

# Symantec Enterprise Vault™

## Installing and Configuring

10.0

# Symantec Enterprise Vault: Installing and Configuring

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: 2012-09-03.

## 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 ..... 19
	When to use this guide ..... 19
	Introducing this guide ..... 19
	Where to get more information about Enterprise Vault ..... 20
	“How To” articles on the Symantec Enterprise Support site ..... 22
	Enterprise Vault training modules ..... 22
	Comment on the documentation ..... 22
Section 1	Enterprise Vault requirements ..... 25
Chapter 2	Enterprise Vault hardware requirements ..... 27
	Hardware requirements for Enterprise Vault server ..... 27
	Running Enterprise Vault on a virtual server ..... 28
	Additional processing capacity for initial archiving ..... 28
	Hardware requirements for SQL Server ..... 29
	Network requirements for Enterprise Vault ..... 30
	About the storage requirements for Enterprise Vault ..... 30
	Storage for vault stores ..... 31
	Storage for Enterprise Vault indexes ..... 34
	Storage requirements for SQL databases ..... 35
	Storage requirements for the Enterprise Vault cache folder ..... 37
	Storage requirements for shopping baskets ..... 38
	Local storage requirements for temporary files ..... 38
Chapter 3	Enterprise Vault required software and settings ..... 41
	About the Enterprise Vault prerequisite software and settings ..... 41
	About the Enterprise Vault Deployment Scanner ..... 42
	Basic software requirements for Enterprise Vault ..... 42
	Required operating system components for Enterprise Vault ..... 42
	Vault ..... 42
	Windows PowerShell ..... 46

SQL server software .....	46
SQLXML .....	47
Microsoft Data Access Components (MDAC) .....	47
Net.Tcp port sharing on Index Servers .....	47
Best practice settings for Enterprise Vault servers .....	47
Message queue cleanup interval: MessageCleanupInterval .....	47
Message queue message storage limit: MachineQuota .....	48
Disable opportunistic locking: OplocksDisabled .....	48
Disable loopback check: DisableLoopbackCheck .....	49
Disable strict name checking: DisableStrictNameChecking .....	49
Maximum Outlook attachments and recipients: AttachmentMax and RecipientMax .....	50
TCP/IP maximum ports and TCP timed wait delay .....	51
Preinstallation tasks for Enterprise Vault server .....	52
Creating the Vault Service account .....	52
Creating a SQL login account .....	55
About assigning permissions and roles in SQL databases .....	57
Creating Enterprise Vault DNS aliases .....	58
Turning off or reconfiguring Windows Firewall .....	59
Securing data locations .....	59
About User Account Control (UAC) .....	60

Chapter 4	Additional requirements for Operations Manager .....	61
	About additional requirements for Operations Manager .....	61
	Where and when to install Operations Manager .....	61
	Additional prerequisite software for Operations Manager .....	62
	Additional preinstallation tasks for Operations Manager .....	62

Chapter 5	Additional requirements for Enterprise Vault Reporting .....	63
	About the requirements for Enterprise Vault Reporting .....	63
	Where and when to install Enterprise Vault Reporting .....	63
	Prerequisites for Enterprise Vault Reporting .....	64
	Enterprise Vault reports that require monitoring or auditing to be enabled .....	64
	Preparing for the installation of Enterprise Vault Reporting .....	65



## Chapter 6

## Additional requirements for Exchange Server

archiving .....	67
About Exchange Server archiving .....	67
Preinstallation tasks for all Exchange Server versions .....	68
Installing Outlook on the Enterprise Vault server .....	68
Creating the Enterprise Vault system mailbox .....	68
Removing the restriction on NSPI connections to a Windows Server 2008 domain controller .....	69
Creating a user profile and an Outlook profile on the Enterprise Vault server .....	70
Preinstallation tasks for Exchange Server 2010 and 2007 .....	70
Creating a mailbox for the Vault Service account .....	71
Creating an Exchange Server 2007 Public Folder store .....	71
Configuring the Exchange 2010 throttling policy on the Vault Service account .....	72
Granting the Vault Service account Send As permission on the system mailboxes .....	74
Assigning Exchange Server permissions to the Vault Service account .....	74
Preinstallation tasks for Exchange Server 2003 and 2000 .....	77
Assigning permissions on Microsoft Exchange Server 2003 and 2000 .....	77
Enterprise Vault client access with Exchange Server archiving .....	78
Prerequisites for the Enterprise Vault Outlook Add-In .....	79
Prerequisites for Enterprise Vault Client for Mac OS X .....	80
OWA clients .....	81
Customized shortcuts .....	81
Archive search and Archive Explorer in standalone browser .....	81
Prerequisites for OWA .....	82
Prerequisites for RPC over HTTP .....	84
Prerequisites for RPC over HTTP with Exchange Server 2003 .....	84
Prerequisites for Outlook Anywhere access to Enterprise Vault .....	84
Prerequisites for Enterprise Vault Mobile Search .....	85
About configuring Enterprise Vault Mobile Search .....	85
Prerequisites for Enterprise Vault Mobile Search in a production environment .....	85
Hardware requirements for the Enterprise Vault Mobile Search server .....	85

