Symantec Enterprise Vault™

Upgrading to Enterprise Vault 11.0.1

Symantec

Symantec Enterprise Vault: Upgrading to Enterprise Vault 11.0.1

Last updated: 2014-11-25.

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 help you resolve specific problems with a Symantec product. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

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

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

www.symantec.com/business/support/

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

Contacting Technical Support

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

www.symantec.com/business/support/

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

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

- Product release level
- Hardware information

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

Licensing and registration

If your Symantec product requires registration or a license key, access our Technical Support web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

Support agreement resources

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

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

Contents

Chapter 1

About this guide

This chapter includes the following topics:

Introducing this guide

This guide describes how to upgrade to Enterprise Vault 11.0.1.

If you are performing a new installation of Enterprise Vault, see the Enterprise Vault 11.0.1 *ReadMeFirst*. Then follow the installation instructions in *Installing and Configuring*, which is in the `Symantec Enterprise Vault\Documentation` folder on the Enterprise Vault 11.0.1 release media.

For the most up-to-date versions of this guide and of the *ReadMeFirst*, see the following page on the Symantec Support website:

http://www.symantec.com/docs/DOC7411

Where to get more information about Enterprise Vault

Table 1-1 lists the documentation that accompanies Enterprise Vault.

Table 1-1 Enterprise Vault documentation set

Document	Comments
Symantec Enterprise Vault Documentation Library	Includes all the following documents in Windows Help (`.chm`) format so that you can search across them all. It also includes links to the guides in Acrobat (`.pdf`) format. You can access the library in several ways, including the following: ■ On the Windows **Start** menu, click **Start** > **Programs** > **Enterprise Vault** > **Documentation**. ■ In Windows Explorer, browse to the `Documentation\`*`language`* subfolder of the Enterprise Vault installation folder, and then open the `EV_Help.chm` file. ■ On the **Help** menu in the Administration Console, click **Help on Enterprise Vault**.
Introduction and Planning	Provides an overview of Enterprise Vault functionality.
Deployment Scanner	Describes how to check the required 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 IMAP	Describes how to configure IMAP client access to Exchange archives, and to Internet mail archives.
Setting up SharePoint Server Archiving	Describes how to archive content from Microsoft SharePoint servers.
Setting up SMTP Archiving	Describes how to archive SMTP messages from other messaging servers.
Administrator's Guide	Describes how to perform day-to-day administration procedures.

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

Document	Comments
Backup and Recovery	Describes how to implement an effective backup strategy to prevent data loss, and how to provide a means for recovery in the event of a system failure.
NSF Migration	Describes how to migrate content from Domino and Notes NSF files into Enterprise Vault archives.
PST Migration	Describes how to migrate content from Outlook PST files into Enterprise Vault archives.
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.
PowerShell Cmdlets	Describes how to perform various administrative tasks by running the Enterprise Vault PowerShell cmdlets.
Registry Values	A reference document that lists the registry values with which you can modify many aspects of Enterprise Vault behavior.
Help for Administration Console	The online Help for the Enterprise Vault Administration Console.
Help for Enterprise Vault Operations Manager	The online Help for Enterprise Vault Operations Manager.

For the latest information on supported devices and versions of software, see the *Enterprise Vault Compatibility Charts* book, which is available from this address:

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

“How To” articles on the Symantec Support website

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

To access the "How To" articles on the Symantec Support website

1. Type the following in the address bar of your web browser, and then press **Enter**:

   http://www.symantec.com/business/support/all_products.jsp

2. In the Supported Products A-Z page, choose the required product, such as Enterprise Vault for Microsoft Exchange.
3. Search for a word or phrase by using the Knowledge Base Search feature, or browse the list of most popular subjects.

Enterprise Vault training modules

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

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

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

Comment on the documentation

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

Please include the following information with your comment:

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

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

We appreciate your feedback.

Chapter 2

Before you begin

This chapter includes the following topics:

Server upgrade paths

This guide describes how to upgrade to Enterprise Vault 11.0.1. The only possible server upgrade paths to this version are from the following:

- Enterprise Vault 10.0 or any Enterprise Vault 10.0 service pack.
- Enterprise Vault 11.0 original release.

If your Enterprise Vault servers are running a version of Enterprise Vault that is older than Enterprise Vault 10.0, you must first upgrade to Enterprise Vault 10.0 and then upgrade to Enterprise Vault 11.0.1.

Note: Enterprise Vault hotfixes that you have installed do not affect the upgrades. You do not have to remove Enterprise Vault hotfixes before you upgrade.

Note: Do not upgrade to Enterprise Vault 10.0 and then immediately upgrade to Enterprise Vault 11.0.1. You must complete the Enterprise Vault 10.0 post-installation tasks as described in the Enterprise Vault 10.0 upgrade instructions, before you upgrade to Enterprise Vault 11.0.1.

Documentation

The Enterprise Vault documentation is in the `Symantec Enterprise Vault\Documentation` folder on the Enterprise Vault 11.0.1 media.

For the latest information on supported software and storage devices, see the *Enterprise Vault Compatibility Charts* at the following page on the Symantec Support website:

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

Chapter 3

Points to note when upgrading from Enterprise Vault 10.0

This chapter includes the following topics:

About this chapter

Read this chapter if you are upgrading from any release of Enterprise Vault 10.0.

Read this chapter before you upgrade. You may need to take action to review or modify your configuration before or after the upgrade.

For a list of the new features and fixes in Enterprise Vault 11.0.1, see the *Enterprise Vault 11.0.1* release notes document.

Order of upgrade in an environment with Compliance Accelerator or Discovery Accelerator

If the Enterprise Vault environment that you are upgrading includes Compliance Accelerator or Discovery Accelerator, you must upgrade the Accelerator versions to 11.0.1 or later.

Compliance Accelerator 11.0.1 works with Enterprise Vault 11.0.1 only, so you must upgrade Enterprise Vault before you upgrade Compliance Accelerator.

Discovery Accelerator 11.0.1 works with Enterprise Vault 10.0.1 and later. The version of Discovery Accelerator can be the same as, but must not be lower than, the version of Enterprise Vault.

The order in which you must upgrade the various components differs from the normal order.

Order in which to perform the upgrade

1. If your environment includes Discovery Accelerator, install Discovery Accelerator 11.0.1 on the Discovery Accelerator server. Then upgrade the Discovery Accelerator databases, and install the Discovery Accelerator 11.0.1 client software on each client computer.
2. Upgrade Enterprise Vault to version 11.0.1 on all Enterprise Vault servers.

   Note: If your environment includes Compliance Accelerator, do not start the Enterprise Vault Storage service on any Enterprise Vault Storage server until you have upgraded to Compliance Accelerator 11.0.1. This ensures that the random sampling feature works seamlessly before and after the upgrade.
3. Upgrade Enterprise Vault to version 11.0.1 on all Compliance Accelerator and Discovery Accelerator servers.
4. If your environment includes Compliance Accelerator, install Compliance Accelerator 11.0.1 on the Compliance Accelerator server. Then upgrade the Compliance Accelerator databases, and install the Compliance Accelerator 11.0.1 client software on each client computer.

   Note the following:

   - Only start the Enterprise Vault Storage service on the Enterprise Vault Storage servers after you have fully upgraded Compliance Accelerator.
   - In Compliance Accelerator 11.0.1, all the functions of the Journaling Connector have been incorporated into Enterprise Vault itself. So, there is no longer a need to configure and maintain one or more Journaling Connector installations. When you upgrade, Compliance Accelerator automatically removes any existing Journaling Connector installation.

For more information on supported versions and upgrade paths, see the *Enterprise Vault Compatibility Charts* at http://www.symantec.com/docs/TECH38537 and the article *Supported upgrade paths for Enterprise Vault, Compliance Accelerator, Discovery Accelerator and Discovery Collector* at http://www.symantec.com/docs/TECH53174.

Admin service TEMP folder security checks

From Enterprise Vault version 11.0.1, the Admin service checks the accounts that have access to the `TEMP` folder, which can contain sensitive data. If the Admin service finds unauthorized access permissions, it writes an error to the event log and terminates immediately.

Access to the TEMP folder must be granted using a SID that is authorized in one of the following ways:

- The SID identifies one of the following: local Administrators group, local Backup Operators group, Domain Admins group, local system, System Operators group.
- The SID identifies one of the accounts that is listed in the TempFolderExceptions registry value.
  For more information, see the section called "Granting additional users and groups access to the TEMP folder" in the *Installing and Configuring* guide.
- Access is granted using the Creator Owner SID, and the current owner of the TEMP folder is allowed access under the previous conditions.
- The SID identifies a user, and it is the same as the SID of the user under which the Admin service is running.

The Enterprise Vault Admin service checks the folder's discretionary access control list (DACL). If there is no DACL, the check fails and the service terminates immediately. If the DACL is present, the Admin service checks the SID in each access control entry (ACE) and terminates immediately if access to the TEMP folder is granted using a SID that is not authorized correctly.

For more information about Enterprise Vault TEMP folder requirements, see the following technical note on the Symantec Support website:

http://www.symantec.com/docs/TECH224726

Clearwell compatibility with Enterprise Vault

For details of the compatibility of Clearwell with Enterprise Vault, see the *Clearwell eDiscovery Platform Compatibility Matrix*, which is available from http://www.symantec.com/docs/TECH211911.

Enabling fast browsing for Enterprise Vault Search

Enterprise Vault can create metadata indexes for use with Enterprise Vault Search. These indexes enable faster browsing of archived items. If there is no metadata index for an archive, Enterprise Vault Search uses the archive's own index but browsing is slower.

When you upgrade from Enterprise Vault 10.0 no archives are enabled for fast browsing.

Fast browsing is always enabled for IMAP.

If you choose to enable fast browsing, you can do so in the following ways:

- Use the Administration Console. You can choose to enable new archives at the time that they are created. On the **Archive Settings** tab of Site properties you can enable all archives of a particular type. For example, you can enable all Exchange mailbox archives.

  You can also enable archives individually, by editing the properties of each archive. This method is not suitable if you need to enable more than a few archives.
- Use a PowerShell script. The New-EVMDSBuildTask PowerShell script lets you enable a large number of archives for fast browsing.

Changes to storage queues

Enterprise Vault 11.0 introduced a new storage queue for each Storage service. Following upgrade, Enterprise Vault creates the new storage queue automatically when you start the Storage service.

For more information, including details of how to change the storage queue location, see “Managing the Storage queue” in the *Administrator’s Guide*.

Exchange Server 2013 support

Enterprise Vault 10.0.3 introduced support for Exchange Server 2013 archiving.

If you plan to implement Exchange 2013 archiving, check that the additional requirements for archiving Exchange Server 2013 targets are satisfied. See “Additional requirements for Exchange Server archiving” in *Installing and Configuring*.

If you use a database availability group (DAG) in your Exchange Server environment, you must set up archiving for all members of the DAG. See “Using Exchange Server database availability groups” in *Setting up Exchange Server Archiving*.

The Enterprise Vault documentation is in the `Symantec Enterprise Vault\Documentation` folder on the Enterprise Vault 11.0.1 media.

For more information about the configuration of Exchange 2013 archiving, see the following article on the Symantec Support website:

http://www.symantec.com/docs/HOWTO82293

Support for Outlook 2013 SP1 on the Enterprise Vault server

Enterprise Vault 11.0.1 supports Outlook 2013 SP1 (32-bit version) on the Enterprise Vault server.

The following versions of Outlook 2013 are not supported:

- Outlook 2013 SP1 (64-bit version)
- Outlook 2013 Original Release

Note: Outlook performance counters must be disabled when Outlook 2013 SP1 is installed on the Enterprise Vault server. The Enterprise Vault Admin service automatically disables the Outlook performance counters if it detects Outlook 2013 on the Enterprise Vault server.

To upgrade to Outlook 2013 SP1

1. Stop the Enterprise Vault Admin service on the Enterprise Vault server.
2. Install Outlook 2013 SP1.
3. Restart all the Enterprise Vault services.

Enterprise Vault 10.0 original release server hotfix required to support the Outlook Add-In

---

Note: This section applies only if you are upgrading from the Enterprise Vault 10.0 original release.

If you plan to roll out the Enterprise Vault 11.0.1 Outlook Add-In to users before you upgrade the Enterprise Vault servers, you must apply a hotfix to the Enterprise Vault servers to avoid the restrictions listed in this section.

The link to the relevant technical note and the hotfix that is required to support the Enterprise Vault 11.0.1 Outlook Add-In with Enterprise Vault server 10.0 original release is as follows:

http://www.symantec.com/docs/TECH175942

The following restrictions apply to the Enterprise Vault 11.0.1 Outlook Add-In if you have not installed the hotfix on Enterprise Vault servers that have not been upgraded:

- You cannot view the Enterprise Vault properties of a mailbox, a mailbox folder, or a public folder. The **Enterprise Vault Properties** page says that the functionality is not available.
- You cannot change the setting of the option to suspend archiving for a mailbox.
- When you store items manually in full mode, Enterprise Vault displays the light mode **Store in Vault** dialog box. The light mode dialog box does not include options to choose a vault or a retention category.

Assigning the required permissions to the Vault Service account

Note: This section applies only if you are upgrading from Enterprise Vault 10.0.3 or later.

From Enterprise Vault 10.0.3 the Enterprise Vault databases contain a set of roles that let you revoke the Vault Service account's ownership of the databases, and assign only the minimum permissions it needs to run Enterprise Vault.

If you have revoked the Vault Service account's ownership of the databases, you must assign the Vault Service account to the EVUpgradeRole before you begin the upgrade.

