

# Symantec Enterprise Vault™

Upgrading to Enterprise Vault 9.0.4



# Symantec Enterprise Vault: Upgrading to Enterprise Vault 9.0.4

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: 2012-05-29.

## Legal Notice

Copyright © 2012 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, Veritas, 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 Web site 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	<a href="mailto:customercare_apac@symantec.com">customercare_apac@symantec.com</a>
Europe, Middle-East, and Africa	<a href="mailto:semea@symantec.com">semea@symantec.com</a>
North America and Latin America	<a href="mailto:supportsolutions@symantec.com">supportsolutions@symantec.com</a>



# 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 8.0 .....	19
About this chapter .....	20
Changes to prerequisite software .....	20
All Enterprise Vault servers must run the same version of Enterprise Vault .....	20
Supported versions of Enterprise Vault in Compliance Accelerator and Discovery Accelerator environments .....	20
Remove database mirroring before the upgrade .....	21
Enterprise Vault 9.0.4 FSA Agent is not supported on Windows 2000 computers .....	21
Exchange Server 2010 support .....	22
Upgrading Enterprise Vault Outlook Add-Ins .....	22
Changes to Vault Cache advanced settings and Outlook Add-Ins registry values .....	23
Vault store database modifications .....	23
Consolidation of archived item metadata .....	24
FSA Reporting changes .....	24
Support for multiple FSA Reporting databases .....	24
Enhanced FSA Reporting proxy server support .....	25
FSA Reporting data collection changes .....	25

	FSA Reporting is disabled for a file server if the domain name is not resolved .....	27
Chapter 4	Points to note when upgrading from Enterprise Vault 9.0 .....	29
	About this chapter .....	29
	All Enterprise Vault servers must run the same version of Enterprise Vault .....	30
	Supported versions of Enterprise Vault in Compliance Accelerator and Discovery Accelerator environments .....	30
	Remove database mirroring before the upgrade .....	30
	Enterprise Vault 9.0.4 FSA Agent is not supported on Windows 2000 computers .....	31
	Exchange 2010 throttling policy script has changed .....	31
	Vault store database modifications .....	32
Chapter 5	Steps to upgrade your system .....	33
	Overview of the upgrade process .....	33
Chapter 6	Enterprise Vault server preparation .....	35
	About Enterprise Vault server preparation .....	35
	Backing up the system .....	36
	Backing up Enterprise Vault data .....	36
	Backing up changed language files .....	36
	Running Enterprise Vault Deployment Scanner .....	37
	Setting database permissions .....	37
	Allowing the MSMQ queues to empty .....	38
	Checking the archiving and expiry schedules .....	38
Chapter 7	Single server: upgrading the Enterprise Vault server software .....	39
	About upgrading a single Enterprise Vault server .....	39
	Installing the Enterprise Vault 9.0.4 server software on a single server .....	39
	Upgrading the Directory database .....	40
	Starting the Storage service and upgrading the storage databases .....	41
	Backing up the upgraded Enterprise Vault databases .....	42
	Starting all the Enterprise Vault services .....	42



Chapter 8	Multiple servers: upgrading the Enterprise Vault server software .....	43
	About upgrading multiple Enterprise Vault servers .....	43
	Installing the Enterprise Vault 9.0.4 server software on multiple servers .....	43
	Upgrading the Directory database .....	44
	Starting the Storage service on all servers and upgrading the storage databases .....	46
	Backing up the upgraded Enterprise Vault databases .....	47
	Starting all the Enterprise Vault services .....	47
Chapter 9	Veritas Cluster Server: upgrading the Enterprise Vault server software .....	49
	About upgrading a Veritas cluster .....	49
	Veritas Cluster Server: installing the Enterprise Vault 9.0.4 software .....	50
	Upgrading the Directory database .....	51
	Starting the Storage service on all servers and upgrading the storage databases .....	52
	Backing up the upgraded Enterprise Vault databases .....	53
	Starting all the Enterprise Vault services .....	53
Chapter 10	Windows Server Failover Clustering: upgrading the Enterprise Vault server software .....	55
	About upgrading a Windows Server Failover Cluster .....	55
	Windows Server Failover Clustering: installing the Enterprise Vault 9.0.4 software .....	56
	Upgrading the Directory database .....	59
	Starting the Storage service on all servers and upgrading the storage databases .....	60
	Backing up the upgraded Enterprise Vault databases .....	61
	Starting all the Enterprise Vault services .....	61
Chapter 11	Extra configuration tasks .....	63
	About the extra configuration tasks .....	63
	Upgrading MOM and SCOM .....	63
	Extra configuration for servers with no Internet connection .....	64
	Enabling device-level sharing for EMC Centera partitions .....	65

Chapter 12	Upgrading stand-alone Administration Consoles .....	67
	Upgrading stand-alone Administration Consoles .....	67
Chapter 13	Upgrading Enterprise Vault Reporting .....	69
	Upgrading Enterprise Vault Reporting .....	69
	Installing the Enterprise Vault Reporting component .....	70
	Running the Enterprise Vault Reporting Configuration utility .....	70
	Troubleshooting Enterprise Vault Reporting and FSA Reporting .....	71
Chapter 14	Upgrading Exchange Server forms .....	73
	About upgrading Exchange Server forms .....	73
Chapter 15	Upgrading Domino mailbox archiving .....	75
	About upgrading Domino mailbox archiving .....	75
	Domino client version required to run EVInstall.nsf .....	75
	Preparing for the upgrade of Domino mailbox archiving .....	76
	Upgrading Domino mailbox archiving .....	77
	Granting the Domino archiving user access to mail files .....	78
	Identifying internal mail recipients .....	80
	Checking the custom filter rules .....	81
	Minimizing the potential performance effects of shortcut deletion .....	82
Chapter 16	Upgrading the FSA Agent .....	83
	About upgrading the FSA Agent .....	83
	Upgrading FSA Agent services that are clustered for high availability .....	85
	Upgrading the FSA Agent on a target Windows file server from the Administration Console .....	86
	Upgrading the FSA Agent on an FSA Reporting proxy server from the Administration Console .....	87
	Upgrading the FSA Agent manually .....	88
Chapter 17	Upgrading the FSA metadata .....	91
	About upgrading the FSA metadata .....	91

Chapter 18	Upgrading OWA and RPC Extensions .....	93
	About upgrading OWA and RPC Extensions .....	93
	Upgrading Enterprise Vault OWA 2010 Extensions .....	94
	Upgrading Enterprise Vault OWA 2007 Extensions .....	94
	Upgrading Enterprise Vault OWA 2003 Extensions .....	95
	Preparing EVServers.txt .....	95
	OWA 2003: Installing the Enterprise Vault OWA 2003 Extensions .....	96
	Upgrading Enterprise Vault OWA 2000 Extensions .....	96
	Preparing EVServers.txt .....	96
	OWA 2000: Installing the Enterprise Vault OWA 2000 Extensions .....	97
Chapter 19	Upgrading SharePoint Server components .....	99
	About upgrading the SharePoint components .....	99
	Upgrading the Enterprise Vault SharePoint components .....	100
Chapter 20	Upgrading custom filters .....	101
	Upgrading Exchange Journal archiving filters .....	101



# 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 9.0.4.

If you are performing a new installation of Enterprise Vault, see the Enterprise Vault 9.0.4 *ReadMeFirst*. Then follow the installation instructions in *Installing and Configuring*, which is in the `Documentation` folder on the Enterprise Vault 9.0.4 release media.

