Veritas Enterprise Vault™

Upgrade Instructions

12

VERITAS™

Veritas Enterprise Vault: Upgrade Instructions

Last updated: 2015-12-03.

Legal Notice

Veritas Technologies LLC
500 E Middlefield Road
Mountain View, CA 94043

http://www.veritas.com

Technical Support

Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within the company to answer your questions in a timely fashion.

Our 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 our support offerings, you can visit our website at the following URL:

www.veritas.com/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.veritas.com/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 Technical Support
  - Recent software configuration changes and network changes

Licensing and registration

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

www.veritas.com/support

Customer service

Customer service information is available at the following URL:

www.veritas.com/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
- Advice about technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs, DVDs, or manuals

Support agreement resources

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

Worldwide (except Japan)	CustomerCare@veritas.com
Japan	CustomerCare_Japan@veritas.com

Contents

Chapter 1

About this guide

This chapter includes the following topics:

Introducing this guide

This guide describes how to upgrade Enterprise Vault.

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

For the most up-to-date versions of the *ReadMeFirst* file and *Installing and Configuring* guide, see the following article on the Veritas Support website:

http://www.veritas.com/docs/000099905

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
Veritas 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 Domino Server Archiving	Describes how to archive items from Domino mail files and journal databases.
Setting up Exchange Server Archiving	Describes how to archive items from Microsoft Exchange user mailboxes, journal mailboxes, and public folders.
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 Internet mail archives.
Setting up SMTP Archiving	Describes how to archive SMTP messages from other messaging servers.
Setting up SharePoint Server Archiving	Describes how to archive content from Microsoft SharePoint 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.
Classification	Describes how to assign classification values to the metadata properties of all new and existing archived items. Users of applications such as Enterprise Vault Search and Compliance Accelerator can then use the classification values to filter the items when they conduct searches or reviews.
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.veritas.com/docs/000097605

“How To” articles on the Veritas Support website

Most of the information in the Enterprise Vault administration guides is also available online as articles on the Veritas 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 Veritas Support website

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

   http://www.veritas.com/support/en_US/products-a-z

2. In the **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 and eDiscovery Tech Center (http://www.veritas.com/elibrary) is an eLibrary of self-paced learning modules developed around key features, best practices, and common technical support questions.

More advanced instructor-led training, virtual training, and on-demand classes are also available. For information about them, see http://www.veritas.com/education-services/training-courses.

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@veritas.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 12. The only possible server upgrade paths to this version are from the following:

- Enterprise Vault 11.0
- 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.

Documentation

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

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

http://www.veritas.com/docs/000097605

Chapter 3

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.

Vault service account requires a new SQL permission

The Vault Service account requires the VIEW ANY DEFINITION permission. For more information, see “Creating a SQL login account” in the *Installing and Configuring* guide.

Enterprise Vault 12 requires uniform SQL collation

Enterprise Vault 12 requires that SQL has a uniform collation across the Master and all the Enterprise Vault databases. An inconsistent collation prevents you from upgrading, so you must ensure there is a uniform collation before you upgrade.

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

Compliance Accelerator 12 works with Enterprise Vault 11.0.1 and later, so you must upgrade Enterprise Vault before you upgrade Compliance Accelerator.

Discovery Accelerator 12 works with Enterprise Vault 11.0 and later. The version of Discovery Accelerator must not be lower than the version of Enterprise Vault.

Order in which to perform the upgrade

1. If your environment includes Discovery Accelerator:
   - Install Discovery Accelerator 12 on the Discovery Accelerator server
   - Then upgrade the Discovery Accelerator databases
   - Then install the Discovery Accelerator 12 client software on each client computer
2. Upgrade Enterprise Vault to version 12 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 12. This order ensures that the random sampling feature works seamlessly before and after the upgrade.
3. Upgrade Enterprise Vault to version 12 on all Compliance Accelerator and Discovery Accelerator servers.
4. If your environment includes Compliance Accelerator:

- Install Compliance Accelerator 12 on the Compliance Accelerator server
- Then upgrade the Compliance Accelerator databases
- Install the Compliance Accelerator 12 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.

For more information on supported versions and upgrade paths, see the *Enterprise Vault Compatibility Charts* at http://www.veritas.com/docs/000097605 and the article *Supported upgrade paths for Enterprise Vault, Compliance Accelerator, Discovery Accelerator and Discovery Collector* at http://www.veritas.com/docs/TECH53174.