Revoke the Vault Service account's membership of the EVUpgradeRole when you have completed the upgrade.

For more details, see the following document on the Symantec Support website:

http://www.symantec.com/docs/HOWTO80670

Requirements for upgrading the Enterprise Vault databases

The following sections discuss the additional space requirements for the upgrade of the Enterprise Vault databases.

Note: Enterprise Vault does not let you proceed with the upgrade unless a suitable amount of space is available for the Directory database upgrade.

See "Directory database upgrade requirements" on page 27.

Directory database upgrade requirements

When the Directory service starts for the first time after you install the Enterprise Vault 11.0.1 software, it upgrades the Directory database schema.

The upgrade of the Directory database schema requires additional disk space on the SQL Server computer, mainly for log file growth. You can reclaim most of this additional space by routine database maintenance after the upgrade.

The required amount of space for the upgrade depends on which recovery model the database uses.

Table 3-1 lists the additional space requirements.

Table 3-1 Space required for the upgrade of the Directory database

Directory database recovery model	Required additional space on the volume that holds the database transaction log files
Simple or Bulk-logged	Twice the combined size of the Directory database data files
Full	Four times the combined size of the Directory database data files

Note: Enterprise Vault does not let you proceed with the upgrade unless this additional space is available.

These estimated space requirements are based on the assumption that you perform the recommended maintenance activities when you back up the database before the upgrade.

See "Backing up Enterprise Vault data" on page 39.

The upgrade of a large Directory database may take a long time to complete. The upgrade time depends on the size of the database, the database recovery model, the upgrade path, and the available resources.

Changes to best practice settings

Note: This section applies only if you are upgrading from the Enterprise Vault 10.0 original release.

The Enterprise Vault installation program checks whether the Enterprise Vault uses the best practice registry values. If not all the best practice registry values are set the installation program can set them automatically.

The following changes have been made to the best practice settings:

- New setting: **AttachmentMax**
- New setting: **RecipientMax**
- Changed setting: **MachineQuota**. Changed from 4 GB to 8 GB.

For information about these settings, see the section "Best practice settings for Enterprise Vault servers" in the *Administrator's Guide*.

Changes to index roll-over

Note: This section applies only if you are upgrading from the Enterprise Vault 10.0 original release.

In the Enterprise Vault 10.0 original release there was a single setting that controlled the maximum size of an index volume. In Enterprise Vault 11.0.1 there is a setting for the indexes of each archive type, as follows:

- Maximum items in a mailbox index volume
- Maximum items in a journal index volume
- Maximum items in a public folder index volume
- Maximum items in a SharePoint index volume
- Maximum items in a shared index volume
- Maximum items in a file system index volume

When you install Enterprise Vault 11.0.1, all these settings have a default of 5,000,000 items. If you have previously modified the maximum size of index volumes you must change the appropriate setting after you install Enterprise Vault 11.0.1.

For details of the individual settings, see the section “Computer properties advanced settings” in the *Administrator's Guide*.

Changes to support FSA targets without Administrator privileges for the Vault Service account

Note: The following changes were introduced with Enterprise Vault 10.0.3.

File System Archiving previously required that the Vault Service account was a member of the local Administrators group on target Windows file servers. Now the

Vault Service account can run as a member of the built-in local Print Operators group, with some additional permissions and privileges.

This change enables Enterprise Vault to archive from file servers when the granting of local Administrator rights is not advisable, for example:

- If the file server is a domain controller. An account that is a member of the local Administrators group on a domain controller is promoted to a Domain Administrator, which has far more privileges than Enterprise Vault requires. We recommend that you do not make the Vault Service account a Domain Administrator.
- If your company forbids the granting of local Administrator rights to computer service accounts.

See “Permissions and privileges required by the Vault Service account on Windows file servers” in the *Setting up File System Archiving* guide.

Note the following changes that take effect after an upgrade to Enterprise Vault 10.0.3 or later:

- When you install or upgrade the FSA Agent, Enterprise Vault no longer adds the Vault Service account to the local Administrators group on the file server. Now it adds the Vault Service account to the Print Operators group, and grants the additional required permissions and privileges.
- To install the FSA Agent, or to configure the FSA resource for a file server cluster, you must use an account that is a member of the local Administrators group on the file server or file servers.
- To configure the FSA resource for a file server cluster, the account must also have Full Control permission on the Enterprise Vault server's `FSA Cluster` folder. This folder is in the `Utilities` subfolder of the Enterprise Vault installation folder, for example `C:\Program Files (x86)\Enterprise Vault\Utilities\FSA Cluster`.
- If you change the Vault Service account, you must ensure that the new account is granted the required permissions and privileges on all target Windows file servers. A new utility is provided to help you to perform this task. See “EVFSASetRightsAndPermissions” in the *Utilities* guide.

About upgrading FSA targets that run a Server Core installation of Windows

Note: This section applies if you are upgrading from Enterprise Vault 10.0.2, and you have FSA targets that run a Server Core installation of Windows Server 2008 R2.

Enterprise Vault 10.0.3 added support for File Blocking and FSA Reporting from Server Core installations of some versions of Windows.

If you have Enterprise Vault FSA targets that run a Server Core installation of Windows Server 2008 R2, note that after the upgrade you can configure them for File Blocking or FSA Reporting if you want. After the upgrade these servers can also act as proxy servers for FSA Reporting, and as File Blocking agent servers for NetApp filers.

For more details of the FSA support for Windows Server Core installations at this release, see the Enterprise Vault *Compatibility Charts*, at http://www.symantec.com/docs/TECH38537.

Default File Blocking location is no longer supported

Note: The following changes were introduced with Enterprise Vault 10.0.3

Previously, if neither a local quarantine location nor a central quarantine location was available for File Blocking, Enterprise Vault used the `Quarantine` subfolder of the file server's Enterprise Vault installation folder as a default location.

From Enterprise Vault 10.0.3, File Blocking does not support a default quarantine location. If neither the local quarantine location nor a central quarantine location is available, Enterprise Vault logs an error in the event log and the file is not quarantined.

If you use File Blocking, make sure that suitable quarantine locations are defined and available. To avoid the risk of quarantined files filling the system drive, do not place a quarantine location on the system drive. Specify a location that has sufficient free space to hold the quarantined files, and monitor regularly the space that the quarantined files occupy.

See “Configuring File Blocking” in the *Setting up File System Archiving* guide.

Changes to retention category settings for the deletion of archived items

In the properties of a retention category, the setting **Prevent deletion of archived items in this category** is replaced on upgrade by the following two settings:

- **Prevent automatic deletion of expired items with this category**
- **Prevent user deletion of items with this category**

On upgrade, both of these settings are turned on for an existing retention category if **Prevent deletion of archived items in this category** was turned on.

In File System Archiving note that of the two new settings, only **Prevent user deletion of items with this category** overrides the archiving policy setting **Delete archived file when placeholder is deleted**.

File System Archiving of files under Dynamic Access Control

Note: Read this section if you are upgrading from Enterprise Vault 10.0.3 and you use File System Archiving.

On upgrade, File System Archiving's volume and folder policies include a new option on the **Permissions** tab which lets you choose whether to archive or ignore files that are under Dynamic Access Control (DAC).

The default policy setting is not to archive any files that are under Dynamic Access Control. Note that this is a change in behavior from Enterprise Vault 10.0.3, where File System Archiving did not recognize DAC-related access control entries.

For more information about archiving files that are under Dynamic Access Control, see "About archiving from Windows Server 2012 file servers" in the *Setting up File System Archiving* guide.

Chapter 4

Points to note when upgrading from Enterprise Vault 11.0

This chapter includes the following topics:

About this chapter

Read this chapter before performing the upgrade. You may need to take action to review or modify your configuration before or after the upgrade.

Order of upgrade in an environment with Compliance Accelerator or Discovery Accelerator

If the Enterprise Vault environment that you are upgrading includes Compliance Accelerator or Discovery Accelerator, you must upgrade the Accelerator versions to 11.0.1 or later.

Compliance Accelerator 11.0.1 works with Enterprise Vault 11.0.1 only, so you must upgrade Enterprise Vault before you upgrade Compliance Accelerator.

Discovery Accelerator 11.0.1 works with Enterprise Vault 10.0.1 and later. The version of Discovery Accelerator can be the same as, but must not be lower than, the version of Enterprise Vault.

The order in which you must upgrade the various components differs from the normal order.

Order in which to perform the upgrade

1. If your environment includes Discovery Accelerator, install Discovery Accelerator 11.0.1 on the Discovery Accelerator server. Then upgrade the Discovery Accelerator databases, and install the Discovery Accelerator 11.0.1 client software on each client computer.
2. Upgrade Enterprise Vault to version 11.0.1 on all Enterprise Vault servers.

   Note: If your environment includes Compliance Accelerator, do not start the Enterprise Vault Storage service on any Enterprise Vault Storage server until you have upgraded to Compliance Accelerator 11.0.1. This ensures that the random sampling feature works seamlessly before and after the upgrade.
3. Upgrade Enterprise Vault to version 11.0.1 on all Compliance Accelerator and Discovery Accelerator servers.
4. If your environment includes Compliance Accelerator, install Compliance Accelerator 11.0.1 on the Compliance Accelerator server. Then upgrade the Compliance Accelerator databases, and install the Compliance Accelerator 11.0.1 client software on each client computer.

   Note the following:

   - Only start the Enterprise Vault Storage service on the Enterprise Vault Storage servers after you have fully upgraded Compliance Accelerator.
   - In Compliance Accelerator 11.0.1, all the functions of the Journaling Connector have been incorporated into Enterprise Vault itself. So, there is no longer a need to configure and maintain one or more Journaling Connector installations. When you upgrade, Compliance Accelerator automatically removes any existing Journaling Connector installation.

For more information on supported versions and upgrade paths, see the *Enterprise Vault Compatibility Charts* at http://www.symantec.com/docs/TECH38537 and the article *Supported upgrade paths for Enterprise Vault, Compliance Accelerator, Discovery Accelerator and Discovery Collector* at http://www.symantec.com/docs/TECH53174.

Admin service TEMP folder security checks

From Enterprise Vault version 11.0.1, the Admin service checks the accounts that have access to the TEMP folder, which can contain sensitive data. If the Admin service finds unauthorized access permissions, it writes an error to the event log and terminates immediately.

Access to the TEMP folder must be granted using a SID that is authorized in one of the following ways:

- The SID identifies one of the following: local Administrators group, local Backup Operators group, Domain Admins group, local system, System Operators group.
- The SID identifies one of the accounts that is listed in the TempFolderExceptions registry value.
  For more information, see the section called "Granting additional users and groups access to the TEMP folder" in the *Installing and Configuring* guide.
- Access is granted using the Creator Owner SID, and the current owner of the TEMP folder is allowed access under the previous conditions.
- The SID identifies a user, and it is the same as the SID of the user under which the Admin service is running.

The Enterprise Vault Admin service checks the folder's discretionary access control list (DACL). If there is no DACL, the check fails and the service terminates immediately. If the DACL is present, the Admin service checks the SID in each access control entry (ACE) and terminates immediately if access to the TEMP folder is granted using a SID that is not authorized correctly.

For more information about Enterprise Vault TEMP folder requirements, see the following technical note on the Symantec Support website:

http://www.symantec.com/docs/TECH224726

Support for Outlook 2013 SP1 on the Enterprise Vault server

Enterprise Vault 11.0.1 supports Outlook 2013 SP1 (32-bit version) on the Enterprise Vault server.

The following versions of Outlook 2013 are not supported:

- Outlook 2013 SP1 (64-bit version)
- Outlook 2013 Original Release

Note: Outlook performance counters must be disabled when Outlook 2013 SP1 is installed on the Enterprise Vault server. The Enterprise Vault Admin service automatically disables the Outlook performance counters if it detects Outlook 2013 on the Enterprise Vault server.

To upgrade to Outlook 2013 SP1

1. Stop the Enterprise Vault Admin service on the Enterprise Vault server.
2. Install Outlook 2013 SP1.
3. Restart all the Enterprise Vault services.

Chapter 5

Steps to upgrade your system

This chapter includes the following topics:

Overview of the upgrade process

Overview of the upgrade process

1. Prepare the Enterprise Vault servers for the upgrade:

   See "About Enterprise Vault server preparation" on page 38.

2. Install and configure the Enterprise Vault 11.0.1 server software as described in the appropriate chapter for your installation.

   See "About upgrading a single Enterprise Vault server" on page 43.

   See "About upgrading multiple Enterprise Vault servers" on page 49.

   See "About upgrading a Veritas cluster" on page 55.

   See "About upgrading a Windows Server Failover Cluster" on page 62.

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

   See "Upgrading standalone Administration Consoles" on page 69.

4. Upgrade any computers that are running Enterprise Vault Reporting.

   See "Upgrading Enterprise Vault Reporting" on page 71.

5. Perform the post-installation tasks as necessary:

   - Upgrade Exchange Server forms.

See "About upgrading Exchange Server forms" on page 77.

- Upgrade Domino mailbox archiving.
  See "About upgrading Domino mailbox archiving" on page 78.
- Upgrade the FSA Agent on the Windows servers on which it is installed.
  See "About upgrading the FSA Agent" on page 86.
- Upgrade OWA and RPC extensions.
  See "About upgrading OWA and RPC Extensions" on page 91.
- Upgrade SharePoint Server components.
  See "About upgrading the SharePoint components" on page 96.
- Upgrade SMTP Archiving components.
  See "About upgrading SMTP Archiving" on page 99.
- Upgrade each Enterprise Vault site to use Enterprise Vault Search rather than the legacy search applications (Archive Explorer, Browser Search, and Integrated Search).
  See "About Enterprise Vault Search" on page 100.
- Upgrade Enterprise Vault API applications.
  See "Upgrading any applications that use the Enterprise Vault API Runtime" on page 115.