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

[www.symantec.com/docs/TECH147785](http://www.symantec.com/docs/TECH147785)

## 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 Help	<p>Includes all the following documentation so that you can search across all files. You can access this file by doing either of the following:</p> <ul style="list-style-type: none"> <li>■ On the Windows <b>Start</b> menu, click <b>Start &gt; Programs &gt; Enterprise Vault &gt; Documentation</b>.</li> <li>■ In the Administration Console, click <b>Help &gt; Help on Enterprise Vault</b>.</li> </ul>
<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 files 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](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](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

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](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](mailto: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

The only possible server upgrade paths to Enterprise Vault 9.0.4 are from the following:

- The Enterprise Vault 8.0 original release, or any Enterprise Vault 8.0 service pack.
- The Enterprise Vault 9.0 original release, Enterprise Vault 9.0.1, Enterprise Vault 9.0.2, or Enterprise Vault 9.0.3.

If your Enterprise Vault servers are running a version of Enterprise Vault that is older than Enterprise Vault 8.0, you must first upgrade to Enterprise Vault 8.0 and then upgrade to Enterprise Vault 9.0.4.

---

**Note:** Do not upgrade to Enterprise Vault 8.0 and then immediately upgrade to Enterprise Vault 9.0.4. You must complete the Enterprise Vault 8.0 post-installation tasks as described in the Enterprise Vault 8.0 upgrade instructions, before you upgrade to Enterprise Vault 9.0.4.

---

## Documentation

Do the following before you upgrade your system:

- Read the Enterprise Vault *ReadMeFirst* and the *Enterprise Vault 9.0.4* release notes document.

For the most up-to-date versions of those documents and this guide, see the following page on the Symantec Support Web site:

[www.symantec.com/docs/TECH147785](http://www.symantec.com/docs/TECH147785)

- Check that the prerequisites for Enterprise Vault 9.0.4 are satisfied, as described in the *Installing and Configuring* manual. The manual is in the `Documentation` folder on the Enterprise Vault 9.0.4 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 Web site:

[www.symantec.com/docs/TECH38537](http://www.symantec.com/docs/TECH38537)

# Points to note when upgrading from Enterprise Vault 8.0

This chapter includes the following topics:

- [About this chapter](#)
- [Changes to prerequisite software](#)
- [All Enterprise Vault servers must run the same version of Enterprise Vault](#)
- [Supported versions of Enterprise Vault in Compliance Accelerator and Discovery Accelerator environments](#)
- [Remove database mirroring before the upgrade](#)
- [Enterprise Vault 9.0.4 FSA Agent is not supported on Windows 2000 computers](#)
- [Exchange Server 2010 support](#)
- [Upgrading Enterprise Vault Outlook Add-Ins](#)
- [Changes to Vault Cache advanced settings and Outlook Add-Ins registry values](#)
- [Vault store database modifications](#)
- [Consolidation of archived item metadata](#)
- [FSA Reporting changes](#)

## About this chapter

Read this chapter if you are upgrading from any version of Enterprise Vault 8.0.

As a result of the changes described in this chapter you may need to take action to review or modify your configuration before or after the upgrade.

For a full list of new features and changes, see the Enterprise Vault *ReadMeFirst* and the *Enterprise Vault 9.0.4* release notes document.

## Changes to prerequisite software

The minimum prerequisite software requirements have changed for Enterprise Vault 9.0.

The main changes are as follows:

- The minimum SQL Server version is now SQL Server 2005 SP2.
- The minimum SharePoint archiving target version is now SharePoint Server 2007 (MOSS 2007).

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

For information about prerequisite software, see the *Enterprise Vault Compatibility Charts* at [www.symantec.com/docs/TECH38537](http://www.symantec.com/docs/TECH38537).

## 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.

## Supported versions of Enterprise Vault in Compliance Accelerator and Discovery Accelerator environments

The major version of Discovery Accelerator or Compliance Accelerator must be the same as, or one later than, the major version of Enterprise Vault.

For example, you can run Discovery Accelerator 9.0 with Enterprise Vault 8.0 servers, but you cannot run Discovery Accelerator 8.0 with Enterprise Vault 9.0.

If the major version of Discovery Accelerator or Compliance Accelerator is the same as the major version of Enterprise Vault, the minor version (Service Pack)

of Discovery Accelerator must be the same as, or later than, the minor version of Enterprise Vault.

For example, you can run Discovery Accelerator 9.0.4 with Enterprise Vault 9.0.3 servers, but you cannot run Discovery Accelerator 9.0.3 with Enterprise Vault 9.0.4.

See the *Enterprise Vault Compatibility Charts* at [www.symantec.com/docs/TECH38537](http://www.symantec.com/docs/TECH38537).

## Remove database mirroring before the upgrade

If you use Microsoft SQL Server database mirroring with your Enterprise Vault databases, you must remove the database mirroring before you upgrade the Enterprise Vault server software. Enterprise Vault fails to upgrade its databases if mirroring is configured.

For more information, see the following technical note on the Symantec Support Web site:

[www.symantec.com/docs/TECH64763](http://www.symantec.com/docs/TECH64763)

## Enterprise Vault 9.0.4 FSA Agent is not supported on Windows 2000 computers

Read this section if you have Windows 2000 computers as FSA targets, or if you use Windows 2000 computers as proxy servers for FSA Reporting.

The Enterprise Vault 9.0.4 FSA Agent is not supported on Windows 2000 computers. From Enterprise Vault 9.0.3, Enterprise Vault uses Microsoft's FIPS-compliant encryption and hashing algorithms, which are available only on Windows 2003 and later. If you attempt to push install the Enterprise Vault 9.0.4 FSA Agent on a Windows 2000 computer, Enterprise Vault prevents the installation.

[Table 3-1](#) describes the support of FSA Agent-related features for Windows 2000 computers when the Enterprise Vault server runs Enterprise Vault 9.0.4.

Table 3-1

Support of FSA Agent features for Windows 2000 computers at Enterprise Vault 9.0.4

FSA Agent feature	Support for Windows 2000 computers at Enterprise Vault 9.0.4	Action required
Placeholder shortcuts and File Blocking	Supported only if the Windows 2000 file server runs one of the following versions of the FSA Agent: <ul style="list-style-type: none"><li>■ 9.0 original release</li><li>■ 9.0.1</li><li>■ 9.0.2</li></ul>	To use placeholders or File Blocking you must install the Enterprise Vault 9.0 original release, 9.0.1, or 9.0.2 FSA Agent on the Windows 2000 file server after you have upgraded the Enterprise Vault server to Enterprise Vault 9.0.4.  The Enterprise Vault 9.0.2 FSA Agent files are available to download from the following technical note on the Symantec Support Web site:  <a href="http://www.symantec.com/docs/TECH174423">www.symantec.com/docs/TECH174423</a>
FSA Reporting	<b>Not supported.</b>  Note also that Windows 2000 computers cannot act as proxy file servers for FSA Reporting.	If any Windows 2000 computers act as FSA Reporting proxy servers, change the FSA Reporting proxy server to a non-Windows 2000 computer.  See "Changing the FSA Reporting proxy server for a non-Windows file server" in the <i>Reporting</i> guide.

