

Symantec Enterprise Vault™

Upgrading to Enterprise Vault 10.0.4



Symantec Enterprise Vault: Upgrading to Enterprise Vault 10.0.4

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

Last updated: 2013-07-04.

Legal Notice

Copyright © 2013 Symantec Corporation. All rights reserved.

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

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

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

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

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

Symantec Corporation
350 Ellis Street, Mountain View, CA 94043

<http://www.symantec.com>

Technical Support

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

Symantec's support offerings include the following:

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

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

<http://support.symantec.com>

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

Contacting Technical Support

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

<http://support.symantec.com>

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

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

- Product release level

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

Licensing and registration

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

<http://support.symantec.com>

Customer service

Customer service information is available at the following URL:

<http://support.symantec.com>

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

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

Support agreement resources

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

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

Contents

Technical Support	3
Chapter 1 About this guide	13
Introducing this guide	13
Where to get more information about Enterprise Vault	13
“How To” articles on the Symantec Enterprise Support site	15
Enterprise Vault training modules	16
Comment on the documentation	16
Chapter 2 Before you begin	17
Server upgrade paths	17
Documentation	17
Chapter 3 Points to note when upgrading from Enterprise Vault 9.0	19
About this chapter	20
Changes to prerequisite hardware and software	20
Order of upgrade in an environment with Compliance Accelerator or Discovery Accelerator	20
Exchange Server 2013 support	21
Enterprise Vault 9.0–9.0.3 server hotfixes required to support the Outlook Add-In	21
All Enterprise Vault servers must run the same version of Enterprise Vault	22
FSA no longer supports archiving from Windows 2000 file servers	22
Changes to support FSA targets without Administrator privileges for the Vault Service account	22
Default File Blocking location is no longer supported	23
Enterprise Vault installation path cannot contain non-ASCII characters	24
Requirements for upgrading the Enterprise Vault databases	24
Directory database upgrade requirements	24
Storage database upgrade requirements	25

	Changes to indexing at Enterprise Vault 10.0	26
	About unfinished index rebuild and repair tasks on upgrade	27
	Exchange throttling policy script has changed	27
	Upgrading FSA metadata	28
	Upgrading Enterprise Vault Domino Server archiving	28
	Securing data locations	29
	Paths to index locations cannot contain non-ASCII characters	30
	Changes to retention category settings for the deletion of archived items	30
Chapter 4	Points to note when upgrading from Enterprise Vault 10.0	33
	About this chapter	34
	Order of upgrade in an environment with Compliance Accelerator or Discovery Accelerator	34
	Exchange Server 2013 support	34
	Enterprise Vault 10.0 original release server hotfix required to support the Outlook Add-In	35
	Assigning the required permissions to the Vault Service account	35
	Requirements for upgrading the Enterprise Vault databases	36
	Directory database upgrade requirements	36
	Changes to best practice settings	37
	Changes to index roll-over	38
	Changes to support FSA targets without Administrator privileges for the Vault Service account	38
	About upgrading FSA targets that run a Server Core installation of Windows	39
	Default File Blocking location is no longer supported	40
	Changes to retention category settings for the deletion of archived items	40
	File System Archiving of files under Dynamic Access Control	41
Chapter 5	Steps to upgrade your system	43
	Overview of the upgrade process	43
Chapter 6	Enterprise Vault server preparation	45
	About Enterprise Vault server preparation	45
	Changing the recovery model of the Directory database	46
	Backing up the system	46
	Backing up Enterprise Vault data	47

	Backing up changed language files	47
	Backing up the SCOM management pack	48
	Running Enterprise Vault Deployment Scanner	48
	Setting database permissions	49
	Allowing the MSMQ queues to empty	49
	Checking the archiving and expiry schedules	49
	Preparing for indexing changes	49
	Adding the 'URL Authorization' IIS security role	50
Chapter 7	Single server: upgrading the Enterprise Vault server software	53
	About upgrading a single Enterprise Vault server	53
	Installing the Enterprise Vault 10.0.4 server software on a single server	54
	Upgrading the Directory database	55
	Starting the Storage service and upgrading the storage databases	56
	Upgrading indexing metadata and schema version	57
	Upgrading the auditing database	58
	Backing up the upgraded Enterprise Vault databases	59
	Starting all the Enterprise Vault services	59
Chapter 8	Multiple servers: upgrading the Enterprise Vault server software	61
	About upgrading multiple Enterprise Vault servers	61
	Installing the Enterprise Vault 10.0.4 server software on multiple servers	62
	Upgrading the Directory database	63
	Starting the Storage service on all servers and upgrading the storage databases	64
	Upgrading indexing metadata and schema version	65
	Upgrading the auditing database	66
	Backing up the upgraded Enterprise Vault databases	67
	Starting all the Enterprise Vault services	67
Chapter 9	Veritas Cluster Server: upgrading the Enterprise Vault server software	69
	About upgrading a Veritas cluster	69
	Veritas Cluster Server: installing the Enterprise Vault 10.0.4 software	70
	Upgrading the Directory database	71

	Starting the Storage service on all servers and upgrading the storage databases	72
	Upgrading indexing metadata and schema version	73
	Moving the index metadata location to a shared drive	74
	Upgrading the auditing database	75
	Backing up the upgraded Enterprise Vault databases	76
	Starting all the Enterprise Vault services	76
Chapter 10	Windows Server Failover Clustering: upgrading the Enterprise Vault server software	77
	About upgrading a Windows Server Failover Cluster	78
	Windows Server Failover Clustering: installing the Enterprise Vault 10.0.4 software	78
	Upgrading the Directory database	82
	Starting the Storage service on all servers and upgrading the storage databases	83
	Upgrading indexing metadata and schema version	85
	Moving the index metadata location to a shared drive	86
	Upgrading the auditing database	86
	Backing up the upgraded Enterprise Vault databases	87
	Starting all the Enterprise Vault services	87
Chapter 11	Upgrading stand-alone Administration Consoles	89
	Upgrading stand-alone Administration Consoles	89
Chapter 12	Upgrading Enterprise Vault Reporting	91
	Upgrading Enterprise Vault Reporting	91
	Installing the Enterprise Vault Reporting component	92
	Running the Enterprise Vault Reporting Configuration utility	92
Chapter 13	Upgrading MOM and SCOM	95
	Upgrading MOM	95
	Upgrading SCOM	95
Chapter 14	Upgrading Exchange Server forms	97
	About upgrading Exchange Server forms	97

Chapter 15	Upgrading Domino mailbox archiving	99
	About upgrading Domino mailbox archiving	99
	Domino client version required to run EVInstall.nsf	100
	Preparing for the upgrade of Domino mailbox archiving	100
	Upgrading Domino mailbox archiving	101
	Granting the Domino archiving user access to mail files	102
	Identifying internal mail recipients	103
	Minimizing the potential performance effects of shortcut deletion	105
Chapter 16	Upgrading the FSA Agent	107
	About upgrading the FSA Agent	107
	Upgrading FSA Agent services that are clustered for high availability	109
	Upgrading the FSA Agent on a target Windows file server from the Administration Console	110
	Upgrading the FSA Agent on an FSA Reporting proxy server from the Administration Console	111
	Upgrading the FSA Agent manually	112
Chapter 17	Upgrading OWA and RPC Extensions	113
	About upgrading OWA and RPC Extensions	113
	Upgrading Enterprise Vault OWA 2010 Extensions	114
	Upgrading Enterprise Vault OWA 2007 Extensions	114
	Upgrading Enterprise Vault OWA 2003 Extensions	115
	Preparing EVServers.txt	116
	OWA 2003: Installing the Enterprise Vault OWA 2003 Extensions	117
	Upgrading Enterprise Vault OWA 2000 Extensions	117
	Preparing EVServers.txt	118
	OWA 2000: Installing the Enterprise Vault OWA 2000 Extensions	118
Chapter 18	Upgrading SharePoint Server components	119
	About upgrading the SharePoint components	119
	Upgrading the Enterprise Vault SharePoint components	120
Chapter 19	Upgrading SMTP archiving	123
	About upgrading SMTP Archiving	123
	Installing the Enterprise Vault SMTP Archiving components	125

Running the Enterprise Vault SMTP Archiving configuration
process 126

Chapter 20 Upgrading custom filters 129

Upgrading Exchange Journal archiving filters 129

Upgrading API custom filters 130

Upgrading Domino Filtering API custom filters 130

About this guide

This chapter includes the following topics:

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

Introducing this guide

This guide describes how to upgrade to Enterprise Vault 10.0.4.

If you are performing a new installation of Enterprise Vault, see the Enterprise Vault 10.0.4 *ReadMeFirst*. Then follow the installation instructions in *Installing and Configuring*, which is in the Symantec Enterprise Vault\Documentation folder on the Enterprise Vault 10.0.4 release media.

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

<http://www.symantec.com/docs/DOC6263>

Where to get more information about Enterprise Vault

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

Table 1-1 Enterprise Vault documentation set

Document	Comments
Symantec Enterprise Vault Documentation Library	<p>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.</p> <p>You can access the library in several ways, including the following:</p> <ul style="list-style-type: none"> ■ On the Windows Start menu, click Start > Programs > Enterprise Vault > Documentation. ■ In Windows Explorer, browse to the <code>Documentation\language</code> subfolder of the Enterprise Vault installation folder, and then open the <code>EV_Help.chm</code> file. ■ On the Help menu in the Administration Console, click Help on Enterprise Vault.
<i>Introduction and Planning</i>	Provides an overview of Enterprise Vault functionality.
<i>Deployment Scanner</i>	Describes how to check the prerequisite software and settings before you install Enterprise Vault.
<i>Installing and Configuring</i>	Provides detailed information on setting up Enterprise Vault.
<i>Upgrade Instructions</i>	Describes how to upgrade an existing Enterprise Vault installation to the latest version.
<i>Setting up Exchange Server Archiving</i>	Describes how to archive items from Microsoft Exchange user mailboxes, journal mailboxes, and public folders.
<i>Setting up Domino Server Archiving</i>	Describes how to archive items from Domino mail files and journal databases.
<i>Setting up File System Archiving</i>	Describes how to archive the files that are held on network file servers.
<i>Setting up SharePoint Server Archiving</i>	Describes how to archive content from Microsoft SharePoint servers.
<i>Setting up SMTP Archiving</i>	Describes how to archive SMTP messages from other messaging servers.
<i>Administrator's Guide</i>	Describes how to perform day-to-day administration, backup, and recovery procedures.

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

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

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

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

“How To” articles on the Symantec Enterprise Support site

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

To access the “How To” articles on the Symantec Enterprise Support site

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

Enterprise Vault training modules

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

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

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

Comment on the documentation

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

Please include the following information with your comment:

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

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

We appreciate your feedback.

Before you begin

This chapter includes the following topics:

- [Server upgrade paths](#)
- [Documentation](#)

Server upgrade paths

This guide describes how to upgrade to Enterprise Vault 10.0.4. The only possible server upgrade paths to this version are from the following:

- Enterprise Vault 9.0 or any Enterprise Vault 9.0 service pack.
- Enterprise Vault 10.0 or any Enterprise Vault 10.0 service pack.

If your Enterprise Vault servers are running a version of Enterprise Vault that is older than Enterprise Vault 9.0, you must first upgrade to Enterprise Vault 9.0 and then upgrade to Enterprise Vault 10.0.4.

Note: Do not upgrade to Enterprise Vault 9.0 and then immediately upgrade to Enterprise Vault 10.0.4. You must complete the Enterprise Vault 9.0 post-installation tasks as described in the Enterprise Vault 9.0 upgrade instructions, before you upgrade to Enterprise Vault 10.0.4.

Documentation

Do the following before you upgrade your system:

- Read through this guide and the Enterprise Vault 10.0.4 *ReadMeFirst*. For the most up-to-date versions of this guide and the *ReadMeFirst*, see the following page on the Symantec Support website:
<http://www.symantec.com/docs/DOC6263>

- Check that the prerequisites for Enterprise Vault 10.0.4 are satisfied, as described in the *Installing and Configuring* guide. The guide is in the `Symantec Enterprise Vault\Documentation` folder on the Enterprise Vault 10.0.4 media. See “[Where to get more information about Enterprise Vault](#)” on page 13.

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

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

Points to note when upgrading from Enterprise Vault 9.0

This chapter includes the following topics:

- [About this chapter](#)
- [Changes to prerequisite hardware and software](#)
- [Order of upgrade in an environment with Compliance Accelerator or Discovery Accelerator](#)
- [Exchange Server 2013 support](#)
- [Enterprise Vault 9.0–9.0.3 server hotfixes required to support the Outlook Add-In](#)
- [All Enterprise Vault servers must run the same version of Enterprise Vault](#)
- [FSA no longer supports archiving from Windows 2000 file servers](#)
- [Changes to support FSA targets without Administrator privileges for the Vault Service account](#)
- [Default File Blocking location is no longer supported](#)
- [Enterprise Vault installation path cannot contain non-ASCII characters](#)
- [Requirements for upgrading the Enterprise Vault databases](#)
- [Changes to indexing at Enterprise Vault 10.0](#)
- [About unfinished index rebuild and repair tasks on upgrade](#)

- Exchange throttling policy script has changed
- Upgrading FSA metadata
- Upgrading Enterprise Vault Domino Server archiving
- Securing data locations
- Paths to index locations cannot contain non-ASCII characters
- Changes to retention category settings for the deletion of archived items

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.

