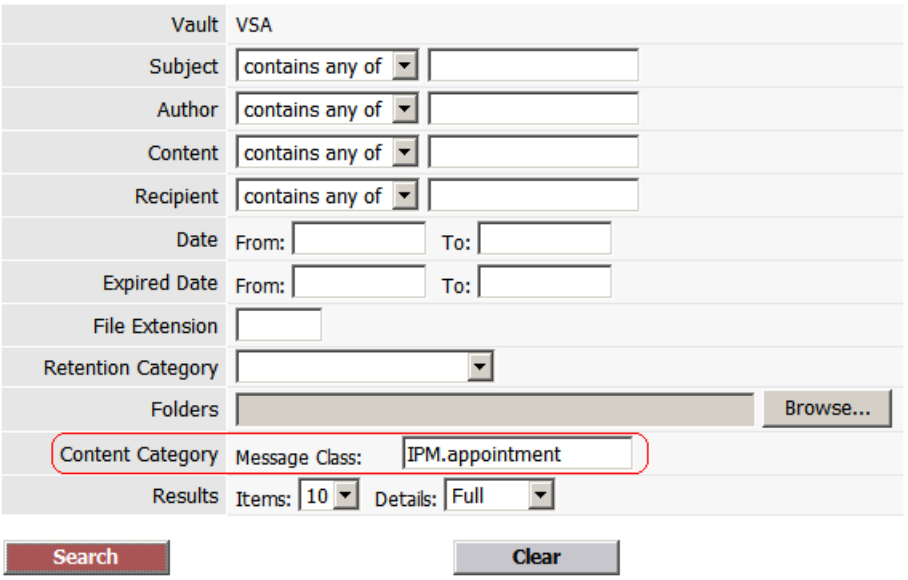


Figure 15-9 Retention category and message class displayed in search results

DTrace log entries for the example custom filter when configuring custom properties

This section gives examples of the lines in the Dtrace log. The lines that are included show the archiving task loading the custom filter, evaluating the appointment item, and applying the rule actions.

In the DTrace log, lines similar to the following show that the example custom filter has loaded successfully.

```
1167927    06:23:38.027    [6860]    (ArchiveTask)    <17472>
EV~I Event ID: 45329 External Filter 'EnterpriseVault.CustomFilter'
initialising... |
1167950    06:23:38.308    [6860]    (ArchiveTask)    <17472>    EV-M
{CustomPropertiesDefinition} Loading Custom Properties from file:
\C:\PROGRAM FILES (X86)\ENTERPRISE VAULT\Custom Filter Rules\
```

```
Custom Properties.xml
1167951    06:23:38.308     [6860]    (ArchiveTask)    <17472>    EV-L
{CustomPropertiesDefinition} Loading Custom Property definitions...
1167952    06:23:38.324     [6860]    (ArchiveTask)    <17472>    EV-L
{CustomPropertiesDefinition} Adding property MSGCLASS [namespace=]
1167953    06:23:38.324     [6860]    (ArchiveTask)    <17472>    EV-L
{CustomPropertiesDefinition} Adding content categories...
1167954    06:23:38.324     [6860]    (ArchiveTask)    <17472>    EV-L
{CustomPropertiesDefinition} Adding category MsgClassTest
1167955    06:23:38.324     [6860]    (ArchiveTask)    <17472>    EV-L
{CustomPropertiesDefinition} Default Category = MsgClassTest
1167956    06:23:38.339     [6860]    (ArchiveTask)    <17472>    EV-L
{CustomPropertiesDefinition} Adding presentation applications...
1167957    06:23:38.339     [6860]    (ArchiveTask)    <17472>    EV-L
{CustomPropertiesDefinition} Adding application search.asp
(Locale='1033')
1167958    06:23:38.339     [6860]    (ArchiveTask)    <17472>    EV:M
[CustomXMLFilter] Setting DEFAULT Content Category to [MsgClassTest]
1167959    06:23:38.339     [6860]    (ArchiveTask)    <17472>    EV:M
Adding External Filter 'EnterpriseVault.CustomFilter' to the list
for processing|
1167960    06:23:38.339     [6860]    (ArchiveTask)    <17472>    EV:M
Successfully added External Filter 'EnterpriseVault.CustomFilter'|
Calling Initialize
1167961    06:23:38.339     [6860]    (ArchiveTask)    <17472>    EV:M
[CustomXMLFilter] Custom Filter initialized on thread.
1167962    06:23:38.339     [6860]    (ArchiveTask)    <17472>    EV:M
CEVFilterController::CreateFilterObject() (Exit) |Success  [0] |
1167963    06:23:38.339     [6860]    (ArchiveTask)    <17472>    EV:M
CEVFilterController::InitializeFiltersFromRegistry - MoveOnFilterFailure
RegKey: [0x00000000]
1167964    06:23:38.339     [6860]    (ArchiveTask)    <17472>    EV:M
CEVFilterController::InitializeFiltersFromRegistry() (Exit) |Success  [0] |
1167965    06:23:38.339     [6860]    (ArchiveTask)    <17472>    EV:M
Successfully enabled external filtering
```

