Symantec Enterprise Vault™

Upgrading to Enterprise Vault 8.0 SP3

Symantec Information Foundation™

symantec™

Symantec Enterprise Vault: Upgrading to Enterprise Vault 8.0 SP3

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

Last updated: October 29, 2009.

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 maintenance 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 Web-based support that provides rapid response and up-to-the-minute information

■ Upgrade assurance that delivers automatic software upgrade protection

■ Global support that is available 24 hours a day, 7 days a week

■ Advanced features, including Account Management Services

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

www.symantec.com/techsupp/

Contacting Technical Support

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

www.symantec.com/techsupp/

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

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

■ Product release level

■ Hardware information

■ Available memory, disk space, and NIC information

■ Operating system

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

Licensing and registration

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

www.symantec.com/techsupp/

Customer service

Customer service information is available at the following URL:

www.symantec.com/techsupp/

Customer Service is available to assist with 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 maintenance 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

Maintenance agreement resources

If you want to contact Symantec regarding an existing maintenance agreement, please contact the maintenance 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

Additional enterprise services

Symantec offers a comprehensive set of services that allow you to maximize your investment in Symantec products and to develop your knowledge, expertise, and global insight, which enable you to manage your business risks proactively.

Enterprise services that are available include the following:

Symantec Early Warning Solutions	These solutions provide early warning of cyber attacks, comprehensive threat analysis, and countermeasures to prevent attacks before they occur.
Managed Security Services	These services remove the burden of managing and monitoring security devices and events, ensuring rapid response to real threats.
Consulting Services	Symantec Consulting Services provide on-site technical expertise from Symantec and its trusted partners. Symantec Consulting Services offer a variety of prepackaged and customizable options that include assessment, design, implementation, monitoring, and management capabilities. Each is focused on establishing and maintaining the integrity and availability of your IT resources.
Educational Services	Educational Services provide a full array of technical training, security education, security certification, and awareness communication programs.

To access more information about Enterprise services, please visit our Web site at the following URL:

www.symantec.com

Select your country or language from the site index.

Contents

About this guide

This chapter includes the following topics:

- Introducing this guide
- Product documentation
- Comment on the documentation

Introducing this guide

This guide describes how to upgrade to Enterprise Vault 8.0 Service Pack 3 (SP3).

If you are performing a new installation of Enterprise Vault, see the Enterprise Vault 8.0 SP3 ReadMeFirst. Then follow the installation instructions in *Installing and Configuring*, which is in the `Documentation` folder on the Enterprise Vault 8.0 SP3 release media.

For the most up-to-date versions of this document and of the ReadMeFirst, see the following page on the Symantec Enterprise Support site:

http://entsupport.symantec.com/docs/308966

Product documentation

Table 1-1 lists the documentation that is available in the `Documentation` folder of the Enterprise Vault media.

Table 1-1   Enterprise Vault documentation set

Document	Comments
Symantec Enterprise Vault Help	Includes all the following documentation so that you can search across all files. You can access this file by doing either of the following: ■ On the Windows **Start** menu, click **Start > Programs > Enterprise Vault > Documentation**. ■ In the Administration Console, click **Help > 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 the documents that are held on 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://entsupport.symantec.com/docs/276547

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.

Before you begin

This chapter includes the following topics:

- Server upgrade paths
- Documentation

Server upgrade paths

This guide describes how to upgrade to Enterprise Vault 8.0 SP3 from Enterprise Vault 8.0 or from any version of Enterprise Vault 2007.

The only possible server upgrade paths to Enterprise Vault 8.0 SP3 are from Enterprise Vault 8.0, 8.0 SP1, 8.0 SP2, or Enterprise Vault 2007.

If your Enterprise Vault servers are running a version of Enterprise Vault that is older than Enterprise Vault 2007, you must first upgrade to Enterprise Vault 2007 and then upgrade to Enterprise Vault 8.0 SP3.

Documentation

Do the following before you upgrade your system:

- Read the Enterprise Vault 8.0 SP3 ReadMeFirst.
- Check that the prerequisites for Enterprise Vault 8.0 SP3 are satisfied, as described in the *Installing and Configuring* manual.
- Have to hand the Enterprise Vault *Installing and Configuring* manual. The manual is in the `Documentation` folder on the Enterprise Vault Enterprise Vault 8.0 SP3 media.

See "Product documentation" on page 13.

For the latest information on supported software and storage devices, see the
Enterprise Vault Compatibility Charts at
http://entsupport.symantec.com/docs/276547.

Points to note when upgrading from Enterprise Vault 2007

This chapter includes the following topics:

About this chapter

The changes that are described in this chapter affect the way that your Enterprise Vault system works after the upgrade from Enterprise Vault 2007.

As a result of some of these changes, you may need to take action to review or modify your configuration after the upgrade.

For a full list of new features and changes, see the Enterprise Vault 8.0 SP3 ReadMeFirst.

Considerations when upgrading Outlook Add-Ins

The order in which you upgrade servers and users' computers affects the functionality that users experience. This section describes how the upgrade order affects users.

Upgrading when users do not have Offline Vault

If you do not use Offline Vault there is no requirement for you to upgrade the Enterprise Vault 2007 Outlook Add-Ins. The existing Outlook Add-Ins are compatible with Enterprise Vault 8.0 SP3. The only limitation is that new client functionality is not available until you upgrade.

If you decide to upgrade the Outlook Add-Ins you can do so before or after you upgrade the Enterprise Vault servers.

Upgrading when users have Offline Vault

If you use Offline Vault then you do need to upgrade the Outlook Add-Ins. You can upgrade Enterprise Vault 2007 Outlook Add-Ins before or after you upgrade Enterprise Vault 2007 servers.

The order in which you perform the upgrades affects the way Enterprise Vault handles the change from Offline Vault to Vault Cache, as follows:

- **When you upgrade servers and then the Outlook Add-Ins:** Vault Cache is automatically enabled. Users do not see any message and they do not need to take any special action.

- **When you upgrade Outlook Add-Ins and then the servers:**
  - Offline Vault automatically enters read-only mode. Users still have access to their existing Offline Vault, but Enterprise Vault no longer updates the contents of the Offline Vault.

- When a user opens Outlook, Enterprise Vault displays a message. The message says that the Enterprise Vault administrator has temporarily disabled updates to the user's Offline Vault, and that the user will be notified when updates are re-enabled. The user can choose not to show the message again.

- If the value of the Offline Vault advanced setting **Show Setup Wizard** is **Off** in the Exchange Desktop policy, the message is not displayed.

- When you upgrade the Enterprise Vault servers, Vault Cache is automatically enabled in the Outlook Add-Ins.

Virtual Vault may be enabled automatically

By default, Enterprise Vault automatically enables Virtual Vault for all users who already have Offline Vault.

It is important that you review the Virtual Vault settings to make sure that they do not conflict with your requirements.

For example, the Virtual Vault default settings enable users to move items into Virtual Vault folders to archive them. If you have hidden the **Store in Vault** option from users you may also want to disable **Users can archive items** in the Virtual Vault **Advanced** policy settings.

See the following:

- The chapter "Setting up Vault Cache and Virtual Vault" in the *Setting up Exchange Server Archiving* manual

- The *Virtual Vault Best Practice Guide*, which is available from http://entsupport.symantec.com/docs/334852.

The upgrade disables sharing

Enterprise Vault 8.0 uses a new optimized single instance storage model.

See "Optimized single instance storage" in the ReadMeFirst.

On upgrade, Enterprise Vault makes the following changes in each Enterprise Vault site:

- It creates a vault store group named the Default Upgrade Group, and places all of the site's vault stores into that group.

- It sets the sharing level of each vault store in the Default Upgrade Group to "No sharing".

Note: If a partition was configured to share archived items before the upgrade, it no longer does so after the upgrade until you change the vault store's sharing level from "No sharing".

Note: Enterprise Vault does not employ optimized single instance storage when items are stored to partitions that are hosted on EMC Centera devices. Enterprise Vault 8.0 continues to provide a separate device-level sharing option to take advantage of the sharing capabilities of Centera.

Before you configure sharing with optimized single instance storage, it is important to consider what sort of sharing regime is suitable for your organization. For example:

- You may need to keep parts of your organization separated with information barriers, or firewalls.

- Network connectivity between the required computers must be sufficient to provide acceptable storage and retrieval times.

There are limits to what you can change after you have configured sharing. Changes to vault store sharing levels do not act retrospectively. Also, you can only move a vault store into a different vault store group if both of the following apply:

- The vault store is one that Enterprise Vault upgraded, or one that you created in the Default Upgrade Group.

- The vault store's sharing level is "No sharing" and has never been changed.

For information on how to set up a suitable sharing regime, see the "Setting up storage" chapter in *Installing and Configuring*.

Changes to backup procedures

Enterprise Vault 2007 used registry values to control backup mode.

Enterprise Vault Vault 8.0 introduces a new backup mode for vault stores and index locations. This feature enables you to back up vault stores and index locations without the need to restart Enterprise Vault services or set registry values.

The Storage service checks for the old registry values when it starts. There is a warning event if the Storage service finds any of the registry values.

The Enterprise Vault 2007 registry values are still supported in Enterprise Vault 8.0. You can ignore the warning if you want to continue to use the old registry values.

See the 'Backing up Enterprise Vault' chapter in the *Administrator's Guide*.

Changes to journal archiving may affect backups

In Enterprise Vault 2007 you did not need to back up the journal vault store partitions and vault store database. In Enterprise Vault 8.0 you must do one of the following:

■ Back up the journal archive partitions and database.

■ Use a trigger file to instruct Enterprise Vault that the data has been secured.

Enterprise Vault 2007 did not create Watchfile database records for journal mailbox items when the vault store setting for removal of safety copies was one of the following:

■ Immediately after archive

■ After backup (immediate for Journaling)

Enterprise Vault 8.0 always creates Watchfile database records for items from journal mailboxes, regardless of the safety copies setting.

If you allow the journal archiving to continue without performing backups, the increasing number of Watchfile records eventually causes performance problems.

See the 'Managing safety copies' section in the 'Day-to day administration' section of the *Administrator's Guide*

See the 'Backing up Enterprise Vault' chapter in the *Administrator's Guide*

Upgrade changes to site monitoring settings

Enterprise Vault's single instance storage feature requires that all vault store partitions are backed up. To support this, certain site monitoring settings are enforced during the upgrade to Enterprise Vault 8.0.

The affected settings are on the **Monitoring** tab of the **Site Properties** dialog box.

If the **Enable monitoring for this site** option is not selected, the upgrade selects it, and also selects the **Watchfile** and **Journal Archive** alerts. Both these alerts are then set to their default values.

If the **Enable monitoring for this site** option is already selected, the upgrade also selects the **Watchfile** and **Journal Archive** alerts, but does not change their current values.

These changes are enforced on every site.

Delete archived file on placeholder recall is no longer supported

Enterprise Vault 8.0 File System Archiving does not include the option **Delete archived file when placeholder is recalled**.

After the upgrade, the recall of a placeholder that Enterprise Vault created with this option does not result in the deletion of the archived file.

Note: If you fail to upgrade the FSA Agent on an NTFS file server, the file placeholder service continues to delete the archived file when it recalls a placeholder that was created with this option.

Currently the FSA Agents from Enterprise Vault 2007 SP4 and SP5 are supported.

For the latest information on supported versions, see the *Compatibility Charts* book at the following address:

http://entsupport.symantec.com/docs/276547

Network shares for NTFS partitions with local paths

When the Storage service starts on completion of the upgrade, it creates network shares for any partitions of type "NTFS Volume" if they are specified with a local path, such as a path that begins `C:\..` or `H:\....` The Storage services on remote Enterprise Vault servers use the partition network share when they require access to data on the partition.

See "Partition network shares for NTFS partitions with local paths" in the *Installing and Configuring* manual.

If the Storage service is unable to create a partition network share, the Storage service does not start. Enterprise Vault logs event 7064 in the event log with the following description:

```
The verification of a Partition Network Share failed.
```

The most likely cause is that Enterprise Vault cannot access the root path of the partition. This may be due to any of the following:

- A drive is offline.
- A disk is corrupt.
- The computer's name has changed.
- In a cluster environment, a shared drive was not configured properly.

If the Storage service fails to start after the upgrade, check the event log for this error event. If you see the error event, use Windows Explorer to check whether you can access the local paths to the local NTFS partitions.

New desktop policies and changes to mailbox policies

Enterprise Vault 8.0 introduces desktop policies to manage the behavior and availability of features in the Exchange and Domino Enterprise Vault clients. Many settings that were previously Advanced mailbox policy settings are now located on various tabs on the desktop policy.

The upgrade process creates a new desktop policy for each existing mailbox policy, and moves the mailbox settings that affect the user's desktop experience into the desktop policy.

For Exchange, the following settings on the mailbox policy's **Advanced** tab are moved to the desktop policy:

■ The **Offline Vault** settings are moved to the desktop policy's **Vault Cache** tab or **Advanced** tab.

■ The **Outlook** and **OWA** settings are moved to the desktop policy's **Options** tab or **Advanced** tab. Note that the **Options** tab consolidates many of the settings that are common to **Outlook** and **OWA**, to simplify the configuration of these settings for both Exchange clients.

For Domino, the following settings on the mailbox policy's **Advanced** tab are moved to the desktop policy:

■ The **Desktop** settings are moved to the desktop policy's **Options** tab.

■ The **Vault Cache** settings are moved to the desktop policy's **Vault Cache** tab or **Advanced** tab.

Reviewing Exchange mailbox policy settings after upgrade

The following Exchange mailbox policy **Advanced** settings have changed in Enterprise Vault 8.0. The upgrade may automatically change existing values you have for these settings.

We recommend that you review these settings in your upgraded mailbox policies.

Archive Exchange Managed Folders	This setting now has the following possible values:

- **Off**: Enterprise Vault does not archive items from managed folders.
- **Normal**: Enterprise Vault treats managed folders as normal mailbox folders.
- **Managed**: Default value. Enterprise Vault archives items from managed folders and uses retention settings that are synchronized from Exchange Server.

The value of this setting is treated as follows when you upgrade:

- If the value was **Off**, it remains **Off**.
- If the value was **On**, it is converted to **Normal**. (Enterprise Vault treats managed folders as normal mailbox folders.)