## Exchange Server 2010 support

Enterprise Vault 9.0 introduces support for Exchange Server 2010 archiving.

Check that the additional requirements for archiving Exchange Server 2010 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 2010 environment, you must set up archiving for all members of the DAG. See “Exchange Server 2010 database availability groups” in *Setting up Exchange Server Archiving*.

The Enterprise Vault documentation is in the `Documentation` folder on the Enterprise Vault 9.0.4 media.

## Upgrading Enterprise Vault Outlook Add-Ins

Before you upgrade Enterprise Vault servers to Enterprise Vault 9.0.4, ensure that all Outlook Add-Ins are Enterprise Vault 8.0 or later. Enterprise Vault 9.0 does not support Outlook Add-Ins that are earlier than 8.0.

# Changes to Vault Cache advanced settings and Outlook Add-Ins registry values

If you are upgrading the Outlook Add-Ins from a version earlier than Enterprise Vault 8.0, note that some Vault Cache advanced settings and Outlook Add-Ins registry values have been removed from Enterprise Vault 9.0.

These advanced settings and registry values were present in Enterprise Vault 8.0, including service packs, but they only applied to Outlook Add-In versions earlier than Enterprise Vault 8.0.

The Vault Cache advanced settings that have been removed are as follows:

- |                                   |   |
|-----------------------------------|---|
| ■ Archive Explorer cache interval | ■ Large items size in KB                  |
| ■ Archiving strategy              | ■ Lock for 'Deleted items in Vault Cache' |
| ■ Auto download pause             | ■ Minimum age                             |
| ■ Deleted items in Vault Cache    | ■ Minimum age units                       |
| ■ Download delay                  | ■ 'Refresh Archive Explorer View' option  |
| ■ Download reminder interval      | ■ Show download reminder                  |
| ■ Inactivity period               | ■ Show 'More Settings' in setup wizard    |
| ■ Inactivity period units         | ■ Start date for offline Archive Explorer |
| ■ Large items size                |   |

The Outlook Add-Ins registry values that have been removed are as follows:

- |                           |                         |
|---------------------------|-------------------------|
| ■ OVInactivityPeriod      | ■ OVLargeItemsSizeKB    |
| ■ OVInactivityPeriodUnits | ■ OVUseInactivityPeriod |
| ■ OVMinAgePeriod          | ■ OVUseLargeItemsSize   |
| ■ OVMinAgePeriodUnits     |                         |

## Vault store database modifications

During the upgrade, Enterprise Vault modifies each vault store database to improve SQL query efficiency and introduce new functionality. The modifications include a single update to all the rows of the JournalArchive table, and the creation of a clustered index.

The modification time is proportional to the size of the JournalArchive table. As a rough guide, the upgrade of each vault store database may take up to 5 minutes per million items in the JournalArchive table.

---

**Note:** This modification is not repeated if you have applied the Enterprise Vault hotfix "Centera Collections area filling up and not reducing due to dependency of the JournalArchive table". For details of the hotfix, see the following article on the Symantec Enterprise Support site: [www.symantec.com/docs/TECH144758](http://www.symantec.com/docs/TECH144758).

---

## Consolidation of archived item metadata

Enterprise Vault 9.0 includes a new process that consolidates the metadata for archived items. Enterprise Vault Reporting uses this consolidated metadata in some of its reports. The consolidation of the metadata enables Enterprise Vault Reporting to generate some of its reports more efficiently.

Note the following:

- The upgrade to Enterprise Vault 9.0 deletes the existing metadata that Enterprise Vault Reporting's **Items Archival Rate** report uses for its trend information. If you want a record of this report that includes the pre-upgrade trend data, generate and save the report for legacy purposes before you upgrade.
- If you use File System Archiving then, after you have upgraded the Enterprise Vault servers, you must run the FSA upgrade utility to upgrade the FSA metadata in your vault stores to the new consolidated format. Enterprise Vault Reporting cannot report on the FSA items that were archived with previous versions of Enterprise Vault until you run the utility for the associated vault stores.

See [“About upgrading the FSA metadata”](#) on page 91.

## FSA Reporting changes

Enterprise Vault 9.0 introduces a number of changes to FSA Reporting. Some of these changes have implications when you upgrade.

If you use FSA Reporting, read this section before you upgrade.

## Support for multiple FSA Reporting databases

In previous releases, FSA Reporting held all of its scan data in one FSA Reporting database. Enterprise Vault 9.0 introduces support for multiple FSA Reporting databases, to provide scalability. Multiple databases enable FSA Reporting to upload the data faster from multiple file servers, which can reduce scan times significantly. You can also use multiple databases to segregate scan data, for example by geographical location.



When you upgrade to Enterprise Vault 9.0.4, Enterprise Vault retains the existing FSA Reporting database, named `EnterpriseVaultFSAReporting`. After the upgrade completes you can configure the target file servers that have FSA Reporting enabled to use different FSA Reporting databases, if required.

For more information, see the *Reporting* guide.

## Enhanced FSA Reporting proxy server support

Read this section if you use FSA Reporting with non-Windows file servers.

An FSA Reporting proxy server performs FSA Reporting scans on non-Windows file servers. Previous versions of Enterprise Vault provided the following support for FSA Reporting proxy servers:

- Before Enterprise Vault 8.0 SP3, Enterprise Vault assigned the job of proxy server to the Enterprise Vault server that was listed first in the FSA Reporting database's **FileServerConfiguration** table. So a single Enterprise Vault server often acted as proxy server for all of the non-Windows file servers in a site.
- From Enterprise Vault 8.0 SP3 onwards, Enterprise Vault distributed the job of FSA Reporting proxy server for non-Windows file servers between the Enterprise Vault servers in a site.

From Enterprise Vault 9.0 onwards, any of the following can act as an FSA Reporting proxy server, subject to some additional prerequisites:

- An Enterprise Vault server in the Enterprise Vault site.
- A Windows file server that is configured as a file server archiving target in the Enterprise Vault site.
- A Windows server on the network.

The upgrade retains the assigned FSA Reporting proxy servers. After the upgrade you can reallocate the FSA Reporting proxy servers, if you want.

The resource demand on an FSA Reporting proxy server can be significant. For scalability we recommend that you use a separate FSA Reporting proxy server for each non-Windows file server, if possible.

For more information, see the *Reporting* guide.

## FSA Reporting data collection changes

The default values of some FSA Reporting data collection parameters may change as a result of the upgrade. These changes affect some of FSA Reporting's reports after the upgrade.