Changes to prerequisite hardware and software

The hardware and software prerequisites have changed at Enterprise Vault 10.0. For details, see the Enterprise Vault 10.0.4 *ReadMeFirst*.

We recommend that you run Enterprise Vault Deployment Scanner as part of the upgrade process to check that the software prerequisites are all present.

See also the *Enterprise Vault Compatibility Charts* at <http://www.symantec.com/docs/TECH38537>.

For information on how to migrate Enterprise Vault 9.0 servers from 32-bit to 64-bit hardware, see the following page on the Symantec Support website:

<http://www.symantec.com/docs/HOWTO42430>

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

If the Enterprise Vault environment that you are upgrading includes Compliance Accelerator or Discovery Accelerator, the Accelerator version must be upgraded to 10.0.4 or later. The Accelerator version can be up to one major version higher than Enterprise Vault, but it must not be lower than the version of Enterprise Vault.

See the *Enterprise Vault Compatibility Charts* at <http://www.symantec.com/docs/TECH38537>.

You must upgrade the Accelerator product before you upgrade Enterprise Vault. Perform the upgrades in the following order:

- Upgrade the Accelerator product.
- Then upgrade Enterprise Vault on the Accelerator server.
- Finally, upgrade Enterprise Vault on the Enterprise Vault server.

Exchange Server 2013 support

Enterprise Vault 10.0.3 introduced support for Exchange Server 2013 archiving.

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

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

The Enterprise Vault documentation is in the `Symantec Enterprise Vault\Documentation` folder on the Enterprise Vault 10.0.4 media.

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

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

Enterprise Vault 9.0–9.0.3 server hotfixes required to support the Outlook Add-In

Note: This section applies if you are upgrading from Enterprise Vault 9.0.3 or any earlier version of Enterprise Vault 9.0.

If you plan to roll out the Enterprise Vault 10.0.4 Outlook Add-In to users before you upgrade the Enterprise Vault servers, you must apply a hotfix to the Enterprise Vault servers to avoid the restrictions listed in this section. There is a separate hotfix for each affected version of Enterprise Vault.

Table 3-1 provides the links to the relevant technical notes and the hotfixes that are required to support the Enterprise Vault 10.0.4 Outlook Add-In with Enterprise Vault 9.0–9.0.3 servers.

Table 3-1 Enterprise Vault server 9.0–9.0.3 hotfixes for Outlook Add-In support

Enterprise Vault server version	Link to technical note and hotfix
Enterprise Vault 9.0 original release	http://www.symantec.com/docs/TECH175938
Enterprise Vault 9.0.1	http://www.symantec.com/docs/TECH175939
Enterprise Vault 9.0.2	http://www.symantec.com/docs/TECH175940
Enterprise Vault 9.0.3	http://www.symantec.com/docs/TECH175941

The following restrictions apply to the Enterprise Vault 10.0.4 Outlook Add-In if you have not installed the appropriate hotfix on Enterprise Vault servers that have not been upgraded:

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

All Enterprise Vault servers must run the same version of Enterprise Vault

All of the Enterprise Vault servers that connect to the same Directory database must run the same version and service pack of Enterprise Vault.

FSA no longer supports archiving from Windows 2000 file servers

Note that Enterprise Vault 10.0 does not support File System Archiving from file servers that run Windows 2000.

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

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

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

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

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

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

Note the following changes that take effect after the upgrade:

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

Default File Blocking location is no longer supported

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

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

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

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

Enterprise Vault installation path cannot contain non-ASCII characters

The path of the Enterprise Vault installation folder cannot contain non-ASCII characters. The installation program does not let you install to a folder path that contains non-ASCII characters.

If your existing Enterprise Vault 9.0 installation path contains non-ASCII characters, see the following technical note on the Symantec Support website:

<http://www.symantec.com/docs/TECH159463>

Requirements for upgrading the Enterprise Vault databases

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

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

- See “[Directory database upgrade requirements](#)” on page 24.
- See “[Storage database upgrade requirements](#)” on page 25.

Directory database upgrade requirements

When the Directory service starts for the first time after you install the Enterprise Vault 10.0 software, it upgrades the Directory database schema.

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

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

[Table 3-2](#) lists the additional space requirements.

Table 3-2 Space required for the upgrade of the Directory database

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

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

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

See [“Backing up Enterprise Vault data”](#) on page 47.

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

If the Directory database recovery model is currently set to Full, we recommend that you change the recovery model to Simple before you upgrade. This action improves the upgrade speed, and reduces the log file growth during upgrade. After you complete the Enterprise Vault upgrade you can revert to the Full recovery model.

See [“Changing the recovery model of the Directory database”](#) on page 46.

Storage database upgrade requirements

When each Storage service starts for the first time after you install the Enterprise Vault 10.0 software, it upgrades the schemas of the vault store databases that it manages, and the associated fingerprint databases, if required.

The upgrade time for each vault store database is significant if there are tens of millions of items in the JournalDelete table or the JournalArchive table. The vault

store database transaction log will also grow during the upgrade, as it records the changes.

The upgrade of a large vault store database may take a long time to complete, depending on the size of the database and the available resources.

Make sure that you perform the recommended maintenance activities when you back up the databases before the upgrade.

See [“Backing up Enterprise Vault data”](#) on page 47.

Changes to indexing at Enterprise Vault 10.0

Enterprise Vault 10.0 creates 64-bit indexes and does not add new index data to existing 32-bit indexes. The 32-bit indexes are still available for searching. If you use expiry, Enterprise Vault updates the 32-bit indexes to remove details of those archived items that expiry has deleted.

The new 64-bit indexes have indexing levels of Brief or Full. The Medium level is no longer available. When you upgrade to Enterprise Vault 10.0 the behavior is as follows:

- An archive with Brief indexing stays as Brief.
- An archive with Medium indexing changes to Full indexing for the items that are archived in Enterprise Vault 10.0.
- An archive with Full indexing stays as Full. The default for a new archive is Full indexing.

The way you configure index volume rollover has changed at Enterprise Vault 10.0. The **AVSMaxLoc** registry value now applies to 32-bit indexes only. 64-bit indexes use the setting **Maximum items in an index volume** on the **Advanced** tab of the Enterprise Vault server's properties. The default maximum value for 64-bit indexes is 5,000,000 items. Do not change this value unless your technical support provider advises you to do so. For more information on the new setting, see "Computer properties advanced settings" in the *Administrator's Guide*.

Enterprise Vault 10.0 introduces Index Server groups. An Enterprise Vault server that runs an Indexing service (an Index Server) can be added to an Index Server group, or can remain ungrouped. Index Server groups provide load-balanced Indexing services for large or distributed Enterprise Vault environments. In a distributed environment, some Enterprise Vault servers may host Storage services, while others host Indexing services.

See the section "About Index Server groups" in the *Introduction and Planning* guide.

See the chapter "Setting up Index Server groups" in the *Installing and Configuring* guide.

If you use Enterprise Vault building blocks there are some restrictions to the configuration that you can use for Index Server groups.

See the chapter "Failover in a building blocks configuration" in the *Administrator's Guide*.

About unfinished index rebuild and repair tasks on upgrade

We recommend that you let any Index rebuild tasks finish before you perform the upgrade.

The Directory database upgrade handles unfinished index repair tasks and rebuild tasks as follows:

- Index repair tasks are abandoned. After the upgrade you can synchronize an index volume to fix known issues, if required.
- Index rebuild tasks stop, and any partially rebuilt volumes are closed. Enterprise Vault creates a new 64-bit index volume to hold the remaining unindexed items.

Exchange throttling policy script has changed

Note: This section only applies if you are upgrading from the Enterprise Vault 9.0 original release or from Enterprise Vault 9.0.1.

Enterprise Vault includes a PowerShell script called `SetEVThrottlingPolicy.ps1`, which assigns a new throttling policy to the Vault Service account, in support of Exchange 2010 and 2013 archiving.

This script was changed in Enterprise Vault 9.0.2. If you are upgrading from the Enterprise Vault 9.0 original release or from Enterprise Vault 9.0.1, you must run this script again, as described in the section "Configuring the Exchange throttling policy on the Vault Service account" in *Installing and Configuring*.

Upgrading FSA metadata

Note: This section only applies if you previously upgraded to Enterprise Vault 9.0.

If you use File System Archiving and you upgraded to Enterprise Vault 9.0, then before you upgrade to Enterprise Vault 10.0 you must upgrade the FSA metadata in your vault store databases to the new summarized format.

You should have done the FSA metadata upgrade as part of your upgrade to Enterprise Vault 9.0. If you need to upgrade the metadata, a warning message appears in the Enterprise Vault 9.0 Administration Console's Status pane. The message lists the affected Enterprise Vault servers, and the number of vault stores that require upgrading. The message persists until you upgrade the data in all of the affected vault stores.

If you have not yet upgraded your FSA metadata you must use the **FSA upgrade utility** command line tool to perform the required actions.

For information on how to use the FSA upgrade utility, see the Enterprise Vault 9.0 *Utilities* guide.

Upgrading Enterprise Vault Domino Server archiving

The minimum required versions of Domino Server and the Notes client have changed for Enterprise Vault 10.0. Before you start the upgrade you must make sure that the appropriate versions of Domino Server and the Notes client are installed on the required computers.

[Table 3-3](#) lists the minimum requirements.

Table 3-3 Prerequisite minimum software versions for Domino Server archiving

Computer type	Required minimum software versions
Enterprise Vault Domino Gateway	One of the following software combinations: <ul style="list-style-type: none">■ Domino Server 8.5.2 (32-bit version) Fix Pack 2 or higher and Notes client 8.5.2 or higher■ Domino Server 8.5.3 (64-bit version) and Notes client 8.5.3
Domino mail server	Domino Server 7.0 or above
Enterprise Vault server	Notes client 8.5.2

Table 3-3 Prerequisite minimum software versions for Domino Server archiving
(continued)

Computer type	Required minimum software versions
Remote Enterprise Vault Administration Console computer	Notes client 8.5.2
The workstation from which you intend to run EVInstall.nsf to install the Notes client and iNotes (DWA) extensions	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.

For details of the latest information on supported versions of Domino software, see the *Enterprise Vault Compatibility Charts* at <http://www.symantec.com/docs/TECH38537>.

Securing data locations

It is important to secure the locations that are used for storing Enterprise Vault data. Only authorized accounts should have access to the network shares and folders that are to be used for indexes and vault store partitions. Typically you implement access control on these locations using security ACLs.

If you use a network share for Enterprise Vault data, then before the upgrade you must ensure that the Vault Service account has full access to the network share on the remote server.

A recommended way to manage access to Enterprise Vault data locations on network shares is to create a domain security group for this purpose. This approach avoids the need to propagate new permissions to all subfolders and files if you change the Vault Service account.

To secure data locations

- 1 Check the ACL on network shares and folders that you plan to use for index locations and vault store partition folders.
Accounts other than the Vault Service account and local administrators should not have, or inherit, access to these locations.
- 2 If you want to manage access to network shares using a group, create a domain security group in Active Directory, for example EVDataAccess.
- 3 Add the Vault Service account to the new group.
- 4 Grant the new group full access to the network shares and folders that you plan to use for index locations and vault store partitions.

Paths to index locations cannot contain non-ASCII characters

Indexes created by Enterprise Vault 10.0 cannot be in locations that have characters higher than ASCII 127 in the path names. That is, the paths cannot contain characters other than letters (a-z, A-Z), digits (0-9), or punctuation.

When the Indexing service starts it checks for those index locations that have invalid characters in their path names. If there are any such index locations, the Indexing service does the following:

- Closes all index locations that contain invalid characters in their paths. Indexes in these locations remain searchable and can be updated by expiry. No new index data is written to these locations.

- Logs the following event:

```
Event ID:          41312
Task Category:    Index Admin Service
Level:            Error
Description:
The Indexing Service could not complete all the
required startup routines:
Some of the open index locations contained invalid characters.
This index locations have been closed. Service will be stopped.
```

- Shuts down so that you can review the index locations.

If the Indexing service shuts down because of invalid path names, do the following:

- 1 In the Administration Console, expand **Indexing**.
- 2 Expand **Ungrouped Servers**.
- 3 Right-click the Indexing Server where you want to add a new index location.
- 4 Click the **Index Locations** tab.
- 5 Add or close index locations as required.
- 6 When you have reviewed the index locations, restart the Indexing service.