For information about assigning permission for managed folder synchronization in Exchange Server 2007, see *Installing and Configuring*. For information about archiving from managed folders, see the *Administrator's Guide*.

Strip calendar attachments	This setting is renamed to **Strip attachments to non-shortcut items** when you upgrade.

The setting controls whether attachments are removed from calendar items, meeting requests, and contacts after archiving. If Enterprise Vault removes an attachment, it now replaces it with a link to the attachment. The default has changed from **Off** to **On**.

The value of the setting is not changed when you upgrade.

If you have upgraded policies in which this setting is **Off**, we recommend that you change the setting to **On** to save mailbox space. This recommendation applies particularly if you use archiving based on quota, or on age and quota.

Note: Turning on **Strip attachments to non-shortcut items** does not make Enterprise Vault remove attachments from non-shortcut items that are already archived.

Reviewing Exchange desktop policy settings after upgrade

Enterprise Vault changes the following Exchange mailbox policy Offline Vault **Advanced** settings when it transfers them to the Exchange desktop policy on upgrade. We recommend that you review the settings in your desktop policies after upgrade.

| Show options | This setting is transferred to the following two settings on the desktop policy **Vault Cache** tab in the Administration Console: |

- **Vault Cache properties**. This setting controls whether the **Tools** > **Enterprise Vault** > **Vault Cache** properties menu option is available in Outlook.
- **Vault Cache options**. This setting controls whether the **Options** tab is available in the **Vault Cache** Properties dialog box.

If **Show options** was set to show the **Tools** > **Enterprise Vault** > **Offline Vault Options** menu option, then the **Vault Cache properties** and **Vault Cache options** settings are selected. Otherwise, these two settings are not selected.

| Synchronize archive types | If this setting was set to **All public folder archives**, Enterprise Vault makes the following changes on upgrade: |

The desktop policy Vault Cache Advanced setting **Synchronize archive types** is set to **Default mailbox**. This setting means that the Vault Cache synchronizes only the primary mailbox.

On the desktop policy's **Vault Cache** tab, the setting **Make Vault Cache available for users** is not selected.

Note that the default values have changed for some of the other settings that are moved to the desktop policy. You may want to note these changes if you create new desktop policies. These changes do not affect the migrated values in your upgraded policies.

Table 3-1   Changed Exchange desktop policy settings

Enterprise Vault 2007 Exchange mailbox policy "Advanced" tab setting	Enterprise Vault 2007 default value	Location in Enterprise Vault 8.0 Exchange desktop policy	Enterprise Vault 8.0 default value
Offline Vault settings			
Offline archives enabled state	Users enable	**Make Vault Cache available for users** on the **Vault Cache** tab	**None**. (Turns off Vault Cache, but does not affect Vault Caches that are already enabled.)
Outlook settings			

Table 3-1   Changed Exchange desktop policy settings *(continued)*

Enterprise Vault 2007 Exchange mailbox policy "Advanced" tab setting	Enterprise Vault 2007 default value	Location in Enterprise Vault 8.0 Exchange desktop policy	Enterprise Vault 8.0 default value
Allow script in public folders	Keep user's setting	**Advanced** tab	Force On
Allow script in shared folders	Keep user's setting	**Advanced** tab	Force On
Deploy forms locally	When no org forms	**Advanced** tab	Always
Fix Outlook preview pane	Do not apply	**Advanced** tab	Apply automatically
Outlook Add-In behavior	Normal	**Advanced** tab	HTTP-only Outlook Add-In

For more information about the **Advanced** tab settings, see the *Administrator's Guide.*

Reviewing Domino mailbox policy settings after upgrade

The Domino mailbox policy Advanced setting **Strip calendar attachments** has changed in Enterprise Vault 8.0. We recommend that you review this setting in your upgraded mailbox policies.

This setting is renamed **Strip attachments to non-shortcut items** on upgrade.

The setting controls whether attachments are removed from appointments and tasks after archiving. When Enterprise Vault removes an attachment, it now replaces the attachment with a link to the attachment. The default has changed from **Off** to **On**.

The value of the setting is not changed when you upgrade.

If you have upgraded policies in which this setting is **Off**, we recommend that you change the setting to **On** to save mailbox space.

Note: Turning on **Strip attachments to non-shortcut items** does not make Enterprise Vault remove attachments from non-shortcut items that are already archived.

New copy policy option

Note that there is a new Copy Policy option that enables you to copy an existing policy. This option is useful if you want to create a new policy based on an existing one. To copy an existing policy, right-click the policy and select **Copy Policy** from the shortcut menu.

FSA Reporting data collection changes

The default values of some FSA Reporting data collection parameters have changed in recent service packs. These changes affect some reports after upgrade.

Data collection is turned off for duplicate files reports

When you upgrade, Enterprise Vault turns off the collection of data for FSA Reporting's duplicate files reports. Data collection for these reports incurs a performance overhead that is best avoided unless you want to use these reports.

The **CheckDuplicates** parameter determines whether FSA Reporting collects data for the duplicate files reports. Table 3-2 describes the changes to this parameter.

Table 3-2   Change to the CheckDuplicates parameter from Enterprise Vault 8.0 SP2

Parameter	Description	Supplied value before Enterprise Vault 8.0 SP2	Supplied value from Enterprise Vault 8.0 SP2
CheckDuplicates	Determines whether FSA Reporting collects data for the duplicate files reports: ■ Duplicate Files on a Server ■ Duplicate Files Summary ■ Top Duplicate Files per Volume	**True** (Collect data)	**False** (Do not collect data)

If you run these reports after the upgrade, the reports by default contain only the data that FSA Reporting collected before the upgrade.

If you want FSA Reporting to gather data for these reports after the upgrade, change the value of the **CheckDuplicates** parameter in the **Properties** table of the **EnterpriseVaultFSAReporting** database.

See "Changing parameter values for the File Collector service" in the *Reporting* guide.

Changed parameter values for the inactive files reports and the largest files report

At Enterprise Vault 8.0 SP3 the default values of the data collection parameters for some reports have changed, to improve the data scan performance. Table 3-3 describes the changes.

Table 3-3   Changes to the FSA Reporting data collection parameters at Enterprise Vault 8.0 SP3

Parameter	Description	Supplied value before Enterprise Vault 8.0 SP3 (units)	Supplied value from Enterprise Vault 8.0 SP3 (units)
DAYSOLD	Sets the data collection periods for the three "Inactive Files" reports	**30,60,90,180,365,730,1095** (days)	**90,180,365,730** (days)
MBLARGE	Sets the minimum file size for the "Largest files per Volume" report.	**10** (MB)	**1024** (MB)
TopFiles	Sets the number of files to list in the "Largest Files per Volume" report.	**100** (files)	**10** (files)

On upgrade:

■ If you had changed the value before the upgrade, Enterprise Vault retains your value.

■ Otherwise, Enterprise Vault applies the new supplied value.

You can change the values of these parameters in the **Properties** table of the **EnterpriseVaultFSAReporting** database.

See "Changing parameter values for the File Collector service" in the *Reporting* guide.

Changes to FSA Reporting's duplicate files reports

Note that the following FSA Reporting reports are changed when you upgrade:

- The "Duplicate Files Summary" report now displays data based on the server name instead of the user name.

- The "Duplicate Files on a Server" report now displays data based on the volume name instead of the user name.
  Click a volume name in the report to view the new report "Top Duplicate Files per Volume", which displays the top 100 largest duplicate files in the volume.

For details of all the FSA reports, see the section "The data analysis reports" in the *Reporting* manual.

Distributed FSA Reporting proxy server allocation

Read this section if you run FSA Reporting on multiple NetApp or EMC Celerra file servers, in a site with multiple Enterprise Vault servers.

Enterprise Vault now distributes the job of FSA Reporting proxy server for non-NTFS file servers among the Enterprise Vault servers in a site:

- Previously, Enterprise Vault assigned the job of proxy server to the Enterprise Vault server that was listed first in the FSA Reporting database's **FileServerConfiguration** table. So a single Enterprise Vault server often acted as proxy server for all of the non-NTFS file servers in a site.

- Now Enterprise Vault does as follows when you enable a non-NTFS file server for FSA Reporting:

  - It determines which of the available Enterprise Vault servers currently performs the job of proxy server for the fewest file servers.

  - It then assigns the job of proxy server to that Enterprise Vault server.

This distributed allocation allows for more efficient FSA Reporting scans and scan data uploads.

To use the new distributed allocation mechanism after you upgrade, disable and then re-enable FSA Reporting on each of the non-NTFS file servers.

For more information about the new proxy server allocation mechanism, see the *Reporting* guide.

Points to note when upgrading from Enterprise Vault 8.0

This chapter includes the following topics:

■ FSA Reporting data collection changes

■ FSA Reporting proxy server allocation

■ Upgrading Enterprise Vault 8.0 Outlook Add-Ins

FSA Reporting data collection changes

The default values of some FSA Reporting data collection parameters have changed in recent service packs. These changes affect some reports after upgrade.

Data collection is turned off for duplicate files reports

Note: This section applies if you upgrade from any version of Enterprise Vault before Enterprise Vault 8.0 SP2.

When you upgrade, Enterprise Vault turns off the collection of data for FSA Reporting's duplicate files reports. Data collection for these reports incurs a performance overhead that is best avoided unless you want to use these reports.

The **CheckDuplicates** parameter determines whether FSA Reporting collects data for the duplicate files reports. Table 4-1 describes the changes to this parameter.

Table 4-1   Change to the CheckDuplicates parameter from Enterprise Vault 8.0 SP2

Parameter	Description	Supplied value before Enterprise Vault 8.0 SP2	Supplied value from Enterprise Vault 8.0 SP2
CheckDuplicates	Determines whether FSA Reporting collects data for the duplicate files reports: ■ Duplicate Files on a Server ■ Duplicate Files Summary ■ Top Duplicate Files per Volume	**True** (Collect data)	**False** (Do not collect data)

If you run these reports after the upgrade, the reports by default contain only the data that FSA Reporting collected before the upgrade.

If you want FSA Reporting to gather data for these reports after the upgrade, change the value of the **CheckDuplicates** parameter in the **Properties** table of the **EnterpriseVaultFSAReporting** database.

See "Changing parameter values for the File Collector service" in the *Reporting* guide.

Changed parameter values for the inactive files reports and the largest files report

At Enterprise Vault 8.0 SP3 the default values of the data collection parameters for some reports have changed, to improve data scan performance. Table 4-2 describes the changes.

Table 4-2   Changes to the FSA Reporting data collection parameters at
                     Enterprise Vault 8.0 SP3

Parameter	Description	Supplied value before Enterprise Vault 8.0 SP3 (units)	Supplied value from Enterprise Vault 8.0 SP3 (units)
DAYSOLD	Sets the data collection periods for the three "Inactive Files" reports	**30,60,90,180,365,730,1095** (days)	**90,180,365,730** (days)
MBLARGE	Sets the minimum file size for the "Largest files per Volume" report.	**10** (MB)	**1024** (MB)
TopFiles	Sets the number of files to list in the "Largest Files per Volume" report.	**100** (files)	**10** (files)

On upgrade:

■ If you had changed the value before the upgrade, Enterprise Vault retains your value.

■ Otherwise, Enterprise Vault applies the new supplied value.

You can change the values of these parameters in the **Properties** table of the **EnterpriseVaultFSAReporting** database.

See "Changing parameter values for the File Collector service" in the *Reporting* guide.

FSA Reporting proxy server allocation

Read this section if you run FSA Reporting on multiple NetApp or EMC Celerra file servers, in a site with multiple Enterprise Vault servers.

Enterprise Vault now distributes the job of FSA Reporting proxy server for non-NTFS file servers among the Enterprise Vault servers in a site:

■ Previously, Enterprise Vault assigned the job of proxy server to the Enterprise Vault server that was listed first in the FSA Reporting database's

FileServerConfiguration table. So a single Enterprise Vault server often acted as proxy server for all of the non-NTFS file servers in a site.

- Now Enterprise Vault does as follows when you enable a non-NTFS file server for FSA Reporting:

  - It determines which of the available Enterprise Vault servers currently performs the job of proxy server for the fewest file servers.

  - It then assigns the job of proxy server to that Enterprise Vault server.

This distributed allocation allows for more efficient FSA Reporting scans and scan data uploads.

To use the new distributed allocation mechanism after you upgrade, disable and then re-enable FSA Reporting on each of the non-NTFS file servers.

For more information about the new proxy server allocation mechanism, see the *Reporting* guide.

Upgrading Enterprise Vault 8.0 Outlook Add-Ins

You do not need to upgrade earlier versions of the Enterprise Vault 8.0 Outlook Add-Ins. The earlier Outlook Add-Ins are compatible with Enterprise Vault 8.0 SP3. The only limitation is that new client functionality is not available until you upgrade.

When you upgrade from Enterprise Vault 8.0 or later, you can upgrade the Enterprise Vault Outlook Add-Ins before or after you upgrade the Enterprise Vault servers.

Virtual Vault may be enabled automatically

By default, Enterprise Vault automatically enables Virtual Vault for all users who already have Vault Cache.

It is important that you review the Virtual Vault settings to make sure that they do not conflict with your requirements.

For example, the Virtual Vault default settings enable users to move items into Virtual Vault folders to archive them. If you have hidden the **Store in Vault** option from users you may also want to disable **Users can archive items** in the Virtual Vault **Advanced** policy settings.

See the following:

- The chapter "Setting up Vault Cache and Virtual Vault" in the *Setting up Exchange Server Archiving* manual

■ The *Virtual Vault Best Practice Guide*, which is available from
http://entsupport.symantec.com/docs/334852.

Steps to upgrade your system

This chapter includes the following topics:

■ Upgrading to Enterprise Vault 8.0 SP3

■ Overview of the upgrading process

Upgrading to Enterprise Vault 8.0 SP3

To upgrade to Enterprise Vault 8.0 SP3

1 If your existing Enterprise Vault system supports Domino journaling or mailbox archiving, you need to perform a number of steps before installing Enterprise Vault.

See "Preparing to upgrade Domino archiving" on page 93.

2 If you are upgrading from the original release of Enterprise Vault 2007 (with no service packs applied), then before upgrading any Enterprise Vault server on which FSA Reporting is already configured, ensure that the FSA Reporting .com hotfix is applied.