### Data collection is turned off for duplicate files reports

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

The affected reports are as follows:

- Duplicate Files on a Server
- Duplicate Files Summary
- Top Duplicate Files per Volume

The **CheckDuplicates** database parameter determines whether FSA Reporting collects data for the duplicate files reports. [Table 3-2](#) describes the changes to the value of this parameter.

**Table 3-2** Change to the CheckDuplicates parameter value

Parameter	Description	Supplied value before Enterprise Vault 8.0 SP2	Supplied value from Enterprise Vault 8.0 SP2 onwards
<b>CheckDuplicates</b>	Determines whether FSA Reporting collects data for the duplicate files reports.	<b>True</b> (Collect data)	<b>False</b> (Do not collect data)

After the upgrade, the duplicate files reports by default contain only the data that FSA Reporting had collected before the upgrade.

After the upgrade, if you want FSA Reporting to gather data for the duplicate files reports you must change the value of the **CheckDuplicates** parameter in the Enterprise Vault Directory database.

See "Modifying the FSA Reporting data collection parameters" in the *Reporting* guide.

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

**Note:** This section applies if you upgrade from any version of Enterprise Vault before Enterprise Vault 8.0 SP3.

From Enterprise Vault 8.0 SP3 onwards the default values of the data collection parameters for some reports were changed, to improve data scan performance. [Table 3-3](#) describes the changes.

**Table 3-3** Changes to the FSA Reporting data collection parameters

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

On upgrade to Enterprise Vault 9.0.4:

- If you changed the value of any of these parameters before the upgrade, Enterprise Vault retains your value.
- Otherwise, Enterprise Vault applies the new supplied value.

You can change the values of these parameters in the Enterprise Vault Directory database.

See "Modifying the FSA Reporting data collection parameters" in the *Reporting* guide.

## FSA Reporting is disabled for a file server if the domain name is not resolved

Enterprise Vault disables FSA Reporting for a file server during the upgrade of the FSA Reporting database, if the file server's fully qualified domain name cannot be resolved.

To re-enable FSA Reporting after the upgrade, go to the target file server's properties, and on the **Reporting Data Collection** tab select the FSA Reporting database.

# Points to note when upgrading from Enterprise Vault 9.0

This chapter includes the following topics:

- [About this chapter](#)
- [All Enterprise Vault servers must run the same version of Enterprise Vault](#)
- [Supported versions of Enterprise Vault in Compliance Accelerator and Discovery Accelerator environments](#)
- [Remove database mirroring before the upgrade](#)
- [Enterprise Vault 9.0.4 FSA Agent is not supported on Windows 2000 computers](#)
- [Exchange 2010 throttling policy script has changed](#)
- [Vault store database modifications](#)

## About this chapter

Read this chapter if you are upgrading from the Enterprise Vault 9.0 original release, Enterprise Vault 9.0.1, Enterprise Vault 9.0.2, or Enterprise Vault 9.0.3.

As a result of the changes described in this chapter, 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 9.0.4, see the *Enterprise Vault 9.0.4* release notes document.

## 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.

## Supported versions of Enterprise Vault in Compliance Accelerator and Discovery Accelerator environments

The major version of Discovery Accelerator or Compliance Accelerator must be the same as, or one later than, the major version of Enterprise Vault.

For example, you can run Discovery Accelerator 9.0 with Enterprise Vault 8.0 servers, but you cannot run Discovery Accelerator 8.0 with Enterprise Vault 9.0.

If the major version of Discovery Accelerator or Compliance Accelerator is the same as the major version of Enterprise Vault, the minor version (Service Pack) of Discovery Accelerator must be the same as, or later than, the minor version of Enterprise Vault.

For example, you can run Discovery Accelerator 9.0.4 with Enterprise Vault 9.0.3 servers, but you cannot run Discovery Accelerator 9.0.3 with Enterprise Vault 9.0.4.

See the *Enterprise Vault Compatibility Charts* at [www.symantec.com/docs/TECH38537](http://www.symantec.com/docs/TECH38537).

## Remove database mirroring before the upgrade

If you use Microsoft SQL Server database mirroring with your Enterprise Vault databases, you must remove the database mirroring before you upgrade the Enterprise Vault server software. Enterprise Vault fails to upgrade its databases if mirroring is configured.

For more information, see the following technical note on the Symantec Support Web site:

[www.symantec.com/docs/TECH64763](http://www.symantec.com/docs/TECH64763)

# Enterprise Vault 9.0.4 FSA Agent is not supported on Windows 2000 computers

Read this section if you have Windows 2000 computers as FSA targets, or if you use Windows 2000 computers as proxy servers for FSA Reporting.

The Enterprise Vault 9.0.4 FSA Agent is not supported on Windows 2000 computers. From Enterprise Vault 9.0.3, Enterprise Vault uses Microsoft's FIPS-compliant encryption and hashing algorithms, which are available only on Windows 2003 and later. If you attempt to push install the Enterprise Vault 9.0.4 FSA Agent on a Windows 2000 computer, Enterprise Vault prevents the installation.

[Table 4-1](#) describes the support of FSA Agent-related features for Windows 2000 computers when the Enterprise Vault server runs Enterprise Vault 9.0.4.

**Table 4-1** Support of FSA Agent features for Windows 2000 computers at Enterprise Vault 9.0.4

FSA Agent feature	Support for Windows 2000 computers at Enterprise Vault 9.0.4	Action required
Placeholder shortcuts and File Blocking	Supported only if the Windows 2000 file server runs one of the following versions of the FSA Agent: <ul style="list-style-type: none"> <li>■ 9.0 original release</li> <li>■ 9.0.1</li> <li>■ 9.0.2</li> </ul>	To use placeholders or File Blocking you can run the Enterprise Vault 9.0 original release, 9.0.1, or 9.0.2 FSA Agent on the Windows 2000 file server.  If a suitable version of the FSA Agent is not already installed you can download and manually install the Enterprise Vault 9.0.2 FSA Agent. The Enterprise Vault 9.0.2 FSA Agent files are available to download from the following technical note on the Symantec Support Web site:  <a href="http://www.symantec.com/docs/TECH174423">www.symantec.com/docs/TECH174423</a>
FSA Reporting	<b>Not supported.</b>  Note also that Windows 2000 computers cannot act as proxy file servers for FSA Reporting.	If any Windows 2000 computers act as FSA Reporting proxy servers, then before you upgrade you must change the FSA Reporting proxy server to a non-Windows 2000 computer.  See "Changing the FSA Reporting proxy server for a non-Windows file server" in the <i>Reporting</i> guide.

## Exchange 2010 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 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 2010 throttling policy on the Vault Service account" in *Installing and Configuring*.

## Vault store database modifications

---

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

---

During the upgrade, Enterprise Vault modifies each vault store database to improve SQL query efficiency and introduce new functionality. The modifications include a single update to all the rows of the JournalArchive table, and the creation of a clustered index.

The modification time is proportional to the size of the JournalArchive table. As a rough guide, the upgrade of each vault store database may take up to 5 minutes per million items in the JournalArchive table.