Windows Server 2003 requirements for Enterprise Vault Mobile Search .....	86
Windows Server 2008 requirements for Enterprise Vault Mobile Search .....	86
Enterprise Vault API Runtime required for Enterprise Vault Mobile Search .....	87

## Chapter 7

Additional requirements for Domino Server archiving .....	89
Domino Server archiving prerequisites for all Enterprise Vault servers .....	89
Prerequisites for Domino mailbox archiving .....	89
Prerequisite software for Enterprise Vault Domino Gateway .....	90
Prerequisite software for target Domino mail servers .....	90
Prerequisites for Enterprise Vault extensions for Lotus Notes clients .....	91
Preinstallation tasks for Domino mailbox archiving .....	91
Register the Enterprise Vault Domino Gateway .....	92
About the user ID for Domino mailbox archiving .....	94
Configuring the server document for each target Domino mail server .....	96
Install and configure Enterprise Vault Domino Gateway .....	97
Prerequisites for Domino journaling archiving .....	99
Prerequisites for Enterprise Vault archiving from Domino Journaling databases .....	99
Configuring access for Enterprise Vault to Domino domain, server, and Journaling location .....	100
Domino mailing list groups .....	101
Client access for Domino journal archiving .....	101

## Chapter 8

Additional prerequisites for File System Archiving (FSA) .....	103
About the prerequisites for FSA .....	103
Enterprise Vault server requirements for FSA .....	103
About FSA shortcuts .....	104
Placeholder shortcut requirements .....	105
About the FSA Agent .....	105
Preparing file servers for FSA .....	106
Client requirements for FSA .....	107

Chapter 9	Additional prerequisites for SharePoint Server archiving .....	109
	About the Enterprise Vault server requirements for SharePoint Server archiving .....	109
	Prerequisites for SharePoint Servers .....	109
	About SharePoint security certificates .....	111
Chapter 10	Additional prerequisites for SMTP archiving .....	113
	About the prerequisites for SMTP archiving .....	113
	Microsoft SMTP Server computer requirements .....	113
	EML file holding area and Enterprise Vault server requirements .....	114
	Client access for SMTP archiving .....	115
Chapter 11	Additional requirements for a standalone Enterprise Vault Administration Console .....	117
	About the prerequisites for a standalone Enterprise Vault Administration Console .....	117
Chapter 12	Additional requirements for the Discovery Search Service .....	119
	About additional requirements for the Discovery Search Service .....	119
	Additional prerequisite software for Discovery Search Service .....	119
Section 2	Installing Enterprise Vault .....	121
Chapter 13	Licenses and license keys .....	123
	Overview of Enterprise Vault licensing .....	123
	Obtaining license keys for Enterprise Vault .....	124
	Installing Enterprise Vault license key files .....	125
	Replacing Enterprise Vault licenses and installing additional licenses .....	125
Chapter 14	Installing Enterprise Vault .....	127
	Installing Enterprise Vault .....	127

Chapter 15	Postinstallation tasks .....	131
	Default security for the Enterprise Vault Web Access application .....	131
	Customizing security for the Enterprise Vault Web Access application .....	132
	Customizing the port or protocol for the Enterprise Vault Web Access application .....	133
	Customizing authentication for the Enterprise Vault Web Access application .....	134
	Customizing security for the Web Access application on client computers .....	135
	Configuring Internet Explorer to use the proxy bypass list .....	136
	Configuring Internet Explorer to trust the Web Access application computer .....	137
	Publishing Enterprise Vault server details to FDCC-compliant computers .....	137
	Enabling remote access to the Enterprise Vault Web Access application computer .....	139
Chapter 16	Uninstalling Enterprise Vault .....	141
	Uninstalling Enterprise Vault .....	141
	Reinstalling Enterprise Vault .....	142
Section 3	Configuring Enterprise Vault .....	143
Chapter 17	About configuring Enterprise Vault .....	145
	About configuring Enterprise Vault .....	145
Chapter 18	Running the Enterprise Vault configuration wizard .....	147
	When to run the Enterprise Vault configuration wizard .....	147
	What the Enterprise Vault configuration wizard does .....	148
	Running the Enterprise Vault configuration wizard .....	148
	Troubleshooting configuration of the Enterprise Vault Monitoring database .....	151