See http://entsupport.symantec.com/docs/290725 for instructions on applying the hotfix.

3 Enterprise Vault 8.0 SP3 requires additional prerequisite software for FSA Reporting. If FSA Reporting is configured on any Enterprise Vault server, install the following software on the SQL Server computer that hosts the FSA Reporting database:

■ Microsoft SQLXML 4.0

■ Microsoft MSXML 6.0

32-bit and 64-bit versions of the `.msi` installation files for SQLXML 4.0 and MSXML 6.0 are included in the `Server/Support Files` folder of the Enterprise Vault media.

4 Upgrade all Enterprise Vault servers (that is, all servers that are running the Enterprise Vault Directory service), and all computers on which the Enterprise Vault Reporting component is installed.

See "Overview of the upgrading process" on page 41.

5 Perform any of the extra configuration tasks that are relevant to your Enterprise Vault installation.

See "About the extra configuration tasks" on page 83.

6 Upgrade any computers that are running just the Enterprise Vault Administration Console.

Then perform the following additional steps, as required:

■ If Exchange Server archiving is implemented, optionally upgrade the Exchange Server forms on the Exchange Server.
See "About upgrading Exchange Server forms" on page 91.

■ If File System Archiving is implemented, upgrade the FSA Agent on all the NTFS file servers on which it is installed.
See "About upgrading the FSA Agent on NTFS file servers" on page 99.

■ If OWA or RPC over HTTP (Outlook Anywhere) users have Enterprise Vault access, upgrade all OWA and RPC servers.
See "About upgrading OWA and RPC Extensions" on page 103.

■ Upgrade all SharePoint servers that are being archived.
See "Upgrading the Enterprise Vault SharePoint components" on page 110.

■ To enable Exchange Server mailbox users to have the full functionality of Enterprise Vault 8.0, upgrade the Enterprise Vault Outlook Add-Ins on users' desktop computers.
See the *Setting up Exchange Server Archiving* manual.

Note: On upgraded systems, Outlook is still required on all Enterprise Vault servers that host the Enterprise Vault Storage service, even if Exchange Server archiving is not being performed. Outlook is required in order to access items that were archived using earlier versions of Enterprise Vault.

Overview of the upgrading process

This chapter describes how to upgrade your Enterprise Vault servers (that is, all servers that run the Enterprise Vault Directory service). If you are upgrading an Enterprise Vault 2007 system that supports Domino mailbox archiving, this includes any Enterprise Vault Domino Gateway servers.

This chapter also describes how to upgrade computers on which Enterprise Vault Reporting is installed.

Note: The actions that the Enterprise Vault installation program and Configuration wizard perform depend on whether you are upgrading from an Enterprise Vault 2007 environment or from an Enterprise Vault 8.0 environment. For simplicity, the upgrade instructions do not distinguish between these two environments unless necessary.

In summary, the upgrade procedure is as follows:

1 Prepare:

- Back up the system.
  See "Backing up the system" on page 43.

- Run the Deployment Scanner.
  See "Running the Deployment Scanner" on page 44.

- Set the database permissions.
  See "Setting database permissions" on page 45.

- Allow the MSMQ queues to empty.
  See "Allow the MSMQ queues to empty" on page 45.

- Check the archiving and expiry schedules.
  See "Checking the archiving and expiry schedules" on page 45.

2 Install and configure the Enterprise Vault 8.0 SP3 server software as described in the appropriate chapter for your installation.

See "Installing on a single server" on page 47.

See "Installing on multiple servers" on page 55.

See "Veritas cluster: installing the Enterprise Vault 8.0 SP3 software" on page 65.

See "Microsoft cluster: installing the Enterprise Vault 8.0 SP3 software" on page 73.

3 Perform post-installation tasks as necessary:

- Upgrade Domino mailbox archiving, if applicable.
  See "Domino clients required for installation" on page 93.

- Perform the post-configuration tasks.

Enterprise Vault server preparation

This chapter includes the following topics:

- Backing up the system

- Running the Deployment Scanner

- Setting database permissions

- Allow the MSMQ queues to empty

- Checking the archiving and expiry schedules

Backing up the system

You need to back up your databases and any changed language files.

Backing up Enterprise Vault data

Before upgrading your Enterprise Vault environment, back up all Enterprise Vault data in accordance with your normal backup procedures.

You need to back up all the following:

- Enterprise Vault system databases

- Vault store partitions and vault store databases

- Index locations

Once you have backed up your vault store partitions, the Storage service marks the relevant files as backed up, and this removes the entries from the WatchFile table. The storage service performs these tasks at preconfigured intervals. You

should wait for the WatchFile table to reduce in size before you proceed with the upgrade. If you do not wait, the Storage service can take some time to restart after the upgrade is complete. You can use the usage report at http://*evserver*/enterprisevault/usage.asp to check the number of files in the **Awaiting Backup** column.

Backing up changed language files

The installation procedure will overwrite the files in the following Enterprise Vault server language folders:

```
Enterprise Vault\Languages\Mailbox Messages\language
```

where `language` indicates the language used.

The installation does not modify the live versions of these files that you have in the Enterprise Vault folder (normally `C:\Program Files\Enterprise Vault`).

If you have made changes that you want to keep to the files in the language folders, copy the files to another location.

Running the Deployment Scanner

Before you upgrade to Enterprise Vault 8.0 SP3, we strongly recommend that you run the Deployment Scanner to check prerequisite software and settings.

The Deployment Scanner is included in the `Deployment Scanner` folder on the Enterprise Vault 8.0 SP3 media.

Use the Vault Service account when running the Deployment Scanner.

To install Deployment Scanner, Windows Installer 3.1 must be installed on the Enterprise Vault server computers. You can download Windows Installer 3.1 from the Microsoft Download Center. You must have local Administrator permissions in order to install Deployment Scanner.

Note: If you choose to check SQL Server, the report may show a warning that "SQL databases contain entities with mixed collations". See the following TechNotes for details of how to fix the problem:

http://entsupport.symantec.com/docs/304556

http://entsupport.symantec.com/docs/293475

Setting database permissions

For the time you install and configure Enterprise Vault, the Vault Service account must be the database owner of all Enterprise Vault databases.

If you changed the database owner after Enterprise Vault was installed, you must make the Vault Service account the owner before you upgrade.

This permission is required to enable database schema and other updates to be enacted with appropriate privileges.

If it is not acceptable to make the Vault Service account the database owner of all Enterprise Vault databases, there is a set of minimum permissions you can apply.

See the following TechNote on the Symantec Support Web site:

http://entsupport.symantec.com/docs/316189

Allow the MSMQ queues to empty

Before you upgrade to Enterprise Vault 8.0 SP3, we recommend that you allow the MSMQ queues to empty.

Note: If you upgrade from Enterprise Vault 2007 with items still on the queues, the Enterprise Vault services may log red events the first time they start after the upgrade.

Checking the archiving and expiry schedules

In order to give you time to examine the new installation before archiving starts, you may want to disable archiving and expiry before you upgrade the servers. You can then enable them again when you have checked installation.

In the case of Exchange Server archiving, note that the first run of the archiving service will update archived items to match changes to shortcuts and retention categories. This may take a significant time, so you may prefer to plan for the first archiving run to take longer than normal.

See "Moved shortcuts and changed retention categories" in the ReadMeFirst file.

Single server: installing the Enterprise Vault server software

This chapter includes the following topics:

- Installing on a single server
- Starting the Directory service
- Upgrading from Enterprise Vault 2007: Running the Configuration wizard
- Starting the Storage service
- Upgrading from Enterprise Vault 2007: Upgrading the auditing database
- Upgrading from Enterprise Vault 2007: Running the Operations Manager Configuration utility
- Running the Enterprise Vault Reporting Configuration utility

Installing on a single server

This section describes how to install the Enterprise Vault server software when you have only one server that runs Enterprise Vault tasks.

To install the Enterprise Vault 8.0 SP3 server software

1 Log on as the Vault Service account.

2 Stop the Enterprise Vault Admin service. This stops the Admin service itself, and any other Enterprise Vault services.

3   Stop any other services or applications that can lock Enterprise Vault files. For example:

■   Enterprise Vault Administration Console

■   Enterprise Vault Accelerator Manager service

■   Enterprise Vault Placeholder service

■   Enterprise Vault File Blocking service

■   Enterprise Vault File Collector service

■   Windows Event Viewer

4   Close Computer Management.

5   If you are installing on an Enterprise Vault Domino Gateway, make sure that the Domino server on the Enterprise Vault Domino Gateway is shut down and that `EVInstall.nsf` is not being accessed locally.

6   Load the Enterprise Vault 8.0 SP3 media.

7   Using Windows Explorer, open the folder `\Enterprise Vault 8.0 SP3\Server`.

8   Double-click the file `setup.exe` to start the installation.

9   Work through the installation.

10 Install the Enterprise Vault Reporting component on computers on which Enterprise Vault Reporting is installed.

11 On computers on which the Enterprise Vault Reporting component is installed, modify the `ReportDeploymentDefinition.XML` file.

See "To modify the ReportDeploymentDefinition.XML file" on page 48.

To modify the ReportDeploymentDefinition.XML file

1   Find the `ReportDeploymentDefinition.XML` file on the computer on which the Enterprise Vault Reporting component is installed. The file is in the `evreports` folder under the Enterprise Vault installation folder, typically `C:\Program Files\Enterprise Vault\evreports`.

2   Make a backup copy of the `ReportDeploymentDefinition.XML`file.

3   Use Windows Notepad to open the original file.

4 Find the Report element that has the filename parameter **Audit Details.rdl**.

The Report element looks like the following:

```
<Report evItemCategory="GenericReports" englishName="Archived
Items Access" resourceId="Audit_Details_Title" filename=
"Audit Details.rdl" rdsName="EnterpriseVaultDS" hidden=
"false" evUniqueId="D7F307E4-E306-4f17-98FB-58702B6D635D"
evVersion="8.0.2.0" />
```

Change the value of the **evVersion** parameter at the end of the element from **8.0.2.0** to **8.0.3.0**, so that the element looks like the following:

```
<Report evItemCategory="GenericReports" englishName="Archived
Items Access" resourceId="Audit_Details_Title" filename=
"Audit Details.rdl" rdsName="EnterpriseVaultDS" hidden=
"false" evUniqueId="D7F307E4-E306-4f17-98FB-58702B6D635D"
evVersion="8.0.3.0" />
```

5 Find the Report element that has the filename parameter **Audit Trending.rdl**.

Change the value of the **evVersion** parameter in this Report element from **8.0.2.0** to **8.0.3.0**

6 Find the Report element that has the filename parameter **Duplicate Files Summary Report.rdl**. Note that there are two spaces between the words **Summary** and **Report**.

Change the value of the **evVersion** parameter in this Report element from **8.0.2.0** to **8.0.3.0**

7 Find the Report element that has the filename parameter **Server Duplicate Files.rdl**.

Change the value of the **evVersion** parameter in this Report element from **8.0.2.0** to **8.0.3.0**

Note: Do not change the values of any other **evVersion** parameters in the file.

8 Save the `ReportDeploymentDefinition.XML` file.

The Enterprise Vault software installation is now complete, but you must obtain license keys for any additional services that you intend to run.

Starting the Directory service

After the upgrade installation you must start the Enterprise Vault Directory service.

To start the Directory service

1 Use Windows Services to start the Enterprise Vault Directory service. When the Directory service starts, it automatically upgrades the Directory database schema and synchronizes new Exchange archiving policy advanced settings into existing policies.

2 Wait for event 8576 to be logged in the Enterprise Vault event log:

```
The Directory service has completed the automatic upgrade of the
EnterpriseVaultDirectory Database
```

Upgrading from Enterprise Vault 2007: Running the Configuration wizard

If you are upgrading from Enterprise Vault 2007 you must run the Configuration wizard, as described in this section. If you are upgrading from any version of Enterprise Vault 8.0 you do not need to run the Configuration wizard.

Before you run the Configuration wizard, you must already have completed the following:

■ Installed the Enterprise Vault 8.0 SP3 server software.

■ Started the Directory service and allowed it to complete the automatic schema upgrade.

To run the Configuration wizard

1 Start the Admin service. Also start the Admin service on all servers in other Enterprise Vault Sites that share the same Directory database.

Note: Do not continue until all the Admin services have started.

---

2 Log on as the Vault Service account.

3 Ensure that the Directory service is running.

4 Click **Start** > **Programs** > **Enterprise Vault** > **Enterprise Vault Configuration** to start the Configuration wizard.

5 The only available option on the first screen of the Configuration wizard is **Upgrade this configuration**. Click **Next**.

6 On the next screen, click **Next** to start the upgrade. There is a prompt for the Vault Service account password.

7   Enter the Vault Service account password and click **OK**. The Configuration
    wizard shows a progress bar while it configures the system. Depending on
    the existing configuration, the wizard may omit some configuration steps.
    The wizard does the following, as necessary:

- Creates a log file for the upgrade in the Enterprise Vault `Reports` folder.
  The log file name is `UpgradeEVServerToV8.0` *date*`.log`, where *date* is
  the date and time when the file was created.

- Creates a Task Controller service on any Enterprise Vault server that does
  not already have a Task Controller service.

- Re-encrypts the password values in the Directory database entries, if
  necessary, using the new Directory encryption services.

- Updates the Roles-based Administration database with new roles, tasks
  and operations, and creates a log file in the Enterprise Vault `Reports`
  folder. The log file name is `_EvAzUtil` *date*`.log`, where *date* is the date
  and time when the file was created.

- If necessary, creates the Enterprise Vault Operations Manager database.

- Checks the Vault Service account permissions on all servers.

- Updates the Enterprise Vault DCOM settings on all servers in the
  Enterprise Vault environment.

8   Click **Finish** to close the Configuration wizard.

9   Stop all Enterprise Vault services.

10 Start the Enterprise Vault Admin service and the Directory service.

11 If you stopped the IIS Admin service before the installation, start any services
    that were stopped by this service.

Manually configuring the Monitoring database

If the Configuration wizard warned you that there was an error configuring the
Monitoring database, you must configure the database manually.

See the following TechNote on the Symantec Support Web site:

http://entsupport.symantec.com/docs/287449

Starting the Storage service

The first time an Enterprise Vault 8.0 SP3 Storage service starts, it upgrades the
storage databases.