---

**Note:** This modification is not repeated if you have applied the Enterprise Vault hotfix "Centera Collections area filling up and not reducing due to dependency of the JournalArchive table". For details of the hotfix, see the following article on the Symantec Enterprise Support site: [www.symantec.com/docs/TECH144758](http://www.symantec.com/docs/TECH144758).

---



# Steps to upgrade your system

This chapter includes the following topics:

- [Overview of the upgrade process](#)

## Overview of the upgrade process

This chapter describes how to upgrade your Enterprise Vault servers (that is, all servers that run the Enterprise Vault Directory service). If you are upgrading an Enterprise Vault 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 35.
- 2 Install and configure the Enterprise Vault 9.0.4 server software as described in the appropriate chapter for your installation.  
See [“About upgrading a single Enterprise Vault server”](#) on page 39.  
See [“About upgrading multiple Enterprise Vault servers”](#) on page 43.  
See [“About upgrading a Veritas cluster”](#) on page 49.  
See [“About upgrading a Windows Server Failover Cluster”](#) on page 55.
- 3 Perform any of the extra configuration tasks that are relevant to your Enterprise Vault installation.  
See [“About the extra configuration tasks”](#) on page 63.

- 4 Upgrade any computers that are running just the Enterprise Vault Administration Console.  
See [“Upgrading stand-alone Administration Consoles”](#) on page 67.
- 5 Upgrade any computers that are running Enterprise Vault Reporting.  
See [“Upgrading Enterprise Vault Reporting”](#) on page 69.
- 6 Perform the post-installation tasks as necessary:
  - Upgrade Exchange Server forms.  
See [“About upgrading Exchange Server forms”](#) on page 73.
  - Upgrade Exchange Journal archiving filters.  
See [“Upgrading Exchange Journal archiving filters”](#) on page 101.
  - Upgrade Domino mailbox archiving.  
See [“About upgrading Domino mailbox archiving”](#) on page 75.
  - Upgrade the FSA Agent on the Windows servers on which it is installed.  
See [“About upgrading the FSA Agent”](#) on page 83.
  - If you upgraded from any version of Enterprise Vault 8.0, upgrade the FSA metadata in the vault store databases.  
See [“About upgrading the FSA metadata”](#) on page 91.
  - Upgrade OWA and RPC extensions.  
See [“About upgrading OWA and RPC Extensions”](#) on page 93.
  - Upgrade SharePoint Server components.  
See [“About upgrading the SharePoint components”](#) on page 99.

# Enterprise Vault server preparation

This chapter includes the following topics:

- [About Enterprise Vault server preparation](#)
- [Backing up the system](#)
- [Running Enterprise Vault Deployment Scanner](#)
- [Setting database permissions](#)
- [Allowing the MSMQ queues to empty](#)
- [Checking the archiving and expiry schedules](#)

## About Enterprise Vault server preparation

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

Perform the following actions in the order they are listed:

- Back up the system.  
See [“Backing up the system”](#) on page 36.
- Run Enterprise Vault Deployment Scanner.  
See [“Running Enterprise Vault Deployment Scanner”](#) on page 37.
- Set database permissions.  
See [“Setting database permissions”](#) on page 37.
- Allow the MSMQ queues to empty.  
See [“Allowing the MSMQ queues to empty”](#) on page 38.

- Check the archiving and expiry schedules.  
See “[Checking the archiving and expiry schedules](#)” on page 38.

## Backing up the system

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

### Backing up Enterprise Vault data

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

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 Web site:

[www.symantec.com/docs/TECH74666](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.

## Running Enterprise Vault Deployment Scanner

Before you upgrade to Enterprise Vault 9.0.4, we strongly recommend that you run Enterprise Vault Deployment Scanner to check prerequisite software and settings.

Deployment Scanner is included in the `Deployment Scanner` folder on the Enterprise Vault 9.0.4 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:

[www.symantec.com/docs/TECH55063](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 Web site:

[www.symantec.com/docs/TECH65841](http://www.symantec.com/docs/TECH65841)

## Allowing the MSMQ queues to empty

Before you upgrade to Enterprise Vault 9.0.4, 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.

---

**Note:** The following applies only if you use Exchange Server archiving, and you upgrade to Enterprise Vault 8.0 and then immediately to Enterprise Vault 9.0 without running Exchange Server archiving on the Enterprise Vault 8.0 system.

---

Enterprise Vault 8.0 introduced changes to shortcuts and retention categories for Exchange Server archiving. The first run of Exchange archiving after the upgrade updates archived items to match these changes. This update process may take a significant time, so plan for the first archiving run to take longer than normal.

See "Moved shortcuts and changed retention categories" in the Enterprise Vault 8.0 *ReadMeFirst*.

# 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 9.0.4 server software on a single server](#)
- [Upgrading the Directory database](#)
- [Starting the Storage service and upgrading the storage databases](#)
- [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 9.0.4 server software on a single server

This section describes how to install the Enterprise Vault 9.0.4 server software when you have only one server that runs Enterprise Vault services.

### To install the Enterprise Vault 9.0.4 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 9.0.4 media.
- 7 Use Windows Explorer to open the following folder:  
`\Symantec Enterprise Vault 9.0.4\Server`
- 8 Double-click the file `setup.exe` to start the installation.
- 9 Work through the installation to upgrade the Enterprise Vault components.
- 10 If the installer 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.

### 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 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.

The storage databases usually require a database schema upgrade, depending on your upgrade path. If a vault store database schema upgrade is required, the Storage service updates each vault store database. If a fingerprint database schema upgrade is required, the Storage service then upgrades each fingerprint database.

If a vault store database schema upgrade is required, 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 four instances of this pair of events, as different scripts are run.
- Event 6959: The upgrade of the database has completed.

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 four 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.`

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

## 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 9.0.4 server software on multiple servers](#)
- [Upgrading the Directory database](#)
- [Starting the Storage service on all servers and upgrading the storage databases](#)
- [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 9.0.4 server software on multiple servers

The following procedure describes how to install the Enterprise Vault 9.0.4 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 9.0.4 server software**

- 1 Log on to the Enterprise Vault server as the Vault Service account.
- 2 Start **Computer Management** and go to **Services and Applications**.
- 3 Under **Services**, stop the Enterprise Vault Admin service. This action stops the Admin service itself and other Enterprise Vault services, including the Enterprise Vault Directory service.  
  
Stop any other services or applications that use Enterprise Vault. For example:
  - Enterprise Vault Administration Console
  - Enterprise Vault Accelerator Manager service
- 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 If you are installing on an Enterprise Vault Domino Gateway, make sure that the Domino server on the Enterprise Vault Domino Gateway is shut down and that `EVInstall.nsf` is not accessed locally.
- 6 Load the Enterprise Vault 9.0.4 media.
- 7 Use Windows Explorer to open the following folder:  
  
`\Symantec Enterprise Vault 9.0.4\Server`
- 8 Double-click the file `setup.exe` to start the installation.
- 9 Work through the installation to upgrade the Enterprise Vault components.
- 10 If the installer prompts you to restart the server, restart the server and then log on again as the Vault Service account so that the installer can complete the upgrade.
- 11 When the installation is complete, the installer re-enables the Enterprise Vault services. Do not start any Enterprise Vault services at this time.
- 12 Repeat steps 1 to 11 for 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.