Changes to retention category settings for the deletion of archived items

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

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

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

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

32	Points to note when upgrading from Enterprise Vault 9.0
	Changes to retention category settings for the deletion of archived items

Points to note when upgrading from Enterprise Vault 10.0

This chapter includes the following topics:

- [About this chapter](#)
- [Order of upgrade in an environment with Compliance Accelerator or Discovery Accelerator](#)
- [Exchange Server 2013 support](#)
- [Enterprise Vault 10.0 original release server hotfix required to support the Outlook Add-In](#)
- [Assigning the required permissions to the Vault Service account](#)
- [Requirements for upgrading the Enterprise Vault databases](#)
- [Changes to best practice settings](#)
- [Changes to index roll-over](#)
- [Changes to support FSA targets without Administrator privileges for the Vault Service account](#)
- [About upgrading FSA targets that run a Server Core installation of Windows](#)
- [Default File Blocking location is no longer supported](#)
- [Changes to retention category settings for the deletion of archived items](#)
- [File System Archiving of files under Dynamic Access Control](#)

About this chapter

Read this chapter if you are upgrading from the Enterprise Vault 10.0 original release, Enterprise Vault 10.0.1, Enterprise Vault 10.0.2, or Enterprise Vault 10.0.3.

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

For a list of the new features and fixes in Enterprise Vault 10.0.4, see the *Enterprise Vault 10.0.4* release notes document.

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

If the Enterprise Vault environment that you are upgrading includes Compliance Accelerator or Discovery Accelerator, the Accelerator version must be upgraded to 10.0.4 or later. The Accelerator version can be up to one major version higher than Enterprise Vault, but it must not be lower than the version of Enterprise Vault.

See the *Enterprise Vault Compatibility Charts* at <http://www.symantec.com/docs/TECH38537>.

You must upgrade the Accelerator product before you upgrade Enterprise Vault. Perform the upgrades in the following order:

- Upgrade the Accelerator product.
- Then upgrade Enterprise Vault on the Accelerator server.
- Finally, upgrade Enterprise Vault on the Enterprise Vault server.

Exchange Server 2013 support

Enterprise Vault 10.0.3 introduced support for Exchange Server 2013 archiving.

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

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

The Enterprise Vault documentation is in the `Symantec Enterprise Vault\Documentation` folder on the Enterprise Vault 10.0.4 media.

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

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

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

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

If you plan to roll out the Enterprise Vault 10.0.4 Outlook Add-In to users before you upgrade the Enterprise Vault servers, you must apply a hotfix to the Enterprise Vault servers to avoid the restrictions listed in this section.

The link to the relevant technical note and the hotfix that is required to support the Enterprise Vault 10.0.4 Outlook Add-In with Enterprise Vault server 10.0 original release is as follows:

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

The following restrictions apply to the Enterprise Vault 10.0.4 Outlook Add-In if you have not installed the hotfix on Enterprise Vault servers that have not been upgraded:

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

Assigning the required permissions to the Vault Service account

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

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

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

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

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

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

Requirements for upgrading the Enterprise Vault databases

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

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

See “[Directory database upgrade requirements](#)” on page 36.

Directory database upgrade requirements

When the Directory service starts for the first time after you install the Enterprise Vault 10.0.4 software, it upgrades the Directory database schema.

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

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

[Table 4-1](#) lists the additional space requirements.

Table 4-1 Space required for the upgrade of the Directory database

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

Table 4-1 Space required for the upgrade of the Directory database (*continued*)

Directory database recovery model	Required additional space on the volume that holds the database transaction log files
Full	Four times the combined size of the Directory database data files

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

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

See [“Backing up Enterprise Vault data”](#) on page 47.

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

If the Directory database recovery model is currently set to Full, we recommend that you change the recovery model to Simple before you upgrade. This action improves the upgrade speed, and reduces the log file growth during upgrade. After you complete the Enterprise Vault upgrade you can revert to the Full recovery model.

See [“Changing the recovery model of the Directory database”](#) on page 46.

Changes to best practice settings

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

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

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

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

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

Changes to index roll-over

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

In the Enterprise Vault 10.0 original release there was a single setting that controlled the maximum size of an index volume. In Enterprise Vault 10.0.4 there is a setting for the indexes of each archive type, as follows:

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

When you install Enterprise Vault 10.0.4, all these settings have a default of 5,000,000 items. If you have previously modified the maximum size of index volumes you must change the appropriate setting after you install Enterprise Vault 10.0.4.

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

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

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

File System Archiving previously required that the Vault Service account was a member of the local Administrators group on target Windows file servers. Now the Vault Service account can run as a member of the built-in local Print Operators group, with some additional permissions and privileges.

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

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

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

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

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

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

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

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

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

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

Default File Blocking location is no longer supported

Note: The following changes were introduced with Enterprise Vault 10.0.3

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

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

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

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

Changes to retention category settings for the deletion of archived items

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

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

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

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

File System Archiving of files under Dynamic Access Control

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

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

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

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

Steps to upgrade your system

This chapter includes the following topics:

- [Overview of the upgrade process](#)

Overview of the upgrade process

This chapter provides an overview of the Enterprise Vault upgrade process. It includes the instructions on how to upgrade your Enterprise Vault servers (that is, all servers that run the Enterprise Vault Directory service). If you are upgrading an Enterprise Vault 9.0 system that supports Domino mailbox archiving, this includes any Enterprise Vault Domino Gateway servers.

Overview of the upgrade process

- 1 Prepare the Enterprise Vault servers for the upgrade:
See [“About Enterprise Vault server preparation”](#) on page 45.
- 2 Install and configure the Enterprise Vault 10.0.4 server software as described in the appropriate chapter for your installation.
See [“About upgrading a single Enterprise Vault server”](#) on page 53.
See [“About upgrading multiple Enterprise Vault servers”](#) on page 61.
See [“About upgrading a Veritas cluster”](#) on page 69.
See [“About upgrading a Windows Server Failover Cluster”](#) on page 78.
- 3 Upgrade any computers that are running just the Enterprise Vault Administration Console.
See [“Upgrading stand-alone Administration Consoles”](#) on page 89.

- 4 Upgrade any computers that are running Enterprise Vault Reporting.
See [“Upgrading Enterprise Vault Reporting”](#) on page 91.
- 5 Perform the post-installation tasks as necessary:
 - Upgrade MOM and SCOM.
See [“Upgrading MOM”](#) on page 95.
See [“Upgrading SCOM”](#) on page 95.
 - Upgrade Exchange Server forms.
See [“About upgrading Exchange Server forms”](#) on page 97.
 - Upgrade Domino mailbox archiving.
See [“About upgrading Domino mailbox archiving”](#) on page 99.
 - Upgrade the FSA Agent on the Windows servers on which it is installed.
See [“About upgrading the FSA Agent”](#) on page 107.
 - Upgrade OWA and RPC extensions.
See [“About upgrading OWA and RPC Extensions”](#) on page 113.
 - Upgrade SharePoint Server components.
See [“About upgrading the SharePoint components”](#) on page 119.
 - Upgrade SMTP Archiving components.
See [“About upgrading SMTP Archiving”](#) on page 123.
 - Upgrade custom filters.
See [“Upgrading Exchange Journal archiving filters”](#) on page 129.
See [“Upgrading API custom filters”](#) on page 130.
See [“Upgrading Domino Filtering API custom filters”](#) on page 130.

Enterprise Vault server preparation

This chapter includes the following topics:

- [About Enterprise Vault server preparation](#)
- [Changing the recovery model of the Directory database](#)
- [Backing up the system](#)
- [Running Enterprise Vault Deployment Scanner](#)
- [Setting database permissions](#)
- [Allowing the MSMQ queues to empty](#)
- [Checking the archiving and expiry schedules](#)
- [Preparing for indexing changes](#)
- [Adding the 'URL Authorization' IIS security role](#)

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:

- Change the recovery model of the Directory database, if required.
See [“Changing the recovery model of the Directory database”](#) on page 46.
- Back up the system.
See [“Backing up the system”](#) on page 46.

- Run Enterprise Vault Deployment Scanner.
See [“Running Enterprise Vault Deployment Scanner”](#) on page 48.
- Set database permissions.
See [“Setting database permissions”](#) on page 49.
- Allow the MSMQ queues to empty.
See [“Allowing the MSMQ queues to empty”](#) on page 49.
- Check the archiving and expiry schedules.
See [“Checking the archiving and expiry schedules”](#) on page 49.
- Prepare for indexing changes
See [“Preparing for indexing changes”](#) on page 49.
- Add the 'URL Authorization' IIS security role
See [“Adding the 'URL Authorization' IIS security role”](#) on page 50.

Changing the recovery model of the Directory database

If the Directory database recovery model is currently set to Full, we recommend that you change the recovery model to Simple before you upgrade. This action improves the upgrade speed, and reduces the log file growth during upgrade. After you complete the Enterprise Vault upgrade you can revert to the Full recovery model.

For upgrades from Enterprise Vault 9.0: See [“Requirements for upgrading the Enterprise Vault databases”](#) on page 24.

For upgrades from Enterprise Vault 10.0: See [“Requirements for upgrading the Enterprise Vault databases”](#) on page 36.

Note: Back up the **EnterpriseVaultDirectory** database before you change the recovery model to Simple. Back up the database again after you revert the recovery model to Full.

For information about viewing or changing the recovery model of a SQL database, see the following article on the Microsoft website:

<http://msdn.microsoft.com/en-us/library/ms189272.aspx>

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

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

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

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

When you have backed up your vault store partitions, the Storage service marks the relevant files as backed up, and this removes the entries from the WatchFile table. The Storage service performs these tasks at preconfigured intervals. You should wait for the WatchFile table to reduce in size before you proceed with the upgrade. If you do not wait, the Storage service can take some time to restart after the upgrade is complete. You can use the usage report at <http://evserver/enterprisevault/usage.asp> to check the number of files in the **Awaiting Backup** column.

Backing up changed language files

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

`Enterprise Vault\Languages\Mailbox Messages\language`

where *language* indicates the language used.

The installation does not modify the live versions of these files that you have in the Enterprise Vault folder, for example `C:\Program Files (x86)\Enterprise Vault`.

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

Backing up the SCOM management pack

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

A new SCOM management pack was introduced in Enterprise Vault 10.0.3. The Enterprise Vault upgrade procedure deletes the folder that contains the old SCOM management pack.

You can use both the old and the new management packs together, although there is no requirement to do so. If you want to keep a copy of the old management pack, copy the `SCOM` subfolder of the Enterprise Vault program folder to another location. For example, if Enterprise Vault is installed in `C:\Program Files\Enterprise Vault (x86)` then the folder to back up is as follows:

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

You do not need to restore the backed up files after the upgrade.

Running Enterprise Vault Deployment Scanner

Before you upgrade to Enterprise Vault 10.0.4, we strongly recommend that you run Enterprise Vault Deployment Scanner to check prerequisite software and settings.

Deployment Scanner is included in the `Symantec Enterprise Vault\Deployment Scanner` folder on the Enterprise Vault 10.0.4 media. You must have local Administrator permissions to install Deployment Scanner.

Use the Vault Service account when running Deployment Scanner.

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

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

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

Setting database permissions

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

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

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

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

See the following technical note on the Symantec Support website:

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

Allowing the MSMQ queues to empty

Before you upgrade to Enterprise Vault 10.0.4, we recommend that you allow the MSMQ queues to empty.

Note: If you upgrade Enterprise Vault with items still on the queues, the Enterprise Vault services may log red 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.

Preparing for indexing changes

Note: This section applies only if you are upgrading from any release of Enterprise Vault 9.

Perform the following steps for each Enterprise Vault server that hosts an Indexing service, before you start the upgrade.

- Configure the Enterprise Vault server cache for the Indexing service. You must make sure that the Enterprise Vault server cache location is configured, and that it is not located on a disk that already has high I/O usage. From Enterprise

Vault 10.0, indexing uses the Enterprise Vault server cache. If the cache is not specified, or is inaccessible, the Indexing service does not start.

See [“To configure the Enterprise Vault server cache for the Indexing service”](#) on page 50.

- Check that at least one index location is available.

See [“To check that at least one index location is available”](#) on page 50.

For an Enterprise Vault cluster, perform the steps on each of the primary nodes in the cluster. You do not need to perform the steps on the failover nodes.

To configure the Enterprise Vault server cache for the Indexing service

- 1 In the Administration Console, right-click the Enterprise Vault server and then click **Properties**.
- 2 Click the **Cache** tab, and then make sure that a suitable cache location is configured.

To ensure optimum performance, the cache should be located on fast, locally-attached storage. Do not locate the cache on a disk that has competing, high I/O demand. For example, do not place the server cache on the same disk as any of the following:

- Enterprise Vault index locations
- Enterprise Vault storage partitions
- MSMQ
- SQL Server databases

If you have previously configured a cache location that will compete for I/O in this manner, relocate the cache.