Chapter 6

Enterprise Vault server preparation

This chapter includes the following topics:

About Enterprise Vault server preparation

Before you upgrade the Enterprise Vault software you must prepare for the upgrade, as described in this chapter.

Perform the following actions in the order they are listed:

- Back up the system.
  See "Backing up the system" on page 39.
- Run Enterprise Vault Deployment Scanner.
  See "Running Enterprise Vault Deployment Scanner" on page 41.
- Set database permissions.
  See "Setting database permissions" on page 41.
- Allow the MSMQ queues to empty.

See "Allowing the MSMQ queues to empty" on page 42.

- Check the archiving and expiry schedules.
  See "Checking the archiving and expiry schedules" on page 42.

Backing up the system

You need to back up your Enterprise Vault data and any changed language files.

If you use SCOM, you may want to back up the management pack.

Backing up Enterprise Vault data

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

See the *Backup and Recovery* guide.

Note: When you back up your databases, perform the recommended database maintenance steps that are described in the following technical note on the Symantec Support website:

http://www.symantec.com/docs/TECH74666

These maintenance steps shrink the database, rebuild the table indexes, and update the database statistics. Such actions enable the upgrade of the databases to proceed more quickly.

When 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 overwrites 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, for example `C:\Program Files (x86)\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.

Backing up the Enterprise Vault 10.0 SCOM management pack

The Enterprise Vault 11.0.1 management pack replaces the Enterprise Vault 10.0 management pack. If you want to keep a copy of the old management pack, copy the `SCOM` subfolder of the Enterprise Vault program folder to another location. For example, if Enterprise Vault is installed in `C:\Program Files\Enterprise Vault (x86)` then the folder to back up is as follows:

```
C:\Program Files\Enterprise Vault (x86)\SCOM
```

Do not restore the backed up files after the upgrade.

Updating required Windows features

The Enterprise Vault Install Launcher can automatically check that a server has the required Windows features and can add any features that are missing.

For details of the features that the Install Launcher can add, see "Automatically preparing an Enterprise Vault server" in the *Installing and Configuring* guide.

To run the Prepare my system option

1. Load the Enterprise Vault media on to the server.
2. If Windows AutoPlay is enabled on the server, Windows shows an AutoPlay dialog box. Click **Run Setup.exe**.

   If AutoPlay is not enabled, use Windows Explorer to open the root folder of the installation media and then double-click the file `Setup.exe`.

   The **Install Launcher** opens.
3. In the list in the left pane of the Install Launcher, click **Enterprise Vault**.
4. Click **Server Preparation**.
5. Click **Prepare my system**. The Windows features are added immediately, with no further prompts. The server may restart automatically after the features have been added.

Running Enterprise Vault Deployment Scanner

Before you upgrade to Enterprise Vault 11.0.1, we strongly recommend that you run Enterprise Vault Deployment Scanner to check required software and settings.

Use the Vault Service account when running 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 technical note for details of how to fix the problem:

http://www.symantec.com/docs/TECH55063

If you make changes to your configuration as a result of running Deployment Scanner, repeat your system backup if necessary.

To run the Deployment Scanner

1. Log in to the Vault Service account.
2. Load the Enterprise Vault media.
3. If Windows AutoPlay is enabled on the server, Windows shows an AutoPlay dialog box. Click **Run Setup.exe**.

   If AutoPlay is not enabled, use Windows Explorer to open the root folder of the installation media and then double-click the file `Setup.exe`.
4. In the left pane of the **Symantec Enterprise Vault Install Launcher** window, click **Enterprise Vault** and then click **Server Preparation**.
5. In the right pane, click **Deployment Scanner** and then click **Run the Deployment Scanner**. The Deployment Scanner starts.

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 technical note on the Symantec Support website:

http://www.symantec.com/docs/TECH65841

Allowing the MSMQ queues to empty

Before you upgrade to Enterprise Vault 11.0.1, we recommend that you allow the MSMQ queues to empty.

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

Checking the archiving and expiry schedules

To allow time to examine the new installation before archiving starts, you may want to disable archiving and expiry before you upgrade the servers. You can enable the servers again when you have checked the installation.

Chapter 7

Single server: upgrading the Enterprise Vault server software

This chapter includes the following topics:

About upgrading a single Enterprise Vault server

This chapter describes how to upgrade the Enterprise Vault server software and databases when you have only one server that runs Enterprise Vault services.

Perform the procedures in this chapter in the order that they are listed.

Installing the Enterprise Vault 11.0.1 server software on a single server

This section describes how to install the Enterprise Vault 11.0.1 server software when you have only one server that runs Enterprise Vault services.

To install the Enterprise Vault 11.0.1 server software on a single server

1. Log on to the Enterprise Vault server 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 use Enterprise Vault. For example:
   - Enterprise Vault Administration Console
   - Enterprise Vault Accelerator Manager service
4. Close any other applications that may be running on the server, including the Control Panel, Computer Management, Windows Services, and the Windows Event Viewer.
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 11.0.1 media.
7. If Windows AutoPlay is enabled on the server, Windows shows an AutoPlay dialog box. Click **Run Setup.exe**.

   If AutoPlay is not enabled, use Windows Explorer to open the root folder of the installation media and then double-click the file `Setup.exe`.
8. In the list in the left pane of the **Symantec Enterprise Vault Install Launcher** window, click **Enterprise Vault**.
9. Click **Server Installation**.
10. In the right pane, click **Upgrade existing server**.
11. Click **Install**. The Enterprise Vault installation wizard starts.
12. Work through the installation wizard to upgrade the Enterprise Vault components.
13. If the installation wizard prompts you to restart the server, restart and then log on again as the Vault Service account so that the installer can complete the upgrade.

Upgrading the Directory database and the Storage databases

Enterprise Vault 11.0 introduced a new utility to upgrade the Directory database and Storage databases. Database Upgrader is a command line utility that is faster and more convenient than the older upgrade mechanism.

Database Upgrader upgrades the Enterprise Vault databases in the following order:

- Directory database
- Vault store databases (processed simultaneously)
- Vault store group databases (processed simultaneously)

Running Enterprise Vault Database Upgrader

To run Database Upgrader

1. Stop all Enterprise Vault services. If more than one site uses the same Enterprise Vault Directory database, stop all Enterprise Vault services in all the sites.
2. Log on to any Enterprise Vault server as the Vault Service account.
3. Open a Command Prompt window with administrator privileges.
4. In the Command Prompt window, change to the Enterprise Vault installation folder (for example, `C:\Program Files (x86)\Enterprise Vault`).
5. Enter the following command:

   ```
   EVDatabaseUpgrader
   ```

   Note: Do not start more than one instance of Database Upgrader.

Database Upgrader provides logging information to show the progress of the database upgrade.

Monitoring the progress of Database Upgrader

Database Upgrader provides the following progress information:

- Progress text in the Command Prompt window.
- In the Enterprise Vault Event Log, event 41522 at the start of each database upgrade.
- Event 41523 after the successful upgrade of each database.

- Event 13399 at the start of each database upgrade script. There may be several of these events for each database.
- Event 13400 at the end of each database upgrade script. There may be several of these events for each database.
- A detailed log file in the Enterprise Vault `Reports` folder.

Upgrading the auditing database

If you upgrade a system that uses Enterprise Vault auditing, upgrade the Enterprise Vault auditing database manually as follows.

To upgrade the auditing database

1. Make sure that you have backed up the **EnterpriseVaultAudit** database.
2. Make sure that the Enterprise Vault services are stopped.
3. Start SQL Server Management Studio, and in the left pane under **Databases** select the EnterpriseVaultAudit database.
4. From the **File** menu, click **Open** > **File**.
5. Navigate to the Enterprise Vault installation folder (typically `C:\Program Files (x86)\Enterprise Vault`) and select the file `Audit_Schema_Upgrade.sql`. Click **Open**.
6. From the **Query** menu, click **Execute**.

   After a short time SQL Server Management Studio indicates that the query has completed successfully.
7. From the **File** menu, click **Open** > **File**.
8. In the installation folder, select the file `AuditDBRoles.sql`. Click **Open**.
9. From the **Query** menu, click **Execute**.

   After a short time SQL Server Management Studio indicates that the query has completed successfully.
10. Exit from SQL Server Management Studio.

Upgrading the Monitoring and Reporting databases

1. Start the Directory service on one Enterprise Vault server.
2. Wait for the following events to be logged in the Symantec Enterprise Vault event log:
   - Event 41121

- (If FSA Reporting is installed) Event 24576

Backing up the upgraded Enterprise Vault databases

Back up the upgraded Enterprise Vault databases as follows.

To back up the upgraded Enterprise Vault databases

1. Stop any running Enterprise Vault services on the Enterprise Vault server.
2. Back up all Enterprise Vault databases.

Upgrading indexing metadata and schema version

Note: This section does not apply if you are upgrading from Enterprise Vault 10.0.3 or later.

Because of an index schema update you must upgrade the indexing metadata.

The index upgrade may take some time. For example, an Enterprise Vault server with the minimum recommended specification may take 40 minutes or longer to process 5,000 index volumes.

During the upgrade the Indexing service logs progress events every 10 minutes.

To upgrade the index metadata and schema version, do the following on each Enterprise Vault Index server

1. Start the Enterprise Vault Directory service and the Indexing service. The Indexing service automatically upgrades index metadata.

   The following events are logged:

   ```
   Event 41395 Index Volume metadata upgrade required
   Event 41372 Index Volume metadata synchronization started
   ```

2. Wait for one of the following events to be logged:

   ```
   Event 41373 Index Volume metadata synchronization completed
   Event 41377 Index Volume metadata synchronization completed
   ```

   The metadata upgrade is now complete.

3 The Indexing service now upgrades the schema version in index volumes.

The following events are logged:

```
Event 41465 Enterprise Vault will now upgrade n index volumes
Event 41467 Enterprise Vault has completed the upgrade
            of index volumes with the latest schema version
```

The index volumes cannot be upgraded when they are in read-only mode, offline mode, or backup mode. If event 41467 indicates that some volumes could not be upgraded, those volumes will be upgraded when they are next loaded.

4 When the indexing upgrade is complete the following event is logged:

```
Event 41302 The Indexing Service has completed its initialization
```

Starting all the Enterprise Vault services

Caution: If your Enterprise Vault environment includes Compliance Accelerator, do not start the Enterprise Vault Storage service and Task Controller service until you have upgraded to Compliance Accelerator 11.0.1. This ensures that all the randomly-sampled items that Compliance Accelerator collects for monitored employees are correctly tagged with the employees' department IDs.

Start all the Enterprise Vault services on the Enterprise Vault server.

Chapter 8

Multiple servers: upgrading the Enterprise Vault server software

This chapter includes the following topics:

About upgrading multiple Enterprise Vault servers

This chapter describes how to upgrade the Enterprise Vault server software and databases, when you have multiple servers that run Enterprise Vault services.

Perform the procedures in this chapter in the order that they are listed.

Installing the Enterprise Vault 11.0.1 server software on multiple servers

The following procedure describes how to install the Enterprise Vault 11.0.1 server software on all the servers that run Enterprise Vault services.

Perform the following procedure on each computer on which the Enterprise Vault services are installed.

To install the Enterprise Vault 11.0.1 server software

1. Log on to the Enterprise Vault server 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 use Enterprise Vault. For example:
   - Enterprise Vault Administration Console
   - Enterprise Vault Accelerator Manager service
4. Close any other applications that may be running on the server, including the Control Panel, Computer Management, Windows Services, and the Windows Event Viewer.
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 11.0.1 media.
7. If Windows AutoPlay is enabled on the server, Windows shows an AutoPlay dialog box. Click **Run Setup.exe**.

   If AutoPlay is not enabled, use Windows Explorer to open the root folder of the installation media and then double-click the file `Setup.exe`.
8. In the list in the left pane of the **Symantec Enterprise Vault Install Launcher** window, click **Enterprise Vault**.
9. Click **Server Installation**.
10. In the right pane, click **Upgrade existing server**.
11. Click **Install**. The Enterprise Vault installation wizard starts.
12. Work through the installation wizard to upgrade the Enterprise Vault components.

13 If the installation wizard prompts you to restart the server, restart and then log on again as the Vault Service account so that the installer can complete the upgrade.

14 When the installation is complete, the installer re-enables the Enterprise Vault services. Do not start any Enterprise Vault services at this time.

15 Repeat this procedure on every computer on which the Enterprise Vault services are installed.

Upgrading the Directory database and the Storage databases

Enterprise Vault 11.0 introduced a new utility to upgrade the Directory database and Storage databases. Database Upgrader is a command line utility that is faster and more convenient than the older upgrade mechanism.

Database Upgrader upgrades the Enterprise Vault databases in the following order:

- Directory database
- Vault store databases (processed simultaneously)
- Vault store group databases (processed simultaneously)

Running Enterprise Vault Database Upgrader

To run Database Upgrader

1 Stop all Enterprise Vault services on all servers in the Enterprise Vault site. If more than one site uses the same Enterprise Vault Directory database, stop all Enterprise Vault services in all the sites.

2 Log on to any Enterprise Vault server as the Vault Service account.

3 Open a Command Prompt window with administrator privileges.

4 In the Command Prompt window, change to the Enterprise Vault installation folder (for example, `C:\Program Files (x86)\Enterprise Vault`).

5 Enter the following command:

```
EVDatabaseUpgrader
```

Note: Do not start more than one instance of Database Upgrader.