You must start the Storage service and wait for the Storage service to complete the upgrade. The Storage service logs appropriate entries in the event log.

To start the Storage services, do the following

1   Use Windows Services to start the Enterprise Vault Storage service. When the Storage service starts, it automatically upgrades the fingerprint databases. Event 6959 will be logged for each vault store database that is upgraded.

2   Wait for event 6221 to be logged in the Enterprise Vault event log:

    Storage Service started.

Upgrading from Enterprise Vault 2007: Upgrading the auditing database

If you upgrade an Enterprise Vault 2007 system in which you enabled auditing, you must upgrade the Enterprise Vault auditing database schema.

To upgrade the auditing database schema

1   Make sure that you have backed up the **EnterpriseVaultAudit** database.

2   For Microsoft SQL Server 2000, start SQL Query Analyzer. For Microsoft SQL Server 2005 or 2008, start SQL Server Management Studio.

3   In the left pane of SQL Query Analyzer or SQL Server Management Studio, select the **EnterpriseVaultAudit** database.

4   From the **File** menu, click **Open > File**.

5   Navigate to the Enterprise Vault installation folder (typically C:\Program Files\Enterprise Vault) and select the file **Audit_Schema_Upgrade.sql**.

6   From the **Query** menu, click **Execute**.

    After a short time SQL Query Analyzer or SQL Server Management Studio indicates that the script has completed successfully.

7   Exit from SQL Query Analyzer or SQL Server Management Studio.

Upgrading from Enterprise Vault 2007: Running the Operations Manager Configuration utility

If you are upgrading from Enterprise Vault 2007 and the Enterprise Vault Operations Manager component is installed, you must run the Operations Manager Configuration utility.

Do not run the Operations Manager Configuration utility until you have successfully run the Enterprise Vault Configuration wizard.

To run the Operations Manager Configuration utility

1   Log on to the server using the Vault Service account.

2   On the Windows **Start** menu, click **Programs** > **Enterprise Vault** > **Operations Manager Web App Configuration** to display the Operations Manager Configuration utility.

3   Enter the domain, user name, and password for the Monitoring user account. This is the account under which Operations Manager runs.

4   Click **Configure** to configure Operations Manager.

Perform the above procedure on each server on which the Operations Manager component is installed.

Running the Enterprise Vault Reporting Configuration utility

If the Enterprise Vault Reporting component is installed on any computer, you must run the Reporting Configuration utility on that computer.

To run the Reporting Configuration utility

1   On the Windows **Start** menu, click **Programs** > **Enterprise Vault** > **Enterprise Vault Reports Configuration** to display the Reporting Configuration utility.

2   Select **Configure Reporting and deploy or upgrade reports**.

3   Type in the domain, user name, and password for the Reporting user account.

4   If you are using SQL Server 2005 Reporting Services, select the SQL Reporting Services Instance.

5   Select the language in which to deploy the reports.

6   Select or type in the name of the Directory database SQL Server.

7   Click **Configure** to deploy the reports.

Perform the above procedure on each server on which the Enterprise Vault Reporting component is installed.

Manually deploying the reports

If the Reporting Configuration utility indicated that there was an error deploying Enterprise Vault reports, see the following TechNote on the Symantec Enterprise Support site:

http://entsupport.symantec.com/docs/288139

Multiple servers: installing the Enterprise Vault server software

This chapter includes the following topics:

- Installing on multiple servers
- Starting the Directory service
- Upgrading from Enterprise Vault 2007: Running the Configuration wizard
- Starting the Storage service on all servers
- Starting all Enterprise Vault services on other servers
- Upgrading from Enterprise Vault 2007: Upgrading the auditing database
- Upgrading from Enterprise Vault 2007: Running the Operations Manager Configuration utility
- Running the Enterprise Vault Reporting Configuration utility

Installing on multiple servers

The Directory service computer referred to in the following instructions is the computer specified on the **Connect** tab of the **Enterprise Vault** container properties in the Administration Console.

To install the Enterprise Vault 8.0 SP3 server software

1   Log on as the Vault Service account to each Enterprise Vault server other than the Directory service computer, and stop the Enterprise Vault Admin service. This action stops the Admin service itself, and any other Enterprise Vault services.

2   Stop any other services or applications that can lock Enterprise Vault files. For example:

   ■ Enterprise Vault Administration Console

   ■ Enterprise Vault Accelerator Manager service

   ■ Enterprise Vault Placeholder service

   ■ Enterprise Vault File Blocking service

   ■ Enterprise Vault File Collector service

   ■ Windows Event Viewer

3   Log on as the Vault Service account on the Directory service computer.

4   Start **Computer Management** and go to **Services and Applications**.

5   Under **Services**, stop the Enterprise Vault Admin service. This action stops the Admin service itself and other Enterprise Vault services, including the Enterprise Vault Directory service.

   Stop any other services or applications that use Enterprise Vault. For example:

   ■ Enterprise Vault Administration Console

   ■ Enterprise Vault Accelerator Manager service

   ■ Enterprise Vault Placeholder service

   ■ Enterprise Vault File Blocking service

   ■ Enterprise Vault File Collector service

6   If you are installing on an Enterprise Vault Domino Gateway, make sure that the Domino server on the Enterprise Vault Domino Gateway is shut down and that `EVInstall.nsf` is not accessed locally.

7   Close any applications that may be running on the server, including the Control Panel, Computer Management, and the Event Log viewer.

8   Load the Enterprise Vault 8.0 SP3 media.

9   Using Windows Explorer, open the folder `\Enterprise Vault 8.0 SP3\Server`.

10 Double-click the file `setup.exe` to start the installation.

11 Work through the installation.

12 Install the Enterprise Vault software on the other servers in your Enterprise Vault environment.

Install the Enterprise Vault Reporting component on computers on which Enterprise Vault Reporting is installed.

13 On computers on which the Enterprise Vault Reporting component is installed, modify the `ReportDeploymentDefinition.XML` file.

See "To modify the ReportDeploymentDefinition.XML file" on page 57.

To modify the ReportDeploymentDefinition.XML file

1 Find the `ReportDeploymentDefinition.XML` file on the computer on which the Enterprise Vault Reporting component is installed. The file is in the `evreports` folder under the Enterprise Vault installation folder, typically `C:\Program Files\Enterprise Vault\evreports`.

2 Make a backup copy of the `ReportDeploymentDefinition.XML`file.

3 Use Windows Notepad to open the original file.

4 Find the Report element that has the filename parameter **Audit Details.rdl**.

The Report element looks like the following:

```
<Report evItemCategory="GenericReports" englishName="Archived
Items Access" resourceId="Audit_Details_Title" filename=
"Audit Details.rdl" rdsName="EnterpriseVaultDS" hidden=
"false" evUniqueId="D7F307E4-E306-4f17-98FB-58702B6D635D"
evVersion="8.0.2.0" />
```

Change the value of the **evVersion** parameter at the end of the element from **8.0.2.0** to **8.0.3.0**, so that the element looks like the following:

```
<Report evItemCategory="GenericReports" englishName="Archived
Items Access" resourceId="Audit_Details_Title" filename=
"Audit Details.rdl" rdsName="EnterpriseVaultDS" hidden=
"false" evUniqueId="D7F307E4-E306-4f17-98FB-58702B6D635D"
evVersion="8.0.3.0" />
```

5 Find the Report element that has the filename parameter **Audit Trending.rdl**.

Change the value of the **evVersion** parameter in this Report element from **8.0.2.0** to **8.0.3.0**

6   Find the Report element that has the filename parameter **Duplicate Files Summary Report.rdl**. Note that there are two spaces between the words **Summary** and **Report**.

Change the value of the **evVersion** parameter in this Report element from **8.0.2.0** to **8.0.3.0**

7   Find the Report element that has the filename parameter **Server Duplicate Files.rdl**.

Change the value of the **evVersion** parameter in this Report element from **8.0.2.0** to **8.0.3.0**

Note: Do not change the values of any other **evVersion** parameters in the file.

8   Save the `ReportDeploymentDefinition.XML` file.

The Enterprise Vault software installation is now complete, but you must obtain license keys for any additional services that you intend to run.

Starting the Directory service

After the upgrade installation on the Directory service computer, you must ensure that the Directory service is running.

To start the Directory service

1   Use Windows Services to start the Enterprise Vault Directory service. When the Directory service starts, it automatically upgrades the Directory database schema and synchronizes new Exchange archiving policy advanced settings into existing policies.

2   Wait for event 8576 to be logged in the Enterprise Vault event log:

```
The Directory service has completed the automatic upgrade of the
EnterpriseVaultDirectory Database
```

Upgrading from Enterprise Vault 2007: Running the Configuration wizard

If you upgrade from Enterprise Vault 2007 you must run the Configuration wizard, as described in this section. If you upgrade from any version of Enterprise Vault 8.0 you do not need to run the Configuration wizard.

Before you run the Configuration wizard, you must already have completed the following:

- Installed the Enterprise Vault 8.0 SP3 server software on all the Enterprise Vault servers in your environment.
- Started the Directory service on the Directory service computer, and allowed it to complete the automatic schema upgrade.

Note: You need to run the Configuration wizard only once; it is not necessary to run it on all servers. You are recommended to run it on the Directory service computer.

To run the Configuration wizard

1 Start the Admin service on all the Enterprise Vault servers in your environment, including servers in other Enterprise Vault Sites that use the same Directory database.

   Note: Do not continue until all Admin services have started.

2 Log on to the Directory service computer. You must use the Vault Service account to run the Configuration wizard.

3 Ensure that the Directory service computer has network connectivity to all the servers in the Enterprise Vault environment. For example, if your firewall policies allow the MS-DOS `PING` command, you could use `PING` to check that each server is available.

4 Ensure that the Directory service is running.

5 Click **Start** > **Programs** > **Enterprise Vault** > **Enterprise Vault Configuration** to start the Configuration wizard.

6 The only available option on the first screen of the Configuration wizard is **Upgrade this configuration**. Click **Next**.

7 On the next screen, click **Next** to start the upgrade. There is a prompt for the Vault Service account password.

8 Enter the Vault Service account password and click **OK**. The Configuration wizard shows a progress bar while it configures the system. Depending on the existing configuration, the wizard may omit some configuration steps. The wizard does the following, as necessary:

   - Creates a log file for the upgrade in the Enterprise Vault `Reports` folder. The log file name is `UpgradeEVServerToV8.0` *date*`.log`, where *date* is the date and time when the file was created.

- Creates a Task Controller service on any Enterprise Vault server that does not already have a Task Controller service.

- If necessary, uses the new Directory encryption services to re-encrypt the password values in the Directory database entries,

- Updates the Roles-based Administration database with new roles, tasks and operations, and creates a log file in the Enterprise Vault `Reports` folder. The log file name is `_EvAzUtil` *date*`.log`, where *date* is the date and time when the file was created.

- If necessary, creates the Enterprise Vault Operations Manager database.

- Checks the Vault Service account permissions on all servers.

- Updates the Enterprise Vault DCOM settings on all servers in the Enterprise Vault environment.

9 Click **Finish** to close the Configuration wizard.

10 Stop all Enterprise Vault services.

11 Start the Enterprise Vault Admin service and the Directory service.

12 If you stopped the IIS Admin service before the installation, start any services that were stopped by this service.

Manually configuring the Monitoring database

If the Configuration wizard warned you that there was an error configuring the Monitoring database, you must configure the database manually.

See the following TechNote on the Symantec Support Web site:

http://entsupport.symantec.com/docs/287449

Starting the Storage service on all servers

The first time an Enterprise Vault 8.0 SP3 Storage service starts, it upgrades the storage databases.

You must start the Storage service on every server that has a Storage service. You must then wait for the Storage service to complete the upgrade. The Storage service logs appropriate entries in the event log.

To start the Storage services, do the following on every server that has a Storage service

1   Use Windows Services to start the Enterprise Vault Storage service. When the Storage service starts, it automatically upgrades the fingerprint databases. Event 6959 is logged for each vault store database that is upgraded.

2   Wait for event 6221 to be logged in the Enterprise Vault event log:

    ```
    Storage Service started.
    ```

When you have started every Storage service and waited for the completion event, you can continue to the next section to start the other Enterprise Vault services.

Starting all Enterprise Vault services on other servers

Start the Enterprise Vault services on all servers in the site.

If you have upgraded from Enterprise Vault 2007, note the following:

■   Enterprise Vault 8.0 introduced a new single instance storage model to reduce the space required for archives. Vault stores are now grouped into vault store groups.

■   The upgrade turned off all vault store sharing so that you can assess and reconfigure existing vault stores as required.
    See "The upgrade disables sharing" on page 21.

Upgrading from Enterprise Vault 2007: Upgrading the auditing database

If you upgrade an Enterprise Vault 2007 system in which you enabled auditing, you must upgrade the Enterprise Vault auditing database schema.

To upgrade the auditing database schema

1   Make sure that you have backed up the **EnterpriseVaultAudit** database.

2   For Microsoft SQL Server 2000, start SQL Query Analyzer. For Microsoft SQL Server 2005 or 2008, start SQL Server Management Studio.

3   In the left pane of SQL Query Analyzer or SQL Server Management Studio, select the **EnterpriseVaultAudit** database.

4   From the **File** menu, click **Open** > **File**.

5   Navigate to the Enterprise Vault installation folder (typically `C:\Program Files\Enterprise Vault`) and select the file **Audit_Schema_Upgrade.sql**.

6   From the **Query** menu, click **Execute**.

After a short time SQL Query Analyzer or SQL Server Management Studio indicates that the script has completed successfully.

7   Exit from SQL Query Analyzer or SQL Server Management Studio.

Upgrading from Enterprise Vault 2007: Running the Operations Manager Configuration utility

If you upgrade from Enterprise Vault 2007 and the Enterprise Vault Operations Manager component is installed on any server, you must run the Operations Manager Configuration utility on that server.

Do not run the Operations Manager Configuration utility until you have successfully run the Enterprise Vault Configuration wizard on the Directory service computer in your Enterprise Vault system.

To run the Operations Manager Configuration utility

1   Log on to the server using the Vault Service account.

2   On the Windows **Start** menu, click **Programs** > **Enterprise Vault** > **Operations Manager Web App Configuration** to display the Operations Manager Configuration utility.