To check that at least one index location is available

- 1 In the Administration Console, right-click the Enterprise Vault Indexing service and then click **Properties**.
- 2 Click the **Index locations** tab, and then check that at least one index location is configured and has the status of **Open**.

Adding the 'URL Authorization' IIS security role

Note: This section applies only if you are upgrading from any release of Enterprise Vault 9.

Enterprise Vault 10.0 requires the 'URL Authorization' IIS security role. You must add this role to each Enterprise Vault server.

To add the 'URL Authorization IIS security role:

- 1 Start Server Manager.
- 2 In the left pane, expand **Roles**, and then click **Web Server (IIS)**.
- 3 In the right pane, scroll to the **Role Services** section.
- 4 Click **Add Role Services**.
- 5 In the **Security (Installed)** section, select **URL Authorization** and then click **Next**.
- 6 On the **Confirm Installation Selections** page, click **Install**.
- 7 On the **Results** page, click **Close**.

Single server: upgrading the Enterprise Vault server software

This chapter includes the following topics:

- [About upgrading a single Enterprise Vault server](#)
- [Installing the Enterprise Vault 10.0.4 server software on a single server](#)
- [Upgrading the Directory database](#)
- [Starting the Storage service and upgrading the storage databases](#)
- [Upgrading indexing metadata and schema version](#)
- [Upgrading the auditing database](#)
- [Backing up the upgraded Enterprise Vault databases](#)
- [Starting all the Enterprise Vault services](#)

About upgrading a single Enterprise Vault server

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

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

Installing the Enterprise Vault 10.0.4 server software on a single server

This section describes how to install the Enterprise Vault 10.0.4 server software when you have only one server that runs Enterprise Vault services.

To install the Enterprise Vault 10.0.4 server software on a single server

- 1 Log on to the Enterprise Vault server as the Vault Service account.
- 2 Stop the Enterprise Vault Admin service. This stops the Admin service itself, and any other Enterprise Vault services.
- 3 Stop any other services or applications that use Enterprise Vault. For example:
 - Enterprise Vault Administration Console
 - Enterprise Vault Accelerator Manager service
- 4 Close any other applications that may be running on the server, including the Control Panel, Computer Management, Windows Services, and the Windows Event Viewer.
- 5 If you are installing on an Enterprise Vault Domino Gateway, make sure that the Domino server on the Enterprise Vault Domino Gateway is shut down and that `EVInstall.nsf` is not being accessed locally.
- 6 Load the Enterprise Vault 10.0.4 media.
- 7 If Windows AutoPlay is enabled on the server, Windows shows an AutoPlay dialog box. Click **Run Setup.exe**.

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

Upgrading the Directory database

Follow this procedure to start the Enterprise Vault Directory service and upgrade the Directory database.

When the Directory service starts for the first time, it upgrades the Directory database schema and synchronizes new Exchange archiving policy advanced settings into existing policies.

The Directory service also migrates archive permissions. Note that this migration can take some time, depending on the size of your Enterprise Vault environment.

The Directory database updates include changes to support the new File System Archiving check for existing archives before creating an archive for a folder path. This update can take some time, depending on the number of FSA target folders with archive points.

To upgrade the Directory database

- 1 Use Windows Services to start the Enterprise Vault Directory service.
- 2 Open the Windows Event Viewer and view the Symantec Enterprise Vault event log.

As the Directory database upgrade proceeds, Enterprise Vault logs a number of events, including the following:

- Event 8575: the Directory service has started the automatic upgrade of the EnterpriseVaultDirectory database.
- Events 13399 and 13400: These events indicate that the execution of a SQL script to update the database has started and completed, respectively. You may see up to six instances of this pair of events, as different scripts run to update the database.

Additionally, event 13401 is logged at the beginning of any upgrade scripts that may take a long time to run.

- 3 Wait for event 8576 to be logged in the Symantec Enterprise Vault event log:

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

Note: The upgrade of a large Directory database may take a long time to complete (possibly several hours, in extreme cases). The upgrade time depends on the size of the database, the database recovery model, the upgrade path, and the available resources.

After event 8576, the Monitoring Configuration Utility generates some additional event log entries. The utility checks whether the Monitoring database requires upgrading, and upgrades it if required.

Starting the Storage service and upgrading the storage databases

Follow this procedure to start the Enterprise Vault Storage service. When the Storage service starts for the first time it upgrades the vault store databases and fingerprint databases, if required.

To start the Storage service and upgrade the storage databases

- 1 Start the Enterprise Vault Storage service.
- 2 Open the Windows Event Viewer and view the Symantec Enterprise Vault event log.

A vault store database schema upgrade is required for Enterprise Vault 10.0.4. Enterprise Vault logs the following events for each vault store database:

- Event 6958: The upgrade of the database has started.
- Events 13399 and 13400: The execution of a SQL script to update the database has started and completed, respectively. You may see up to five instances of this pair of events, as different scripts are run.
- Event 6959: The upgrade of the database has completed.

Note: It may take some time for the completion event to appear. The upgrade of each database may take several minutes, depending on the age of the data, the size of the database, the upgrade path, and the available resources.

A fingerprint database schema upgrade may be required, depending on your upgrade path. If a fingerprint database schema upgrade is required, Enterprise Vault logs the following events for each fingerprint database:

- Event 7035: The upgrade of the database has started.
- Events 13399 and 13400: The execution of a SQL script to update the database has started and completed, respectively. You may see up to five instances of this pair of events, as different scripts are run.
- Event 7036: The upgrade of the database has completed.

Note: It may take a long time for the completion event to appear. The time that is required to upgrade each database depends on the size of the database, the upgrade path, and the available resources.

- 3 Wait for event 6221 to be logged in the Symantec Enterprise Vault event log:

`Storage Service started.`

Upgrading indexing metadata and schema version

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

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

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

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

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

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

The following events are logged:

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

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

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

The metadata upgrade is now complete.

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

The following events are logged:

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

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

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

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

Upgrading the auditing database

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

To upgrade the auditing database

- 1 Make sure that you have backed up the **EnterpriseVaultAudit** database.
- 2 Stop all the Enterprise Vault services.
- 3 Start SQL Server Management Studio, and in the left pane under **Databases** select the EnterpriseVaultAudit database.

- 4 From the **File** menu, click **Open > File**.
- 5 Navigate to the Enterprise Vault installation folder (typically `C:\Program Files (x86)\Enterprise Vault`) and select the file `Audit_Schema_Upgrade.sql`.
- 6 From the **Query** menu, click **Execute**.
After a short time SQL Server Management Studio indicates that the query executed successfully.
- 7 Exit from SQL Server Management Studio.

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 the Directory database.

Note: If you changed the recovery model of the Directory database from Full to Simple before the upgrade, revert the database to the Full recovery model before you perform the backup.

When you back up the database you can use the routine maintenance steps to reclaim most of the additional disk space that the upgrade required.

- 3 Back up each vault store database and fingerprint database, if Enterprise Vault upgraded them when you started the Storage service.
- 4 Back up the auditing database, if you have one.

Starting all the Enterprise Vault services

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

Multiple servers: upgrading the Enterprise Vault server software

This chapter includes the following topics:

- [About upgrading multiple Enterprise Vault servers](#)
- [Installing the Enterprise Vault 10.0.4 server software on multiple servers](#)
- [Upgrading the Directory database](#)
- [Starting the Storage service on all servers and upgrading the storage databases](#)
- [Upgrading indexing metadata and schema version](#)
- [Upgrading the auditing database](#)
- [Backing up the upgraded Enterprise Vault databases](#)
- [Starting all the Enterprise Vault services](#)

About upgrading multiple Enterprise Vault servers

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

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

Installing the Enterprise Vault 10.0.4 server software on multiple servers

The following procedure describes how to install the Enterprise Vault 10.0.4 server software on all the servers that run Enterprise Vault services.

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

To install the Enterprise Vault 10.0.4 server software

- 1 Log on to the Enterprise Vault server as the Vault Service account.
- 2 Stop the Enterprise Vault Admin service. This stops the Admin service itself, and any other Enterprise Vault services.
- 3 Stop any other services or applications that use Enterprise Vault. For example:
 - Enterprise Vault Administration Console
 - Enterprise Vault Accelerator Manager service
- 4 Close any other applications that may be running on the server, including the Control Panel, Computer Management, Windows Services, and the Windows Event Viewer.
- 5 If you are installing on an Enterprise Vault Domino Gateway, make sure that the Domino server on the Enterprise Vault Domino Gateway is shut down and that `EVInstall.nsf` is not being accessed locally.
- 6 Load the Enterprise Vault 10.0.4 media.
- 7 If Windows AutoPlay is enabled on the server, Windows shows an AutoPlay dialog box. Click **Run Setup.exe**.

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

- 13 If the installation wizard prompts you to restart the server, restart and then log on again as the Vault Service account so that the installer can complete the upgrade.
- 14 When the installation is complete, the installer re-enables the Enterprise Vault services. Do not start any Enterprise Vault services at this time.
- 15 Repeat this procedure on every computer on which the Enterprise Vault services are installed.

Upgrading the Directory database

Follow this procedure to upgrade the Enterprise Vault Directory database.

Note: Do not start the Directory services on other Enterprise Vault servers until you have successfully completed this procedure on one Enterprise Vault server.

When the Directory service starts for the first time, it upgrades the Directory database schema and synchronizes new Exchange archiving policy advanced settings into existing policies.

The Directory service also migrates archive permissions. Note that this migration can take some time, depending on the size of your Enterprise Vault environment.

The Directory database updates include changes to support the new File System Archiving check for existing archives before creating an archive for a folder path. This update can take some time, depending on the number of FSA target folders with archive points.

To upgrade the Directory database

- 1 On one Enterprise Vault server only, use Windows Services to start the Enterprise Vault Directory service.

Note: Choose an Enterprise Vault server that has good network connectivity with the SQL Server computer that hosts the Enterprise Vault Directory database.

- 2 Open the Windows Event Viewer and view the Symantec Enterprise Vault event log.

As the Directory database upgrade proceeds, Enterprise Vault logs a number of events, including the following:

- Event 8575: the Directory service has started the automatic upgrade of the EnterpriseVaultDirectory database.
 - Events 13399 and 13400: These events indicate that the execution of a SQL script to update the database has started and completed, respectively. You may see up to six instances of this pair of events, as different scripts run to update the database.
Additionally, event 13401 is logged at the beginning of any upgrade scripts that may take a long time to run.
- 3 Wait for event 8576 to be logged in the Symantec Enterprise Vault event log:
- ```
The Directory service has completed the automatic upgrade of the EnterpriseVaultDirectory Database
```

---

**Note:** The upgrade of a large Directory database may take a long time to complete (possibly several hours, in extreme cases). The upgrade time depends on the size of the database, the database recovery model, the upgrade path, and the available resources.

---

After event 8576, the Monitoring Configuration Utility generates some additional event log entries. The utility checks whether the Monitoring database requires upgrading, and upgrades it if required.

## Starting the Storage service on all servers and upgrading the storage databases

Perform the following procedure for each server that has an Enterprise Vault Storage service.

### To start the Storage service on all servers and upgrade the storage databases

- 1 Start the Enterprise Vault Storage service.
- 2 Open the Windows Event Viewer and view the Symantec Enterprise Vault event log.

A vault store database schema upgrade is required for Enterprise Vault 10.0.4. Enterprise Vault logs the following events for each vault store database:

- Event 6958: The upgrade of the database has started.
- Events 13399 and 13400: The execution of a SQL script to update the database has started and completed, respectively. You may see up to five instances of this pair of events, as different scripts are run.
- Event 6959: The upgrade of the database has completed.



---

**Note:** It may take some time for the completion event to appear. The upgrade of each database may take several minutes, depending on the age of the data, the size of the database, the upgrade path, and the available resources.

---

A fingerprint database schema upgrade may be required, depending on your upgrade path. If a fingerprint database schema upgrade is required, Enterprise Vault logs the following events for each fingerprint database:

- Event 7035: The upgrade of the database has started.
- Events 13399 and 13400: The execution of a SQL script to update the database has started and completed, respectively. You may see up to five instances of this pair of events, as different scripts are run.
- Event 7036: The upgrade of the database has completed.

---

**Note:** It may take a long time for the completion event to appear. The time that is required to upgrade each database depends on the size of the database, the upgrade path, and the available resources.

---

### 3 Wait for event 6221 to be logged in the Symantec Enterprise Vault event log:

`Storage Service started.`

Start the Storage service on every server and wait for event 6221 to be logged before you continue.

## Upgrading indexing metadata and schema version

---

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

---

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

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

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

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

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

The following events are logged:

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

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

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

The metadata upgrade is now complete.

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

The following events are logged:

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

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

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

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

## Upgrading the auditing database

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

To upgrade the auditing database

- 1 Make sure that you have backed up the **EnterpriseVaultAudit** database.
- 2 Stop all the Enterprise Vault services on all servers.
- 3 Start SQL Server Management Studio, and in the left pane under **Databases** select the **EnterpriseVaultAudit** database.