Database Upgrader provides logging information to show the progress of the database upgrade.

Monitoring the progress of Database Upgrader

Database Upgrader provides the following progress information:

- Progress text in the Command Prompt window.
- In the Enterprise Vault Event Log, event 41522 at the start of each database upgrade.
- Event 41523 after the successful upgrade of each database.
- Event 13399 at the start of each database upgrade script. There may be several of these events for each database.
- Event 13400 at the end of each database upgrade script. There may be several of these events for each database.
- A detailed log file in the Enterprise Vault `Reports` folder.

Upgrading the auditing database

If you upgrade a system that uses Enterprise Vault auditing, upgrade the Enterprise Vault auditing database manually as follows.

To upgrade the auditing database

1. Make sure that you have backed up the **EnterpriseVaultAudit** database.
2. Make sure that all the Enterprise Vault services are stopped on all Enterprise Vault servers.
3. Start SQL Server Management Studio, and in the left pane under **Databases** select the **EnterpriseVaultAudit** database.
4. From the **File** menu, click **Open** > **File**.
5. Navigate to the Enterprise Vault installation folder (typically `C:\Program Files (x86)\Enterprise Vault`) and select the file `Audit_Schema_Upgrade.sql`. Click **Open**.
6. From the **Query** menu, click **Execute**.

   After a short time SQL Server Management Studio indicates that the script has completed successfully.
7. From the **File** menu, click **Open** > **File**.
8. In the installation folder, select the file `AuditDBRoles.sql`. Click **Open**.

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

After a short time SQL Server Management Studio indicates that the query has completed successfully.

10 Exit from SQL Server Management Studio.

Upgrading the Monitoring and Reporting databases

1 Start the Directory service on one Enterprise Vault server.

2 Wait for the following events to be logged in the Symantec Enterprise Vault event log:

- Event 41121
- (If FSA Reporting is installed) Event 24576

Backing up the upgraded Enterprise Vault databases

Back up the upgraded Enterprise Vault databases as follows.

To back up the upgraded Enterprise Vault databases

1 Stop any running Enterprise Vault services on the Enterprise Vault servers.

2 Back up all Enterprise Vault databases.

Upgrading indexing metadata and schema version

Note: This section does not apply if you are upgrading from Enterprise Vault 10.0.3 or later.

Because of an index schema update you must upgrade the indexing metadata.

The index upgrade may take some time. For example, an Enterprise Vault server with the minimum recommended specification may take 40 minutes or longer to process 5,000 index volumes.

During the upgrade the Indexing service logs progress events every 10 minutes.

To upgrade the index metadata and schema version, do the following on each Enterprise Vault Index server

1. Start the Enterprise Vault Directory service and Indexing service. The Indexing service automatically upgrades index metadata.

   The following events are logged:

   ```
   Event 41395 Index Volume metadata upgrade required
   Event 41372 Index Volume metadata synchronization started
   ```

2. Wait for one of the following events to be logged:

   ```
   Event 41373 Index Volume metadata synchronization completed
   Event 41377 Index Volume metadata synchronization completed
   ```

   The metadata upgrade is now complete.

3. The Indexing service now upgrades the schema version in index volumes.

   The following events are logged:

   ```
   Event 41465 Enterprise Vault will now upgrade n index volumes
   Event 41467 Enterprise Vault has completed the upgrade
               of index volumes with the latest schema version
   ```

   The index volumes cannot be upgraded when they are in read-only mode, offline mode, or backup mode. If event 41467 indicates that some volumes could not be upgraded, those volumes will be upgraded when they are next loaded.

4. When the indexing upgrade is complete the following event is logged:

   ```
   Event 41302 The Indexing Service has completed its initialization
   ```

Starting all the Enterprise Vault services

Caution: If your Enterprise Vault environment includes Compliance Accelerator, do not start the Enterprise Vault Storage service and Task Controller service until you have upgraded to Compliance Accelerator 11.0.1. This ensures that all the randomly-sampled items that Compliance Accelerator collects for monitored employees are correctly tagged with the employees' department IDs.

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

Chapter 9

Veritas Cluster Server: upgrading the Enterprise Vault server software

This chapter includes the following topics:

About upgrading a Veritas cluster

This chapter describes how to upgrade the Enterprise Vault server software and databases, when the servers that run Enterprise Vault tasks are part of a Veritas cluster.

Perform the procedures in this chapter in the order that they are listed.

Installing the Enterprise Vault 11.0.1 server software

This section describes how to install the Enterprise Vault 11.0.1 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 server software on all nodes in the cluster before you start Enterprise Vault services or run the configuration wizard.

To install the Enterprise Vault 11.0.1 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 the following important points:

   - 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.
   - 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.
   - 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
4. Close any applications that may be running on the server, including the Control Panel, Computer Management, Windows Services, and the Windows Event Viewer.
5. Load the Enterprise Vault 11.0.1 media.
6. If Windows AutoPlay is enabled on the server, Windows shows an AutoPlay dialog box. Click **Run Setup.exe**.

   If AutoPlay is not enabled, use Windows Explorer to open the root folder of the installation media and then double-click the file `Setup.exe`.
7. In the list in the left pane of the **Symantec Enterprise Vault Install Launcher** window, click **Enterprise Vault**.
8. Click **Server Installation**.

9 In the right pane, click **Upgrade existing server**.

10 Click **Install**. The Enterprise Vault installation wizard starts.

11 Work through the installation wizard to upgrade the Enterprise Vault components.

12 If the installation wizard prompts you to restart the server, restart and then log on again as the Vault Service account so that the installer can complete the upgrade.

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

Upgrading the Directory database and the Storage databases

Enterprise Vault 11.0 introduced a new utility to upgrade the Directory database and Storage databases. Database Upgrader is a command line utility that is faster and more convenient than the older upgrade mechanism.

Database Upgrader upgrades the Enterprise Vault databases in the following order:

- Directory database
- Vault store databases (processed simultaneously)
- Vault store group databases (processed simultaneously)

Running Enterprise Vault Database Upgrader

To run Database Upgrader

1 Stop all Enterprise Vault services on all servers in the Enterprise Vault site. If more than one site uses the same Enterprise Vault Directory database, stop all Enterprise Vault services in all the sites.

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

3 Open a Command Prompt window with administrator privileges.

4 In the Command Prompt window, change to the Enterprise Vault installation folder (for example, `C:\Program Files (x86)\Enterprise Vault`).

5 Enter the following command:

```
EVDatabaseUpgrader
```

Note: Do not start more than one instance of Database Upgrader.

Database Upgrader provides logging information to show the progress of the database upgrade.

Monitoring the progress of Database Upgrader

Database Upgrader provides the following progress information:

- Progress text in the Command Prompt window.
- In the Enterprise Vault Event Log, event 41522 at the start of each database upgrade.
- Event 41523 after the successful upgrade of each database.
- Event 13399 at the start of each database upgrade script. There may be several of these events for each database.
- Event 13400 at the end of each database upgrade script. There may be several of these events for each database.
- A detailed log file in the Enterprise Vault `Reports` folder.

Upgrading the auditing database

If you upgrade a system that uses Enterprise Vault auditing, upgrade the Enterprise Vault auditing database manually as follows.

To upgrade the auditing database

1. Make sure that you have backed up the **EnterpriseVaultAudit** database.
2. Stop all the Enterprise Vault services.
3. Start SQL Server Management Studio, and in the left pane under **Databases** select the **EnterpriseVaultAudit** database.
4. From the **File** menu, click **Open** > **File**.
5. Navigate to the Enterprise Vault installation folder (typically `C:\Program Files (x86)\Enterprise Vault`) and select the file `Audit_Schema_Upgrade.sql`. Click **Open**.
6. From the **Query** menu, click **Execute**.

   After a short time SQL Server Management Studio indicates that the script has completed successfully.
7. From the **File** menu, click **Open** > **File**.
8. In the installation folder, select the file `AuditDBRoles.sql`. Click **Open**.

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

After a short time SQL Server Management Studio indicates that the query has completed successfully.

10 Exit from SQL Server Management Studio.

Upgrading the Monitoring and Reporting databases

1 On the active node, use the cluster administration tool to bring the Admin service and Directory service resources online.

2 Wait for the following events to be logged in the Symantec Enterprise Vault event log:

- Event 41121
- (If FSA Reporting is installed) Event 24576

Backing up the upgraded Enterprise Vault databases

Back up the upgraded Enterprise Vault databases as follows.

To back up the upgraded Enterprise Vault databases

1 Use the cluster administration tool to take any running Enterprise Vault services offline.

2 Back up all Enterprise Vault databases.

Upgrading indexing metadata and schema version

Note: This section does not apply if you are upgrading from Enterprise Vault 10.0.3 or later.

Because of an index schema update you must upgrade the indexing metadata.

The index upgrade may take some time. For example, an Enterprise Vault server with the minimum recommended specification may take 40 minutes or longer to process 5,000 index volumes.

During the upgrade the Indexing service logs progress events every 10 minutes.

To start the Admin and Directory services

- On the active node, use the cluster administration tools to bring the Admin service and Directory service resources online.

To upgrade the index metadata and schema version, do the following on each Enterprise Vault Index server

1. Start the Enterprise Vault Indexing service. The Indexing service automatically upgrades index metadata.

   The following events are logged:

   ```
   Event 41395 Index Volume metadata upgrade required
   Event 41372 Index Volume metadata synchronization started
   ```

2. Wait for one of the following events to be logged:

   ```
   Event 41373 Index Volume metadata synchronization completed
   Event 41377 Index Volume metadata synchronization completed
   ```

   The metadata upgrade is now complete.

3. The Indexing service now upgrades the schema version in index volumes.

   The following events are logged:

   ```
   Event 41465 Enterprise Vault will now upgrade n index volumes
   Event 41467 Enterprise Vault has completed the upgrade
               of index volumes with the latest schema version
   ```

   The index volumes cannot be upgraded when they are in read-only mode, offline mode, or backup mode. If event 41467 indicates that some volumes could not be upgraded, those volumes will be upgraded when they are next loaded.

4. When the indexing upgrade is complete the following event is logged:

   ```
   Event 41302 The Indexing Service has completed its initialization
   ```

Starting all the Enterprise Vault services

Caution: If your Enterprise Vault environment includes Compliance Accelerator, do not start the Enterprise Vault Storage service and Task Controller service until you have upgraded to Compliance Accelerator 11.0.1. This ensures that all the randomly-sampled items that Compliance Accelerator collects for monitored employees are correctly tagged with the employees' department IDs.

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

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

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

Test that the cluster failover works correctly for Enterprise Vault.

Chapter 10

Windows Server Failover Clustering: upgrading the Enterprise Vault server software

This chapter includes the following topics:

About upgrading a Windows Server Failover Cluster

This chapter describes how to upgrade the Enterprise Vault server software and databases, when the servers that run Enterprise Vault tasks are part of a Windows cluster.

Perform the procedures in this chapter in the order that they are listed.

Installing the Enterprise Vault 11.0.1 server software

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

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

To install the Enterprise Vault 11.0.1 server software

1. Log on to the active node as the Vault Service account.
2. Use Failover Cluster Manager or the command line utility `cluster` to take the Admin service resource offline. This takes all the Enterprise Vault services offline.

   Note the following important points:

   - Do not take the EnterpriseVaultServerInstance offline.
   - 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.
   - 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.
   - 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 Failover Cluster Manager to stop clustered services. For example:

   - Enterprise Vault Administration Console
   - Enterprise Vault Accelerator Manager service
4. Close any applications that may be running on the server, including the Control Panel, Computer Management, Windows Services, and the Windows Event Viewer.
5. Load the Enterprise Vault 11.0.1 media.
6. If Windows AutoPlay is enabled on the server, Windows shows an AutoPlay dialog box. Click **Run Setup.exe**.

   If AutoPlay is not enabled, use Windows Explorer to open the root folder of the installation media and then double-click the file `Setup.exe`.

7 In the list in the left pane of the **Symantec Enterprise Vault Install Launcher** window, click **Enterprise Vault**.

8 Click **Server Installation**.

9 In the right pane, click **Upgrade existing server**.

10 Click **Install**. The Enterprise Vault installation wizard starts.

11 Work through the installation wizard to upgrade the Enterprise Vault components.

12 If the installation wizard prompts you to restart the server, restart and then log on again as the Vault Service account so that the installer can complete the upgrade.

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

Upgrading the Directory database and the Storage databases

Enterprise Vault 11.0 introduced a new utility to upgrade the Directory database and Storage databases. Database Upgrader is a command line utility that is faster and more convenient than the older upgrade mechanism.

Database Upgrader upgrades the Enterprise Vault databases in the following order:

- Directory database
- Vault store databases (processed simultaneously)
- Vault store group databases (processed simultaneously)

Running Enterprise Vault Database Upgrader

To run Database Upgrader

1 Stop all Enterprise Vault services on all servers in the Enterprise Vault site. If more than one site uses the same Enterprise Vault Directory database, stop all Enterprise Vault services in all the sites.

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

3 Open a Command Prompt window with administrator privileges.

4 In the Command Prompt window, change to the Enterprise Vault installation folder (for example, `C:\Program Files (x86)\Enterprise Vault`).

5 Enter the following command:

```
EVDatabaseUpgrader
```

Note: Do not start more than one instance of Database Upgrader.

Database Upgrader provides logging information to show the progress of the database upgrade.

Monitoring the progress of Database Upgrader

Database Upgrader provides the following progress information:

- Progress text in the Command Prompt window.
- In the Enterprise Vault Event Log, event 41522 at the start of each database upgrade.
- Event 41523 after the successful upgrade of each database.
- Event 13399 at the start of each database upgrade script. There may be several of these events for each database.
- Event 13400 at the end of each database upgrade script. There may be several of these events for each database.
- A detailed log file in the Enterprise Vault `Reports` folder.