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.

Enterprise Vault does not automatically enable fast browsing for archives.

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.

eDiscovery Platform compatibility with Enterprise Vault

Before you upgrade Enterprise Vault, see the *eDiscovery Platform Compatibility Matrix* for details of compatibility with Enterprise Vault. This is available from http://www.veritas.com/docs/TECH211911.

Support for Outlook 2013 SP1 on the Enterprise Vault server

Enterprise Vault 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.

Automatic migration of content conversion settings

The Enterprise Vault content conversion functionality is extended to use the functionality that is provided by the Windows TIFF IFilter feature.

Content conversion was previously configurable at server level using registry settings. In this release it is configured at site level. This ensures that conversion is implemented consistently across storage servers in an Enterprise Vault site.

To support this feature, new Content Conversion settings are added to the advanced site settings in the Enterprise Vault Administration Console. During the upgrade process, the new settings are added to each site with default values.

If you previously configured conversion registry settings on an Enterprise Vault server, the setting values are evaluated during upgrade. On each Enterprise Vault server in the site, existing content conversion registry settings are logically upgraded and then deleted if their values match the equivalent site setting. If the value differs from the site settings default, then the registry setting value overrides the site setting value on the local Enterprise Vault server only.

Table 3-1 shows the association between new Content Conversion site settings and existing conversion registry settings.

Table 3-1 Content Conversion site settings and registry settings

Setting name in Content Conversion advanced site properties	Associated registry settings
File types excluded from conversion	Enterprise Vault\ExcludedFileTypesFromConversion
File types converted to text	Enterprise Vault\TextConversionFileTypes Enterprise Vault\ConvertWordToText Enterprise Vault\ConvertExcelToText Enterprise Vault\ConvertRTFCoverToText
Conversion timeout	Enterprise Vault\ConversionTimeout
Conversion timeout for archive file types	Enterprise Vault\ ConversionTimeoutArchiveFiles
Include hidden text	Enterprise Vault\ConversionIncludeHiddenText
Include hidden spreadsheet data	Enterprise Vault\ ConversionIncludeHiddenSpreadsheetData
Show spreadsheet border	Enterprise Vault\ConversionSpreadsheetBorder
Maximum conversion size	Enterprise Vault\MemLimitForTextConversionFallback
Log conversion failure events	Storage\FailedConversionEvents
Log fallback to text events	Storage\FallbackConversionEvents
Log conversion timeout events	Storage\ConversionTimeoutEvents
Log file type not recognized events	Storage\UnrecognisedFileTypeEvents
Log maximum conversion size exceeded events	Storage\RequestedAllocationSizeTooLargeEvents

Chapter 4

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 24.

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

   See "About upgrading a single Enterprise Vault server" on page 28.

   See "About upgrading multiple Enterprise Vault servers" on page 32.

   See "About upgrading a Veritas cluster" on page 36.

   See "About upgrading a Windows Server Failover Cluster" on page 41.

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

   See "Upgrading standalone Administration Consoles" on page 46.

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

   See "Upgrading Enterprise Vault Reporting" on page 48.

5. Perform the post-installation tasks as necessary:

   - Upgrade Exchange Server forms.

See “About upgrading Exchange Server forms” on page 54.

- Upgrade Domino mailbox archiving.
  See “About upgrading Domino mailbox archiving” on page 55.
- Upgrade the FSA Agent on the Windows servers on which it is installed.
  See “About upgrading the FSA Agent” on page 63.
- Upgrade the Enterprise Vault Office Mail App.
  See “About upgrading Enterprise Vault Office Mail App” on page 68.
- Upgrade OWA extensions.
  See “About upgrading OWA Extensions” on page 69.
- Upgrade SharePoint Server components.
  See “About upgrading the SharePoint components” on page 71.
- Upgrade legacy SMTP Archiving components.
  See “About upgrading legacy SMTP Archiving components” on page 73.
- Upgrade Enterprise Vault API applications.
  See “Upgrading any applications that use the Enterprise Vault API Runtime” on page 88.

Chapter 5

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 25.
- Run Enterprise Vault Deployment Scanner.
  See "Running Enterprise Vault Deployment Scanner" on page 26.
- Set database permissions.
  See "Setting database permissions" on page 27.
- Allow the MSMQ queues to empty.

See "Allowing the MSMQ queues to empty" on page 27.