- 4 From the **File** menu, click **Open > File**.
- 5 Navigate to the Enterprise Vault installation folder (typically `C:\Program Files (x86)\Enterprise Vault`) and select the file `Audit_Schema_Upgrade.sql`.
- 6 From the **Query** menu, click **Execute**.  
After a short time SQL Server Management Studio indicates that the script has completed successfully.
- 7 Exit from SQL Server Management Studio.

## 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 the Directory database.

---

**Note:** If you changed the recovery model of the Directory database from Full to Simple before the upgrade, revert the database to the Full recovery model before you perform the backup.

---

When you back up the database you can use the routine maintenance steps to reclaim most of the additional disk space that the upgrade required.

- 3 Back up each vault store database and fingerprint database, if Enterprise Vault upgraded them when you started the Storage service.
- 4 Back up the auditing database, if you have one.

## Starting all the Enterprise Vault services

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



# Veritas Cluster Server: upgrading the Enterprise Vault server software

This chapter includes the following topics:

- [About upgrading a Veritas cluster](#)
- [Veritas Cluster Server: installing the Enterprise Vault 10.0.4 software](#)
- [Upgrading the Directory database](#)
- [Starting the Storage service on all servers and upgrading the storage databases](#)
- [Upgrading indexing metadata and schema version](#)
- [Moving the index metadata location to a shared drive](#)
- [Upgrading the auditing database](#)
- [Backing up the upgraded Enterprise Vault databases](#)
- [Starting all the Enterprise Vault services](#)

## 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.

## Veritas Cluster Server: installing the Enterprise Vault 10.0.4 software

This section describes how to install the Enterprise Vault 10.0.4 server software when the servers that run Enterprise Vault tasks are part of a Veritas cluster.

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

### To install the Enterprise Vault 10.0.4 server software

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

Note the following important points:

- You must stop all Enterprise Vault services in the Enterprise Vault site. For example, stop the services on non-clustered servers, such as an Enterprise Vault Domino Gateway.
  - If you install on an Enterprise Vault Domino Gateway, make sure that the Domino server on the Enterprise Vault Domino Gateway is shut down and that `EVInstall.nsf` is not accessed locally.
  - If there are multiple sites that share the Enterprise Vault Directory, you must also stop all Enterprise Vault services in the other sites.
- 3 Stop any other services or applications that can lock Enterprise Vault files. For example:
    - Enterprise Vault Administration Console
    - Enterprise Vault Accelerator Manager service
  - 4 Close any applications that may be running on the server, including the Control Panel, Computer Management, Windows Services, and the Windows Event Viewer.
  - 5 Load the Enterprise Vault 10.0.4 media.
  - 6 If Windows AutoPlay is enabled on the server, Windows shows an AutoPlay dialog box. Click **Run Setup.exe**.

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

- 8 Click **Server Installation**.
- 9 In the right pane, click **Upgrade existing server**.
- 10 Click **Install**. The Enterprise Vault installation wizard starts.
- 11 Work through the installation wizard to upgrade the Enterprise Vault components.
- 12 If the installation wizard prompts you to restart the server, restart and then log on again as the Vault Service account so that the installer can complete the upgrade.
- 13 Install the Enterprise Vault software on the other servers in your Enterprise Vault environment, including any cluster failover nodes.

## Upgrading the Directory database

After the upgrade of the Enterprise Vault software on the active node you must start the Admin service and the Directory service.

When the Directory service starts for the first time, it upgrades the Directory database schema and synchronizes new Exchange archiving policy advanced settings into existing policies.

The Directory service also migrates archive permissions. Note that this migration can take some time, depending on the size of your Enterprise Vault environment.

The Directory database updates include changes to support the new File System Archiving check for existing archives before creating an archive for a folder path. This update can take some time, depending on the number of FSA target folders with archive points.

### To upgrade the Directory database

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

Do not bring any other Enterprise Vault resources online.

- 2 Open the Windows Event Viewer and view the Symantec Enterprise Vault event log.

As the Directory database upgrade proceeds, Enterprise Vault logs a number of events, including the following:

- Event 8575: the Directory service has started the automatic upgrade of the EnterpriseVaultDirectory database.
- Events 13399 and 13400: These events indicate that the execution of a SQL script to update the database has started and completed, respectively.

You may see up to six instances of this pair of events, as different scripts run to update the database.

Additionally, event 13401 is logged at the beginning of any upgrade scripts that may take a long time to run.

- 3 Wait for event 8576 to be logged in the Symantec Enterprise Vault event log:

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

---

**Note:** The upgrade of a large Directory database may take a long time to complete (possibly several hours, in extreme cases). The upgrade time depends on the size of the database, the database recovery model, the upgrade path, and the available resources.

---

After event 8576, the Monitoring Configuration Utility generates some additional event log entries. The utility checks whether the Monitoring database requires upgrading, and upgrades it if required.

- 4 Start the Admin service and the Directory service on all the Enterprise Vault servers in your environment, including servers in other Enterprise Vault sites that use the same Directory database.

---

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

---

## Starting the Storage service on all servers and upgrading the storage databases

Perform the following procedure for each server that has an Enterprise Vault Storage service.

### To start the Storage service on all servers and upgrade the storage databases

- 1 Use the cluster administration tools to bring the Enterprise Vault Storage service online.
- 2 Open the Windows Event Viewer and view the Symantec Enterprise Vault event log.

A vault store database schema upgrade is required for Enterprise Vault 10.0.4. Enterprise Vault logs the following events for each vault store database:

- Event 6958: The upgrade of the database has started.



- Events 13399 and 13400: The execution of a SQL script to update the database has started and completed, respectively. You may see up to five instances of this pair of events, as different scripts are run.
- Event 6959: The upgrade of the database has completed.

---

**Note:** It may take some time for the completion event to appear. The upgrade of each database may take several minutes, depending on the age of the data, the size of the database, the upgrade path, and the available resources.

---

A fingerprint database schema upgrade may be required, depending on your upgrade path. If a fingerprint database schema upgrade is required, Enterprise Vault logs the following events for each fingerprint database:

- Event 7035: The upgrade of the database has started.
- Events 13399 and 13400: The execution of a SQL script to update the database has started and completed, respectively. You may see up to five instances of this pair of events, as different scripts are run.
- Event 7036: The upgrade of the database has completed.

---

**Note:** It may take a long time for the completion event to appear. The time that is required to upgrade each database depends on the size of the database, the upgrade path, and the available resources.

---

- 3 Wait for event 6221 to be logged in the Symantec Enterprise Vault event log:

Storage Service started.

Start every Storage service and wait for event 6221 to be logged before you continue.

## Upgrading indexing metadata and schema version

---

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

---

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

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

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

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

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

The following events are logged:

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

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

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

The metadata upgrade is now complete.

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

The following events are logged:

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

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

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

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

## Moving the index metadata location to a shared drive

---

**Note:** This section applies only if you are upgrading from any release of Enterprise Vault 9.

---

For each primary node you must move Enterprise Vault's index metadata folder to a shared drive in the cluster. The index metadata folder is the folder in which Enterprise Vault stores indexing configuration data and reporting data.

Perform the following procedure for each primary node in the cluster.

**To move the index metadata location to a shared drive**

- 1 Make sure that the Enterprise Vault Indexing service is stopped.
- 2 In Windows Explorer, browse to the `evindexing\data` subfolder of the Enterprise Vault program folder, typically `C:\Program Files (x86)\Enterprise Vault`.
- 3 Move the `IndexMetaData` folder from the `data` subfolder to a shared drive in the cluster.
- 4 Make sure that the Enterprise Vault Directory service and Admin service are online.
- 5 In the left pane of the Administration Console, right-click the Enterprise Vault Indexing service and then click **Properties**.
- 6 On the **General** tab, set **Index metadata location** to the path for the `IndexMetaData` folder on the shared drive, for example `V:\IndexMetaData`.

## Upgrading the auditing database

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

**To upgrade the auditing database**

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

## 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 the Directory database.

---

**Note:** If you changed the recovery model of the Directory database from Full to Simple before the upgrade, revert the database to the Full recovery model before you perform the backup.

---

When you back up the database you can use the routine maintenance steps to reclaim most of the additional disk space that the upgrade required.

- 3 Back up each vault store database and fingerprint database, if Enterprise Vault upgraded them when you started the Storage service.
- 4 Back up the auditing database, if you have one.

## 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.

# Windows Server Failover Clustering: upgrading the Enterprise Vault server software

This chapter includes the following topics:

- [About upgrading a Windows Server Failover Cluster](#)
- [Windows Server Failover Clustering: installing the Enterprise Vault 10.0.4 software](#)
- [Upgrading the Directory database](#)
- [Starting the Storage service on all servers and upgrading the storage databases](#)
- [Upgrading indexing metadata and schema version](#)
- [Moving the index metadata location to a shared drive](#)
- [Upgrading the auditing database](#)
- [Backing up the upgraded Enterprise Vault databases](#)
- [Starting all the Enterprise Vault services](#)

## 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.

## Windows Server Failover Clustering: installing the Enterprise Vault 10.0.4 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.

Follow the appropriate instructions for your upgrade path:

- See [“Upgrading from Enterprise Vault 9.0.3, 9.0.4, or any version of 10.0: To install the Enterprise Vault 10.0.4 server software”](#) on page 78.
- See [“Upgrading from the Enterprise Vault 9.0 original release, 9.0.1, or 9.0.2: To install the Enterprise Vault 10.0.4 server software”](#) on page 81.

### Upgrading from Enterprise Vault 9.0.3, 9.0.4, or any version of 10.0: To install the Enterprise Vault 10.0.4 server software

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

Note the following important points:

- Do not take the EnterpriseVaultServerInstance offline.
- You must stop all Enterprise Vault services in the Enterprise Vault site. For example, stop the services on non-clustered servers, such as an Enterprise Vault Domino Gateway.
- If you install on an Enterprise Vault Domino Gateway, make sure that the Domino server on the Enterprise Vault Domino Gateway is shut down and that `EVInstall.nsf` is not accessed locally.

- If there are multiple sites that share the Enterprise Vault Directory, you must also stop all Enterprise Vault services in the other sites.
- 3 Stop any other services or applications that can lock Enterprise Vault files. Use Failover Cluster Manager to stop clustered services. For example:
  - Enterprise Vault Administration Console
  - Enterprise Vault Accelerator Manager service
- 4 Close any applications that may be running on the server, including the Control Panel, Computer Management, Windows Services, and the Windows Event Viewer.
- 5 Open a command window and enter the following command to remove the registry checkpoint binding to the Admin service:

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

where *EVResourceGroupName* is the name of the Enterprise Vault cluster service (resource group).

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

```
cluster resource EVResourceGroupName-EnterpriseVaultAdminService
/check
```

The output looks similar to the following:

```
Listing registry checkpoints for resource
 'EVResourceGroupName-EnterpriseVaultAdminService'...
Resource Registry Checkpoint

EVResourceGroupName-EnterpriseVaultAdminService None
```

- 7 In the command window, enter the following command to check whether the EnterpriseVaultServerInstance resource has registry checkpoint binding:

```
cluster resource EVResourceGroupName-EnterpriseVaultServerInstance
/check
```

Do as follows, depending on the result:

- Go to step 10 if the output looks similar to the following, which indicates that the EnterpriseVaultServerInstance already has registry checkpoint binding:

```
Listing registry checkpoints for resource
 'EVResourceGroupName-EnterpriseVaultServerInstance'...
Resource Registry Checkpoint
```

```

EVResourceGroupName-EnterpriseVaultServerInstance

'Software\KVS\Enterprise Vault'
```

- Or continue from step 8 if the output looks similar to the following, which indicates that the EnterpriseVaultServerInstance resource does not have registry checkpoint binding:

```
Listing registry checkpoints for resource
 'EVResourceGroupName-EnterpriseVaultServerInstance'...
Resource Registry Checkpoint

EVResourceGroupName-EnterpriseVaultServerInstance None
```

- 8 In the command window, enter the following command to add registry checkpoint binding to the EnterpriseVaultServerInstance resource:

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

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

```
cluster resource EVResourceGroupName-EnterpriseVaultServerInstance
/check
```

The output looks similar to the following:

```
Listing registry checkpoints for resource
 'EVResourceGroupName-EnterpriseVaultServerInstance'...
Resource Registry Checkpoint

EVResourceGroupName-EnterpriseVaultServerInstance

'Software\KVS\Enterprise Vault'
```

- 10 Load the Enterprise Vault 10.0.4 media.
- 11 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.

- 12 In the list in the left pane of the **Symantec Enterprise Vault Install Launcher** window, click **Enterprise Vault**.
- 13 Click **Server Installation**.



- 14** In the right pane, click **Upgrade existing server**.
- 15** Click **Install**. The Enterprise Vault installation wizard starts.
- 16** Work through the installation wizard to upgrade the Enterprise Vault components.
- 17** 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.
- 18** Install the Enterprise Vault software on the other servers in your Enterprise Vault environment, including any cluster failover nodes.