Lines similar to the following show the appointment is evaluated using the example filter rule, and matches:

```
1171158    06:23:49.996     [6860]    (ArchiveTask)    <17472>    EV:H
[CustomXMLFilter] Custom Filter processing message 'test appointment'
1171159    06:23:49.996     [6860]    (ArchiveTask)    <17472>    EV:L
...
1171161    06:23:49.996     [6860]    (ArchiveTask)    <17472>    EV:H
```

```
[CustomRules][CRuleSet] Getting rule data...
...
1171164    06:23:50.058     [6860]    (ArchiveTask)    <17472>    EV:H
[CustomXMLFilter] New RuleDataXML is now '<?xml version="1.0"
encoding="UTF-16"?> <RULE_DATA><DATATYPE NAME="NAMEDPROPERTIES">
<DATA NAME="TAG"><VALUE>MSGCLASS</VALUE> </DATA></DATATYPE>
</RULE_DATA>'
1171165    06:23:50.058     [6860]    (ArchiveTask)    <17472>    EV:L
[CustomXMLFilter] GetMessageNamedProperties - XML RULE Data ='
<?xml version="1.0" encoding="UTF-16"?><RULE_DATA><DATATYPE NAME=
"NAMEDPROPERTIES"><DATA NAME="TAG"><VALUE>MSGCLASS</VALUE></DATA>
</DATATYPE></RULE_DATA>'
...
1171167    06:23:50.058     [6860]    (ArchiveTask)    <17472>    EV:L
[CustomXMLFilter] GetMessageNamedProperties - Getting Tag =
'MSGCLASS' from custom properties
...
1171169    06:23:50.058     [6860]    (ArchiveTask)    <17472>    EV:M
CEVFilterController::get_MessageClass - Returning
'Original Message Class' = IPm.Appointment
1171170    06:23:50.058     [6860]    (ArchiveTask)    <17472>    EV:L
[CustomXMLFilter] Custom tag 'MSGCLASS' and name
'0x001A', set to IPm.Appointment
1171171    06:23:50.058     [6860]    (ArchiveTask)    <17472>    EV:L
[CustomXMLFilter] Adding property 'PR_MESSAGE_CLASS (0x001a)'
to Items XML. [tag='MSGCLASS', value=
'IPm.Appointment']
1171172    06:23:50.058     [6860]    (ArchiveTask)    <17472>    EV:L
[CustomRules][CRule] Evaluating item against MBX DIFF_RET_CAT rule...
1171173    06:23:50.058     [6860]    (ArchiveTask)    <17472>    EV:L
[CustomRules][CNamedPropClause] testing against ANY of 1 NamedProps
1171174    06:23:50.058     [6860]    (ArchiveTask)    <17472>    EV:L
[CustomRules][CNamedPropClause] : ipm.appointment  MATCHED
ipm.appointment
1171175    06:23:50.058     [6860]    (ArchiveTask)    <17472>    EV:L
[CustomRules][CNamedPropClause] match with test ''ipm.appointment''
1171176    06:23:50.058     [6860]    (ArchiveTask)    <17472>    EV:L
[CustomRules][CNamedPropClause] Named prop clause: MSGCLASS  MATCHED
ANY PROP Values
1171177    06:23:50.058     [6860]    (ArchiveTask)    <17472>    EV:L
[CustomRules][CRule] Finished evaluating item against MBX DIFF_RET_CAT
rule; matches
```