3   Enter the domain, user name, and password for the Monitoring user account. This account is the one under which Operations Manager runs.

4   Click **Configure** to configure Operations Manager.

5   Repeat this procedure on every other server on which the Operations Manager component is installed.

Running the Enterprise Vault Reporting Configuration utility

If the Enterprise Vault Reporting component is installed on any computer, you must run the Reporting Configuration utility on that computer.

To run the Reporting Configuration utility

1   On the Windows **Start** menu, click **Programs** > **Enterprise Vault** > **Enterprise Vault Reports Configuration** to display the Reporting Configuration utility.

2   Select **Configure Reporting and deploy or upgrade reports**.

3   Type in the domain, user name, and password for the Reporting user account.

4   If you are using SQL Server 2005 Reporting Services, select the SQL Reporting Services Instance.

5   Select the language in which to deploy the reports.

6   Select or type in the name of the Directory database SQL Server.

7   Click **Configure** to deploy the reports.

8   Repeat this procedure on every other server on which the Enterprise Vault Reporting component is installed.

Manually deploying the reports

If the Reporting Configuration utility indicated that there was an error deploying Enterprise Vault reports, see the following TechNote on the Symantec Enterprise Support site:

http://entsupport.symantec.com/docs/288139

Veritas cluster: installing the Enterprise Vault server software

This chapter includes the following topics:

- Veritas cluster: installing the Enterprise Vault 8.0 SP3 software

- Starting Enterprise Vault services

- Starting the Storage service on all servers

- Starting all Enterprise Vault services on other servers

- Upgrading from Enterprise Vault 2007: Upgrading the auditing database

- Upgrading from Enterprise Vault 2007: Running the Operations Manager Configuration utility

- Running the Enterprise Vault Reporting Configuration utility

Veritas cluster: installing the Enterprise Vault 8.0 SP3 software

This section describes how to install the Enterprise Vault server software when the servers that run Enterprise Vault tasks are part of a Veritas cluster.

Note that Enterprise Vault does not support high-availability upgrades. You must install the servers software on all nodes in the cluster before you start Enterprise Vault services or run the configuration wizard.

To install the Enterprise Vault 8.0 SP3 server software

1   Log on to the active node as the Vault Service account.

2   Use VCS cluster administration tools to take all Enterprise Vault service resources offline.

> **Note:** You must stop all Enterprise Vault services in the Enterprise Vault Site. For example, stop the services on non-clustered servers, such as an Enterprise Vault Domino Gateway.

> **Note:** If you install on an Enterprise Vault Domino Gateway, make sure that the Domino server on the Enterprise Vault Domino Gateway is shut down and that EVInstall.nsf is not accessed locally.

> **Note:** If there are multiple Sites that share the Enterprise Vault Directory you must also stop all Enterprise Vault services in the other Sites.

3   Stop any other services or applications that can lock Enterprise Vault files. For example:

- Enterprise Vault Administration Console

- Enterprise Vault Accelerator Manager service

- Enterprise Vault Placeholder service

- Enterprise Vault File Blocking service

- Enterprise Vault File Collector service

4   Close any applications that may be running in the server, including the Control Panel, Computer Management, the Event Log viewer, and the Windows Event Viewer.

5   Load the Enterprise Vault 8.0 SP3 media.

6   Use Windows Explorer to open the following folder:

    \Enterprise Vault 8.0 SP3\Server.

7   Double-click the file setup.exe to start the installation.

8   Work through the installation.

9   Install the Enterprise Vault software on the other servers in your Enterprise Vault environment, including any cluster failover nodes.

      Install the Enterprise Vault Reporting component on computers on which Enterprise Vault Reporting is installed.

10   On computers on which the Enterprise Vault Reporting component is installed, modify the `ReportDeploymentDefinition.XML` file.

To modify the ReportDeploymentDefinition.XML file

1   Find the `ReportDeploymentDefinition.XML` file on the computer on which the Enterprise Vault Reporting component is installed. The file is in the `evreports` folder under the Enterprise Vault installation folder, typically `C:\Program Files\Enterprise Vault\evreports`.

2   Make a backup copy of the `ReportDeploymentDefinition.XML`file.

3   Use Windows Notepad to open the original file.

4   Find the Report element that has the filename parameter **Audit Details.rdl**.

      The Report element looks like the following:

```
<Report evItemCategory="GenericReports" englishName="Archived
Items Access" resourceId="Audit_Details_Title" filename=
"Audit Details.rdl" rdsName="EnterpriseVaultDS" hidden=
"false" evUniqueId="D7F307E4-E306-4f17-98FB-58702B6D635D"
evVersion="8.0.2.0" />
```

      Change the value of the **evVersion** parameter at the end of the element from **8.0.2.0** to **8.0.3.0**, so that the element looks like the following:

```
<Report evItemCategory="GenericReports" englishName="Archived
Items Access" resourceId="Audit_Details_Title" filename=
"Audit Details.rdl" rdsName="EnterpriseVaultDS" hidden=
"false" evUniqueId="D7F307E4-E306-4f17-98FB-58702B6D635D"
evVersion="8.0.3.0" />
```

5   Find the Report element that has the filename parameter **Audit Trending.rdl**.

      Change the value of the **evVersion** parameter in this Report element from **8.0.2.0** to **8.0.3.0**

6   Find the Report element that has the filename parameter **Duplicate Files Summary Report.rdl**. Note that there are two spaces between the words **Summary** and **Report**.

Change the value of the **evVersion** parameter in this Report element from **8.0.2.0** to **8.0.3.0**

7   Find the Report element that has the filename parameter **Server Duplicate Files.rdl**.

Change the value of the **evVersion** parameter in this Report element from **8.0.2.0** to **8.0.3.0**

Note: Do not change the values of any other **evVersion** parameters in the file.

8   Save the `ReportDeploymentDefinition.XML` file.

The Enterprise Vault software installation is now complete, but you must obtain license keys for any additional services that you intend to run.

Starting Enterprise Vault services

After the upgrade installation on the active node you must start the Admin and Directory services.

To start the Directory service;

1   Use VCS cluster administration tools to bring the Admin and Directory service resources online.

Do not bring any other Enterprise Vault resources online.

2   Wait for event 8576 to be logged in the Enterprise Vault event log:

```
The Directory service has completed the automatic upgrade of the
EnterpriseVaultDirectory Database
```

3   Start the Admin service on all the Enterprise Vault servers in your environment, including servers in other Enterprise Vault Sites that use the same Directory database.

Note: Do not continue until all the Admin services have started.

---

4 If you have upgraded from any version of Enterprise Vault 8.0, go to step 10.

If you have upgraded from Enterprise Vault 2007 continue with this procedure to run the Configuration wizard.

Note: You need to run the Configuration wizard only once; it is not necessary to run it on all servers.

---

5 Click **Start** > **Programs** > **Enterprise Vault** > **Enterprise Vault Configuration** to start the Configuration wizard.

6 The only available option on the first screen of the Configuration wizard is **Upgrade this configuration**. Click **Next**.

7 On the next screen, click **Next** to start the upgrade. There is a prompt for the Vault Service account password.

8 Enter the Vault Service account password and click **OK**. The Configuration wizard shows a progress bar while it configures the system. Depending on the existing configuration, the wizard may omit some configuration steps. The wizard does the following, as necessary:

- Creates a log file for the upgrade in the Enterprise Vault `Reports` folder. The log file name is `UpgradeEVServerToV8.0` *date*`.log`, where *date* is the date and time when the file was created.

- Creates a Task Controller service on any Enterprise Vault server that does not already have a Task Controller service.

- If necessary, uses the new Directory encryption services to re-encrypt the password values in the Directory database.

- Updates the Roles-based Administration database with new roles, tasks and operations, and creates a log file in the Enterprise Vault `Reports` folder. The log file name is `_EvAzUtil` *date*`.log`, where *date* is the date and time when the file was created.

- If necessary, creates the Enterprise Vault Operations Manager database.

- Checks the Vault Service account permissions on all servers.

- Updates the Enterprise Vault DCOM settings on all servers in the Enterprise Vault environment.

9 Click **Finish** to close the Configuration wizard.

10 If you stopped the IIS Admin service before the installation, start any services that were stopped by this service.

11 Use the cluster administration tools to bring all the Enterprise Vault services online.

12 Test that the cluster failover works correctly for Enterprise Vault.

Starting the Storage service on all servers

The first time an Enterprise Vault 8.0 SP3 Storage service starts, it upgrades the storage databases.

You must start the Storage service on every server that has a Storage service. You must then wait for the Storage service to complete the upgrade. The Storage service logs appropriate entries in the event log.

To start the Storage services, do the following on every server that has a Storage service

1 Use Windows Services to start the Enterprise Vault Storage service. When the Storage service starts, it automatically upgrades the fingerprint databases. Event 6959 is logged for each vault store database that is upgraded.

2 Wait for event 6221 to be logged in the Enterprise Vault event log:

```
Storage Service started.
```

When you have started every Storage service and waited for the completion event, you can continue to the next section to start the other Enterprise Vault services.

Starting all Enterprise Vault services on other servers

Start the Enterprise Vault services on all servers in the site.

If there are multiple Sites that share the Enterprise Vault Directory you can start all Enterprise Vault services in the other Sites.

If you have upgraded from Enterprise Vault 2007, note the following:

■ Enterprise Vault 8.0 introduced a new single instance storage model to reduce the space required for archives. Vault stores are now grouped into vault store groups.

■ The upgrade turned off all vault store sharing so that you can assess and reconfigure existing vault stores as required.
See "The upgrade disables sharing" on page 21.

Upgrading from Enterprise Vault 2007: Upgrading the auditing database

If you upgrade an Enterprise Vault 2007 system in which you enabled auditing, you must upgrade the Enterprise Vault auditing database schema.

To upgrade the auditing database schema

1   Make sure that you have backed up the **EnterpriseVaultAudit** database.

2   For Microsoft SQL Server 2000, start SQL Query Analyzer. For Microsoft SQL Server 2005 or 2008, start SQL Server Management Studio.

3   In the left pane of SQL Query Analyzer or SQL Server Management Studio, select the **EnterpriseVaultAudit** database.

4   From the **File** menu, click **Open** > **File**.

5   Navigate to the Enterprise Vault installation folder (typically `C:\Program Files\Enterprise Vault`) and select the file **Audit_Schema_Upgrade.sql**.

6   From the **Query** menu, click **Execute**.

    After a short time SQL Query Analyzer or SQL Server Management Studio indicates that the script has completed successfully.

7   Exit from SQL Query Analyzer or SQL Server Management Studio.

Upgrading from Enterprise Vault 2007: Running the Operations Manager Configuration utility

Note: This section does not apply if you have upgraded from Enterprise Vault 8.0.

If you upgrade from Enterprise Vault 2007 and the Enterprise Vault Operations Manager component is installed on any server, you must run the Operations Manager Configuration utility on that server.

Do not run the Operations Manager Configuration utility until you have successfully run the Enterprise Vault Configuration wizard on the Directory service computer in your Enterprise Vault system.

To run the Operations Manager Configuration utility

1 Log on to the server using the Vault Service account.

2 On the Windows **Start** menu, click **Programs** > **Enterprise Vault** > **Operations Manager Web App Configuration** to display the Operations Manager Configuration utility.

3 Enter the domain, user name, and password for the Monitoring user account. This is the account under which Operations Manager runs.

4 Click **Configure** to configure Operations Manager.

5 Repeat this procedure on each server on which the Operations Manager component is installed.

Running the Enterprise Vault Reporting Configuration utility

If the Enterprise Vault Reporting component is installed on any computer, you must run the Reporting Configuration utility on that computer.

To run the Reporting Configuration utility

1 On the Windows **Start** menu, click **Programs** > **Enterprise Vault** > **Enterprise Vault Reports Configuration** to display the Reporting Configuration utility.

2 Select **Configure Reporting and deploy or upgrade reports**.

3 Type in the domain, user name, and password for the Reporting user account.

4 If you are using SQL Server 2005 Reporting Services, select the SQL Reporting Services Instance.

5 Select the language in which to deploy the reports.

6 Select or type in the name of the Directory database SQL Server.

7 Click **Configure** to deploy the reports.

8 Repeat this procedure on each server on which the Enterprise Vault Reporting component is installed.

Manually deploying the reports

If the Reporting Configuration utility indicated that there was an error deploying Enterprise Vault reports, see the following TechNote on the Symantec Enterprise Support site:

http://entsupport.symantec.com/docs/288139

Chapter 10

Microsoft cluster: installing the Enterprise Vault server software

This chapter includes the following topics:

- Microsoft cluster: installing the Enterprise Vault 8.0 SP3 software
- Starting Enterprise Vault services
- Starting the Storage service on all servers
- Starting all Enterprise Vault services on other servers
- Upgrading from Enterprise Vault 2007: Upgrading the auditing database
- Upgrading from Enterprise Vault 2007: Running the Operations Manager Configuration utility
- Running the Enterprise Vault Reporting Configuration utility

Microsoft cluster: installing the Enterprise Vault 8.0 SP3 software

This section describes how to install the Enterprise Vault server software when the servers that run Enterprise Vault tasks are part of a Microsoft cluster.

Note that Enterprise Vault does not support high-availability upgrades. You must install the servers software on all nodes in the cluster before you start Enterprise Vault services or run the configuration wizard.

To install the Enterprise Vault 8.0 SP3 server software

1   Log on to the active node as the Vault Service account.

2   Use Microsoft Cluster Administrator or the command line utility cluster to take the Admin service resource offline. This takes all the Enterprise Vault services offline.

> **Note:** Do not take the EnterpriseVaultServerInstance offline.

> **Note:** You must stop all Enterprise Vault services in the Enterprise Vault Site. For example, stop the services on non-clustered servers, such as an Enterprise Vault Domino Gateway.

> **Note:** If you install on an Enterprise Vault Domino Gateway, make sure that the Domino server on the Enterprise Vault Domino Gateway is shut down and that `EVInstall.nsf` is not accessed locally.

> **Note:** If there are multiple Sites that share the Enterprise Vault Directory you must also stop all Enterprise Vault services in the other Sites.