Chapter 19	Running the Enterprise Vault Getting Started wizard .....	153
	What the Enterprise Vault Getting Started wizard does .....	153
	Preparing to run the Enterprise Vault Getting Started wizard .....	154
	Running the Enterprise Vault Getting Started wizard .....	154
	About the express and custom modes of the Enterprise Vault Getting Started wizard .....	155
	About indexing configuration with the Enterprise Vault Getting Started wizard .....	155
	About storage configuration with the Enterprise Vault Getting Started wizard .....	156
	About policy definition with the Enterprise Vault Getting Started wizard .....	159
	About Exchange target configuration with the Enterprise Vault Getting Started wizard .....	160
	About Domino target configuration with the Enterprise Vault Getting Started wizard .....	161
	About file target configuration with the Enterprise Vault Getting Started wizard .....	162
	Planning for the Enterprise Vault Getting Started wizard .....	163
Chapter 20	Configuring Enterprise Vault Operations Manager .....	169
	When to run the Enterprise Vault Operations Manager Configuration utility .....	169
	Running the Enterprise Vault Operations Manager Configuration utility .....	170
	Accessing Enterprise Vault Operations Manager .....	170
	Troubleshooting Enterprise Vault Operations Manager .....	171
Chapter 21	Configuring the Discovery Search Service .....	173
	Running the Discovery Search Service Configuration utility .....	173
	Manually configuring a request endpoint for the Discovery Search Service .....	174
	Manually configuring a result endpoint for the Discovery Search Service .....	176
	Setting up the Discovery Search Service web applications to require secure (HTTPS) connections .....	177

Section 4	Initial Enterprise Vault setup .....	181
Chapter 22	Initial Enterprise Vault setup .....	183
	License keys .....	183
	Using the Enterprise Vault Administration Console .....	183
	Starting the Enterprise Vault Administration Console .....	184
	About administration roles in the Enterprise Vault Administration Console .....	185
	Adding core Enterprise Vault services with the Administration Console .....	186
	Creating Enterprise Vault retention categories .....	186
	About the properties of Enterprise Vault retention categories .....	187
	Performance issues when an Enterprise Vault server has no Internet connection .....	189
Chapter 23	Setting up storage .....	193
	About setting up storage for Enterprise Vault archives .....	193
	About Enterprise Vault single instance storage .....	194
	About sharing levels and sharing boundaries .....	196
	How Enterprise Vault single instance storage works .....	198
	About the fingerprint database .....	199
	Deletion of SIS parts .....	199
	Requirements for Enterprise Vault single instance storage .....	200
	About EMC Centera device-level sharing .....	200
	About sharing partitions on storage devices that support the Enterprise Vault storage streamer API .....	201
	Developing a suitable sharing regime for Enterprise Vault single instance storage .....	201
	Creating vault store groups .....	203
	About creating vault stores .....	204
	About Enterprise Vault safety copies .....	204
	Creating a vault store .....	207
	Creating vault store partitions .....	208
	Initial states of vault store partitions .....	209
	About collections and migration .....	210
	Creating a vault store partition .....	211
	Partition network shares for NTFS partitions with local paths .....	214
	Configuring sharing for a vault store group .....	215