Lines similar to the following show the example filter rule actions are applied to the test message:

```
1171179    06:23:50.058     [6860]    (ArchiveTask)    <17472>    EV:M
[CustomXMLFilter] Reading MBX DIFF_RET_CAT rule properties...
...
1171181    06:23:50.074     [6860]    (ArchiveTask)    <17472>    EV:M
[CustomXMLFilter] Setting recognised ACTION to [1]
1171182    06:23:50.074     [6860]    (ArchiveTask)    <17472>    EV:M
[CustomXMLFilter] Setting message content category to [MsgClassTest]
...
1171184    06:23:50.074     [6860]    (ArchiveTask)    <17472>    EV:M
CEVFilterController::get_MessageClass - Returning
'Original Message Class' = IPm.appointment
...
1171187    06:23:50.074     [6860]    (ArchiveTask)    <17472>    EV:L
[CustomXMLFilter] Adding property 'PR_MESSAGE_CLASS (0x001a)'
to index property set 'MsgClassTest' [tag='MSGCLASS',
value='IPm.appointment']
1171188    06:23:50.074     [6860]    (ArchiveTask)    <17472>    EV:M
[CustomXMLFilter] Setting retention category to
[167A06CB31E01744F8500E3D54FC80BEC1b10000evsite]
1171189    06:23:50.074     [6860]    (ArchiveTask)    <17472>    EV:M
Returning IndexedPropertiesSet = <?xml version="1.0"
encoding="UTF-16"?>|<ARCHIVED_ITEM xmlns:o="urn:kvsplc-com:
archived_item" version="1.0"><MSG><PROPSETLIST><PROPSET
NAME="MsgClassTest" SEARCH="y" RESULTS="y"><PROP NAME="MSGCLASS">
<VALUE>IPm.appointment</VALUE></PROP></PROPSET>
</PROPSETLIST></MSG></ARCHIVED_ITEM>|
1171190    06:23:50.074     [6860]    (ArchiveTask)    <17472>    EV:M
Returning Create Shortcut = TRUE
1171191    06:23:50.074     [6860]    (ArchiveTask)    <17472>    EV:M
Returning Delete Original = TRUE
1171192    06:23:50.074     [6860]    (ArchiveTask)    <17472>    EV:M
Returning Vault Id = 1E5850B2EA77101459FCD56CBC4D3A5871110000evsite
1171193    06:23:50.074     [6860]    (ArchiveTask)    <17472>    EV:M
Returning Retention Category = 167A06CB31E01744F8500E3D54FC80BEC
1b10000evsite
1171194    06:23:50.074     [6860]    (ArchiveTask)    <17472>    EV:M
Returning Action = 1
1171195    06:23:50.074     [6860]    (ArchiveTask)    <17472>    EV:L
CEVFilterController::FilteringCompleted() (Entry) |
1171196    06:23:50.074     [6860]    (ArchiveTask)    <17472>    EV:M
```

```
CEVFilterController::FilteringCompleted() (Exit) |Success  [0] |
...
1171200    06:23:50.089     [6860]    (ArchiveTask)    <17472>    EV:M
EF: Item will be archived|Mailbox: /o=EV Training/
ou=First Administrative Group/cn=Recipients/cn=VSA|Folder: Calendar|
Message: test appointment
1171201    06:23:50.089     [6860]    (ArchiveTask)    <17472>    EV:L
CArchivingAgent::ExternalFiltering() (Exit) |Success  [0] |
1171202    06:23:50.089     [6860]    (ArchiveTask)    <17472>    EV:M
CArchivingAgent::ProcessItemInternal - After call to ExternalFiltering.
RetentionCategory[167A06CB31E01744F8500E3D54FC80BEC1b10000evsite]
ArchiveId[1E5850B2EA77101459FCD56CBC4D3A5871110000evsite]
ContainingArchiveId[1DF2DFF131A9AFB4EB0B493648330C02B1110000evsite]
IndexedPropertiesSet[<?xml version="1.0" encoding="UTF-16"?>|
<ARCHIVED_ITEM xmlns:o="urn:kvsplc-com:archived_item" version="1.0">
<MSG><PROPSETLIST><PROPSET NAME="MsgClassTest" SEARCH="y" RESULTS="y">
<PROP NAME="MSGCLASS"><VALUE>IPm.appointment</VALUE>
</PROP></PROPSET></PROPSETLIST></MSG></ARCHIVED_ITEM>|]
MessageModified[FALSE] RetryCount[0] [0x00000000]
```

Index

F

G

I

J

K

L

M

O

P

R

S

T

U

V

W