3   Stop any other services or applications that can lock Enterprise Vault files. Use Microsoft Cluster Administrator to stop clustered services. For example:

   ■ Enterprise Vault Administration Console

   ■ Enterprise Vault Accelerator Manager service

   ■ Enterprise Vault Placeholder service

   ■ Enterprise Vault File Blocking service

   ■ Enterprise Vault File Collector service

4   Close any applications that may be running in the server, including the Control Panel, Computer Management, the Event Log viewer, and the Windows Event Viewer.

5 Open a command window and enter the following command to remove the registry checkpoint binding to the Admin service:

On 32-bit Windows systems:

```
cluster resource evserver1-EnterpriseVaultAdminService
/removecheck:"Software\KVS\Enterprise Vault"
```

On 64-bit Windows systems:

```
cluster resource evserver1-EnterpriseVaultAdminService
/removecheck:"Wow6432Node\Software\KVS\Enterprise Vault"
```

where *evserver1* is the name of the virtual server.

6 To check that the binding has been removed, enter the following command:

```
cluster resource evserver1-EnterpriseVaultAdminService /check
```

The output looks similar to the following:

```
Listing registry checkpoints for resource
        'evserver1-EnterpriseVaultAdminService'...
Resource           Registry Checkpoint
------------------- --------------------------------------------
evserver1-EnterpriseVaultAdminService None
```

7 In the command window, enter the following command to add registry checkpoint binding to the **EnterpriseVaultServerInstance** resource

On 32-bit Windows systems:

```
cluster resource evserver1-EnterpriseVaultServerInstance
/addcheck:"Software\KVS\Enterprise Vault"
```

On 64-bit Windows systems:

```
cluster resource evserver1-EnterpriseVaultServerInstance
/addcheck:"Wow6432Node\Software\KVS\Enterprise Vault"
```

8   Enter the following command to check that the binding has been applied:

    ```
    cluster resource evserver1-EnterpriseVaultServerInstance /check
    ```

    The output looks similar to the following:

    ```
    Listing registry checkpoints for resource
              'evserver1-EnterpriseVaultServerInstance'...
    Resource              Registry Checkpoint
    -------------------- -------------------------------------------
    evserver1-EnterpriseVaultServerInstance 'Software\KVS\Enterprise Vault'
    ```

9   Load the Enterprise Vault 8.0 SP3 media.

10 Use Windows Explorer to open the following folder:

    ```
    \Enterprise Vault 8.0 SP3\Server
    ```

11 Double-click the file `setup.exe` to start the installation.

12 Work through the installation.

13 Install the Enterprise Vault software on the other servers in your Enterprise
    Vault environment, including any cluster failover nodes.

    Install the Enterprise Vault Reporting component on computers on which
    Enterprise Vault Reporting is installed.

14 On computers on which the Enterprise Vault Reporting component is installed,
    modify the `ReportDeploymentDefinition.XML` file.

    See "To modify the ReportDeploymentDefinition.XML file" on page 76.

To modify the ReportDeploymentDefinition.XML file

1   Find the `ReportDeploymentDefinition.XML` file on the computer on which
    the Enterprise Vault Reporting component is installed. The file is in the
    `evreports` folder under the Enterprise Vault installation folder, typically
    `C:\Program Files\Enterprise Vault\evreports`.

2   Make a backup copy of the `ReportDeploymentDefinition.XML` file.

3   Use Windows Notepad to open the original file.

4 Find the Report element that has the filename parameter **Audit Details.rdl**.

The Report element looks like the following:

```
<Report evItemCategory="GenericReports" englishName="Archived
Items Access" resourceId="Audit_Details_Title" filename=
"Audit Details.rdl" rdsName="EnterpriseVaultDS" hidden=
"false" evUniqueId="D7F307E4-E306-4f17-98FB-58702B6D635D"
evVersion="8.0.2.0" />
```

Change the value of the **evVersion** parameter at the end of the element from **8.0.2.0** to **8.0.3.0**, so that the element looks like the following:

```
<Report evItemCategory="GenericReports" englishName="Archived
Items Access" resourceId="Audit_Details_Title" filename=
"Audit Details.rdl" rdsName="EnterpriseVaultDS" hidden=
"false" evUniqueId="D7F307E4-E306-4f17-98FB-58702B6D635D"
evVersion="8.0.3.0" />
```

5 Find the Report element that has the filename parameter **Audit Trending.rdl**.

Change the value of the **evVersion** parameter in this Report element from **8.0.2.0** to **8.0.3.0**

6 Find the Report element that has the filename parameter **Duplicate Files Summary Report.rdl**. Note that there are two spaces between the words **Summary** and **Report**.

Change the value of the **evVersion** parameter in this Report element from **8.0.2.0** to **8.0.3.0**

7 Find the Report element that has the filename parameter **Server Duplicate Files.rdl**.

Change the value of the **evVersion** parameter in this Report element from **8.0.2.0** to **8.0.3.0**

Note: Do not change the values of any other **evVersion** parameters in the file.

8 Save the `ReportDeploymentDefinition.XML` file.

The Enterprise Vault software installation is now complete, but you must obtain license keys for any additional services that you intend to run.

Starting Enterprise Vault services

After the upgrade installation on the active node, you must start the Admin and Directory services.

To start the Admin and Directory services on the active node

1   Use the cluster administration tools to bring the Admin and Directory services resources online.

    Do not bring any other Enterprise Vault resources online.

2   Wait for event 8576 to be logged in the Enterprise Vault event log:

    ```
    The Directory service has completed the automatic upgrade of the
    EnterpriseVaultDirectory Database
    ```

3   Start the Admin service on all the Enterprise Vault servers in your environment, including servers in other Enterprise Vault Sites that use the same Directory database.

    Note: Do not continue until all the Admin services have started.

4   If you have upgraded from any version of Enterprise Vault 8.0, go to step 10.

    If you have upgraded from Enterprise Vault 2007 continue with this procedure to run the Configuration wizard.

    Note: You need to run the Configuration wizard only once; it is not necessary to run it on all servers.

5   On the active node, click **Start** > **Programs** > **Enterprise Vault** > **Enterprise Vault Configuration** to start the Configuration wizard.

6   The only available option on the first screen of the Configuration wizard is **Upgrade this configuration**. Click **Next**.

7   On the next screen, click **Next** to start the upgrade. There is a prompt for the Vault Service account password.

8   Enter the Vault Service account password and click **OK**. The Configuration wizard shows a progress bar while it configures the system. Depending on the existing configuration, the wizard may omit some configuration steps. The wizard does the following, as necessary:

    ■   Creates a log file for the upgrade in the Enterprise Vault Reports folder. The log file name is UpgradeEVServerToV8.0 *date*.log, where *date* is the date and time when the file was created.

    ■   If necessary, uses the new Directory encryption services to re-encrypt the password values in the Directory database entries.

- Updates the Roles-based Administration database with new roles, tasks and operations, and creates a log file in the Enterprise Vault `Reports` folder. The log file name is `_EvAzUtil` *date*`.log`, where *date* is the date and time when the file was created.

- If necessary, creates the Enterprise Vault Operations Manager database.

- Checks the Vault Service account permissions on all servers.

- Updates the Enterprise Vault DCOM settings on all servers in the Enterprise Vault environment.

9   Click **Finish** to close the Configuration wizard.

10 If you stopped the IIS Admin service before the installation, start any services that were stopped by this service.

11 Use the cluster administration tools to bring the all the Enterprise Vault services online.

12 Test that the cluster failover works correctly for Enterprise Vault.

Starting the Storage service on all servers

The first time an Enterprise Vault 8.0 SP3 Storage service starts, it upgrades the storage databases.

You must start the Storage service on every server that has a Storage service. You must then wait for the Storage service to complete the upgrade. The Storage service logs appropriate entries in the event log.

To start the Storage services, do the following on every server that has a Storage service

1   Use Windows Services to start the Enterprise Vault Storage service. When the Storage service starts, it automatically upgrades the fingerprint databases. Event 6959 is logged for each vault store database that is upgraded.

2   Wait for event 6221 to be logged in the Enterprise Vault event log:

    Storage Service started.

When you have started every Storage service and waited for the completion event, you can continue to the next section to start the other Enterprise Vault services.

Starting all Enterprise Vault services on other servers

Start the Enterprise Vault services on all servers in the site.

If there are multiple Sites that share the Enterprise Vault Directory you can start all Enterprise Vault services in the other Sites.

If you have upgraded from Enterprise Vault 2007, note the following:

■ Enterprise Vault 8.0 introduced a new single instance storage model to reduce the space required for archives. Vault stores are now grouped into vault store groups.

■ The upgrade turned off all vault store sharing so that you can assess and reconfigure existing vault stores as required.
See

Upgrading from Enterprise Vault 2007: Upgrading the auditing database

If you upgrade an Enterprise Vault 2007 system in which you enabled auditing, you must upgrade the Enterprise Vault auditing database schema.

To upgrade the auditing database schema

1   Make sure that you have backed up the **EnterpriseVaultAudit** database.

2   For Microsoft SQL Server 2000, start SQL Query Analyzer. For Microsoft SQL Server 2005 or 2008, start SQL Server Management Studio.

3   In the left pane of SQL Query Analyzer or SQL Server Management Studio, select the **EnterpriseVaultAudit** database.

4   From the **File** menu, click **Open** > **File**.

5   Navigate to the Enterprise Vault installation folder (typically `C:\Program Files\Enterprise Vault`) and select the file **Audit_Schema_Upgrade.sql**.

6   From the **Query** menu, click **Execute**.

After a short time SQL Query Analyzer or SQL Server Management Studio indicates that the script has completed successfully.

7   Exit from SQL Query Analyzer or SQL Server Management Studio.

Upgrading from Enterprise Vault 2007: Running the Operations Manager Configuration utility

Note: This section does not apply if you have upgraded from Enterprise Vault 8.0.

If you upgrade from Enterprise Vault 2007 and the Enterprise Vault Operations Manager component is installed on any server, you must run the Operations Manager Configuration utility on that server.

Do not run the Operations Manager Configuration utility until you have successfully run the Enterprise Vault Configuration wizard on the Directory service computer in your Enterprise Vault system.

To run the Operations Manager Configuration utility

1   Log on to the server using the Vault Service account.

2   On the Windows **Start** menu, click **Programs** > **Enterprise Vault** > **Operations Manager Web App Configuration** to display the Operations Manager Configuration utility.

3   Enter the domain, user name, and password for the Monitoring user account. This account is the one under which Operations Manager runs.

4   Click **Configure** to configure Operations Manager.

5   Repeat this procedure on every other server on which the Operations Manager component is installed.

Running the Enterprise Vault Reporting Configuration utility

If the Enterprise Vault Reporting component is installed on any computer, you must run the Reporting Configuration utility on that computer.

To run the Reporting Configuration utility

1   On the Windows **Start** menu, click **Programs** > **Enterprise Vault** > **Enterprise Vault Reports Configuration** to display the Reporting Configuration utility.

2   Select **Configure Reporting and deploy or upgrade reports**.

3   Type in the domain, user name, and password for the Reporting user account.

4   If you are using SQL Server 2005 Reporting Services, select the SQL Reporting Services Instance.

5   Select the language in which to deploy the reports.

6   Select or type in the name of the Directory database SQL Server.

7   Click **Configure** to deploy the reports.

8   Repeat this procedure on every other server on which the Enterprise Vault Reporting component is installed.

Manually deploying the reports

If the Reporting Configuration utility indicated that there was an error deploying Enterprise Vault reports, see the following TechNote on the Symantec Enterprise Support site:

http://entsupport.symantec.com/docs/288139

Extra configuration tasks

This chapter includes the following topics:

About the extra configuration tasks

Work through the appropriate sections of this chapter, depending on your upgrade path.

Upgrading MOM and SCOM

◆ This section applies to all upgrades if you use MOM or SCOM.

If you use Microsoft Operations Manager (MOM) or System Center Operations Manager 2007 (SCOM) to monitor Enterprise Vault events then you must install the new management pack.

To install the Enterprise Vault MOM management pack

1 Start the MOM Administrator Console.

2 In the left pane, right-click **Processing Rule Groups** and, on the shortcut menu, click **Import Management Pack**.

3 Select the Enterprise Vault Management Pack, `EnterpriseVault.akm`, and work through the rest of the **Import Options** wizard.

To install the Enterprise Vault SCOM management pack

1 Start the SCOM operations console.

2 Start the import wizard and import `EnterpriseVault.xml`. The file is in the SCOM subfolder of the Enterprise Vault program folder (normally C:\Program Files\Enterprise Vault\SCOM).

The wizard automatically converts the file to a MOM 2005 Backward Compatibility pack.

Extra configuration for servers with no internet connection

◆ This section applies if you upgraded to Enterprise Vault 8.0 SP3 from Enterprise Vault 2007 or Enterprise Vault 8.0 original release or Enterprise Vault 8.0 SP1. If you upgraded from Enterprise Vault 8.0 SP2 you can ignore this section.

Enterprise Vault servers that do not have an internet connection can take a long time to start processes that use .NET Framework. When there is no internet connection there is a delay because the server cannot contact the Certificate Authority to verify signed assemblies. Eventually the verification attempt times out and the process continues.

If your Enterprise Vault server does not have an internet connection there are two methods you can use to prevent the Certificate Authority check, and the delay, as follows:

■ Disable the Certificate Authority check for all .NET Framework programs on the server.
See "Disabling Certificate Authority checks for the server" on page 85.

■ Disable the Certificate Authority check for individual Enterprise Vault programs.
See "Disabling the Certificate Authority checks for individual programs" on page 85.

Disabling Certificate Authority checks for the server

This section describes how to edit the `machine.config` file to disable Certificate Authority checks for the whole server.

To disable the Certificate Authority check for the whole server

1   Use Windows Notepad to open the `machine.config` file. The file is in the `CONFIG` folder under the .NET Framework installation folder (typically `C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG`.)

2   Add the following text to the file:

```
<configuration>
    <runtime>
        <generatePublisherEvidence enabled="false"/>
    </runtime>
</configuration>
```

3   Save the file.

If you later need to re-enable the Certificate Authority checks you can edit `machine.config` again.