Upgrading the auditing database

If you upgrade a system that uses Enterprise Vault auditing, upgrade the Enterprise Vault auditing database manually as follows.

To upgrade the auditing database

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

2 Stop all the Enterprise Vault services.

3 Start SQL Server Management Studio, and in the left pane under **Databases** select the **EnterpriseVaultAudit** database.

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

5 Navigate to the Enterprise Vault installation folder (typically `C:\Program Files (x86)\Enterprise Vault`) and select the file `Audit_Schema_Upgrade.sql`. Click **Open**.

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

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

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

8 In the installation folder, select the file `AuditDBRoles.sql`. Click **Open**.

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

After a short time SQL Server Management Studio indicates that the query has completed successfully.

10 Exit from SQL Server Management Studio.

Upgrading the Monitoring and Reporting databases

1 On the active node, use the cluster administration tool to bring the Admin service and Directory service resources online.

2 Wait for the following events to be logged in the Symantec Enterprise Vault event log:

- Event 41121
- (If FSA Reporting is installed) Event 24576

Backing up the upgraded Enterprise Vault databases

Back up the upgraded Enterprise Vault databases as follows.

To back up the upgraded Enterprise Vault databases

1 Stop any running Enterprise Vault services.

2 Back up all Enterprise Vault databases.

Upgrading indexing metadata and schema version

Note: This section does not apply if you are upgrading from Enterprise Vault 10.0.3 or later.

Because of an index schema update you must upgrade the indexing metadata.

The index upgrade may take some time. For example, an Enterprise Vault server with the minimum recommended specification may take 40 minutes or longer to process 5,000 index volumes.

During the upgrade the Indexing service logs progress events every 10 minutes.

To start the Admin and Directory services

- On the active node, use the cluster administration tools to bring the Admin service and Directory service resources online.

To upgrade the index metadata and schema version, do the following on each Enterprise Vault Index server

1. Start the Enterprise Vault Indexing service. The Indexing service automatically upgrades index metadata.

   The following events are logged:

   ```
   Event 41395 Index Volume metadata upgrade required
   Event 41372 Index Volume metadata synchronization started
   ```

2. Wait for one of the following events to be logged:

   ```
   Event 41373 Index Volume metadata synchronization completed
   Event 41377 Index Volume metadata synchronization completed
   ```

   The metadata upgrade is now complete.

3. The Indexing service now upgrades the schema version in index volumes.

   The following events are logged:

   ```
   Event 41465 Enterprise Vault will now upgrade n index volumes
   Event 41467 Enterprise Vault has completed the upgrade
               of index volumes with the latest schema version
   ```

   The index volumes cannot be upgraded when they are in read-only mode, offline mode, or backup mode. If event 41467 indicates that some volumes could not be upgraded, those volumes will be upgraded when they are next loaded.

4. When the indexing upgrade is complete the following event is logged:

   ```
   Event 41302 The Indexing Service has completed its initialization
   ```

Starting all the Enterprise Vault services

Caution: If your Enterprise Vault environment includes Compliance Accelerator, do not start the Enterprise Vault Storage service and Task Controller service until you have upgraded to Compliance Accelerator 11.0.1. This ensures that all the randomly-sampled items that Compliance Accelerator collects for monitored employees are correctly tagged with the employees' department IDs.

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

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

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

Test that the cluster failover works correctly for Enterprise Vault.

Chapter 11

Upgrading standalone Administration Consoles

This chapter includes the following topics:

Upgrading standalone Administration Consoles

If you have any computers on which only the Enterprise Vault Administration Console component is installed, you must upgrade the standalone Administration Console.

Note that the supported versions of Windows for standalone Administration Consoles have changed for Enterprise Vault 11.0. A standalone Administration Console must run one of the following versions of Windows:

- Windows 7
- Windows 8
- Windows Server 2008 R2
- Windows Server 2012

To upgrade a standalone Administration Console

1. Log on to the computer as the Vault Service account.
2. Make sure that the Administration Console is not running.
3. Load the Enterprise Vault 11.0.1 media.
4. If Windows AutoPlay is enabled on the server, Windows shows an AutoPlay dialog box. Click **Run Setup.exe**.

   If AutoPlay is not enabled, use Windows Explorer to open the root folder of the installation media and then double-click the file `Setup.exe`.

5 In the list in the left pane of the **Symantec Enterprise Vault Install Launcher** window, click **Enterprise Vault**.

6 Click **Server Installation**.

7 In the right pane, click **Upgrade existing server**.

8 Click **Install**. The Enterprise Vault installation wizard starts.

9 Work through the installation to upgrade the Administration Console component.

Chapter 12

Upgrading Enterprise Vault Reporting

This chapter includes the following topics:

Upgrading Enterprise Vault Reporting

You must upgrade Enterprise Vault Reporting on the computers on which it is installed.

Table 12-1 lists the steps that are required to upgrade Enterprise Vault Reporting.

Table 12-1 Steps to install Enterprise Vault Reporting

Step	Action	Description
Step 1	Install the Enterprise Vault 11.0.1 Reporting component on each computer on which the Enterprise Vault Reporting component is installed.	See "Installing the Enterprise Vault Reporting component" on page 72.
Step 2	Run the Enterprise Vault Reporting Configuration utility on each computer on which the Enterprise Vault Reporting component is installed.	See "Running the Enterprise Vault Reporting Configuration utility" on page 72.

Installing the Enterprise Vault Reporting component

You must install the Enterprise Vault 11.0.1 Reporting component on each computer on which the Enterprise Vault Reporting component is already installed.

If the Reporting component is installed on an Enterprise Vault server, you can install the Enterprise Vault 11.0.1 Reporting component when you install the other Enterprise Vault components.

Use the following procedure to install the Enterprise Vault Reporting component on any additional computers on which it is installed.

To install the Enterprise Vault Reporting component

1. Log on to the computer with the Vault Service account.
2. Load the Enterprise Vault 11.0.1 media.
3. If Windows AutoPlay is enabled on the server, Windows shows an AutoPlay dialog box. Click **Run Setup.exe**.

   If AutoPlay is not enabled, use Windows Explorer to open the root folder of the installation media and then double-click the file `Setup.exe`.
4. In the list in the left pane of the **Symantec Enterprise Vault Install Launcher** window, click **Enterprise Vault**.
5. Click **Server Installation**.
6. In the right pane, click **Upgrade existing server**.
7. Click **Install**. The Enterprise Vault installation wizard starts.
8. Work through the installation to upgrade the Enterprise Vault Reporting component.

Running the Enterprise Vault Reporting Configuration utility

Perform the following procedure on each computer on which the Enterprise Vault Reporting component is installed. Do not run the utility until you have done the following:

- Installed the Enterprise Vault 11.0.1 software on the Enterprise Vault servers.
- Installed the Enterprise Vault 11.0.1 Reporting component on each computer on which the Reporting component is installed.

To run the Enterprise Vault Reporting Configuration utility

1. Start the Reporting Configuration utility, **Enterprise Vault Reports Configuration**.
2. Select **Configure Reporting and deploy or upgrade reports**.
3. Type the domain, user name, and password for the Reporting user account.
4. Select the SQL Server 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.

   If the Reporting Configuration utility indicates that there was an error deploying Enterprise Vault reports, see the following technical note on the Symantec Support website:

   http://www.symantec.com/docs/TECH51288

   The Enterprise Vault Reporting Configuration utility synchronizes the report security settings with the current administrator roles. If you subsequently add, remove, or modify roles from Authorization Manager in the Administration Console, Enterprise Vault must synchronize Enterprise Vault Reporting again to reflect the changes.

   See "Enabling the synchronization of Enterprise Vault Reporting roles-based security" in the *Reporting* guide.

Chapter 13

Upgrading MOM and SCOM

This chapter includes the following topics:

Upgrading MOM

If you use Microsoft Operations Manager (MOM) 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.

Upgrading the Enterprise Vault SCOM management pack

You must install the new Enterprise Vault management pack to use the improved monitoring.

About the supplied management packs

Table 13-1 describes the management packs that come with Enterprise Vault.

Table 13-1 SCOM management packs in Enterprise Vault

Management pack	Description
Symantec.EnterpriseVault.Latest.mp	Required for monitoring Enterprise Vault 11.0.1. Importing the pack creates an **Enterprise Vault 11** node under the **Symantec Enterprise Vault** node in SCOM.
Symantec.EnterpriseVault.mp	Required for monitoring Enterprise Vault 10.0.4 and earlier. Importing the pack creates **Enterprise Vault 10** and **Enterprise Vault 9.0-10.0.2** nodes under the **Symantec Enterprise Vault** node in SCOM, where the first of these nodes is for Enterprise Vault 10.0.3 and 10.0.4 monitoring. The pack is an updated version of the pack that accompanied Enterprise Vault 10.0.4. It does not provide the new monitoring facilities in the 11.0.1 pack.
Symantec.EnterpriseVault.Library.mp	A common library that is required for monitoring all versions of Enterprise Vault.
Symantec.EnterpriseVault.Reports.mp	Required so that reports can be viewed.

You must import both the Symantec.EnterpriseVault.Latest.mp and Symantec.EnterpriseVault.Library.mp packs to implement the new monitoring facilities in Enterprise Vault 11.0.1. In an environment where you have both Enterprise Vault 10.0 servers and Enterprise Vault 11.0.1 servers, you can import all three packs to monitor both sets of servers.

About the upgrade procedure

The upgrade procedure for the Enterprise Vault management pack depends on which version of Operations Manager you use, as follows:

- If you use Operations Manager 2012, you can import the Enterprise Vault 11.0.1 management pack without first deleting the previous management pack.
- If you use Operations Manager 2007 R2, you must delete any Enterprise Vault 10.0 management pack before you import the Enterprise Vault 11.0.1 management pack.

After you have imported the required packs then, in SCOM, you must re-associate the Run As account to which you have assigned the Monitoring Application role with the Symantec Enterprise Vault Monitoring Run As profile. The *Administrator's Guide* describes how to do this.

To delete the previous Enterprise Vault management pack in Operations Manager 2007 R2

1. In the Operations console, click the **Administration** button.
2. In the **Administration** list, click **Management Packs**.
3. In the **Management Packs** pane, right-click the Enterprise Vault management pack and then click **Delete**.

   If any other management packs depend on the Enterprise Vault pack, a "Dependent Management Packs" error message appears. Before you can continue, you must first take a backup copy of the dependent packs and then either delete them or edit them to remove their dependency on the Enterprise Vault pack.

   You can now import the Enterprise Vault 11.0.1 management pack.

Chapter 14

Upgrading Exchange Server forms

This chapter includes the following topics:

About upgrading Exchange Server forms

By default, Enterprise Vault 11.0.1 deploys the Exchange Server forms to users' computers automatically.

If you use forms from the Organization Forms Library instead of using the Enterprise Vault client to deploy the forms automatically then you must upgrade the forms in the Organization Forms Library.

If you decide 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`, `EVPendingRestore.fdm`, and `EVPendingArchiveHTTP.fdm`, always uninstall the existing copies first. Do not install the new forms on top of the existing copies.
- By default, Enterprise Vault deploys the forms automatically into personal forms libraries.

Chapter 15

Upgrading Domino mailbox archiving

This chapter includes the following topics:

About upgrading Domino mailbox archiving

You must follow the instructions in this chapter to upgrade Domino mailbox archiving after you have upgraded the Enterprise Vault server software.

Note: Enterprise Vault 10.0.3 introduced support for 64-bit Domino on the Enterprise Vault Domino Gateway. If you upgrade to 64-bit Domino on the Enterprise Vault Domino Gateway, you must subsequently reinstall Enterprise Vault.

Domino client version required to run EVInstall.nsf

You must use a suitable version of the Notes client on the workstation from which you run `EVInstall.nsf`.

The version of the Notes client must be no older than the newest version of the Domino Server that is installed on the Enterprise Vault Domino Gateway and the Domino mail servers.

Preparing for the upgrade of Domino mailbox archiving

This section describes how to prepare your Domino servers for the upgrade of Domino mailbox archiving.

Complete the following procedure on all Enterprise Vault Domino Gateway servers and on all Domino mail servers on which you have updated these forms to include the Enterprise Vault customizations:

- `Forms9.nsf`
- `Forms85.nsf`
- `Forms8.nsf`
- `Forms7.nsf`

Note: The following procedure requires you to replace the forms files with the original Domino versions. When you replace the forms files you lose any non-Enterprise Vault customizations that you made to them. If you made any non-Enterprise Vault customizations to the forms files, you must reapply these changes to the files after you have upgraded to Enterprise Vault 11.0.1.

To prepare for the upgrade of Domino mailbox archiving

1. Stop the HTTP task.
2. Skip this step if you are upgrading Enterprise Vault 11.0 with Domino 9.

   Delete `Forms9_x.nsf` and `Forms85_x.nsf` if they exist on the server.
3. Skip this step if you are upgrading Enterprise Vault 11.0 with Domino 9.

   Replace the `Forms9.nsf`, `Forms85.nsf`, `Forms8.nsf`, and `Forms7.nsf` files with the original Domino versions that you backed up before you installed the previous version of Enterprise Vault.

4 If the forms databases have replication enabled, the changes that EVInstall makes are replicated to all Domino mail servers. If you want to prevent the replication to other mail servers, disable the replication of `Forms7.nsf`, `Forms8.nsf`, `Forms85.nsf`, and `Forms9.nsf`.