Chapter 24	Adding index locations .....	217
	About Enterprise Vault index locations .....	217
	Creating an Enterprise Vault index location .....	217
Chapter 25	Setting up Index Server groups .....	219
	About Index Server groups .....	219
	Do I need to create Index Server groups? .....	220
	Do you have more than one Enterprise Vault server? .....	221
	Do you use or plan to use journal archiving or File System Archiving? .....	221
	Do you use or plan to use Compliance Accelerator or Discovery Accelerator? .....	222
	Is the server loading evenly distributed across existing Enterprise Vault servers? .....	222
	Are there more than approximately 5,000 mailbox archives per Enterprise Vault server? .....	223
	Creating an Index Server group .....	223
	Adding an Index Server to an Index Server group .....	225
	Removing an Index Server from an Index Server group .....	226
	Assigning a vault store to an Index Server group .....	227
	Unassigning a vault store from an Index Server group .....	228
	Assigning a vault store to a different indexer .....	228
Chapter 26	Reviewing the default settings for the site .....	231
	Reviewing the default settings for the Enterprise Vault site .....	231
	Setting the archiving schedule for the Enterprise Vault site .....	232
	About the Web Access application settings .....	233
Section 5	Clustering Enterprise Vault with Veritas Cluster Server .....	235
Chapter 27	Introducing clustering with VCS .....	237
	Supported VCS configurations and software .....	237
	About Enterprise Vault and the VCS GenericService agent .....	238
	Typical Enterprise Vault configuration in a VCS cluster .....	238
	Order in which to install and configure the components in a VCS environment .....	239

Chapter 28	Installing and configuring Veritas Storage Foundation HA for Windows .....	241
	Installing and configuring Veritas Storage Foundation HA for Windows with Enterprise Vault .....	241
	Managing disk groups and volumes in a Veritas Storage Foundation HA environment .....	243
Chapter 29	Configuring the VCS service group for Enterprise Vault .....	245
	About configuring the VCS service group for Enterprise Vault .....	245
	Before you configure the VCS service group for Enterprise Vault .....	246
	Creating a VCS service group for Enterprise Vault .....	247
	Modifying an existing VCS service group .....	249
	Deleting a VCS service group .....	250
Chapter 30	Running the Enterprise Vault Configuration wizard .....	251
	Before you run the Enterprise Vault Configuration wizard .....	251
	Setting up Enterprise Vault in an active/passive VCS configuration .....	252
	Adding VCS cluster support in a first-time Enterprise Vault installation .....	252
	Upgrading an existing Enterprise Vault installation to a VCS cluster .....	254
	About setting up Enterprise Vault in a VCS N+1 configuration .....	258
	Configuring two Enterprise Vault server nodes and a spare node in a VCS N+1 cluster .....	259
	Configuring two Enterprise Vault servers to run on any of the three nodes in a VCS cluster .....	261
	Disallowing two Enterprise Vault servers on the same node in a VCS cluster .....	262
Chapter 31	Implementing an SFW HA-VVR disaster recovery solution with Enterprise Vault .....	265
	About installing and configuring SFW HA-VVR with Enterprise Vault .....	265
	Overview of the steps for installing and configuring SFW HA-VVR .....	267
	Setting up the VCS cluster on the primary site .....	267
	Setting up the VCS cluster on the secondary site .....	268



	Adding the VVR components for replication .....	269
	Adding the GCO components for wide-area recovery .....	269
Chapter 32	Troubleshooting clustering with VCS .....	271
	VCS logging .....	271
	Enterprise Vault Cluster Setup wizard error messages .....	272
	Viewing the clustered message queues for an Enterprise Vault virtual server .....	273
Section 6	Clustering Enterprise Vault with Windows Server Failover Clustering .....	275
Chapter 33	Introducing clustering with Windows Server Failover Clustering .....	277
	About clustering Enterprise Vault with Windows Server Failover Clustering .....	277
	Supported Windows Server Failover Clustering configurations .....	278
	Required software and restrictions on clustering Enterprise Vault with Windows Server Failover Clustering .....	278
	Typical Enterprise Vault configuration in a Windows Server failover cluster .....	279
	Control of Enterprise Vault services in a Windows Server failover cluster .....	280
	About cluster services and Enterprise Vault service resources in a Windows Server failover cluster .....	280
	What happens at failover in a Windows Server failover cluster .....	281
Chapter 34	Preparing to cluster with Windows Server Failover Clustering .....	283
	Preparing to cluster Enterprise Vault with Windows Server Failover Clustering .....	283
	Setting up the shared disks and volumes for a Windows Server failover cluster .....	284
	Setting up the Enterprise Vault cluster services for a Windows Server failover cluster .....	285