- Check the archiving and expiry schedules.
  See "Checking the archiving and expiry schedules" on page 27.

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 Veritas Support website:

http://www.veritas.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.

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 Enterprise Vault, we strongly recommend that you run 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.veritas.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 **Veritas 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

Before you upgrade Enterprise Vault, you must ensure that the Vault Service account has all the necessary permissions.

You can verify the Vault Service account's permissions against the procedure in "Creating a SQL login account", in the *Installing and Configuring* guide.

Allowing the MSMQ queues to empty

Before you upgrade Enterprise Vault, we recommend that you allow the MSMQ queues to empty. 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 6

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 on a single server

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

Preparation

To prepare to upgrade the Enterprise Vault 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.

Installing Enterprise Vault (wizard)

To use the wizard to install Enterprise Vault

1. Load the Enterprise Vault 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 **Veritas Enterprise Vault Install Launcher** window, click **Enterprise Vault**.
4. Click **Server Installation**.
5. In the right pane, click **Upgrade existing server**.
6. Click **Install**. The Enterprise Vault installation wizard starts.
7. Work through the installation wizard to upgrade the Enterprise Vault components.
8. 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.

Installing Enterprise Vault (command line)

The following procedure describes how to upgrade the Enterprise Vault installation. If you want to add or remove components, see the "Installing Enterprise Vault" chapter in the *Installing and Configuring* guide for a complete description of the command-line options.

Caution: If a system restart is needed during silent installation, the server restarts automatically. If the server restarts, log on again as the Vault Service account so that the installer can complete the upgrade.

To install Enterprise Vault from the command line

1. Log on to the Enterprise Vault server as 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. Close the AutoPlay dialog box.
4. Open a command prompt window and navigate to the following folder on the Enterprise Vault media:

   ```
   \Veritas Enterprise Vault\Server\x64
   ```

5. Run `setup (x64).exe` as follows:

   ```
   "setup (x64).exe" /s
   ```

6. If the server restarts, log on again as the Vault Service account so that the installer can complete the upgrade.

Upgrading the Enterprise Vault databases

Before you start any Enterprise Vault services, you must upgrade the Enterprise Vault databases.

Enterprise Vault provides a PowerShell cmdlet called `Start-EVDatabaseUpgrade`, which you can use to upgrade all Enterprise Vault databases.

To upgrade Enterprise Vault's databases

1. On the Enterprise Vault server, log in using the Vault Service account.
2. Run the Enterprise Vault Management Shell.

3 In the Enterprise Vault Management Shell, run the following command:

```
Start-EVDatabaseUpgrade
```

Note that you can also run `Start-EVDatabaseUpgrade -verbose` if you want to see detailed output.

4 Wait for `Start-EVDatabaseUpgrade` to complete the upgrade of all the databases.

When the upgrade is complete, you can examine the upgrade reports for errors.

`Start-EVDatabaseUpgrade` writes the reports in the `Reports\DBUpgrade` subfolder of the Enterprise Vault installation folder (for example `C:\Program Files (x86)\Enterprise Vault`).

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.

Starting all the Enterprise Vault services

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

Chapter 7

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 on multiple servers

The following procedure describes how to install the Enterprise Vault 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.

Preparation

To prepare to upgrade the Enterprise Vault 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.

Installing Enterprise Vault (wizard)

To use the wizard to install Enterprise Vault

1. Load the Enterprise Vault 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 **Veritas Enterprise Vault Install Launcher** window, click **Enterprise Vault**.
4. Click **Server Installation**.
5. In the right pane, click **Upgrade existing server**.
6. Click **Install**. The Enterprise Vault installation wizard starts.
7. Work through the installation wizard to upgrade the Enterprise Vault components.
8. 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.

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

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

Installing Enterprise Vault (command line)

The following procedure describes how to upgrade the Enterprise Vault installation. If you want to add or remove components, see the "Installing Enterprise Vault" chapter in the *Installing and Configuring* guide for a complete description of the command-line options.

Caution: If a system restart is needed during silent installation, the server restarts automatically. If the server restarts, log on again as the Vault Service account so that the installer can complete the upgrade.

To install Enterprise Vault from the command line

1 Log on to the Enterprise Vault server as 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. Close the AutoPlay dialog box.