To re-enable Certificate Authority checks

1   Use Windows Notepad to open `machine.config`.

2   Delete the following text from the <configuration> section of the file:

```
<generatePublisherEvidence enabled="false"/ >
```

3   Save the file.

Disabling the Certificate Authority checks for individual programs

This section describes how to edit individual configuration files to disable the Certificate Authority checks for individual Enterprise Vault programs.

The configuration files that you need to edit are in the Enterprise Vault program folder (typically `C:\Program Files\Enterprise Vault`). You may not have all the files present in your installation. The complete list of files is as follows:

```
EvExchangePolicySyncTask.exe.config
EvFileSvrArcMngr.exe.config
EvFSAArchivingTask.exe.config
EvLotusDominoArchivingTask.exe.config
EVLotusDominoJournalTask.exe.config
```

```
EvLotusDominoPolicySyncTask.exe.config
EvSharePointArchiveTask.exe.config
PstCollectorTask.exe.config
PstLocatorTask.exe.config
PstMigratorTask.exe.config
```

To disable the certification check for individual programs

1   Use Windows Notepad to open each of the configuration files.

2   Add the following text to the <configuration> section of the file:

```
<runtime>
 <generatePublisherEvidence enabled="false"/>
</runtime>
```

3   Save the file.

If you later need to re-enable the Certificate Authority checks you can edit each of the files again.

To re-enable the certification check for individual programs

1   Use Windows Notepad to open each of the configuration files.

2   Delete the following text from the <configuration> section of each file:

```
<generatePublisherEvidence enabled="false"/ >
```

3   Save the file.

Manually changing Enterprise Vault DCOM settings

◆   This section applies if you upgraded to Enterprise Vault 8.0 SP3 from Enterprise Vault 2007. If you upgraded from any version of Enterprise Vault 8.0 you can ignore this section.

Follow the procedure below if the Configuration wizard warned you that there was an error updating the DCOM settings of Enterprise Vault servers. If there was no such warning you can ignore this section.

To update the DCOM settings

1   Make sure that the Enterprise Vault Admin service is running on all Enterprise Vault servers in the Site.

2   Start the Enterprise Vault Administration Console

3   In the left pane of the Administration Console, right-click the Directory icon
    and then, on the shortcut menu, click **Properties**.

4   In the Directory Properties, click the **Service Account** tab.

5   Enter the password for the account and enter it again to confirm it.

6   Click **OK**.

Setting the cache location for each Enterprise Vault server

◆   This section applies if you upgraded to Enterprise Vault 8.0 SP3 from
    Enterprise Vault 2007. If you upgraded from any version of Enterprise Vault
    8.0 you can ignore this section.

Enterprise Vault 8.0 uses a server cache on each Enterprise Vault server, as follows:

■   As a temporary server store for items that need to be downloaded to users'
    Vault Caches.

■   To store temporary files when retrieving from Celerra devices.

There is now a minimum size of 10 GB for the server Cache location and the default
size is 20 GB.

You must set a server cache location for each Enterprise Vault server if you intend
to use Vault Cache or if you use a Celerra device with Enterprise Vault.

The Vault Service account must have read and write access to the location you
select.

Because anti-virus software can potentially change data in the cache, it is
important to exclude the cache location in your virus checking application.

To set a cache location

1   Start the Administration Console and expand the Enterprise Vault Servers
    container.

2   Do the following for each Enterprise Vault server:

    ■   Right-click the Enterprise Vault server and, on the shortcut menu, click
        Properties.

    ■   Click the **Cache** tab.

    ■   Specify the **Cache location** that you want to use.

    ■   Specify the **Maximum cache size**.

    ■   Click **OK**.

Note that the changes you make on a server do not take effect until the next restart of the Admin service on that server.

Enabling device-level sharing for EMC Centera partitions

◆ This section applies if you ever upgraded to the orginal release of Enterprise Vault 8.0.

In Enterprise Vault 2007, if **Share archived items** is selected in the properties of a Centera partition, an upgrade to the Enterprise Vault 8.0 original release erroneously turns off the device-level sharing.

This error does not occur on upgrade to any version of Enterprise Vault 8.0 other than the Enterprise Vault 8.0 original release.

Note: On upgrade from Enterprise Vault 2007 to Enterprise Vault 8.0, the **Share archived items** setting is renamed **Enable device-level sharing**.

If necessary, re-enable device-level sharing for the Centera partitions.

To enable device-level sharing for a Centera partition

1 In the Administration Console, double-click the Centera partition to display its properties.

2 On the **General** tab of the partition properties, select **Enable device-level sharing**.

3 Click **OK**.

Additional configuration for systems with FSA Reporting

Perform the additional configuration steps that are appropriate for your upgrade.

Upgrading from the Enterprise Vault 2007 original release

◆ This section applies if you upgraded from a system running the Enterprise Vault 2007 original release (with no service packs applied), and on which FSA Reporting was configured.

To perform the additional configuration for FSA Reporting

1   Change the Authentication mode of the SQL Server where the FSA Reporting database is located from Mixed Mode authentication to Windows authentication.

2   Restart the SQL Server.

3   Restart all Enterprise Vault services.

4   Run the FSA Reporting Configuration wizard. This will take you through the steps to configure the credentials of the Windows account that FSA Reporting will use when accessing the FSA Reporting database.

   To run the wizard:

   ■   In the Administration Console, expand the Enterprise Vault site.

   ■   Expand the **Targets** container.

   ■   Right-click the **File Servers** container and, on the shortcut menu, click **Configure FSA Reporting**.

   ■   Work through the wizard to configure the credentials of the Windows user account that FSA Reporting will use. The nominated account does not require any specific privileges.

   ■   If you have already configured Enterprise Vault Reporting, you can use the reporting user account, if you want to do so.

5   Do the following only if the Enterprise Vault server is running Windows 2000 Advanced Server:

   ■   Go to **Settings** > **Control Panel** > **Administrative Tools** > **Local Security Policy**.

   ■   Select **Security Settings** > **Local Policies** > **User Rights Assignment**.

   ■   In the right pane, double-click **Act as part of the operating system**.

   ■   On the **Local Security Policy Setting** dialog, click **Add** and add a local ASPNET user for the policy.

   ■   Restart the IIS Admin service.

   ■   Restart the Enterprise Vault services.

6   Run the Enterprise Vault Reporting Configuration utility again, as described in 'Running the Enterprise Vault Reporting Configuration utility'.

Additional tasks for all systems with FSA Reporting configured

◆   This section applies to all systems on which FSA Reporting is configured.

See the Enterprise Vault technical note "FSA Reporting deployment guidelines" at http://entsupport.symantec.com/docs/327402.

The technical note includes some additional configuration steps that you may need to perform after the upgrade.

Upgrading Exchange Server forms

This chapter includes the following topics:

■ About upgrading Exchange Server forms

About upgrading Exchange Server forms

By default, Enterprise Vault 8.0 deploys the Exchange Server forms to users' computers automatically.

If you have forms in your Organization Forms Library you do not need to upgrade them if either of the following is true:

■ You have upgraded from Enterprise Vault 2007.

■ You have upgraded from any version of Enterprise Vault 8.0 and you have not changed the default behavior.

The upgrade from Enterprise Vault 2007 to Enterprise Vault 8.0 automatically sets the desktop policy Advanced setting **Deploy Forms Locally** to **Always**. This means that the Enterprise Vault Outlook Add-Ins automatically install the Enterprise Vault forms into users' local forms libraries. The new forms are not installed until you upgrade users' Outlook Add-Ins.

You must upgrade the forms that are in the Organization Forms Library if you change **Deploy Forms Locally** to **Never**, **Delete**, or **When no Org Forms**.

If you do need to upgrade the forms that are in the Organization Forms Library, follow the instructions in the "Distributing Exchange Server Forms" chapter of *Setting up Exchange Server Archiving*.

Note the following:

- When you upgrade or reinstall the Enterprise Vault forms `EVPendingArchive.fdm`, `EVShortcut.fdm`, `EVPendingDelete.fdm`, and `EVPendingRestore.fdm`, always uninstall the existing copies first. Do not install the new forms on top of the existing copies.

- You can configure clients to download the forms automatically into personal forms libraries.

Upgrading Domino mailbox archiving

This chapter includes the following topics:

- Domino clients required for installation
- Preparing to upgrade Domino archiving
- Upgrading Domino mailbox archiving
- Granting the Domino archiving user access to mail files

Domino clients required for installation

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

For details of the required hotfixes and the latest information on supported versions of Domino software, see the *Enterprise Vault Compatibility Charts* at http://entsupport.symantec.com/docs/276547.

Preparing to upgrade Domino archiving

This section describes the preparation you must do before you upgrade Domino archiving.

To prepare for upgrading Domino mailbox archiving

1   On all Enterprise Vault Domino Gateway servers and on all Domino Mail Servers on which you have updated `Forms8.nsf`, `Forms7.nsf`, and `Forms6.nsf` to include the Enterprise Vault customizations, do the following:

- Stop the HTTP task.

- If the forms databases have replication enabled, the changes that EVIinstall makes are replicated to all Domino mail servers. To prevent the replication to other mail servers, disable the replication of the Forms6.nsf, Forms7.nsf, Forms8.nsf, and Forms85.nsf databases before you run EVInstall.nsf.

- Replace the `Forms8.nsf`, `Forms7.nsf`, and `Forms6.nsf` files with the original Domino versions that you backed up before you installed the previous version of Enterprise Vault.

- Update the ACL on these `.nsf` files to give the ID used to run EVInstall manager access to these originals.

Note: Since you are replacing the `Forms85.nsf`, `Forms8.nsf`, `Forms7.nsf`, and `Forms6.nsf` files with the original Domino versions, any additional (non-Enterprise Vault) customizations to these files will be lost. If you have made any additional customizations to `Forms85.nsf`, `Forms8.nsf`, `Forms7.nsf`, or `Forms6.nsf`, reapply these changes to the files after you have upgraded to Enterprise Vault 8.0 SP3.

---

2 On the Enterprise Vault Domino Gateway server, delete the following files, if they exist, from the `ev` subfolder of the Domino Data folder (for example, `C:\Lotus\Domino\Data\ev`):

- `EV_*.nsf`

- `EVA_*.nsf`

- `blank*.nsf`

Upgrading Domino mailbox archiving

This section describes how to upgrade Domino mailbox archiving.

To upgrade Domino mailbox archiving

1 Use the Domino Administrator to sign the Symantec Enterprise Vault 8.0 - Domino Installer (`EVInstall.nsf`) with the ID of the user that will be used to run it.

2 Do the following on the Enterprise Vault Domino Gateway, in the order listed:

- Ensure that you have the correct Notes client and hotfixes required.
  See

- Run `EVInstall.nsf`.

■ In the application page, select the Enterprise Vault Domino Gateway and a target Domino mail server.

■ Select **Modify Domino Web Access Forms Files**.

■ If you intend to make Vault Cache available to users, select **Install Vault Cache**.

■ Click **Install Symantec Enterprise Vault 8.0 database design templates** to start the process.
The application takes several minutes to create the new Enterprise Vault templates.

■ On the Enterprise Vault Domino Gateway and the Domino mail server where the database design templates were created, run the Designer task to update the Enterprise Vault design templates with design elements inherited from their corresponding master templates.
To run the Designer task, enter the appropriate command in the server console, as follows:

On a Domino 8.5 Enterprise Vault Domino Gateway	No action required.
On a Domino 8.0.x Enterprise Vault Domino Gateway	No action required.
On a Domino 8.0.x mail server	No action required.
On a Domino 7.0 Enterprise Vault Domino Gateway	`load design -f EVDG_DWA7.ntf`
On a Domino 7.0 mail server	`load design -f EV_DWA7.ntf`
On a Domino 6.5.x mail server	`load design -f EV_iNotes6.ntf`

3 Deploy the templates created on the Domino mail server to each of the target Domino mail servers that has the same Domino Server version. For example, if you ran `EVInstall.nsf` against a Domino Server 7.0.2 target server, deploy the templates to all Domino Server 7.0.2 mail servers.

Deploy the templates by creating replicas of the Enterprise Vault mail templates and running `Load Design` on each mail server.

(It is important that you copy the templates created on the Domino mail server and not those created on the Enterprise Vault Domino Gateway.)

4 If you have other target mail servers with different Domino Server versions (for example, 7.0.3), do the following until you have deployed the templates to all mail server targets:

■ Run `EVInstall.nsf` on the Enterprise Vault Domino Gateway again.

■ In the application page, clear the **Enterprise Vault Domino Gateway** selection.

■ Select a target Domino mail server.

■ If you require DWA, select **Modify Domino Web Access Forms Files**.

■ Click **Install Symantec Enterprise Vault 8.0 database design templates** to start the process.

5 Deploy the templates and run `Load Design` as before, on each mail server.

Note that this command updates all databases on the server. It may be quicker to restrict the scope of the command so that it updates just those databases that need changing. In this case, use the Load Design `-I` or `-d` or `-f` switches to update all Enterprise Vault mail databases that have had any of the following templates applied to them:

■ `ev_dwa*.ntf`

■ `ev_iNotes*.ntf`

■ `ev_Mail*.ntf`

See the Domino help for more information about Load Design switches.

6 If necessary, upgrade Notes 7 on Enterprise Vault servers to Notes 8.0.

If you have upgraded from a version of Enterprise Vault earlier than 8.0 SP2 the retention folder functionality may affect the permissions that the archiving task requires. The minimum permissions that are required depend on which version of Notes is installed on the Enterprise Vault server on which the archiving task runs.

The simplest way to provide the required permissions is to install Notes 8 on each Enterprise Vault server that runs a Domino archiving task. If you do not want to install Notes 8, you may need to change the permissions on all mail files.

See the section 'Granting the Domino archiving user access to mail files' in *Installing and Configuring*.

Granting the Domino archiving user access to mail files

The Domino archiving user account needs permissions to all the mail files to be archived. We recommend that you provide **Manager** access to the mail files. The minimum permissions that are required depend on which version of Notes is installed on the Enterprise Vault server on which the archiving task runs.

The minimum permissions required to mail files are as follows:

■ When Notes 8 is installed on the Enterprise Vault server the account requires a minimum of **Editor** access with **Delete Documents** and **Create shared folders/views**.

■ When Notes 7 is installed on the Enterprise Vault server the account requires a minimum of **Designer** access with **Delete Documents**.