5 Update the ACLs on the original Domino `.nsf` files to give Manager access to the ID of the user that will run EVInstall.

Upgrading Domino mailbox archiving

This section describes how to upgrade Domino mailbox archiving.

To upgrade Domino mailbox archiving

1 Make sure that you have a suitable version of the Notes client installed on the workstation from which you want to run `EVInstall.nsf`.

See "Domino client version required to run EVInstall.nsf" on page 78.

2 Do the following in the order listed:

- From your chosen workstation, connect to the Enterprise Vault Domino Gateway server and run `EVInstall.nsf`.
- In the application page, select the Enterprise Vault Domino Gateway and a target Domino mail server.
- If you use the browser-based Enterprise Vault Search facilities or you require iNotes (DWA), select **Modify Domino Web Access Forms Files**.
- Click **Install Symantec Enterprise Vault 11.0.1 database design templates** to start the process.
  The application takes several minutes to create the new Enterprise Vault templates.

3 Deploy the templates created on the Domino mail server to each target Domino mail server that has the same Domino Server version. For example, if you ran `EVInstall.nsf` against a Domino Server 8.5.1 target server, deploy the templates to all Domino Server 8.5.1 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.

Note that the command `Load Design` 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 command's `-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.

4 If you have other target mail servers with different Domino Server versions (for example, 8.5.0), do the following until you have deployed the templates to all mail server targets:

- Run `EVInstall.nsf` again.
- In the application page, clear the **Enterprise Vault Domino Gateway** selection.
- Select a target Domino mail server.
- If you require iNotes (DWA), select **Modify Domino Web Access Forms Files**.
- Click **Install Symantec Enterprise Vault 11.0.1 database design templates** to start the process.
  The application takes several minutes to create the new Enterprise Vault templates.
- Deploy the templates and run `Load Design` as before, on each mail server.

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 account requires a minimum of **Editor** access with **Delete Documents** and **Create shared folders/views**.

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, 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.

Identifying internal mail recipients

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

In order to specify the domains that require local address lookup, you must make some changes to the registry on the Enterprise Vault servers that run the journaling and archiving tasks.

To specify local lookup domains

1. On an Enterprise Vault server that runs a Domino archiving or journaling task, create a new registry key named **NotesDomains** in the following location:

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \Wow6432Node
   \KVS
    \Enterprise Vault
     \Agents
```

2. Under the new **NotesDomains** key, create a subkey for each Notes domain. For example, if you have Notes domains 'MyNotesDomain1' and 'MyNotesDomain2' you create subkeys 'MyNotesDomain1' and 'MyNotesDomain2'.
3. Under each of the Notes domain subkeys, create a new String value named **InternalSMTPDomains**.
4. Assign to each InternalSMTPDomains value a string that lists the domains for which you want to use local lookup. Use semi-colons (;) to separate domains. For example:

```
exampledomain1.com;exampledomain2.com
```

5. Under each of the Notes domain subkeys, create a new DWORD value called **EnableLocalPartLookup**.
6. Give **EnableLocalPartLookup** one of the following values:
   - 0 to disable local part lookup
   - 1 to enable local part lookup
7. Repeat all these steps for other Enterprise Vault servers that run Domino archiving or journaling tasks.

Table 15-1 shows how the NotesDomains registry key controls how Enterprise Vault identifies internal mail recipients.

Table 15-1 Effects of NotesDomains registry key

Registry key or value	Effect on Enterprise Vault behavior
NotesDomains key is missing	Full address lookup and a warning in the event log.

Table 15-1 Effects of NotesDomains registry key *(continued)*

Registry key or value	Effect on Enterprise Vault behavior
NotesDomains key is present but has no key for the current Notes domain	Original address is recorded. No lookup.
NotesDomains key is present and has a key for the current Notes domain	■ If EnableLocalPartLookup is set to 0, perform a full address lookup. ■ If EnableLocalPartLookup is set to 1, perform a full address and local part lookup for addresses that match the Domain. If the InternalSMTPDomains list is present and the SMTP domain matches a domain in the list, SMTP messages being archived from journals are checked with full address and local part lookup. If the InternalSMTPDomains list is not present or there is no match, full address lookup is used.

Run the Domino provisioning task

When you have completed the upgrade of Domino mailbox archiving, you must run the Domino provisioning task to synchronize Domino permissions to Enterprise Vault archives.

Chapter 16

Upgrading the FSA Agent

This chapter includes the following topics:

Compatible versions of the FSA Agent and Enterprise Vault server

The version of the FSA Agent that comes with Enterprise Vault 11.0.1 does not support File System Archiving from Windows file servers that run either of the following:

- Windows Server 2003 x86 and x64 editions
- Windows Server 2008 x86 editions

When a server is running one of these versions of Windows, you cannot install the 11.0.1 version of the FSA Agent on it. Similarly, you cannot add the server as an archiving target through the 11.0.1 version of the Administration Console.

Note that the 10.0 version of the FSA Agent does support archiving from servers that run Windows Server 2003 or Windows Server 2008 x86. This version of the FSA Agent is compatible with Enterprise Vault 11.0.1, so you can continue to archive

from these servers after you upgrade to Enterprise Vault 11.0.1. However, if you ever remove the servers as archiving targets through the Administration Console, you cannot add them back again.

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

- The Enterprise Vault *Compatibility Charts* at http://www.symantec.com/docs/TECH38537.
- For FSA Reporting, the Enterprise Vault technical note at http://www.symantec.com/docs/TECH57334.

About upgrading the FSA Agent

We recommend that you upgrade the FSA Agent on the Windows computers on which it is installed. 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: Do not install the FSA Agent on Enterprise Vault servers. Enterprise Vault servers do not require the FSA Agent.

FSA Agent installation requires an up-to-date VeriSign root certificate on the target computer. Certificate updates usually happen automatically over the Internet. If the certificate is out-of-date, for example because the computer has no Internet connection, the FSA Agent installation fails with a “Signature verification failed” error in the FSA Agent installation log. For more details and for instructions on how to update the root certificate, see the following technical note on the Symantec Support website:

http://www.symantec.com/docs/TECH179712

You can upgrade the FSA Agent from an Enterprise Vault Administration Console, or by installing the files manually on the file server.

To install or upgrade the FSA Agent you must use an account that is a member of the local Administrators group on the file server.

If you upgrade the FSA Agent from the Administration Console then if the file server's firewall is enabled it must be suitably configured. Otherwise the Administration Console wizard fails with the message “Error: The RPC server is unavailable”. See the following technical note on the Symantec Support website:

http://www.symantec.com/docs/TECH76080

From Enterprise Vault 9.0.2 and Enterprise Vault 10.0, the FSA Agent requires the Microsoft Visual C++ 2005 redistributable package. If you upgrade the FSA Agent from the Administration Console, the wizard installs the required Visual C++ packages automatically. If you perform a manual upgrade, you must install the required Visual C++ packages, as described in the manual upgrade procedure.

Table 16-1 describes the options for upgrading the FSA Agent.

Table 16-1 Upgrading the FSA Agent

To do this	See this section
Upgrade FSA Agent services that are clustered for high availability.	See "Upgrading FSA Agent services that are clustered for high availability" on page 87.
Upgrade the FSA Agent on target Windows file servers from the Administration Console.	See "Upgrading the FSA Agent on a target Windows file server from the Administration Console" on page 88.
Upgrade the FSA Agent on FSA Reporting proxy servers from the Administration Console.	See "Upgrading the FSA Agent on an FSA Reporting proxy server from the Administration Console" on page 89.
Upgrade the FSA Agent manually.	See "Upgrading the FSA Agent manually" on page 90.

Upgrading FSA Agent services that are clustered for high availability

Use this procedure to upgrade FSA Agent services that are clustered for high availability.

To upgrade FSA Agent services that are clustered for high availability

1 Perform these steps in the order shown:

- Run the Enterprise Vault Administration Console with an account that is a member of the local Administrators group on each file server node. The account must also have Full Control permission on the Enterprise Vault server's `FSA Cluster` folder. This folder is in the `Utilities` subfolder of the Enterprise Vault installation folder; for example, `C:\Program Files (x86)\Enterprise Vault\Utilities\FSA Cluster`.
- 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:

- Upgrade the FSA Agent from the Administration Console.
  See "Upgrading the FSA Agent on a target Windows file server from the Administration Console" on page 88.
- Upgrade the FSA Agent manually on each file server node.
  See "Upgrading the FSA Agent manually" on page 90.

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

- Run the Enterprise Vault Administration Console with an account that is a member of the local Administrators group on each file server node. The account must also have Full Control permission on the Enterprise Vault server's `FSA Cluster` folder. This folder is in the `Utilities` subfolder of the Enterprise Vault installation folder, for example `C:\Program Files (x86)\Enterprise Vault\Utilities\FSA Cluster`.
- 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 on a target Windows file server from the Administration Console

Use the following procedure to upgrade the FSA Agent by using the Administration Console's Install FSA Agent wizard.

Before you upgrade the FSA Agent on a target Windows file server, note that while the upgrade proceeds, Enterprise Vault stops the three FSA Agent services on the file server:

- Enterprise Vault File Placeholder service. While this service is stopped, Enterprise Vault cannot create placeholders or perform placeholder recalls on the Windows file server.
- Enterprise Vault File Collector service. While this service is stopped, no FSA Reporting scans run on the following:
  - The file server.
  - Any non-Windows file servers for which the file server acts as the FSA Reporting proxy server.
- Enterprise Vault File Blocking service. While this service is stopped, File Blocking does not work on the following:
  - The file server.
  - Any NetApp filers for which the file server performs File Blocking.

To upgrade the FSA Agent on a target Windows file server from the Administration Console

1. Run the Enterprise Vault Administration Console with an account that is a member of the local Administrators group on the file server.
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.

Upgrading the FSA Agent on an FSA Reporting proxy server from the Administration Console

This section applies if you use FSA Reporting with non-Windows file servers.

If you have configured any target Windows file servers or other Windows servers as FSA Reporting proxy servers, you can upgrade the FSA Agent on the proxy servers from the Administration Console.

To upgrade the FSA Agent on an FSA Reporting proxy server from the Administration Console

1. Run the Enterprise Vault Administration Console with an account that is a member of the local Administrators group on the FSA Reporting proxy server.
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 target non-Windows file server and on the shortcut menu click **Upgrade FSA Agent on proxy server for FSA Reporting**.

   This option is not available if the FSA Reporting proxy server is an Enterprise Vault server. Enterprise Vault servers do not require the FSA Agent.

   If the proxy server is a target Windows file server, Enterprise Vault displays a dialog to warn that the FSA Agent services stop while the upgrade proceeds. Click **Yes** if you want to continue.
6. Work through the wizard to upgrade the version of the FSA Agent on the FSA Reporting proxy server.

Upgrading the FSA Agent manually

Use the following procedure to upgrade the FSA Agent on a server by installing the required files manually.

To upgrade the FSA Agent manually

1. Find the required files on the Enterprise Vault server. The files are in the `evpush\Agent` folder under the Enterprise Vault installation folder; for example, `C:\Program Files (x86)\Enterprise Vault\evpush\Agent`.
2. Install the required Microsoft Visual C++ redistributable packages on the file server:
   - `vcredist_x86.exe`
   - `vc2005redist_x86.exe`
   - `vcredist_x64.exe`
3. Log on to the file server with an account that is a member of the local Administrators group on the file server.
4. Run the `Enterprise Vault File System Archiving x64.msi` file on the file server.

Chapter 17

Upgrading OWA and RPC Extensions

This chapter includes the following topics:

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 11.0.1.

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

Note: The Enterprise Vault 11.0.1 OWA extensions for Exchange Server versions 2003, 2007, and 2010 require Windows 2003 SP1 or later on Exchange servers.

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

http://www.symantec.com/docs/TECH69113

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

Upgrading Enterprise Vault OWA 2010 Extensions

To upgrade the Enterprise Vault OWA 2010 Extensions, perform the following steps on each Exchange 2010 CAS server.

To upgrade Enterprise Vault OWA 2010 Extensions

1. Load the Enterprise Vault 11.0.1 media.
2. If Windows AutoPlay is enabled on the server, Windows shows an AutoPlay dialog box. Click **Run Setup.exe**.

   If AutoPlay is not enabled, use Windows Explorer to open the root folder of the installation media and then double-click the file `Setup.exe`.
3. In the list in the left pane of the **Symantec Enterprise Vault Install Launcher** window, click **Enterprise Vault**.
4. Click **Client Installation**.
5. In the right pane, click **OWA Extensions** and then **Open folder**. Windows Explorer starts in the OWA Extensions folder.
6. Open the `OWA 2010 Extensions` folder.
7. Double-click the file `Symantec Enterprise Vault OWA 2010 Extensions x64.msi` to start the installation.
8. Follow the installation instructions.
9. From a browser, enter the URL for the Exchange 2010 CAS server. Open an OWA client and check that you can view archived items.

Upgrading Enterprise Vault OWA 2007 Extensions

The target server for WebDav requests is set in the configuration file, *`Exchange installation path`*`\ClientAccess\Owa\Web.Config`, on the Exchange 2007 CAS server. If you changed the **EnterpriseVault_WebDAVRequestHost** entry in this file to specify a server other than localhost, then the change is preserved when you upgrade the extensions.

Note that if you later repair the extensions in Add or Remove Programs, then the value of the **EnterpriseVault_WebDAVRequestHost** entry is reset to the default value, “localhost”.

To upgrade Enterprise Vault OWA 2007 Extensions

1. Load the Enterprise Vault 11.0.1 media.
2. If Windows AutoPlay is enabled on the server, Windows shows an AutoPlay dialog box. Click **Run Setup.exe**.

   If AutoPlay is not enabled, use Windows Explorer to open the root folder of the installation media and then double-click the file `Setup.exe`.
3. In the list in the left pane of the **Symantec Enterprise Vault Install Launcher** window, click **Enterprise Vault**.
4. Click **Client Installation**.
5. In the right pane, click **OWA Extensions** and then **Open folder**. Windows Explorer starts in the OWA Extensions folder.
6. Open the `OWA 2007 Extensions` folder.
7. 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`
8. Follow the installation instructions.
9. From a browser, enter the URL for the Exchange 2010 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 11.0.1 OWA Extensions, see the *Enterprise Vault Compatibility Charts* at http://www.symantec.com/docs/TECH38537.

To upgrade the Enterprise Vault OWA 2003 Extensions

1. If a populated version of the file `EVServers.txt` already exists in the `OWA 2003 Extensions` folder on the Enterprise Vault server, or in the installation folder on the Exchange Server, then the installer uses this. If more than one populated version of `EVServers.txt` exists, then you are prompted for the file to use. Otherwise you can run the `MakeEVServersTxt.wsf` script to populate the `EVServers.txt` file.

   See "Preparing EVServers.txt" on page 94.

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 95.

See the "Installing the Enterprise Vault Extensions on Exchange Server 2003" section in the *Setting up Exchange Server Archiving* guide 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).

Preparing EVServers.txt

Prepare `EVServers.txt` as follows.

To prepare EVServers.txt

1. Log on to any Enterprise Vault server, using an account that has any Enterprise Vault administrator permissions.
2. Start Windows Explorer and navigate to the `OWA 2003 Extensions` subfolder of the Enterprise Vault installation folder, for example `C:\Program Files (x86)\Enterprise Vault\OWA 2003 Extensions`.
3. Double-click `MakeEVServersTxt.wsf` to run it. The script populates `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.

Chapter 18

Upgrading SharePoint Server components

This chapter includes the following topics:

About upgrading the SharePoint components

This chapter describes how to upgrade Enterprise Vault SharePoint components.

Note: You must upgrade the SharePoint components. The version of the SharePoint components must match the version of Enterprise Vault that is installed on the Enterprise Vault servers.

The upgrade path depends on your version of SharePoint, as follows:

- You can upgrade Enterprise Vault components on any of the following:
  - Microsoft SharePoint Foundation 2010
  - Microsoft SharePoint 2010
  - Microsoft Office SharePoint Sever 2007
  - Windows SharePoint Services 3.0

  See "Upgrading the Enterprise Vault SharePoint components" on page 97.
- If you have started a gradual migration from SharePoint Portal Server 2003 or Windows SharePoint Services 2.0 to Microsoft Office SharePoint Sever 2007 or Windows SharePoint Services 3.0, finish the gradual migration and then upgrade the Enterprise Vault components.

Upgrading the Enterprise Vault SharePoint components

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 as one of the following:
   - The SharePoint Server farm account. This account is sometimes known as the SharePoint database access account.
   - An account that has sufficient permissions to the SharePoint_Config database (the configuration database). The account must be a member of the following SQL Server security roles on the SharePoint_Config database: SharePoint_Shell_Access and WSS_Content_Application_Pools.
     The Vault Service account can be used provided it has these permissions.
2. On your SharePoint Server computer, load the Enterprise Vault 11.0.1 media.
3. If Windows AutoPlay is enabled on the server, Windows shows an AutoPlay dialog box. Click **Run Setup.exe**.

   If AutoPlay is not enabled, use Windows Explorer to open the root folder of the installation media and then double-click the file `Setup.exe`.
4. In the list in the left pane of the **Symantec Enterprise Vault Install Launcher** window, click **Enterprise Vault**.
5. Click **Server Installation**.
6. In the right pane, click **Upgrade existing server** to start the installation.
7. On the **Select Components to Install** screen, ensure that only **Microsoft SharePoint Components** is selected.
8. Click **Next**.
9. Work through the remainder of the installation wizard.

If you upgrade from an Enterprise Vault version earlier than 10.0.2, all the SharePoint policy rules that you had configured for archiving content types are upgraded as follows:

- If you specified the content type before upgrade, the custom content type option is selected and its previous value is shown in the text box.
- If the content type was not specified before upgrade, then all supported SharePoint libraries are selected. For example, **Document Library**, **Picture Library**, **Form Library**, and so on are selected.

If you have HTML shortcuts that were created by versions of Enterprise Vault earlier than 10.0.2, you must run the EVSPShortcutManager utility. The EVSPShortcutManager utility converts HTML shortcuts to new shortcuts that behave exactly like SharePoint documents. For information on how to use EVSPShortcutManager, see the *Utilities* guide.

Chapter 19

Upgrading SMTP archiving

This chapter includes the following topics:

About upgrading SMTP Archiving

Enterprise Vault 11.0.1 introduces a completely new version of SMTP Archiving. Using the SMTP protocol, Enterprise Vault can now apply policy-controlled archiving to any content that is sent to it from applications or products that can send email.

The new implementation of SMTP Archiving does not require the Windows SMTP service or File System Archiving.

If you use a legacy version of Enterprise Vault SMTP Archiving, that version can run concurrently with the new version. The legacy version and the new version must use different port numbers.

If you want to continue to use the legacy Enterprise Vault SMTP Archiving components, install the Enterprise Vault 11.0.1 SMTP Archiving components, and rerun the legacy Enterprise Vault SMTP Archiving configuration process.

Chapter 20

Upgrading your Enterprise Vault sites to use Enterprise Vault Search

This chapter includes the following topics:

About Enterprise Vault Search

One of the main enhancements in Enterprise Vault 11.0, Enterprise Vault Search replaces three legacy search applications: Archive Explorer, Browser Search, and Integrated Search. Enterprise Vault Search provides client users with all the browse

features and search features that are available in those applications. However, the interface has been thoroughly reworked for ease of use and to provide fast access to archived information.

After you upgrade an existing 10.0.*n* installation of Enterprise Vault to 11.0.1, your users continue to access the legacy search applications. To make Enterprise Vault Search available, you can do either of the following:

- Upgrade the entire Enterprise Vault site so that all users will henceforth run Enterprise Vault Search rather than the legacy applications. You can configure the Enterprise Vault Search facilities that you want to make available to users by amending the default search policy.
- Make Enterprise Vault Search available to selected users only by setting up one or more custom provisioning groups, with the associated search policies. Any users who are not the targets of the custom provisioning groups continue to access the legacy applications.

About the server requirements for Enterprise Vault Search

This section describes server requirements for Enterprise Vault Search.

Sometimes other aspects of your Net.Tcp configuration may cause Enterprise Vault Search to fail. If they occur, these failures are reported in the event log and on the status page in the Enterprise Vault Administration Console. For instructions on how to resolve search failures that are caused by Net.Tcp issues, see the following technical note on the Symantec Support website:

http://www.symantec.com/docs/TECH214690

Net.Tcp Listener Adapter service (NetTcpActivator)

Each Enterprise Vault server requires the Net.Tcp Listener Adapter service (NetTcpActivator) for Enterprise Vault Search. This service requires the following Windows Communication Foundation (WCF) Activation features:

- HTTP Activation
- Non-HTTP Activation

The **Prepare my system** option in the Enterprise Vault Install Launcher automatically installs these features, if they are not already installed.

However, if you do not want to use the **Prepare my system** option, you can manually install the WCF Activation features.

To add the requirements for Enterprise Vault Search manually

1. Start Server Manager.
2. Do one of the following:
   - In Windows Server 2008 R2, click **Features** in the left pane and then click **Add Features** in the right pane.
   - In Windows Server 2012, click **Manage** at the top right and then click **Add Roles Features**.

   The **Add Features** wizard appears.
3. Expand **.NET Framework 3.5.1 Features**.
4. Expand **WCF Activation**, and then ensure that both of the following features are checked:
   - HTTP Activation
   - Non-HTTP Activation
5. If the features are already installed, click **Cancel**. Otherwise, click **Next** and then follow the on-screen instructions.

Enterprise Vault on Windows Server 2012

If you install Enterprise Vault on Windows Server 2012, you must perform the steps described in the following Microsoft article before you use Enterprise Vault Search:

http://support.microsoft.com/kb/2803161

About the client requirements for Enterprise Vault Search

Client users require an HTML5-compatible web browser to benefit from all the new features in Enterprise Vault Search. Older browsers are supported, but the client experience may be compromised.

For the latest information on supported web browsers, see the Enterprise Vault *Compatibility Charts* at http://www.symantec.com/docs/TECH38537.

Upgrading an Enterprise Vault site to use Enterprise Vault Search