4 Open a Command Prompt window and navigate to the following folder on the Enterprise Vault media:

```
\Veritas Enterprise Vault\Server\x64
```

5 Run `setup (x64).exe` as follows:

```
"setup (x64).exe" /s
```

6 If the server restarts, log on again as the Vault Service account so that the installer can complete the upgrade.

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

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

Upgrading the Enterprise Vault databases

Before you start any Enterprise Vault services, you must upgrade the Enterprise Vault databases.

Note: You only need to complete this procedure on one Enterprise Vault server.

Enterprise Vault provides a PowerShell cmdlet called `Start-EVDatabaseUpgrade`, which you can use to upgrade all Enterprise Vault databases.

To upgrade Enterprise Vault's databases

1. On any Enterprise Vault server, log in using the Vault Service account.
2. Run the Enterprise Vault Management Shell.
3. In the Enterprise Vault Management Shell, run the following command:

   ```
   Start-EVDatabaseUpgrade
   ```

   Note that you can also run `Start-EVDatabaseUpgrade -verbose` if you want to see detailed output.
4. Wait for `Start-EVDatabaseUpgrade` to complete the upgrade of all the databases.

When the upgrade is complete, you can examine the upgrade reports for errors.

`Start-EVDatabaseUpgrade` writes the reports in the `Reports\DBUpgrade` subfolder of the Enterprise Vault installation folder (for example `C:\Program Files (x86)\Enterprise Vault`).

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.

Starting all the Enterprise Vault services

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

Chapter 8

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 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 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.

Preparation

To prepare to upgrade the Enterprise Vault server software

1. Log on to the active node as the Vault Service account.
2. Use the VCS cluster administration tools to take all the 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.

Installing Enterprise Vault (wizard)

To use the wizard to install Enterprise Vault

1. Load the Enterprise Vault 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 **Veritas Enterprise Vault Install Launcher** window, click **Enterprise Vault**.
4. Click **Server Installation**.

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

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

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

8 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.

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

Installing Enterprise Vault (command line)

The following procedure describes how to upgrade the Enterprise Vault installation. If you want to add or remove components, see the "Installing Enterprise Vault" chapter in the *Installing and Configuring* guide for a complete description of the command-line options.

Caution: If a system restart is needed during silent installation, the server restarts automatically. If the server restarts, log on again as the Vault Service account so that the installer can complete the upgrade.

To install Enterprise Vault from the command line

1 Log on to the active node as 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. Close the AutoPlay dialog box.

4 Open a command prompt window and navigate to the following folder on the Enterprise Vault media:

```
\Veritas Enterprise Vault\Server\x64
```

5 Run `setup (x64).exe` as follows:

```
"setup (x64).exe" /s
```

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

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

Upgrading the Enterprise Vault databases

Before you start any Enterprise Vault services, you must upgrade the Enterprise Vault databases.

Note: You only need to complete this procedure on the active node.

Enterprise Vault provides a PowerShell cmdlet called `Start-EVDatabaseUpgrade`, which you can use to upgrade all Enterprise Vault databases.

To upgrade Enterprise Vault's databases

1. On the active node, log in using the Vault Service account.
2. Run the Enterprise Vault Management Shell.
3. In the Enterprise Vault Management Shell, run the following command:

   ```
   Start-EVDatabaseUpgrade
   ```

   Note that you can also run `Start-EVDatabaseUpgrade -verbose` if you want to see detailed output.
4. Wait for `Start-EVDatabaseUpgrade` to complete the upgrade of all the databases.

When the upgrade is complete, you can examine the upgrade reports for errors.

`Start-EVDatabaseUpgrade` writes the reports in the `Reports\DBUpgrade` subfolder of the Enterprise Vault installation folder (for example `C:\Program Files (x86)\Enterprise Vault`).

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.

Starting all the Enterprise Vault services

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 9

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 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.

Preparation

To prepare to upgrade the Enterprise Vault 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.

Installing Enterprise Vault (wizard)

To use the wizard to install Enterprise Vault

1. Load the Enterprise Vault 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 **Veritas Enterprise Vault Install Launcher** window, click **Enterprise Vault**.
4. Click **Server Installation**.
5. In the right pane, click **Upgrade existing server**.
6. Click **Install**. The Enterprise Vault installation wizard starts.
7. Work through the installation wizard to upgrade the Enterprise Vault components.
8. 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.
9. Install the Enterprise Vault software on the other servers in your Enterprise Vault environment, including any cluster failover nodes.