**Upgrading from the Enterprise Vault 9.0 original release, 9.0.1, or 9.0.2: To install the Enterprise Vault 10.0.4 server software**

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

Note the following important points:

- Do not take the EnterpriseVaultServerInstance offline.
  - You must stop all Enterprise Vault services in the Enterprise Vault site. For example, stop the services on non-clustered servers, such as an Enterprise Vault Domino Gateway.
  - If you install on an Enterprise Vault Domino Gateway, make sure that the Domino server on the Enterprise Vault Domino Gateway is shut down and that `EVInstall.nsf` is not accessed locally.
  - If there are multiple sites that share the Enterprise Vault Directory, you must also stop all Enterprise Vault services in the other sites.
- 3** Stop any other services or applications that can lock Enterprise Vault files. Use Failover Cluster Manager to stop clustered services. For example:
    - Enterprise Vault Administration Console
    - Enterprise Vault Accelerator Manager service
  - 4** Close any applications that may be running on the server, including the Control Panel, Computer Management, Windows Services, and the Windows Event Viewer.
  - 5** Load the Enterprise Vault 10.0.4 media.

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

## Upgrading the Directory database

After the upgrade of the Enterprise Vault software on the active node you must start the Admin service and the Directory service.

When the Directory service starts for the first time, it upgrades the Directory database schema and synchronizes new Exchange archiving policy advanced settings into existing policies.

The Directory service also migrates archive permissions. Note that this migration can take some time, depending on the size of your Enterprise Vault environment.

The Directory database updates include changes to support the new File System Archiving check for existing archives before creating an archive for a folder path. This update can take some time, depending on the number of FSA target folders with archive points.

### To upgrade the Directory database

- 1 On the active node, use the cluster administration tools to bring the Admin service and Directory service resources online.  
  
Do not bring any other Enterprise Vault resources online.
- 2 Open the Windows Event Viewer and view the Symantec Enterprise Vault event log.

As the Directory database upgrade proceeds, Enterprise Vault logs a number of events, including the following:

- Event 8575: the Directory service has started the automatic upgrade of the EnterpriseVaultDirectory database.
- Events 13399 and 13400: These events indicate that the execution of a SQL script to update the database has started and completed, respectively. You may see up to six instances of this pair of events, as different scripts run to update the database.  
 Additionally, event 13401 is logged at the beginning of any upgrade scripts that may take a long time to run.

**3** Wait for event 8576 to be logged in the Symantec Enterprise Vault event log:

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

---

**Note:** The upgrade of a large Directory database may take a long time to complete (possibly several hours, in extreme cases). The upgrade time depends on the size of the database, the database recovery model, the upgrade path, and the available resources.

---

After event 8576, the Monitoring Configuration Utility generates some additional event log entries. The utility checks whether the Monitoring database requires upgrading, and upgrades it if required.

**4** Start the Admin service and the Directory service on all the Enterprise Vault servers in your environment, including servers in other Enterprise Vault sites that use the same Directory database.

---

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

---

## Starting the Storage service on all servers and upgrading the storage databases

Perform the following procedure for each server that has an Enterprise Vault Storage service.

**To start the Storage service on all servers and upgrade the storage databases**

- 1 Use the cluster administration tools to bring the Enterprise Vault Storage service online.
- 2 Open the Windows Event Viewer and view the Symantec Enterprise Vault event log.

A vault store database schema upgrade is required for Enterprise Vault 10.0.4. Enterprise Vault logs the following events for each vault store database:

- Event 6958: The upgrade of the database has started.
- Events 13399 and 13400: The execution of a SQL script to update the database has started and completed, respectively. You may see up to five instances of this pair of events, as different scripts are run.
- Event 6959: The upgrade of the database has completed.

---

**Note:** It may take some time for the completion event to appear. The upgrade of each database may take several minutes, depending on the age of the data, the size of the database, the upgrade path, and the available resources.

---

A fingerprint database schema upgrade may be required, depending on your upgrade path. If a fingerprint database schema upgrade is required, Enterprise Vault logs the following events for each fingerprint database:

- Event 7035: The upgrade of the database has started.
- Events 13399 and 13400: The execution of a SQL script to update the database has started and completed, respectively. You may see up to five instances of this pair of events, as different scripts are run.
- Event 7036: The upgrade of the database has completed.

---

**Note:** It may take a long time for the completion event to appear. The time that is required to upgrade each database depends on the size of the database, the upgrade path, and the available resources.

---

- 3 Wait for event 6221 to be logged in the Symantec Enterprise Vault event log:

Storage Service started.

Start every Storage service and wait for event 6221 to be logged before you continue.

# Upgrading indexing metadata and schema version

---

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

---

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

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

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

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

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

The following events are logged:

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

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

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

The metadata upgrade is now complete.

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

The following events are logged:

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

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

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

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

## Moving the index metadata location to a shared drive

---

**Note:** This section applies only if you are upgrading from any release of Enterprise Vault 9.

---

For each primary node you must move Enterprise Vault's index metadata folder to a shared drive in the cluster. The index metadata folder is the folder in which Enterprise Vault stores indexing configuration data and reporting data.

Perform the following procedure for each primary node in the cluster.

### To move the index metadata location to a shared drive

- 1 Make sure that the Enterprise Vault Indexing service is stopped.
- 2 In Windows Explorer, browse to the `evindexing\data` subfolder of the Enterprise Vault program folder, typically `C:\Program Files (x86)\Enterprise Vault`.
- 3 Move the `IndexMetaData` folder from the `data` subfolder to a shared drive in the cluster.
- 4 Make sure that the Enterprise Vault Directory service and Admin service are online.
- 5 In the left pane of the Administration Console, right-click the Enterprise Vault Indexing service and then click **Properties**.
- 6 On the **General** tab, set **Index metadata location** to the path for the `IndexMetaData` folder on the shared drive, for example `V:\IndexMetaData`.

## Upgrading the auditing database

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

### To upgrade the auditing database

- 1 Make sure that you have backed up the **EnterpriseVaultAudit** database.
- 2 Stop all the Enterprise Vault services.
- 3 Start SQL Server Management Studio, and in the left pane under **Databases** select the **EnterpriseVaultAudit** database.
- 4 From the **File** menu, click **Open > File**.

- 5 Navigate to the Enterprise Vault installation folder (typically `C:\Program Files (x86)\Enterprise Vault`) and select the file `Audit_Schema_Upgrade.sql`.
- 6 From the **Query** menu, click **Execute**.  
After a short time SQL Server Management Studio indicates that the script has completed successfully.
- 7 Exit from SQL Server Management Studio.

## 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 the Directory database.

---

**Note:** If you changed the recovery model of the Directory database from Full to Simple before the upgrade, revert the database to the Full recovery model before you perform the backup.

---

When you back up the database you can use the routine maintenance steps to reclaim most of the additional disk space that the upgrade required.

- 3 Back up each vault store database and fingerprint database, if Enterprise Vault upgraded them when you started the Storage service.
- 4 Back up the auditing database, if you have one.

## 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.





# Upgrading stand-alone Administration Consoles

This chapter includes the following topics:

- [Upgrading stand-alone Administration Consoles](#)

## Upgrading stand-alone Administration Consoles

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

Note that the supported versions of Windows for stand-alone Administration Consoles have changed for Enterprise Vault 10.0. A stand-alone Administration Console must run one of the following versions of Windows:

- Windows Vista SP1 or later
- Windows 7
- Windows Server 2008 R2

### To upgrade a stand-alone Administration Console

- 1 Log on to the Enterprise Vault server as the Vault Service account.
- 2 Make sure that the Administration Console is not running.
- 3 Load the Enterprise Vault 10.0.4 media.
- 4 If Windows AutoPlay is enabled on the server, Windows shows an AutoPlay dialog box. Click **Run Setup.exe**.

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

- 5 In the list in the left pane of the **Symantec Enterprise Vault Install Launcher** window, click **Enterprise Vault**.
- 6 Click **Server Installation**.
- 7 In the right pane, click **Upgrade existing server**.
- 8 Click **Install**. The Enterprise Vault installation wizard starts.
- 9 Work through the installation to upgrade the Administration Console component.

# Upgrading Enterprise Vault Reporting

This chapter includes the following topics:

- [Upgrading Enterprise Vault Reporting](#)
- [Installing the Enterprise Vault Reporting component](#)
- [Running the Enterprise Vault Reporting Configuration utility](#)

## Upgrading Enterprise Vault Reporting

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

[Table 12-1](#) lists the steps that are required to upgrade Enterprise Vault Reporting.

**Table 12-1** Steps to install Enterprise Vault Reporting

| Step   | Action                                                                                                                                    | Description                                                                                    |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|
| Step 1 | Install the Enterprise Vault 10.0.4 Reporting component on each computer on which the Enterprise Vault Reporting component is installed.  | See <a href="#">“Installing the Enterprise Vault Reporting component”</a> on page 92.          |
| Step 2 | Run the Enterprise Vault Reporting Configuration utility on each computer on which the Enterprise Vault Reporting component is installed. | See <a href="#">“Running the Enterprise Vault Reporting Configuration utility”</a> on page 92. |

## Installing the Enterprise Vault Reporting component

You must install the Enterprise Vault 10.0.4 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 10.0.4 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 10.0.4 media.
- 3 If Windows AutoPlay is enabled on the server, Windows shows an AutoPlay dialog box. Click **Run Setup.exe**.

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

- 4 In the list in the left pane of the **Symantec Enterprise Vault Install Launcher** window, click **Enterprise Vault**.
- 5 Click **Server Installation**.
- 6 In the right pane, click **Upgrade existing server**.
- 7 Click **Install**. The Enterprise Vault installation wizard starts.
- 8 Work through the installation to upgrade the Enterprise Vault Reporting component.

## Running the Enterprise Vault Reporting Configuration utility

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

- Installed the Enterprise Vault 10.0.4 software on the Enterprise Vault servers.
- Installed the Enterprise Vault 10.0.4 Reporting component on each computer on which the Reporting component is installed.

### To run the Enterprise Vault Reporting Configuration utility

- 1 Start the Reporting Configuration utility, **Enterprise Vault Reports Configuration**.
- 2 Select **Configure Reporting and deploy or upgrade reports**.
- 3 Type the domain, user name, and password for the Reporting user account.
- 4 Select the SQL Server Reporting Services instance.
- 5 Select the language in which to deploy the reports.
- 6 Select or type in the name of the Directory database SQL Server.
- 7 Click **Configure** to deploy the reports.

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

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

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

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



# Upgrading MOM and SCOM

This chapter includes the following topics:

- [Upgrading MOM](#)
- [Upgrading SCOM](#)

## 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 SCOM

Enterprise Vault 10.0.3 introduced a new System Center Operations Manager (SCOM) sealed management pack.

You cannot upgrade an Enterprise Vault management pack that is earlier than the Enterprise Vault 10.0.3 management pack.

Follow the appropriate procedure for your upgrade path.

**Upgrading from Enterprise Vault 10.0.2 or any earlier version: To install the new SCOM management pack**

- ◆ See "Automatic Monitoring" in the *Administrator's Guide* for details of how to set up SCOM monitoring with the new management pack.

**Upgrading from Enterprise Vault 10.0.3: Upgrading the SCOM management pack**

- 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 **Symantec Enterprise Vault Install Launcher** window, click **Enterprise Vault**.
- 4 Click **Client Installation**.
- 5 In the right pane, click **SCOM Management Pack**.
- 6 Click **Open Folder**. Windows Explorer starts in the folder that contains the Management Pack.
- 7 Double-click the following file:  
  
`Symantec Enterprise Vault Management Pack.exe`
- 8 Read the displayed license and click **Yes** to agree to the terms.
- 9 Specify the folder where you want to place the management pack, and click **OK**.
- 10 In System Center Operations Manager select **Administration**.
- 11 In the left pane, right-click **Administration** and click **Import Management Packs**.
- 12 In the Import Management Packs Wizard, click **Add** and then click **Add from disk**.
- 13 If there is a prompt that asks whether you want to search the online catalog for dependencies, click **No**.
- 14 Navigate to the folder that contains the management pack that you extracted.
- 15 Click `Symantec.EnterpriseVault.mp` and then click **Open**. The wizard adds the management pack to the **Import list**.
- 16 Click **Install**. The wizard imports the management pack.
- 17 Click **Close**.



# Upgrading Exchange Server forms

This chapter includes the following topics:

- [About upgrading Exchange Server forms](#)

## About upgrading Exchange Server forms

By default, Enterprise Vault 10.0.4 deploys the Exchange Server forms to users' computers automatically.

You must upgrade Exchange Server forms provided with Enterprise Vault 10.0.4 if you use Outlook 2010 in your environment.

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.