Chapter 35	Configuring Enterprise Vault in a Windows Server failover cluster .....	289
	About configuring Enterprise Vault in a Windows Server failover cluster .....	289
	Setting up a new Enterprise Vault installation with Windows Server Failover Clustering support .....	290
	Configuring a new Enterprise Vault server with Windows Server Failover Clustering support .....	290
	Configuring a failover node in a Windows Server failover cluster .....	295
	Troubleshooting configuration of the Enterprise Vault Monitoring database .....	296
	Examples of Enterprise Vault installations in various Windows Server Failover Clustering modes .....	296
	Converting an existing Enterprise Vault installation to a Windows Server failover cluster .....	301
	Converting an existing Enterprise Vault server to a server with Windows Server Failover Clustering support .....	302
	Modifying an existing Enterprise Vault cluster .....	306
	Adding a node to an existing Windows Server failover cluster .....	307
	Adding shared storage to an existing Windows Server failover cluster for an Enterprise Vault cluster server .....	307
Chapter 36	Troubleshooting clustering with Windows Server Failover Clustering .....	309
	About this chapter .....	309
	Enterprise Vault event messages and the failover cluster log .....	310
	Resource ownership and dependencies when configuring Enterprise Vault in a failover clustered environment .....	310
	Registry replication on failover clustered nodes .....	310
	Viewing the clustered message queues for an Enterprise Vault cluster server .....	311
	Starting and stopping Enterprise Vault services in a Windows Server Failover Clustering environment .....	311
	Index .....	313

# About this guide

This chapter includes the following topics:

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

## When to use this guide

Work through this guide if you want to perform a new installation of Enterprise Vault.

To upgrade an existing installation of Enterprise Vault, see the *Upgrade Instructions* document.

If you want to install Enterprise Vault Reporting only, see the *Reporting* guide.

## Introducing this guide

This manual provides detailed information on installing and configuring Enterprise Vault. Before you install Enterprise Vault, read the *Introduction and Planning* manual so that you have an understanding of the various components.

To install and configure Enterprise Vault, you need to know how to administer the following products:

- Microsoft Windows Server 2008 R2
- Microsoft SQL Server
- Microsoft Message Queue Server

- Microsoft Internet Information Services (IIS)
- Your archive storage hardware and software

If you are going to be using Enterprise Vault with IBM Domino Server, you also need administrative knowledge of IBM Domino Server and the IBM Lotus Notes client.

If you going to be using Enterprise Vault with Microsoft Exchange Server, you also need administrative knowledge of Exchange Server and Outlook.

If you going to be using Enterprise Vault with Microsoft Windows SharePoint Services and Microsoft SharePoint Portal Server, you need administrative knowledge of these products.

To use the reporting feature of Enterprise Vault Operations Manager, you need administrative knowledge of Microsoft SQL Server Reporting Services.

# 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.

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

Document	Comments
<i>Setting up Exchange Server Archiving</i>	Describes how to archive items from Microsoft Exchange user mailboxes, journal mailboxes, and public folders.
<i>Setting up Domino Server Archiving</i>	Describes how to archive items from Domino mail files and journal databases.
<i>Setting up File System Archiving</i>	Describes how to archive the files that are held on network file servers.
<i>Setting up SharePoint Server Archiving</i>	Describes how to archive content from Microsoft SharePoint servers.
<i>Setting up SMTP Archiving</i>	Describes how to archive SMTP messages from other messaging servers.
<i>Administrator's Guide</i>	Describes how to perform day-to-day administration, backup, and recovery procedures.
<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.





## Enterprise Vault requirements

- [Chapter 2. Enterprise Vault hardware requirements](#)
- [Chapter 3. Enterprise Vault required software and settings](#)
- [Chapter 4. Additional requirements for Operations Manager](#)
- [Chapter 5. Additional requirements for Enterprise Vault Reporting](#)
- [Chapter 6. Additional requirements for Exchange Server archiving](#)
- [Chapter 7. Additional requirements for Domino Server archiving](#)
- [Chapter 8. Additional prerequisites for File System Archiving \(FSA\)](#)
- [Chapter 9. Additional prerequisites for SharePoint Server archiving](#)
- [Chapter 10. Additional prerequisites for SMTP archiving](#)
- [Chapter 11. Additional requirements for a standalone Enterprise Vault Administration Console](#)
- [Chapter 12. Additional requirements for the Discovery Search Service](#)



# Enterprise Vault hardware requirements

This chapter includes the following topics:

- [Hardware requirements for Enterprise Vault server](#)
- [Hardware requirements for SQL Server](#)
- [Network requirements for Enterprise Vault](#)
- [About the storage requirements for Enterprise Vault](#)

## Hardware requirements for Enterprise Vault server

Any computer on which you plan to install Enterprise Vault must be a member of a domain.

[Table 2-1](#) shows the minimum and recommended specifications for a production Enterprise Vault system.