### 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 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.

The storage databases usually require a database schema upgrade, depending on your upgrade path. If a vault store database schema upgrade is required, the Storage service updates each vault store database. If a fingerprint database schema upgrade is required, the Storage service then upgrades each fingerprint database.

If a vault store database schema upgrade is required, 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 four instances of this pair of events, as different scripts are run.
- Event 6959: The upgrade of the database has completed.

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 four 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.

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

## 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 9.0.4 software](#)
- [Upgrading the Directory database](#)
- [Starting the Storage service on all servers and upgrading the storage databases](#)
- [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 9.0.4 software

This section describes how to install the Enterprise Vault 9.0.4 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 9.0.4 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 9.0.4 media.
  - 6 Use Windows Explorer to open the following folder:  
`\Symantec Enterprise Vault 9.0.4\Server`
  - 7 Double-click the file `setup.exe` to start the installation.

- 8 Work through the installation.
- 9 Install the Enterprise Vault software on the other servers in your Enterprise Vault environment, including any cluster failover nodes.

## 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.

### 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 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.

The storage databases usually require a database schema upgrade, depending on your upgrade path. If a vault store database schema upgrade is required, the Storage service updates each vault store database. If a fingerprint database schema upgrade is required, the Storage service then upgrades each fingerprint database.

If a vault store database schema upgrade is required, 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 four instances of this pair of events, as different scripts are run.
- Event 6959: The upgrade of the database has completed.

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 four 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.

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

## 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 9.0.4 software](#)
- [Upgrading the Directory database](#)
- [Starting the Storage service on all servers and upgrading the storage databases](#)
- [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 9.0.4 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 8.0: To install the Enterprise Vault 9.0.4 server software”](#) on page 56.
- See [“Upgrading from Enterprise Vault 9.0: To install the Enterprise Vault 9.0.4 server software”](#) on page 58.

### Upgrading from Enterprise Vault 8.0: To install the Enterprise Vault 9.0.4 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 add registry checkpoint binding to the EnterpriseVaultServerInstance resource

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

- 8 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'
```

- 9 Load the Enterprise Vault 9.0.4 media.
- 10 Use Windows Explorer to open the following folder:  
`\Symantec Enterprise Vault 9.0.4\Server`
- 11 Double-click the file `setup.exe` to start the installation.
- 12 Work through the installation.
- 13 Install the Enterprise Vault software on the other servers in your Enterprise Vault environment, including any cluster failover nodes.

**Upgrading from Enterprise Vault 9.0: To install the Enterprise Vault 9.0.4 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 9.0.4 media.
  - 6 Use Windows Explorer to open the following folder:  
`\Symantec Enterprise Vault 9.0.4\Server`
  - 7 Double-click the file `setup.exe` to start the installation.

- 8 Work through the installation.
- 9 Install the Enterprise Vault software on the other servers in your Enterprise Vault environment, including any cluster failover nodes.

## 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.

### 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 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.

The storage databases usually require a database schema upgrade, depending on your upgrade path. If a vault store database schema upgrade is required, the Storage service updates each vault store database. If a fingerprint database schema upgrade is required, the Storage service then upgrades each fingerprint database.

If a vault store database schema upgrade is required, 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 four instances of this pair of events, as different scripts are run.
- Event 6959: The upgrade of the database has completed.

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 four 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.

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

## 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.

# Extra configuration tasks

This chapter includes the following topics:

- [About the extra configuration tasks](#)
- [Upgrading MOM and SCOM](#)
- [Extra configuration for servers with no Internet connection](#)
- [Enabling device-level sharing for EMC Centera partitions](#)

## About the extra configuration tasks

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

## Upgrading MOM and SCOM

---

**Note:** This section applies to all upgrades if you use MOM or SCOM.

---

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

### To install the Enterprise Vault MOM management pack

- 1 Start the MOM Administrator Console.
- 2 In the left pane, right-click **Processing Rule Groups** and, on the shortcut menu, click **Import Management Pack**.
- 3 Select the Enterprise Vault Management Pack, `EnterpriseVault.akm`, and work through the rest of the **Import Options** wizard.

---

**Note:** The minimum version of SCOM 2007 is now SCOM 2007 R2. You cannot import the Enterprise Vault SCOM management pack into the SCOM 2007 original release.

---

#### To install the Enterprise Vault SCOM management pack

- 1 Start the SCOM operations console.
- 2 Start the import wizard and import `EnterpriseVault.mp`. The file is in the SCOM subfolder of the Enterprise Vault program folder, for example  
`C:\Program Files (x86)\Enterprise Vault\SCOM`.

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

## Extra configuration for servers with no Internet connection

---

**Note:** This section applies if you upgraded to Enterprise Vault 9.0.4 from the Enterprise Vault 8.0 original release, or Enterprise Vault 8.0 SP1. If you upgraded from Enterprise Vault 8.0 SP2 or later you can ignore this section.

---

If your Enterprise Vault server does not have a connection to the Internet, administrators and users can experience delays while Windows tries to check digital certificates.

This issue arises because Enterprise Vault files are digitally signed. By default, when these files are accessed, Windows checks to determine whether the file's digital certificate has been revoked. If no Internet connection is available, the Web application pauses while Windows tries to check the certificate.

The delays are obvious at the following times:

- When you run `Setup.exe` to install Enterprise Vault.
- When you start the Administration Console.
- When users access Web applications such as Archive Explorer or the integrated search.

See the section "Performance issues when an Enterprise Vault server has no Internet connection" in the *Installing and Configuring* manual.



# Enabling device-level sharing for EMC Centera partitions

---

**Note:** This section applies if you ever upgraded to the original release of Enterprise Vault 8.0.

---

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

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

---

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

---

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

## To enable device-level sharing for a Centera partition

- 1 In the Administration Console, double-click the Centera partition to display its properties.
- 2 On the **General** tab of the partition properties, select **Enable device-level sharing**.
- 3 Click **OK**.



# 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.

### 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 9.0.4 media.
- 4 Use Windows Explorer to open the following folder:  
`\Symantec Enterprise Vault 9.0.4\Server`
- 5 Double-click the file `setup.exe` to start the installation.
- 6 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](#)
- [Troubleshooting Enterprise Vault Reporting and FSA Reporting](#)

## Upgrading Enterprise Vault Reporting

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

[Table 13-1](#) lists the steps that are required to upgrade Enterprise Vault Reporting.

**Table 13-1** Steps to install Enterprise Vault Reporting

Step	Action	Description
Step 1	Install the Enterprise Vault 9.0.4 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 70.

**Table 13-1** Steps to install Enterprise Vault Reporting *(continued)*

Step	Action	Description
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 70.

## Installing the Enterprise Vault Reporting component

You must install the Enterprise Vault 9.0.4 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 9.0.4 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 9.0.4 media.
- 3 Use Windows Explorer to open the following folder:  
`\Symantec Enterprise Vault 9.0.4\Server`
- 4 Double-click the file `setup.exe` to start the installation.
- 5 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 9.0.4 software on the Enterprise Vault servers.
- Installed the Enterprise Vault 9.0.4 Reporting component on each computer on which the Reporting component is installed.

### To run the Enterprise Vault Reporting Configuration utility

- 1 On the Windows **Start** menu, click **Programs > Enterprise Vault > Enterprise Vault Reports Configuration**.
- 2 In the Reporting Configuration utility dialog box, 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 technical note *Troubleshooting Enterprise Vault Reporting*.

See “[Troubleshooting Enterprise Vault Reporting and FSA Reporting](#)” on page 71.

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.

## Troubleshooting Enterprise Vault Reporting and FSA Reporting

To troubleshoot problems with Enterprise Vault Reporting or FSA Reporting after the upgrade, refer to the following Enterprise Vault technical notes.

**Table 13-2** Enterprise Vault Reporting troubleshooting technical notes

Technical note	Description and location
<i>Troubleshooting Enterprise Vault Reporting</i>	Describes how to troubleshoot aspects of Enterprise Vault Reporting other than FSA Reporting.  See <a href="http://www.symantec.com/docs/TECH51288">www.symantec.com/docs/TECH51288</a> .

Table 13-2

Enterprise Vault Reporting troubleshooting technical notes

(continued)

Technical note	Description and location
<i>Troubleshooting FSA Reporting</i>	Describes how to troubleshoot FSA Reporting. See <a href="http://www.symantec.com/docs/TECH51475">www.symantec.com/docs/TECH51475</a> .



# Upgrading Exchange Server forms

This chapter includes the following topics:

- [About upgrading Exchange Server forms](#)

## About upgrading Exchange Server forms

By default, Enterprise Vault 9.0.4 deploys the Exchange Server forms to users' computers automatically.

If you are upgrading from Enterprise Vault 8.0, note that the Exchange Server forms in Enterprise Vault 9.0 are functionally the same as the forms that are in Enterprise Vault 8.0. There is no requirement for you to upgrade existing Enterprise Vault 8.0 forms.

If you upgrade from Enterprise Vault 2007 to Enterprise Vault 8.0 and then immediately to Enterprise Vault 9.0, note that the upgrade from Enterprise Vault 2007 to Enterprise Vault 8.0 changed the desktop policy. The upgrade set the desktop policy Advanced setting **Deploy Forms Locally** to **Always**. This policy change means that the Enterprise Vault Outlook Add-Ins automatically install the Enterprise Vault forms into users' local forms libraries. The new forms are not installed until you upgrade users' Outlook Add-Ins.

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`, and

`EVPendingRestore.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](#)
- [Checking the custom filter rules](#)
- [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.

## Domino client version required to run EVInstall.nsf

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

The minimum client version that you can use to run `EVInstall.nsf` is Notes 7.0.2 with appropriate hotfixes.

For details of the required hotfixes and the latest information on supported versions of Domino software, see the *Enterprise Vault Compatibility Charts* at [www.symantec.com/docs/TECH38537](http://www.symantec.com/docs/TECH38537).

## 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:

- Forms85.nsf
- Forms8.nsf
- Forms7.nsf
- Forms6.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 9.0.4.

---

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

- 1 Stop the HTTP task.
- 2 If Forms85\_x.nsf exists on the server, delete it.
- 3 Replace the Forms85.nsf, Forms8.nsf, Forms7.nsf, and Forms6.nsf files with the original Domino versions that you backed up before you installed the previous version of Enterprise Vault.
- 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 Forms6.nsf, Forms7.nsf, Forms8.nsf, and Forms85.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 9.0.4 - Domino Installer (`EVInstall.nsf`) with the ID of the user that will be used to run it.
- 2 Make sure that you have the correct Lotus Notes client and any hotfixes required.

See [“Domino client version required to run EVInstall.nsf”](#) on page 75.

- 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 9.0.4 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 9.0.4 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.

- 6 If necessary, upgrade Notes 7 on Enterprise Vault servers to Notes 8.0 or Notes 8.5.

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

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

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

## Granting the Domino archiving user access to mail files

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

The minimum permissions that are required depend on which version of Notes is installed on the Enterprise Vault server on which the archiving task runs. The minimum permissions required to mail files are as follows:

- When Notes 8 or Notes 8.5 is installed on the Enterprise Vault server, the account requires a minimum of **Editor** access with **Delete Documents** and **Create shared folders/views**.
- When Notes 7 is installed on the Enterprise Vault server, the account requires a minimum of **Designer** access with **Delete Documents**.

---

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

---

If Domino administrators have Manager access to all mail files, 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 Lotus 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:

On a 32-bit installation of Windows:

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

On a 64-bit installation of Windows:

```
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>

## Checking the custom filter rules

In Enterprise Vault 8.0 SP3 changes were made to the display name format that Enterprise Vault uses to look up Lotus Notes users. Enterprise Vault 8.0 SP3 and later releases do not include the domain in display name attributes, </DISPN>, in custom filter rules.

To use the <DISPN> attribute to specify a filter for message authors and recipients, use the format that is shown in the following examples:

```
<DISPN>Kevin Smith/exampleOrg</DISPN>  
<DISPN>Kevin Smith/exampleOU/exampleOrg</DISPN>
```

The following display name format is no longer valid in Enterprise Vault 8.0 SP3 and later releases:

```
<DISPN>Kevin Smith/exampleorg@exampledomain</DISPN>
```

If you have custom filtering configured for Domino Server archiving, check that the correct display name format is used in the existing filter rules files.

## Minimizing the potential performance effects of shortcut deletion

Enterprise Vault 9.0 introduces 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 all the Windows computers on which it is installed, except Windows 2000 computers. 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.

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 [www.symantec.com/docs/TECH38537](http://www.symantec.com/docs/TECH38537).
- For FSA Reporting, the Enterprise Vault technical note at [www.symantec.com/docs/TECH57334](http://www.symantec.com/docs/TECH57334).

For information about the FSA Agent and Windows 2000 computers, see the following:

- For upgrades from any version of Enterprise Vault 8.0: See “[Enterprise Vault 9.0.4 FSA Agent is not supported on Windows 2000 computers](#)” on page 21.

- For upgrades from any version of Enterprise Vault 9.0: See “Enterprise Vault 9.0.4 FSA Agent is not supported on Windows 2000 computers” on page 31.

---

**Note:** If you are upgrading from any version of Enterprise Vault 8.0 and you use FSA Reporting, you must upgrade the FSA Agent on your Windows file servers. Otherwise, FSA Reporting scans do not run.

---

---

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

---

---

**Note:** 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 Web site:

[www.symantec.com/docs/TECH179712](http://www.symantec.com/docs/TECH179712)

---

You can upgrade the FSA Agent from an Enterprise Vault Administration Console, or manually. If you upgrade from an Administration Console you must turn off the Windows Firewall on the file server while you perform the upgrade. Otherwise the Administration Console wizard fails with the message "Error: The RPC server is unavailable". If you do not want to turn off the Windows Firewall, upgrade the FSA Agent manually.