# Upgrading Domino mailbox archiving

This chapter includes the following topics:

- [About upgrading Domino mailbox archiving](#)
- [Domino client version required to run EVInstall.nsf](#)
- [Preparing for the upgrade of Domino mailbox archiving](#)
- [Upgrading Domino mailbox archiving](#)
- [Granting the Domino archiving user access to mail files](#)
- [Identifying internal mail recipients](#)
- [Minimizing the potential performance effects of shortcut deletion](#)

## About upgrading Domino mailbox archiving

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

---

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

---

## Domino client version required to run EVInstall.nsf

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

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

See [“Upgrading Enterprise Vault Domino Server archiving”](#) on page 28.

## Preparing for the upgrade of Domino mailbox archiving

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

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

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

---

**Note:** The following procedure requires you to replace the forms files with the original Domino versions. When you replace the forms files you lose any non-Enterprise Vault customizations that you made to them. If you made any non-Enterprise Vault customizations to the forms files, you must reapply these changes to the files after you have upgraded to Enterprise Vault 10.0.4.

---

### To prepare for the upgrade of Domino mailbox archiving

- 1 Stop the HTTP task.
- 2 Delete `Forms9_x.nsf` and `Forms85_x.nsf` if they exist on the server.
- 3 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 Use the Domino Administrator to sign the Symantec Enterprise Vault 10 - Domino Installer (`EVInstall.nsf`) on the Enterprise Vault Domino Gateway with the ID of the user that will be used to run it.
- 2 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 100.

- 3 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 Enterprise Vault search applications (integrated search and browser search) or you require iNotes (DWA), select **Modify Domino Web Access Forms Files**.
  - Click **Install Symantec Enterprise Vault 10.0.4 database design templates** to start the process.

The application takes several minutes to create the new Enterprise Vault templates.
- 4 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.

- 5 If you have other target mail servers with different Domino Server versions (for example, 8.5.0), do the following until you have deployed the templates to all mail server targets:
  - Run `EVInstall.nsf` again.
  - In the application page, clear the **Enterprise Vault Domino Gateway** selection.
  - Select a target Domino mail server.
  - If you require iNotes (DWA), select **Modify Domino Web Access Forms Files**.
  - Click **Install Symantec Enterprise Vault 10.0.4 database design templates** to start the process.

The application takes several minutes to create the new Enterprise Vault templates.
  - Deploy the templates and run `Load Design` as before, on each mail server.

## Granting the Domino archiving user access to mail files

The Domino archiving user account needs permissions to all the mail files to be archived. We recommend that you provide **Manager** access to the mail files.

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

---

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

---

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

Repeat the following steps for each target Domino mail server.

**To add the Domino archiving user to all mail databases**

- 1 In the Domino Administrator client, navigate to the Domino mail server and click the **Files** tab.
- 2 In the tasks pane, click the **Mail** folder to display a list of all the mail databases in the results pane.
- 3 Select the first mail database, and then press Shift+End to select all the mail databases.
- 4 Right-click and select **Access Control > Manage**.
- 5 Click **Add** and then click the person icon to select the Domino archiving user from the Domino directory list. Click **OK**.
- 6 When the user is in the **Access Control List** dialog box, change the set **User Type** to **Person** and **Access** to **Manager**.
- 7 Select **Delete documents**.
- 8 Click **OK** to add the user to the ACL of all mail databases selected.

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

- Place the Domino server administrator's user name in the Full Access Administrators field in the server document.
- Restart the Domino server.
- In the Domino Administrator client, choose **Administration > Full Access Administration** and complete the procedure described above.
- If necessary, the administrator can then be removed from the Full Access Administrators field.

## Identifying internal mail recipients

You can specify that Enterprise Vault must perform a local address lookup for specific Notes domains. The local lookup enables Enterprise Vault to identify the Notes user name for messages that are addressed to alternate email addresses.

The local lookup results can aid searching in the web applications and in Compliance Accelerator and Discovery Accelerator.

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

#### To specify local lookup domains

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

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

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

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

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

[Table 15-1](#) shows how the NotesDomains registry key controls how Enterprise Vault identifies internal mail recipients.



Table 15-1      Effects of NotesDomains registry key

| Registry key or value                                                   | Effect on Enterprise Vault behavior                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NotesDomains key is missing                                             | Full address lookup and a warning in the event log.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 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  | <ul style="list-style-type: none"> <li>■ If EnableLocalPartLookup is set to 0, perform a full address lookup.</li> <li>■ If EnableLocalPartLookup is set to 1, perform a full address and local part lookup for addresses that match the Domain.</li> </ul> <p>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.</p> <p>If the InternalSMTPDomains list is not present or there is no match, full address lookup is used.</p> |

# Minimizing the potential performance effects of shortcut deletion

Enterprise Vault 9.0 introduced the automatic deletion of shortcuts in Domino mail files. If you have shortcuts that were created by an Enterprise Vault release before Enterprise Vault 9.0, we recommend that you implement shortcut deletion gradually.

If you implement shortcut deletion for all mailboxes immediately, the automatic deletion of old shortcuts from thousands of mailboxes can affect the Domino server and network performance. In particular, the shortcut deletion can affect compaction, replication, and index updates.

To minimize these effects, you can use either of the following methods to introduce shortcut deletion gradually:

- Add shortcut deletion to groups of mailboxes.
- Use an age restriction to limit the number of shortcuts that are deleted. For example, you could delete those shortcuts that are more than 36 months old,

then later change the policy to delete those shortcuts that are older than 30 months old, and so on.

See the section "Configuring mailbox policies" in *Setting up Domino Server Archiving* for details of how to set up shortcut deletion.

# Upgrading the FSA Agent

This chapter includes the following topics:

- [About upgrading the FSA Agent](#)
- [Upgrading FSA Agent services that are clustered for high availability](#)
- [Upgrading the FSA Agent on a target Windows file server from the Administration Console](#)
- [Upgrading the FSA Agent on an FSA Reporting proxy server from the Administration Console](#)
- [Upgrading the FSA Agent manually](#)

## 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:** Enterprise Vault 10.0 does not support File System Archiving from file servers that run Windows 2000.

---

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

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

**Note:** Do not install the FSA Agent on Enterprise Vault servers. Enterprise Vault servers do not require the FSA Agent.

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

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

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

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

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

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

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

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

**Table 16-1** Upgrading the FSA Agent

| To do this                                                                            | See this section                                                                                           |
|---------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|
| Upgrade FSA Agent services that are clustered for high availability.                  | See “Upgrading FSA Agent services that are clustered for high availability” on page 109.                   |
| 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 110. |

Table 16-1 Upgrading the FSA Agent (continued)

| To do this                                                                            | See this section                                                                                                            |
|---------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| Upgrade the FSA Agent on FSA Reporting proxy servers from the Administration Console. | See <a href="#">“Upgrading the FSA Agent on an FSA Reporting proxy server from the Administration Console”</a> on page 111. |
| Upgrade the FSA Agent manually.                                                       | See <a href="#">“Upgrading the FSA Agent manually”</a> on page 112.                                                         |

# 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

- 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.
- 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 110.
  - Upgrade the FSA Agent manually on each file server node.

See [“Upgrading the FSA Agent manually”](#) on page 112.

- 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:
  - On a 32-bit Windows system, run both of the following:
    - `vc redistrib_x86.exe`
    - `vc2005redist_x86.exe`
  - On a 64-bit Windows system, run all of the following:
    - `vc redistrib_x86.exe`
    - `vc2005redist_x86.exe`
    - `vc redistrib_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 appropriate MSI file on the file server:
  - On a 32-bit Windows system, run Enterprise Vault File System Archiving.msi
  - On a 64-bit Windows system, run Enterprise Vault File System Archiving x64.msi



# Upgrading OWA and RPC Extensions

This chapter includes the following topics:

- [About upgrading OWA and RPC Extensions](#)
- [Upgrading Enterprise Vault OWA 2010 Extensions](#)
- [Upgrading Enterprise Vault OWA 2007 Extensions](#)
- [Upgrading Enterprise Vault OWA 2003 Extensions](#)
- [Upgrading Enterprise Vault OWA 2000 Extensions](#)

## About upgrading OWA and RPC Extensions

This chapter describes how you upgrade older versions of the Enterprise Vault OWA and RPC Extensions to Enterprise Vault 10.0.4.

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

---

**Note:** The Enterprise Vault 10.0.4 OWA extensions for Exchange Server versions 2000, 2003, 2007, and 2010 require Windows 2003 SP1 or later on Exchange servers.

---

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

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

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

## Upgrading Enterprise Vault OWA 2010 Extensions

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

### To upgrade Enterprise Vault OWA 2010 Extensions

- 1 Load the Enterprise Vault 10.0.4 media.
- 2 If Windows AutoPlay is enabled on the server, Windows shows an AutoPlay dialog box. Click **Run Setup.exe**.  
  
If AutoPlay is not enabled, use Windows Explorer to open the root folder of the installation media and then double-click the file `Setup.exe`.
- 3 In the list in the left pane of the **Symantec Enterprise Vault Install Launcher** window, click **Enterprise Vault**.
- 4 Click **Client Installation**.
- 5 In the right pane, click **OWA Extensions** and then **Open folder**. Windows Explorer starts in the OWA Extensions folder.
- 6 Open the OWA 2010 Extensions folder.
- 7 Double-click the file `Symantec Enterprise Vault OWA 2010 Extensions x64.msi` to start the installation.
- 8 Follow the installation instructions.
- 9 From a browser, enter the URL for the Exchange 2010 CAS server. Open an OWA client and check that you can view archived items.

## Upgrading Enterprise Vault OWA 2007 Extensions

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

Note that if you later repair the extensions in Add or Remove Programs, then the value of the **EnterpriseVault\_WebDAVRequestHost** entry is reset to the default value, "localhost".

### To upgrade Enterprise Vault OWA 2007 Extensions

- 1 Load the Enterprise Vault 10.0.4 media.
- 2 If Windows AutoPlay is enabled on the server, Windows shows an AutoPlay dialog box. Click **Run Setup.exe**.  
  
If AutoPlay is not enabled, use Windows Explorer to open the root folder of the installation media and then double-click the file `Setup.exe`.
- 3 In the list in the left pane of the **Symantec Enterprise Vault Install Launcher** window, click **Enterprise Vault**.
- 4 Click **Client Installation**.
- 5 In the right pane, click **OWA Extensions** and then **Open folder**. Windows Explorer starts in the OWA Extensions folder.
- 6 Open the `OWA 2007 Extensions` folder.
- 7 Double-click the appropriate `.msi` file to start the installation, depending on whether the Exchange Server is running in 64-bit or 32-bit mode:
  - `Symantec Enterprise Vault OWA 2007 Extensions x64.msi`
  - `Symantec Enterprise Vault OWA 2007 Extensions x86.msi`
- 8 Follow the installation instructions.
- 9 From a browser, enter the URL for the Exchange 2010 CAS server. Open an OWA client and check that you can view archived items.

## Upgrading Enterprise Vault OWA 2003 Extensions

For details of the versions of OWA 2003 control files supported by the Enterprise Vault 10.0.4 OWA Extensions, see the *Enterprise Vault Compatibility Charts* at <http://www.symantec.com/docs/TECH38537>.

### To upgrade the Enterprise Vault OWA 2003 Extensions

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

See [“Preparing EVServers.txt”](#) on page 116.

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

See [“OWA 2003: Installing the Enterprise Vault OWA 2003 Extensions”](#) on page 117.

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

- Install the Enterprise Vault Extensions on an RPC proxy server.
- Install the Enterprise Vault Extensions on an RPC target server.
- Perform a silent installation using the MSI command line.
- Perform an installation using an Active Directory Group Policy Object (GPO).

## Preparing EVServers.txt

Prepare `EVServers.txt` as follows.

### To prepare EVServers.txt

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

- 4 If you are installing the Enterprise Vault Extensions remotely using, for example, Active Directory, then you must copy the `EVServers.txt` file to the same location as the MSI installation file.
- 5 If you are installing the Enterprise Vault Extensions interactively on each server, make `EVServers.txt` and the MSI installation file available to each back-end Exchange Server 2003.

## OWA 2003: Installing the Enterprise Vault OWA 2003 Extensions

---

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

---

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

- 1 Start Windows Explorer and navigate to the folder in which you placed `Symantec Enterprise Vault OWA 2003 Extensions.msi` and `EVServers.txt`.
- 2 Double-click `Symantec Enterprise Vault OWA 2003 Extensions.msi` to start the installation.
- 3 Work through the wizard.

## Upgrading Enterprise Vault OWA 2000 Extensions

Upgrade the Enterprise Vault OWA 2000 Extensions as follows.

**To upgrade the Enterprise Vault OWA 2000 Extensions**

- 1 If a populated version of the file `EVServers.txt` already exists in the `OWA 2000 Extensions` folder on the Enterprise Vault server, or in the installation folder on the Exchange Server, then the installer uses this. If more than one populated version of `EVServers.txt` exists, then you are prompted for the file to use. Otherwise you can run the `MakeEVServersTxt.wsf` script to populate the `EVServers.txt` file.