Installing Enterprise Vault (command line)

The following procedure describes how to upgrade the Enterprise Vault installation. If you want to add or remove components, see the "Installing Enterprise Vault" chapter in the *Installing and Configuring* guide for a complete description of the command-line options.

Caution: If a system restart is needed during silent installation, the server restarts automatically. If the server restarts, log on again as the Vault Service account so that the installer can complete the upgrade.

To install Enterprise Vault from the command line

1. Log on to the active node as 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. Close the AutoPlay dialog box.

4 Open a command prompt window and navigate to the following folder on the Enterprise Vault media:

```
\Veritas Enterprise Vault\Server\x64
```

5 Run `setup (x64).exe` as follows:

```
"setup (x64).exe" /s
```

6 If the server restarts, log on again as the Vault Service account so that the installer can complete the upgrade.

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

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

Upgrading the Enterprise Vault databases

Before you start any Enterprise Vault services, you must upgrade the Enterprise Vault databases.

Note: You only need to complete this procedure on the active node.

Enterprise Vault provides a PowerShell cmdlet called `Start-EVDatabaseUpgrade`, which you can use to upgrade all Enterprise Vault databases.

To upgrade Enterprise Vault's databases

1 On the active node, log in using the Vault Service account.

2 Run the Enterprise Vault Management Shell.

3 In the Enterprise Vault Management Shell, run the following command:

```
Start-EVDatabaseUpgrade
```

Note that you can also run `Start-EVDatabaseUpgrade -verbose` if you want to see detailed output.

4 Wait for `Start-EVDatabaseUpgrade` to complete the upgrade of all the databases.

When the upgrade is complete, you can examine the upgrade reports for errors.

`Start-EVDatabaseUpgrade` writes the reports in the `Reports\DBUpgrade` subfolder of the Enterprise Vault installation folder (for example `C:\Program Files (x86)\Enterprise Vault`).

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.

Starting all the Enterprise Vault services

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

Upgrading standalone Administration Consoles

This chapter includes the following topics:

Upgrading standalone Administration Consoles

If you have any computers on which you have installed the Enterprise Vault Administration Console component only, you must upgrade it. Note that the supported versions of Windows for standalone Administration Consoles are as follows:

- Windows 7
- Windows 8
- Windows 8.1
- Windows 10
- Windows Server 2012

Upgrading a standalone Administration Console (wizard)

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 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 **Veritas 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.

Installing Enterprise Vault (command line)

To upgrade the Administration Console from the command line

1 Log on to the computer as 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. Close the AutoPlay dialog box.

4 Open a Command Prompt window and navigate to the following folder on the Enterprise Vault media:

```
\Veritas Enterprise Vault\Server
```

5 Run the appropriate setup file, as follows:

- On a computer that runs 64-bit version of Windows:

  ```
  "x64\setup (x64).exe" /s
  ```

- On a computer that runs 32-bit version of Windows:

  ```
  "x86\setup (x86).exe" /s
  ```

Chapter 11

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 11-1 lists the steps that are required to upgrade Enterprise Vault Reporting.

Table 11-1 Steps to install Enterprise Vault Reporting

Step	Action	Description
Step 1	Remove the existing Symantec Enterprise Vault folder.	Use the Microsoft SQL Server Reporting Services Report Manager web application to remove the folder.
Step 2	Install the Enterprise Vault 12 Reporting component on each computer on which the Enterprise Vault Reporting component is installed.	See "Installing the Enterprise Vault Reporting component" on page 49.

Table 11-1 Steps to install Enterprise Vault Reporting *(continued)*

Step	Action	Description
Step 3	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 50.

Installing the Enterprise Vault Reporting component

You must remove the existing Symantec Enterprise Vault folder using the Microsoft SQL Server Reporting Services Report Manager web application before you install the Enterprise Vault 12 Reporting component.

You must install the Enterprise Vault 12 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 12 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 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 **Veritas 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 12 software on the Enterprise Vault servers.
- Installed the Enterprise Vault 12 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 Veritas Support website:

   http://www.veritas.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 12

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 12-1 describes the management packs that come with Enterprise Vault.

Table 12-1 SCOM management packs in Enterprise Vault

Management pack	Description
Veritas.EnterpriseVault.12.mp	Required for monitoring Enterprise Vault 12. Importing the pack creates an **Enterprise Vault** 12 node under the **Veritas Enterprise Vault** node in SCOM. This node contains all the servers with Enterprise Vault 12.
Veritas.EnterpriseVault.Library.mp	A common library that is required for monitoring all versions of Enterprise Vault.
Veritas.EnterpriseVault.12.Reports.mp	Required so that reports can be viewed.