---

**Note:** From Enterprise Vault 9.0.2 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 85.
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 86.
For upgrades from any version of Enterprise Vault 9.0:  Upgrade the FSA Agent on FSA Reporting proxy servers from the Administration Console.	See “Upgrading the FSA Agent on an FSA Reporting proxy server from the Administration Console” on page 87.
Upgrade the FSA Agent manually.	See “Upgrading the FSA Agent manually” on page 88.

# Upgrading FSA Agent services that are clustered for high availability

To perform the following procedure, you must run the Administration Console on a computer whose operating system is compatible with the operating system of the file server cluster.

For the latest information on the requirements for managing clustered file servers, see this technical note on the Symantec Support Web site:  
[www.symantec.com/docs/TECH71442](http://www.symantec.com/docs/TECH71442).

## To upgrade FSA Agent services that are clustered for high availability

- Perform these steps in the order shown:
  - In the Administration Console, expand the Enterprise Vault site.
  - Expand the **Targets** container and then the **File Servers** container.
  - Right-click the clustered file server and then, on the shortcut menu, click **FSA Cluster Configuration**.
  - Select the option **Remove the FSA resource from all groups** to remove the FSA resource.
- 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 86.

- Upgrade the FSA Agent manually on each file server node.  
See [“Upgrading the FSA Agent manually”](#) on page 88.
- 3 Perform the following steps in the order shown to reconfigure the FSA services for high availability:
  - In the Administration Console, expand the Enterprise Vault site.
  - Expand the **Targets** container and then the **File Servers** container.
  - Right-click the clustered file server and then, on the shortcut menu, click **FSA Cluster Configuration**.
  - Select the option **Add, remove or reconfigure the FSA resource for groups that have shared disks**, and add the FSA resource back to the groups that have a shared disk.

## Upgrading the FSA Agent 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 Turn off the Windows Firewall 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.
- 7 Turn the file server's Windows Firewall back on when the installation has finished.

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

This section applies if both of the following are true:

- You are upgrading from any version of Enterprise Vault 9.0.
- You use FSA Reporting on 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.

---

**Note:** Do not install the FSA Agent on Enterprise Vault servers, even if they act as FSA Reporting proxy servers. Enterprise Vault servers do not require the FSA Agent.

---

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

- 1 Turn off the Windows Firewall on the FSA Reporting proxy server.  
If you do not want to turn off the Windows Firewall you can install the FSA Agent manually on the FSA Reporting proxy server.  
See [“Upgrading the FSA Agent manually”](#) on page 88.
- 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.
- 7 Turn the Windows Firewall back on when the installation is finished.

## 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:
    - `vcredist_x86.exe`
    - `vc2005redist_x86.exe`
  - On a 64-bit Windows system, run all of the following:
    - `vcredist_x86.exe`
    - `vc2005redist_x86.exe`
    - `vcredist_x64.exe`
- 3 Run the appropriate MSI file on the file server:
  - On a 32-bit Windows system, run `Enterprise Vault File System Archiving.msi`



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



# Upgrading the FSA metadata

This chapter includes the following topics:

- [About upgrading the FSA metadata](#)

## About upgrading the FSA metadata

---

**Note:** This section applies only if you upgraded from any version of Enterprise Vault 8.0.

---

If you use File System Archiving then after you have upgraded the Enterprise Vault servers you must upgrade the FSA metadata in the vault store databases to the new summarized format. The summarized metadata enables Enterprise Vault Reporting to generate some of its reports more efficiently. Enterprise Vault Reporting cannot report on the FSA items that were archived with previous versions of Enterprise Vault until you upgrade the existing FSA metadata.

You can use the **FSA upgrade utility** command-line tool to upgrade the FSA metadata.

---

**Note:** You must upgrade the FSA metadata whether or not you use Enterprise Vault Reporting.

You cannot upgrade from Enterprise Vault 9.0 to the next major release of Enterprise Vault until you have upgraded every vault store that contains FSA data.

---

On upgrade to Enterprise Vault 9.0, Enterprise Vault generates the following warning messages if you need to use the FSA upgrade utility:

- After a Directory service upgrade, a warning message appears in the Administration Console's **Status** pane if FSA data is present. The message lists the affected Enterprise Vault servers, and the number of vault stores that require upgrade on each server. The warning message persists until you upgrade the FSA data in all of the affected vault stores.
- After the upgrade of each vault store that contains FSA data, the Storage service generates a warning message in the Enterprise Vault Event log for that vault store.

For information about how to use the FSA upgrade utility, see the "FSA upgrade utility" section of the *Utilities* guide.

# 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 9.0.4.

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

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

[www.symantec.com/docs/TECH69113](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 9.0.4 media.
- 2 Open the `Symantec Enterprise Vault 9.0.4` folder.
- 3 Open the `OWA 2010 Extensions` folder.
- 4 Double-click the file `Symantec Enterprise Vault OWA 2010 Extensions x64.msi` to start the installation.
- 5 Follow the installation instructions.
- 6 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 on each Exchange 2007 CAS server

- 1 Load the Enterprise Vault 9.0.4 media.
- 2 Open the `Symantec Enterprise Vault 9.0.4` folder.
- 3 Open the `OWA 2007 Extensions` folder.
- 4 Double-click the appropriate .msi file to start the installation, depending on whether the Exchange Server is running in 64-bit or 32-bit mode:
  - `Symantec Enterprise Vault OWA 2007 Extensions x64.msi`
  - `Symantec Enterprise Vault OWA 2007 Extensions x86.msi`

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

## Upgrading Enterprise Vault OWA 2003 Extensions

For details of the versions of OWA 2003 control files supported by the Enterprise Vault 9.0.4 OWA Extensions, see the *Enterprise Vault Compatibility Charts* at [www.symantec.com/docs/TECH38537](http://www.symantec.com/docs/TECH38537).

### To upgrade the Enterprise Vault OWA 2003 Extensions

- 1 Populate the file `EVServers.txt`.  
 See “[Preparing EVServers.txt](#)” on page 95.
- 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 96.

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

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

## 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 Create the file `EVServers.txt`.  
See [“Preparing EVServers.txt”](#) on page 96.
- 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 97.

### 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.

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

- You can upgrade Enterprise Vault components on Microsoft Office SharePoint Server 2007, or Windows SharePoint Services 3.0.  
See [“Upgrading the Enterprise Vault SharePoint components”](#) on page 100.
- 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 [www.symantec.com/docs/TECH38537](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

We recommend that you upgrade the Enterprise Vault SharePoint components on each of your SharePoint Server computers.

## To upgrade the Enterprise Vault SharePoint components

- 1 Log on to the SharePoint Server 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 9.0.4 media.
- 3 Navigate to the following folder:  
`\Symantec Enterprise Vault 9.0.4\Server`
- 4 Double-click `setup.exe` to start the installation.
- 5 On the **Select Components to Install** screen, ensure that only **Microsoft SharePoint Components** is selected.
- 6 Click **Next**.
- 7 Work through the remainder of the installation wizard.

# Upgrading custom filters

This chapter includes the following topics:

- [Upgrading Exchange Journal archiving 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.