The process of upgrading an Enterprise Vault site makes Enterprise Vault Search rather than the legacy search applications available to all users. Note the following:

- If you want some users to run Enterprise Vault Search and others to run the legacy search applications, do not upgrade the site. Instead, set up one or more provisioning groups to make Enterprise Vault Search available to selected users or groups.
  See "Setting up provisioning groups for Enterprise Vault Search" on page 105.
- Any new site that you add after you have upgraded to Enterprise Vault 11.0.1 is automatically enabled for Enterprise Vault Search; the users of the new site do not have access to the legacy search applications.

The upgrade process is not reversible; you cannot restore the legacy search applications afterwards. This process does the following:

- It creates a default search provisioning group with which you can make a standard set of Enterprise Vault Search features available to all users.
- It removes the desktop policy settings for the legacy search applications from the Administration Console.
- It redirects to Enterprise Vault Search all the search requests that users make. In addition, after both of the following have occurred, the upgrade process removes the **Archive Explorer** button from the Enterprise Vault toolbar in Microsoft Outlook and OWA:
  - The Exchange Mailbox Archiving task has resynchronized the users' mailboxes.
  - Outlook users have restarted Outlook, and users of OWA 2003 through 2010 have logged back in to OWA. (OWA 2013 users need only refresh the OWA page to remove the **Archive Explorer** button.)

To upgrade an Enterprise Vault site to use Enterprise Vault Search

1. In the left pane of the Administration Console, right-click the Enterprise Vault site and then click **Properties**.
2. On the **Search** tab, click **Upgrade Search**.
3. Follow the on-screen instructions. After you have done so, the **Search** tab disappears from the **Site Properties** dialog box.

Defining search policies for Enterprise Vault Search

A search policy defines the range of Enterprise Vault Search facilities that you want to make available to users. With a search policy, you can choose to let Enterprise Vault Search users do the following:

- Show the reading pane. This pane displays a preview of the currently selected item in Enterprise Vault Search. For performance reasons, you may want to hide the reading pane to stop recalls from slow storage media, such as tape or optical disks.
- Export the items that are listed in Enterprise Vault Search to an `.nsf`, `.pst`, or `.zip` file, depending on the archive type.

  Some export formats are appropriate for use with certain types of items only. For example, it is not possible to export Outlook messages to a `.nsf` file, or Notes messages to a `.pst` file. A user who chooses to export both Outlook and Notes messages to a single file can export them to a `.zip` file only.
- Copy and move archived items. Both types of operation let users restore an archived item to its original location, the **Restored Items** mailbox folder, or a selected mailbox folder. However, a copy operation also leaves the item in the archive, whereas a move operation deletes it.
- Delete archived items. Note that, even if you define a search policy to grant delete permissions, users can only delete items if you have configured the Enterprise Vault site appropriately. In the Administration Console, open the **Site Properties** dialog box for the Enterprise Vault site and then, on the **Archive Settings** tab, ensure that **Users can delete items from their archives** is checked.

Installing Enterprise Vault 11.0.1 creates a default search policy automatically. You can modify the properties of this default policy and define custom search policies. Then you can assign each policy to a different search provisioning group.

To view and modify the properties of the default search policy

1. In the left pane of the Administration Console, expand your Enterprise Vault site.
2. Expand the **Policies** container.
3. Click the **Search** container.
4. In the right pane, right-click **Default Search Policy** and then click **Properties**.

   You can change the settings on the **Features** tab, but you cannot change the settings on the **General** and **Targets** tabs.

To define a new search policy

1. In the left pane of the Administration Console, expand your Enterprise Vault site.
2. Expand the **Policies** container.
3. Right-click the **Search** container, and then click **New** > **Policy**.

   The **New Search Policy** wizard appears.
4. Follow the on-screen instructions. The wizard prompts you to specify the following:
   - The name of the policy and an optional description of it.
   - The Enterprise Vault Search facilities that you want to make available to users.

Setting up provisioning groups for Enterprise Vault Search

A search provisioning group identifies the users and user groups to whom you want to assign a search policy for Enterprise Vault Search. There are two circumstances in which you might typically want to set up a search provisioning group:

- You want to make Enterprise Vault Search available to selected users or groups in an Enterprise Vault site that you have yet to upgrade to use Enterprise Vault Search.
- Enterprise Vault Search is enabled in the site, but you want to assign a custom search policy to selected users or groups.

You can set up any number of provisioning groups for different sets of targets. However, each provisioning group can target the users in one Active Directory domain or Domino domain, so you require at least as many groups as you have domains.

To set up a search provisioning group

1. In the left pane of the Administration Console, expand your Enterprise Vault site.
2. Expand the **Client Access** container and then expand the **Search** container.

3 Right-click the **Provisioning Groups** container, and then click **New** > **Active Directory Provisioning Group** or **New** > **Domino Provisioning Group**.

The **New Search Provisioning Group** wizard appears.

4 Complete the fields and then click **Create Provisioning Group**. The wizard prompts you to specify the following:

- The name of the provisioning group.
- The search policy to assign.
- The domain to which the provisioning group applies. You can enter the details of a new domain, if necessary.
  For an Active Directory domain, you must choose a trusted domain in your environment and optionally specify the required Global Catalog server. For a Domino domain, you must specify the name and password for the ID file that Enterprise Vault will use to access the domain, and the fully-distinguished name of any Domino server in the domain.
- The targets (individual users and user groups) of the provisioning group.
- The Enterprise Vault server that is to host the Client Access Provisioning task for this provisioning group. This task applies the required search policy to the targets of the provisioning group. You can host the task on any Enterprise Vault server in your site. However, if the task is to provision a Domino domain then you must ensure that Notes is installed on the server.
  Enterprise Vault creates the task automatically if one does not already exist for the nominated domain.

The provisioning group takes effect when the Client Access Provisioning task has run.

Changing the order in which Enterprise Vault processes the search provisioning groups

When you set up a search provisioning group, it automatically has the highest ranking in its domain. In consequence, Enterprise Vault processes the new provisioning group before it processes any other groups in the domain. You can change the order in which Enterprise Vault processes the provisioning groups, if necessary.

To change the order in which Enterprise Vault processes the search provisioning groups

1 In the left pane of the Administration Console, expand your Enterprise Vault site.

2 Expand the **Client Access** container and then expand the **Search** container.

3 Click the **Provisioning Groups** container.

4 Right-click a blank area of the right pane, and then click **Properties**.

The **Provisioning Groups Properties** dialog box appears.

5 In the **Provisioning Groups** list, click a group and then click **Move Up** or **Move Down** to raise or lower its priority.

If users are the targets of multiple provisioning groups, Enterprise Vault processes them as members of the topmost group only. Thereafter, Enterprise Vault ignores these users when it processes the lower priority provisioning groups.

Creating and configuring Client Access Provisioning tasks for Enterprise Vault Search

You require one Client Access Provisioning task for each Active Directory domain or Domino domain in which you want to apply search policies for Enterprise Vault Search. At specified times each day, the task applies the required search policy to users who are the targets of a provisioning group with which you have associated the task. You can host the task on any Enterprise Vault server in your site. However, if the task is to provision a Domino domain then you must ensure that Notes is installed on the server.

Besides processing the search provisioning groups for a domain, a Client Access Provisioning task also processes the domain's IMAP (Exchange Mailbox or Internet Mail) provisioning groups. These two types of provisioning group differ slightly in how the task processes them, in the event that the task is stopped before it has finished assigning the required policies to the target users.

- For a search provisioning group, the task does not assign the search policy to any users. When the task next runs, it starts from the beginning and assigns the policy to all users.
- For an IMAP provisioning group, those users to whom the task assigned a policy before it stopped retain that policy; the other users are not provisioned. However, when the task next runs, it starts from the beginning and reassigns the policy to all users.

If a suitable Client Access Provisioning task does not exist when you set up a search provisioning group, Enterprise Vault automatically creates one. However, you can manually create and configure this task at any time.

To create and configure a Client Access Provisioning task for Enterprise Vault Search

1. In the left pane of the Administration Console, find and then expand the **Enterprise Vault Servers** container.
2. Expand the container for the server to which you want to add the Client Access Provisioning task.
3. Right-click the **Tasks** container, and then click **New** > **Client Access Provisioning Task**.

   The **New Client Access Provisioning Task** dialog box appears.
4. Complete the fields and then click **OK**. The dialog box prompts you to specify the following:
   - The domain with which to associate the task.
   - The name of the task.
   - Whether to start the task now. If you want to configure the task before it starts, turn off this option and follow the instructions in step 5.
     The settings that you can configure include the times at which the task runs each day and the level of reporting that it undertakes for each provisioning run
5. To configure the task, right-click it in the right pane, and then click **Properties**.

   The online Help provides detailed information on each field in the properties dialog box.

Configuring user browsers for Enterprise Vault Search

Most users should not experience any problems when they access Enterprise Vault Search. However, they must set the following in their browsers to use Enterprise Vault Search:

- Allow cookies.
- Enable JavaScript.
- Disable private browsing or the settings that prevent their browsers from storing data about their browsing.
- Internet Explorer only: In the **Internet Options** dialog box, on the **Advanced** tab, ensure that the **Security** setting that is called **Do not save encrypted pages to disk** is unchecked.

You can also minimize potential problems by configuring their web browsers to treat Enterprise Vault Search as a trusted site. How you do this varies from one browser to another, but the procedure for Internet Explorer is as described below.

If you use Active Directory, you can employ a group policy to apply the zone change to all the domain users. To do this, you must edit the Internet Explorer Maintenance settings within the policy.

To configure Internet Explorer to trust Enterprise Vault Search

1. On the client computer, open Internet Explorer.
2. On the **Tools** menu, click **Internet Options**.
3. Click the **Security** tab.
4. Click **Trusted sites**, and then click **Sites**.
5. Enter the fully-qualified domain name of the server on which you installed Enterprise Vault Search, and then click **Add**. For example, you might type **vault.company.com**.
6. Close the **Trusted sites** dialog box, and then close the **Internet Options** dialog box.

Configuring Enterprise Vault Search for use in TMG or similar environments

In Threat Management Gateway (TMG) or similar environments, you may need to relax Enterprise Vault Search's built-in protection against security vulnerabilities so that Internet Explorer users can access it without problem. Note that, when enabled, the security restrictions offer protection in Internet Explorer 9.0 and earlier only; later versions of Internet Explorer employ a different protection mechanism.

To configure Enterprise Vault Search for use in TMG or similar environments

1. Locate the following file on the Enterprise Vault server:

   ```
   C:\Program Files (x86)\Enterprise
   Vault\EVSearch\EVSearchClient\Web.config
   ```

2. Open the file in a text editor such as Windows Notepad.
3. Find the following line, and change the value from 1 to 0:

   ```
   <add key="UseRestrictedSecurity" value="1"/>
   ```

   A value of 1 enforces the security restrictions, whereas 0 relaxes them.
4. Save and close the file.

Setting up Enterprise Vault Search Mobile edition

Designed for use on Android, iOS, and Windows Mobile devices, Enterprise Vault Search Mobile edition is a new feature in Enterprise Vault 11.0.1 that lets users access their archives through the web browsers on their smartphones. Those users for whom you provision Enterprise Vault Search on the desktop and tablet can also run the Mobile edition on their smartphones.

Enterprise Vault Search Mobile edition is a browser-based application that you deploy for intranet or Internet access using Microsoft Internet Information Services (IIS).

Caution: You can install the required components on the Enterprise Vault server. However, if you want to give your users Internet access to Enterprise Vault Search without exposing your Enterprise Vault server to unnecessary security risks, it is advisable to install the components on a proxy server.

Carrying out preinstallation tasks for Enterprise Vault Search Mobile edition

Before installing Enterprise Vault Search Mobile edition, you must perform the following tasks:

- If you want to install Enterprise Vault Search Mobile edition on a proxy server, ensure that the server meets the minimum requirements.
  See "Requirements for installing Enterprise Vault Search Mobile edition on a proxy server" on page 111.
- Obtain a digital certificate from a certification authority such as VeriSign for setting up HTTPS.
- In a configuration providing direct access to the Enterprise Vault Search web server from the Internet, do the following:
  - Verify that the firewall or firewalls are configured to allow HTTPS access to the server on which you plan to install Enterprise Vault Search Mobile edition.
  - Configure any reverse proxy server that is installed in the DMZ.
  - Ensure that the browsers of end-users are configured to allow cookies, enable JavaScript, and disable private browsing.

Requirements for installing Enterprise Vault Search Mobile edition on a proxy server

Caution: To maximize security, install Enterprise Vault Search on a reverse proxy server or protect the server with Microsoft Threat Management Gateway (TMG).

You can install Enterprise Vault Search Mobile edition on a proxy server on which you have also installed the following:

- One of the following versions of Windows:
  - Windows Server 2008 R2
  - Windows Server 2012
  - Windows Server 2012 R2

  The server must have an NTFS file system.
- The Enterprise Vault API Runtime. The process of installing Enterprise Vault Search Mobile edition on the proxy server automatically installs the API Runtime, if it is not already present.
  The version of the API Runtime must match that of Enterprise Vault on the Enterprise Vault server.
- Internet Information Services (IIS) 7.5 or later.
  The following table lists the minimum set of role services that you must install for the Web Server (IIS) role.

Common HTTP Features	■ Static Content ■ Directory Browsing ■ HTTP Errors ■ HTTP Redirection
Application Development	■ ASP.NET ■ ISAPI Extensions ■ ISAPI Filters
Health and Diagnostics	■ HTTP Logging ■ Logging Tools
Security	■ Request Filtering
Performance	■ Static Content Compression
Management Tools	■ IIS Management Console

- Microsoft .NET Framework 3.5 SP1 or SP2.
  The Windows Communication Foundation (WCF) HTTP Activation feature must be installed and enabled. You do not need to install and enable the non-HTTP Activation feature.

In addition, you must ensure the following:

- The proxy server is part of a Windows domain.
- Distributed COM (DCOM) is enabled.
- Port 135 is open on the firewall.
- None of the following is also installed on the proxy server:
  - The Enterprise Vault server software
  - Microsoft SQL Server
  - Microsoft Exchange Server (the target system for Enterprise Vault archiving)

Disabling unsafe cryptographic protocols and cipher suites

If you want to give your users Internet access to Enterprise Vault Search without exposing your proxy server to unnecessary security risks, you can disable unsafe cryptographic protocols and cipher suites on the server.

When a client device uses HTTPS to connect to Enterprise Vault Search on a proxy server, the client and server negotiate a common cryptographic protocol to help secure the channel. If the client and server have multiple protocols in common, Internet Information Services (IIS) tries to secure the channel with one of the protocols that IIS supports. However, some protocols are stronger than others; to maximize the security of your environment, you may therefore want to disable the weak protocols in favor of stronger, Symantec-approved alternatives.

You can comply with Symantec recommendations by configuring the cryptographic protocols and cipher suites on your proxy server as follows:

- Enable the TLS 1.1. and 1.2 protocols.
- Disable the SSL 2.0 protocol.
- Disable the RC2, RC4, and DES cipher suites.

The following articles in the Microsoft Knowledge Base provide guidelines on how to implement these changes:

- http://support.microsoft.com/kb/187498
- http://support.microsoft.com/kb/245030

Installing Enterprise Vault Search Mobile edition

Whether you want to deploy install the required components for Enterprise Vault Search Mobile edition on the Enterprise Vault server or on a proxy server, follow the steps below.

To install Enterprise Vault Search Mobile edition

1. On the server where you want to install Enterprise Vault Search Mobile edition, log in as the Vault Service account.
2. Load the Enterprise Vault installation media.
3. Do one of the following:
   - If an AutoPlay dialog box appears, click **Run Setup.exe**.
   - If AutoPlay is not enabled, use Windows Explorer to open the root folder of the installation media and then double-click the file `Setup.exe`.
4. In the left pane of the Symantec Enterprise Vault Install Launcher, click **Enterprise Vault**.
5. Click **Server Installation**.
6. Choose the required installation option.

   To install Enterprise Vault Search Mobile edition on a proxy server, choose **Installation on an additional server**.
7. Follow the instructions in the Enterprise Vault installation wizard.

   When the wizard prompts you to select the features that you want to install, do one of the following:
   - For installation on a proxy server, uncheck all the options except for **Search Access Components**.

     When you click **Next**, the wizard requests the Vault Site alias. This alias is the DNS alias for the Enterprise Vault site.
   - For installation on an Enterprise Vault server, choose all the required components.

     If you choose to install the Enterprise Vault services, or you have previously installed them on this server, then you cannot uncheck the **Search Access Components** option. The components will be automatically installed.

8. Follow the on-screen instructions to complete the remaining steps in the installation wizard.
9. Ensure the security of transmitted data by configuring the Enterprise Vault Search website for HTTPS.

   The Enterprise Vault Search website is configured in the Default Web Site in IIS. To use HTTPS, you must first configure the Default Web Site in IIS for HTTPS, and install a valid SSL certificate. See the IIS documentation for instructions.

Verifying the installation of Enterprise Vault Search Mobile edition

Before you make Enterprise Vault Search Mobile edition available to users, follow the steps below to verify the installation.

To verify the installation of Enterprise Vault Search Mobile edition

1. Open a web browser on a smartphone that has Internet access.
2. In the **Address** field, enter the Mobile Search URL as follows:

   https://*server*/enterprisevault/search

   Where *server* is the name or IP address of the server on which you installed the search components.
3. Click **Go** or press **Enter** to display the Sign In page.
4. Enter the details of a user who has access to at least one archive.
5. Click **Sign In**.

   If your authentication is valid, you see the home page of Enterprise Vault Search.
6. Perform a search to verify that Enterprise Vault Search can return search results.
7. Click a message in the search results and verify that you can see its contents.

Chapter 21

Upgrading Enterprise Vault API applications

This chapter includes the following topics:

Upgrading any applications that use the Enterprise Vault API Runtime

You may have installed a third-party application that uses the Enterprise Vault API to archive proprietary data or filter the data that Enterprise Vault stores. After upgrading Enterprise Vault, you may need to perform the following additional tasks to upgrade these applications:

- If the application uses the Enterprise Vault API Runtime, you need to update the API Runtime on each computer that hosts the application.
- For a .NET application that uses a specific version of the Enterprise Vault API Runtime, you need to update the binding redirections in the application's configuration file.

  For instructions on how to update the binding redirections, see the document `ReadMeFirst_en.htm`. The document is located with the API Runtime kit in the `API Runtime` folder on the Enterprise Vault media.