You must import both the Veritas.EnterpriseVault.12.mp and Veritas.EnterpriseVault.Library.mp packs to implement the new monitoring facilities in Enterprise Vault 12.

About the upgrade procedure

To upgrade the Enterprise Vault SCOM management pack, import the Enterprise Vault 12 management pack. You do not need to delete the previous management packs.

After you have imported the Enterprise Vault 12 management packs, you may see two nodes depending on whether you have both Enterprise Vault 12 servers and older versions of Enterprise Vault:

- **Symantec Enterprise Vault** - Enterprise Vault 11.0.1 or earlier servers.
- **Veritas Enterprise Vault** - Enterprise Vault 12 servers.

To monitor the existing Enterprise Vault 11.0.x servers, you need to use the Enterprise Vault 11.0.x management packs.

If you no longer need to monitor older versions of Enterprise Vault server, you can delete the previous Enterprise Vault management packs.

To delete the previous Enterprise Vault management packs

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.

Chapter 13

Upgrading Exchange Server forms

This chapter includes the following topics:

About upgrading Exchange Server forms

By default, Enterprise Vault 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 14

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.

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 Enterprise Vault.

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 55.

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 Veritas Enterprise Vault 12 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 Veritas Enterprise Vault 12 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 14-1 shows how the NotesDomains registry key controls how Enterprise Vault identifies internal mail recipients.

Table 14-1 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 14-1 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 15

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 12 does not support File System Archiving from Windows file servers that run Windows Server 2008 R2 or earlier. The minimum supported version is Windows 2008 R2 SP1. You cannot install the 12 version of the FSA Agent on a Windows file server that is running Windows Server 2008 R2 or earlier.

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.veritas.com/docs/000097605.
- For FSA Reporting, the Enterprise Vault technical note at http://www.veritas.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 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 Veritas Support website:

http://www.veritas.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 Veritas Support website:

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

Table 15-1 describes the options for upgrading the FSA Agent.

Table 15-1 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 64.
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 65.
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 66.

Table 15-1 Upgrading the FSA Agent *(continued)*

To do this	See this section
Upgrade the FSA Agent manually.	See "Upgrading the FSA Agent manually" on page 67.

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 65.
   - Upgrade the FSA Agent manually on each file server node.
     See "Upgrading the FSA Agent manually" on page 67.
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 16

Upgrading Enterprise Vault Office Mail App

This chapter includes the following topics:

About upgrading Enterprise Vault Office Mail App

If you have deployed the Enterprise Vault Office Mail App, then you need to upgrade the deployed version after you have upgraded the Enterprise Vault server.

To upgrade Enterprise Vault Office Mail App

1. On the Exchange Server, rerun the New-App command that you originally used to deploy the Enterprise Vault Office Mail App.

   The New-App command lines for deploying the application to individual or multiple users are given in the section, "Deploying the Enterprise Vault Office Mail App", in *Setting up Exchange Server Archiving*.

2. On the Enterprise Vault server, synchronize the mailboxes to which you have deployed the Enterprise Vault Office Mail App.

   If the Exchange Mailbox Archiving task is set to run automatically, it synchronizes mailboxes the next time it runs. Alternatively, you can synchronize the mailboxes manually using the Enterprise Vault Administration Console. Open the properties dialog of the Exchange Mailbox Archiving task, and select the **Synchronization** tab for the manual synchronization options.

Chapter 17

Upgrading OWA Extensions

This chapter includes the following topics:

About upgrading OWA Extensions

This chapter describes how to upgrade the Enterprise Vault OWA 2010 Extensions to Enterprise Vault 12.

You must upgrade the Enterprise Vault OWA Extensions on each Exchange Server CAS computer in your Enterprise Vault environment.

If you have problems when you install the Enterprise Vault OWA Extensions, see the following technical note on the Veritas Support website:

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

This technical note gives detailed troubleshooting information for the 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 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 **Veritas 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 `Veritas 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.

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 SharePoint Server 2013
  - Microsoft SharePoint Foundation 2013

  See "Upgrading the Enterprise Vault SharePoint components" on page 72.
- If you have started a gradual migration from SharePoint Portal Server 2003 or Windows SharePoint Services 2.0 to Microsoft SharePoint Server 2013 or Microsoft SharePoint Foundation 2013, 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 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 **Veritas 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.