Note: If you intend not to archive unread items then the Domino archiving user requires Manager access to the mail files. This is because Domino requires Manager access in order to determine which items are unread.

If Domino administrators have Manager access to all mail files, then you can use the Manage ACL tool in the Domino Administrator client to add the Domino archiving user to all mail databases.

Repeat the following steps for each target Domino mail server.

To add the Domino archiving user to all mail databases

1   In the Domino Administrator client, navigate to the Domino mail server and click the **Files** tab.

2   In the tasks pane, click the **Mail** folder to display a list of all the mail databases in the results pane.

3   Select the first mail database, and then press Shift+End to select all the mail databases.

4   Right-click and select **Access Control** > **Manage**.

5   Click **Add** and then click the person icon to select the Domino archiving user from the Domino directory list. Click **OK**.

6   When the user is in the **Access Control List** dialog box, change the set **User Type** to **Person** and **Access** to **Manager**.

7   Select **Delete documents**.

8   Click **OK** to add the user to the ACL of all mail databases selected.

If no user has Manager access to every mail database, then do the following:

- Place the Domino server administrator's user name in the Full Access Administrators field in the server document.

- Restart the Domino server.

- In the Domino Administrator client choose Administration > Full Access Administration and complete the procedure described above.

- If necessary the administrator can then be removed from the Full Access Administrators field.

Upgrading the FSA Agent on NTFS file servers

This chapter includes the following topics:

About upgrading the FSA Agent on NTFS file servers

We recommend that you upgrade the version of the FSA Agent on your NTFS file servers. Support is provided for backward compatibility, but new features may not be available until the FSA Agent version is aligned with the Enterprise Vault server version.

Note: If you use FSA Reporting, you must upgrade the FSA Agent on your NTFS file servers, otherwise FSA Reporting scans do not proceed.

For details of the compatible versions of the Enterprise Vault server and the FSA Agent, see the following documents:

■ The Enterprise Vault *Compatibility Charts* at http://entsupport.symantec.com/docs/276547.

■ For FSA Reporting, the Enterprise Vault technical note at http://entsupport.symantec.com/docs/297390.

You can upgrade the FSA Agent by using the Install FSA Agent wizard, or manually.

To use the Install FSA Agent wizard on Windows Server 2008, you must temporarily turn off the Windows Firewall on the file server. Otherwise, the wizard fails with the message "Error: The RPC server is unavailable". If you prefer not to do this, install the FSA Agent manually.

Some additional steps are required if the FSA Agent services are clustered for high availability.

Upgrading FSA services that are clustered for high availability

> **Note:** For a Windows Server 2008 file server that is clustered using Microsoft server clusters (MSCS), you must run the Enterprise Vault Administration Console on a Windows Server 2008 computer.

To upgrade FSA services that are clustered for high availability

1 Before upgrading the FSA Agent, perform these steps in the order shown:

   - In the Administration Console, expand the Enterprise Vault site.

   - Expand the **Targets** container and then the **File Servers** container.

   - Right-click the clustered file server and then, on the shortcut menu, click **FSA Cluster Configuration**.

   - Select the option **Remove the FSA resource from all groups** to remove the FSA resource.

2 Upgrade the FSA Agent on the clustered file server by using one of the following methods:

   - Run the Install FSA Agent wizard on the clustered file server.
     See "Upgrading the FSA Agent using the Install FSA Agent wizard" on page 101.

   - Upgrade the FSA Agent manually on each file server node.
     See "Upgrading the FSA Agent manually" on page 101.

3 Perform the following steps in the order shown to reconfigure the FSA services for high availability:

   - In the Administration Console, expand the Enterprise Vault site.

   - Expand the **Targets** container and then the **File Servers** container.

   - Right-click the clustered file server and then, on the shortcut menu, click **FSA Cluster Configuration**.

- ■ Select the option **Add, remove or reconfigure the FSA resource for groups that have shared disks**, and add the FSA resource back to the groups that have a shared disk.

Upgrading the FSA Agent using the Install FSA Agent wizard

You can upgrade the FSA Agent by using the Install FSA Agent wizard.

To upgrade the FSA Agent using the Install FSA Agent wizard

1   If the file server runs Windows Server 2008, turn off the Windows Firewall.

2   In the Administration Console, expand the Enterprise Vault site until the **Targets** container is visible.

3   Expand the **Targets** container.

4   Expand the **File Servers** container.

5   Right-click the file server on which you want to upgrade the FSA Agent and then, on the shortcut menu click **Install FSA Agent**.

6   Work through the wizard.

7   If the file server runs Windows Server 2008, turn the Windows Firewall back on.

Upgrading the FSA Agent manually

You can upgrade the FSA Agent by installing the required files manually.

To upgrade the FSA Agent manually

1   Find the FSA Agent files on the Enterprise Vault server. The files are in the `evpush\Agent` folder under the Enterprise Vault installation folder, typically `C:\Program Files\Enterprise Vault\evpush\Agent`.

2   Run the appropriate executable files on the file server:

- ■ On a 32-bit Windows system run `vcredist_x86.exe`

- ■ On a 64-bit Windows system run `vcredist_x86.exe` and then `vcredist_x64.exe`

3   Run the appropriate MSI file on the file server:

- ■ On a 32-bit Windows system run `Enterprise Vault File System Archiving.msi`

- On a 64-bit Windows system run `Enterprise Vault File System Archiving x64.msi`

Upgrading OWA and RPC Extensions

This chapter includes the following topics:

- About upgrading OWA and RPC Extensions

- Upgrading Enterprise Vault OWA 2007 Extensions

- Upgrading Enterprise Vault OWA 2003 Extensions

- Upgrading Enterprise Vault OWA 2000 Extensions

About upgrading OWA and RPC Extensions

This chapter describes how you upgrade older versions of the Enterprise Vault OWA and RPC Extensions to Enterprise Vault 8.0 SP3.

You must upgrade the Enterprise Vault OWA and RPC Extensions on each OWA and RPC server in your Enterprise Vault environment.

If you have problems with installing Enterprise Vault OWA Extensions, see the following technical note on the Symantec Enterprise Support site:

http://entsupport.symantec.com/docs/321591

This technical note gives detailed troubleshooting information for Enterprise Vault OWA Extensions.

Upgrading Enterprise Vault OWA 2007 Extensions

This procedure is only applicable if you are upgrading an Enterprise Vault 2007 system that uses the OWA 2007 extensions.

To upgrade Enterprise Vault OWA 2007 Extensions on each Exchange 2007 CAS server

1   Load the Enterprise Vault 8.0 SP3 media.

2   Open the `Enterprise Vault 8.0 SP3` folder.

3   Open the `OWA 2007 Extensions` folder.

4   Double-click the appropriate .msi file to start the installation, depending on whether the Exchange Server is running in 64-bit or 32-bit mode:

■   `Symantec Enterprise Vault OWA 2007 Extensions x64.msi`

■   `Symantec Enterprise Vault OWA 2007 Extensions x86.msi`

5   Follow the installation instructions.

6   From a browser, enter the URL for the Exchange 2007 CAS server. Open an OWA client and check that you can view archived items.

Upgrading Enterprise Vault OWA 2003 Extensions

For details of the versions of OWA 2003 control files supported by the Enterprise Vault 8.0 SP3 OWA Extensions, see the *Enterprise Vault Compatibility Charts* at http://entsupport.symantec.com/docs/276547.

To upgrade the Enterprise Vault OWA 2003 Extensions

1   Create the file `evservers.txt`.

     See "Creating evservers.txt" on page 105.

2   Install the Symantec Enterprise Vault OWA 2003 Extensions on back-end servers and on front-end servers.

     See "OWA 2003: Installing the Enterprise Vault OWA 2003 Extensions" on page 105.

See the "Installing the Enterprise Vault Extensions on Exchange Server 2003" section in the *Setting up Exchange Server Archiving* manual if you need to do any of the following:

■   Install the Enterprise Vault Extensions on an RPC proxy server.

■   Install the Enterprise Vault Extensions on an RPC target server.

■   Perform a silent installation using the MSI command line.

■   Perform an installation using an Active Directory Group Policy Object (GPO).

Creating evservers.txt

To create 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 (normally `C:\Program Files\Enterprise Vault\OWA 2003 Extensions`).

3 Double-click `MakeEVServersTxt.wsf` to run it. The script creates `evservers.txt` in the same folder as the script itself.

4 If you are installing the Enterprise Vault Extensions remotely using, for example, Active Directory, then you must copy the `evservers.txt` file to the same location as the MSI installation file.

5 If you are installing the Enterprise Vault Extensions interactively on each server, make `evservers.txt` and the MSI installation file available to each back-end Exchange Server 2003.

OWA 2003: Installing the Enterprise Vault OWA 2003 Extensions

Note: If you are installing on a cluster, you must upgrade the appropriate Enterprise Vault OWA extensions on all nodes that could host the Exchange Virtual Server. On a VCS cluster, each node must be the active node at the time of upgrade.

To install the Enterprise Vault OWA 2003 Extensions on each back-end and front-end Exchange Server

1 Start Windows Explorer and navigate to the folder in which you placed `Symantec Enterprise Vault OWA 2003 Extensions.msi` and `evservers.txt`.

2 Double-click `Symantec Enterprise Vault OWA 2003 Extensions.msi` to start the installation.

3 Work through the wizard.

Upgrading Enterprise Vault OWA 2000 Extensions

To upgrade the Enterprise Vault OWA 2000 Extensions

1   Create the file `evservers.txt`.

    See "Creating evservers.txt" on page 106.

2   Install the Symantec Enterprise Vault OWA 2000 Extensions on back-end servers and on front-end servers.

    See "OWA 2000: Installing the Enterprise Vault OWA 2000 Extensions" on page 106.

Creating evservers.txt

To create 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 2000 Extensions` subfolder of the Enterprise Vault installation folder (normally `C:\Program Files\Enterprise Vault\OWA 2000 Extensions`).

3   Double-click `MakeEVServersTxt.wsf` to run it. The script creates `evservers.txt` in the same folder as the script itself.

4   Copy `evservers.txt` and `Symantec Enterprise Vault OWA 2000 Extensions.msi` to a location that can be accessed from your Exchange Server.

5   If you are installing the Enterprise Vault Extensions remotely using, for example, Active Directory, then you must copy the `evservers.txt` file to the same location as the MSI installation file.

OWA 2000: Installing the Enterprise Vault OWA 2000 Extensions

Note: If you are installing on a cluster, you must upgrade the appropriate Enterprise Vault OWA extensions on all nodes that could host the Exchange Virtual Server. On a VCS cluster, each node must be the active node at the time of upgrade.

To install the Enterprise Vault OWA 2000 Extensions on each back-end and front-end Exchange Server

1   Start Windows Explorer and navigate to the folder in which you placed
    `Symantec Enterprise Vault OWA 2000 Extensions.msi` and `evservers.txt`.

2   Double-click `Symantec Enterprise Vault OWA 2000 Extensions.msi` to
    start the installation.

3   Work through the wizard.

Upgrading SharePoint Server components

This chapter includes the following topics:

- About upgrading the SharePoint components
- Upgrading the Enterprise Vault SharePoint components
- Upgrading the Archive Search Web Parts
- Updating the archived versions history link

About upgrading the SharePoint components

If you are upgrading on MOSS 2007 or WSS 3.0, work through the following section:

- Upgrading the Enterprise Vault SharePoint components

If you are upgrading on WSS 2.0 or SPS 2003, work through the following sections:

- Upgrading the Enterprise Vault SharePoint components
- Upgrading the Archive Search Web Parts
- Updating the archived versions history link

Note that when you upgrade on MOSS 2007 or WSS 3.0, the installation includes an Enterprise Vault HttpModule to support the new shortcut functionality.

Upgrading the Enterprise Vault SharePoint components

We recommend that you upgrade the Enterprise Vault SharePoint components on each of your SharePoint Server computers.

To upgrade the Enterprise Vault SharePoint components

1   Log on to the SharePoint Server using the Vault Service account.

2   Load the Enterprise Vault 8.0 SP3 media on your SharePoint server computer.

3   Navigate to the folder `Enterprise Vault 8.0 SP3` > `Server`.

4   Double-click `Setup.exe` to start the installation.

5   On the **Select Components to Install** screen, ensure that only **Microsoft SharePoint Components** is selected.

6   Click **Next**.

7   Work through the remainder of the installation wizard.

If you are upgrading on MOSS 2007 or WSS 3.0, the upgrade is now complete. The Enterprise Vault web parts are upgraded automatically.

If you are upgrading on WSS 2.0 or SPS 2003, continue to the next section.

Upgrading the Archive Search Web Parts

We recommend that you upgrade the Archive Search Web Part on each of your SharePoint Server computers.

Work through this section if you are upgrading on WSS 2.0 or SPS 2003.

To upgrade the Archive Search Web Parts

1   If the language selected for your SharePoint installation is English, go to step 2.

If the language selected for your SharePoint installation is not English, copy the Web Part package `EV_SharepointWebPartsCab.cab` from the appropriate language folder under `C:\Program Files\Enterprise Vault\Languages\Windows SharePoint Services Web Parts` to the folder containing the `Stsadm.exe` tool, which is typically:

```
C:\Program Files\Common Files\Microsoft Shared\Web Server
Extensions\60\BIN
```

2   On the SharePoint server, open a Command Prompt window and then use the `cd` command to go to the directory containing the `Stsadm.exe` tool and the Web Part CAB file, which is typically:

```
C:\Program Files\Common Files\Microsoft Shared\Web Server
Extensions\60\BIN
```

3   Enter the following command to add the new Web Part on every virtual server on the SharePoint server computer:

```
stsadm.exe -o addwppack -globalinstall -force -filename
"ev_sharepointwebpartscab.cab"
```

4   Restart IIS.

Updating the archived versions history link

Work through this section if you are upgrading on WSS 2.0 or SPS 2003.

You need to reinstall the archived version history link. Failure to do this after an upgrade will result in an error when attempting to view the archived version history.

Note that you only need to perform this task once for all of the SharePoint virtual servers on a computer.

To update the archived versions history link

1   In a browser, enter the following URL:

http://*spcomputername*/_layouts/versionsadmin.aspx

where *spcomputername* is the name of your SharePoint server computer.

2   On the **Enterprise Vault Archived Version History Administration** page, click **Install the archived version history link**.