See [“Preparing EVServers.txt”](#) on page 118.

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

See [“OWA 2000: Installing the Enterprise Vault OWA 2000 Extensions”](#) on page 118.

## Preparing EVServers.txt

Prepare `EVServers.txt` as follows.

### To prepare EVServers.txt

- 1 Log on to any Enterprise Vault server, using an account that has any Enterprise Vault administrator permissions.
- 2 Start Windows Explorer and navigate to the `OWA 2000 Extensions` subfolder of the Enterprise Vault installation folder, for example `C:\Program Files (x86)\Enterprise Vault\OWA 2000 Extensions`.
- 3 Double-click `MakeEVServersTxt.wsf` to run it. The script populates `EVServers.txt` in the same folder as the script itself.
- 4 Copy `EVServers.txt` and `Symantec Enterprise Vault OWA 2000 Extensions.msi` to a location that can be accessed from your Exchange Server.
- 5 If you are installing the Enterprise Vault Extensions remotely using, for example, Active Directory, then you must copy the `EVServers.txt` file to the same location as the MSI installation file.

## OWA 2000: Installing the Enterprise Vault OWA 2000 Extensions

---

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

---

### To install the Enterprise Vault OWA 2000 Extensions on each back-end and front-end Exchange Server

- 1 Start Windows Explorer and navigate to the folder in which you placed `Symantec Enterprise Vault OWA 2000 Extensions.msi` and `EVServers.txt`.
- 2 Double-click `Symantec Enterprise Vault OWA 2000 Extensions.msi` to start the installation.
- 3 Work through the wizard.

# Upgrading SharePoint Server components

This chapter includes the following topics:

- [About upgrading the SharePoint components](#)
- [Upgrading the Enterprise Vault SharePoint components](#)

## About upgrading the SharePoint components

This chapter describes how to upgrade Enterprise Vault SharePoint components.

---

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

---

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

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

See [“Upgrading the Enterprise Vault SharePoint components”](#) on page 120.

- If you are upgrading from Enterprise Vault 8.0, note that from Enterprise Vault 9.0 onwards Enterprise Vault does not support SharePoint Portal Server 2003 or Windows SharePoint Services 2.0. If you use these products, you must upgrade SharePoint before you can upgrade the Enterprise Vault components.

See the *Enterprise Vault Compatibility Charts* at <http://www.symantec.com/docs/TECH38537>.

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

## Upgrading the Enterprise Vault SharePoint components

Upgrade the Enterprise Vault SharePoint components on each of your SharePoint Server computers.

### To upgrade the Enterprise Vault SharePoint components

- 1 Log on to the SharePoint Server as one of the following:
  - The SharePoint Server farm account. This account is sometimes known as the SharePoint database access account.
  - An account that has sufficient permissions to the SharePoint\_Config database (the configuration database). The account must be a member of the following SQL Server security roles on the SharePoint\_Config database: SharePoint\_Shell\_Access and WSS\_Content\_Application\_Pools.  
The Vault Service account can be used provided it has these permissions.
- 2 On your SharePoint Server computer, load the Enterprise Vault 10.0.4 media.
- 3 If Windows AutoPlay is enabled on the server, Windows shows an AutoPlay dialog box. Click **Run Setup.exe**.  
  
If AutoPlay is not enabled, use Windows Explorer to open the root folder of the installation media and then double-click the file `Setup.exe`.
- 4 In the list in the left pane of the **Symantec Enterprise Vault Install Launcher** window, click **Enterprise Vault**.
- 5 Click **Server Installation**.
- 6 In the right pane, click **Upgrade existing server** to start the installation.
- 7 On the **Select Components to Install** screen, ensure that only **Microsoft SharePoint Components** is selected.
- 8 Click **Next**.
- 9 Work through the remainder of the installation wizard.



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

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

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



# Upgrading SMTP archiving

This chapter includes the following topics:

- [About upgrading SMTP Archiving](#)
- [Installing the Enterprise Vault SMTP Archiving components](#)
- [Running the Enterprise Vault SMTP Archiving configuration process](#)

## About upgrading SMTP Archiving

If you have Enterprise Vault SMTP Archiving components installed, then you need to install the Enterprise Vault 10.0.4 SMTP Archiving components, and rerun the Enterprise Vault SMTP Archiving configuration process.

[Table 19-1](#) lists the steps required to upgrade the Enterprise Vault SMTP Archiving components. Repeat all of these steps on each computer on which the Enterprise Vault SMTP Archiving components are installed.

**Table 19-1** Steps to upgrade SMTP Archiving

| Step   | Action                                                                                                                                                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Take a back-up copy of the SMTP Archiving configuration file, EVSMTPArchiveConfig.ini.                                                                | <p>On the computer on which the Enterprise Vault SMTP Archiving components are installed, the configuration file is located in the x64 folder in the Enterprise Vault installation folder. Typically the folder path is C:\Program Files (x86)\Enterprise Vault\x64.</p> <p>Remember to take a back-up copy of the configuration file on each computer on which the Enterprise Vault SMTP Archiving components are installed.</p>                                                                                                                                                                  |
| Step 2 | Install the Enterprise Vault 10.0.4 SMTP Archiving components on the computers on which the Enterprise Vault SMTP Archiving components are installed. | See <a href="#">“Installing the Enterprise Vault SMTP Archiving components”</a> on page 125.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Step 3 | Reinstate your original settings in the new configuration file, EVSMTPArchiveConfig.ini.                                                              | <p>On the computer on which the Enterprise Vault SMTP Archiving components are installed, the new skeleton configuration file is located in the x64 folder in the Enterprise Vault installation folder — typically C:\Program Files (x86)\Enterprise Vault\x64.</p> <p>You can edit the skeleton configuration file, or create a new one.</p> <p>Remember to update the configuration file on each computer on which the Enterprise Vault SMTP Archiving components are installed.</p> <p>For information about the configuration file and its contents, see <i>Setting up SMTP Archiving</i>.</p> |

**Table 19-1** Steps to upgrade SMTP Archiving (*continued*)

| Step   | Action                                                                                                                                                | Description                                                                                          |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| Step 4 | Run the Enterprise Vault SMTP Archiving configuration process on each computer on which the Enterprise Vault SMTP Archiving components are installed. | See <a href="#">“Running the Enterprise Vault SMTP Archiving configuration process”</a> on page 126. |

# Installing the Enterprise Vault SMTP Archiving components

On each computer on which you have already installed the Enterprise Vault SMTP Archiving components, install the Enterprise Vault 10.0.4 SMTP Archiving components as described in the following procedure.

## To install the Enterprise Vault SMTP Archiving components

- 1 Log on to the SMTP Server computer using an account with local administrator privileges.  
Close all applications and MMC consoles before you continue.
- 2 Load the Enterprise Vault 10.0.4 media.
- 3 If Windows AutoPlay is enabled on the server, Windows shows an AutoPlay dialog box. Click **Run Setup.exe**.  
If AutoPlay is not enabled, use Windows Explorer to open the root folder of the installation media and then double-click the file `Setup.exe`.
- 4 In the list in the left pane of the **Symantec Enterprise Vault Install Launcher** window, click **Enterprise Vault**.
- 5 Click **Server Installation**.
- 6 In the right pane, click **Upgrade existing server**.
- 7 Click **Install**. The Enterprise Vault installation wizard starts.
- 8 Work through the installation to upgrade the Enterprise Vault SMTP Archiving components.

## Running the Enterprise Vault SMTP Archiving configuration process

You must run the Enterprise Vault SMTP Archiving configuration process on each computer on which you have installed the Enterprise Vault 10.0.4 SMTP Archiving components. Perform one of the following procedures to run the configuration process.

### To run the Enterprise Vault SMTP Archiving configuration process from a desktop shortcut

- 1 Log on to the computer on which you installed the Enterprise Vault SMTP Archiving components.
- 2 Click the **SMTP Archiving Configuration** shortcut.
- 3 When you are prompted, enter the name of the required SMTP Archiving configuration file, for example `EVSMTPTArchiveConfig.ini`. If the configuration file is not located in the `x64` folder in the Enterprise Vault installation folder, then enter the full path for the required configuration file. For example  
`C:\Program Files (x86)\Enterprise Vault\x64`  
`\EVSMTPTArchiveConfig.ini`.
- 4 Enter **N** when you are asked if you want to disable SMTP Archiving.
- 5 You are prompted for the domain and user name of an account under which to run the SMTP Archiving process. The account must be a standard user account with Read and Change permissions on the holding area, if it is on a network share. Do not use the Vault Service account or a local administrator account.

Enter the domain and user name in the form *domain\user\_name*.

The configuration process parses the configuration file and reports any problems. If the parsing is successful, a message is reported in the Enterprise Vault event log when the SMTP Archiving process starts.

- 6 Restart the IIS Admin service.

### To run the Enterprise Vault SMTP Archiving configuration process from a command prompt

- 1 Log on to the computer on which you installed the Enterprise Vault SMTP Archiving components.
- 2 Open a Command Prompt window and navigate to the `x64` folder in the Enterprise Vault installation folder (typically, `C:\Program Files (x86)\Enterprise Vault`).

- 3 Enter the following command:

```
EVSMTPArchiveConfig config_file
```

Where *config\_file* is the name of the required configuration file. The default file is `EVSMTPArchiveConfig.ini`. If the configuration file is not located in the `x64` folder in the Enterprise Vault installation folder, then enter the full path for the required configuration file. For example, `C:\Program Files (x86)\Enterprise Vault\x64\EVSMTPArchiveConfig.ini`.

- 4 You are prompted for the domain and user name of an account under which to run the SMTP Archiving process. The account must be a standard user account with Read and Change permissions on the holding area, if it is on a network share. Do not use the Vault Service account or a local administrator account.

Enter the domain and user name in the form *domain\user\_name*.

The configuration process parses the configuration file and reports any problems. If the parsing is successful, a message is reported in the Enterprise Vault event log when the SMTP Archiving process starts.

- 5 Restart the IIS Admin service.





# Upgrading custom filters

This chapter includes the following topics:

- [Upgrading Exchange Journal archiving filters](#)
- [Upgrading API custom filters](#)
- [Upgrading Domino Filtering API custom filters](#)

## Upgrading Exchange Journal archiving filters

If the journal report decryption feature is enabled on Exchange Server 2010, then the journal reports for RMS-protected messages have two messages attached: the RMS-protected message, and a clear text copy of the message. Enterprise Vault archives both copies of the message. An advanced setting in the Exchange Journaling policy, **ClearText copies of RMS Protected items**, lets you select whether Enterprise Vault uses the clear text copy or the RMS-protected copy as the primary message during archiving. By default, Enterprise Vault uses the clear text copy as the primary message.

---

**Note:** If the clear text copy is the primary message, the content of RMS-protected messages can be indexed, but single instance sharing between Exchange mailbox and journal archiving is not possible.

---

The policy setting is described in the online help in the Administration Console and in the *Administrator's Guide*.

If you have Enterprise Vault filters configured for Exchange Server journal archiving, it is important to understand the effect of the policy setting values, and to check that the filters work as expected before enabling filtering on your production system.

## Upgrading API custom filters

After you upgrade Enterprise Vault, you must update binding redirections in the associated .NET application configuration files to use the newer version of the Enterprise Vault API runtime. For File System filtering, the .NET application configuration file is `EvFSAArchivingTask.exe.config`. For Domino filtering, the .NET application configuration file is `EVLotusDominoJournalTask.exe.config`. Instructions on how to update .NET binding redirections are given in the following documents:

- The ReadMeFirst file that is located in the folder `Symantec Enterprise Vault\API Runtime` on the Enterprise Vault release media.
- The section “Updating binding redirections in configuration files” in the Enterprise Vault *Application Programmer's Guide*.

## Upgrading Domino Filtering API custom filters

For Enterprise Vault 10.0 the .NET assembly and namespace have changed for filters that are developed using the Domino Filtering API.

Table 20-1 lists the changes to the .NET assembly and namespace.

Table 20-1 Changes to .NET assembly and namespace in Enterprise Vault 10.0

| Item          | Old reference                                 | New reference                                 |
|---------------|-----------------------------------------------|-----------------------------------------------|
| .NET assembly | KVS.EnterpriseVault.LotusDominoInterfaces.dll | Symantec.EnterpriseVault.FilterInterfaces.dll |
| namespace     | KVS.EnterpriseVault.LotusDomino               | Symantec.EnterpriseVault.FilterInterfaces     |

If you have existing filters that were developed using an earlier version of the Domino Filtering API, then you need to upgrade the Domino Filtering API custom filters after upgrading to Enterprise Vault 10.0.

### To upgrade Domino Filtering API custom filters

- 1 Upgrade the filter code to reference the new .NET assembly and namespace. See Table 20-1 on page 130.
- 2 Rebuild the filters.
- 3 Test the filters on a development server to make sure that they work as expected.