Chapter 19

Upgrading legacy SMTP archiving components

This chapter includes the following topics:

About upgrading legacy SMTP Archiving components

Enterprise Vault 11.0.1 introduced a completely new version of SMTP Archiving. The new implementation 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 12 SMTP Archiving components, and rerun the legacy Enterprise Vault SMTP Archiving configuration process.

For guidance on how to migrate from the legacy version of SMTP Archiving to the new version, see the following article on the Veritas Support website:

http://www.veritas.com/docs/000004481

Chapter 20

Upgrading your Enterprise Vault sites to use Enterprise Vault Search

This chapter includes the following topics:

About Enterprise Vault Search

Note: You need only follow the instructions in this chapter if you want to upgrade an Enterprise Vault site in which Enterprise Vault Search was not previously available.

Enterprise Vault Search enables client users to browse and search their archives. This feature replaces the legacy search applications: Archive Explorer, Browser Search, and Integrated Search, which are no longer available.

Server requirements for Enterprise Vault Search

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. Click **Start** > **Control Panel** > **Turn Windows features on or off**.

   The **Add Roles and Features** wizard starts.
2. Click **Next** until the **Features** page is shown.
3. Expand **.NET Framework 4.5 Features**.
4. Expand **WCF Services**.
5. Select **HTTP Activation** and then click **Install**.
6. Work through to the end of the wizard.

How to resolve potential Net.Tcp issues

Other aspects of your Net.Tcp configuration may sometimes cause Enterprise Vault Search to fail. Where this is the case, the 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 Veritas Support website:

http://www.veritas.com/docs/000020737

See also the following article in the Microsoft Knowledge Base:

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

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 out of an archive, within an archive, and from one archive to another. Choosing to allow these actions also allows users to create, rename, move, and delete folders in their archives.
- 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 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. After you install Enterprise Vault, a default search provisioning group is available with which you can assign the default search policy to all users. If you want to assign a custom search policy to selected users or groups, you must set up a custom provisioning group. The default provisioning group continues to target those users whom you do not assign to a custom provisioning group.

You can set up any number of custom 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 view the properties of the default 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. Click the **Provisioning Groups** container.
4. In the right pane, right-click **Default Search Provisioning Group** and then click **Properties**.

   You cannot amend any of the properties.

To set up a custom 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

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.veritas.com/docs/000097605.

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 and local storage.
- Enable JavaScript.
- Disable private browsing or the settings that prevent their browsers from storing data about their browsing.
- If an option to not save encrypted pages to disk is available, disable it.

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 Forefront TMG and similar environments

By default, Enterprise Vault Search implements security best practices for all supported browsers. In some environments, these restrictions can affect the functionality of Enterprise Vault Search. For example, if you implement forms-based authentication through Forefront Threat Management Gateway (TMG), the reading pane of Enterprise Vault Search may contain the logon screen rather than a preview of the selected item.

This issue arises because Enterprise Vault Search uses an attribute to enforce the Restricted Sites zone settings in the reading pane. In fact, this mechanism is needed for Internet Explorer 9 and earlier only; version 10 and later uses a different security mechanism, which Enterprise Vault Search also implements. However, because version 10 and later still respects the older security mechanism, the reading pane

does not work in these later versions either. So, if your users do not run Internet Explorer 9 and earlier, you can configure Enterprise Vault to not use the attribute to enforce the Restricted Sites zone settings. The reading pane then works without reducing security.

To configure Enterprise Vault Search for use in Forefront TMG and 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 enables users to 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 83.
- Obtain a digital certificate from a certification authority 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 and local storage, 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 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.
- 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 4.5.2.
  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, Veritas-approved alternatives.

You can comply with Veritas 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 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 Veritas 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.

Configuring the maximum number of permitted login attempts

By default, users who make five unsuccessful attempts to log in to Enterprise Vault Search Mobile edition are barred for 24 hours from making further login attempts from the same device. You can configure the maximum number of login attempts that you want to permit and the number of hours for which barred users are locked out.

To configure the maximum number of permitted login attempts

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 lines and change the values to the required ones.

   ```
   <add key="EVSMobileMaxFailedAttemptsAllowed" value="5" />
   <add key="EVSMobileLoginRestrictedTimeoutInHours" value="24" />
   ```

4. Save and close the file.

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.