**Table 2-1** Minimum and recommended specifications for an Enterprise Vault server

Item	Minimum and recommended specification
Number of processor cores	Minimum: 4 Recommended: 8  The total number of cores can be achieved by any combination of physical CPUs and their cores.
Power of CPUs	2 GHz

**Table 2-1** Minimum and recommended specifications for an Enterprise Vault server *(continued)*

Item	Minimum and recommended specification
Memory	Minimum: 8 GB Recommended: 16 GB
Disk space	1 GB <b>Note:</b> Enterprise Vault 10.0 prevents installation on a partition with less than 1 GB of free disk space.

In smaller Enterprise Vault environments, you can install all Enterprise Vault’s core services on the same server. However, in larger environments you can consider deploying individual services, such as the Storage service and the Indexing service, on dedicated Enterprise Vault servers.

For more information about distributing Enterprise Vault services, see the *Introduction and Planning* manual.

## Running Enterprise Vault on a virtual server

You can run Enterprise Vault on a virtual server. For more information about the virtualization technologies supported by Enterprise Vault, see the Enterprise Vault *Compatibility Charts* at <http://www.symantec.com/docs/TECH38537>.

If a virtual Enterprise Vault server hosts the Indexing service, we recommend that you use a virtual machine that supports eight processor cores. If the virtual machine does not support this many processor cores, we recommend that you deploy a dedicated virtual server to host only the Indexing service.

For more information about the performance of Enterprise Vault on a virtual server, see the Enterprise Vault *Performance Guide* at <http://www.symantec.com/docs/TECH125795>.

For more information about the deployment of Enterprise Vault on a virtual server, see the Enterprise Vault best practice articles at <http://www.symantec.com/docs/HOWTO75088>.

## Additional processing capacity for initial archiving

If you have a large backlog of data that you want to archive quickly, when you first install Enterprise Vault, you may want to configure additional Enterprise Vault servers for the initial archiving run. When archiving reaches a steady state, the additional Enterprise Vault servers can be redeployed for other purposes.

# Hardware requirements for SQL Server

Enterprise Vault requires a number of SQL databases:

- The Enterprise Vault Directory database holds the configuration information for an Enterprise Vault site.
- Each vault store has a vault store database, which holds configuration information for the vault store and details of the items stored in its archives.
- Each vault store group has a fingerprint database, which holds the fingerprints and other information related to the single instance storage parts that are created for Enterprise Vault single instance storage.
- The Monitoring database holds monitoring information for the Enterprise Vault site.
- If you configure FSA Reporting, Enterprise Vault creates an FSA Reporting database to hold the FSA Reporting data. You can configure additional FSA Reporting databases for scalability or to segregate information, if required.

The SQL Server that manages these databases will typically reside on a different computer from the Enterprise Vault server.

In general, the specification of the SQL Server computer should match that of the Enterprise Vault server. The performance of the SQL Server will also benefit from extra memory; a minimum of 4 GB is recommended. The amount of memory that the SQL Server can use depends on the Windows and SQL Server versions.

[Table 2-2](#) shows the minimum and recommended specifications for a production SQL Server.

**Table 2-2** Minimum and recommended specifications for SQL server

Item	Minimum and recommended specification
Number of processor cores	Minimum: 4 Recommended: 8 The total number of cores can be achieved by any combination of physical CPUs and their cores.
Power of CPUs	2 GHz
Memory	Minimum: 8 GB Recommended: 16 GB

You do not need a separate SQL Server for every Enterprise Vault server. As a general rule, one SQL Server can manage up to eight Enterprise Vault servers.

## Network requirements for Enterprise Vault

Enterprise Vault can generate a considerable volume of network traffic. As a minimum we recommend an environment in which the connections support the expected response time of a 100 Mbps switched Ethernet LAN.

For guidelines on the network traffic you might expect between the various components under different conditions, see the *Enterprise Vault Performance Guide* at <http://www.symantec.com/docs/TECH125795>.

For more information about Enterprise Vault's interoperability with other products in an IPv6 environment, see the *Enterprise Vault Compatibility Charts* at <http://www.symantec.com/docs/TECH38537>.

When you configure sharing with Enterprise Vault single instance storage, Enterprise Vault provides a connectivity test to help you determine whether the network latency is acceptable across the relevant connections.

See “[About Enterprise Vault single instance storage](#)” on page 194.

## About the storage requirements for Enterprise Vault

Storage is required for the following components of Enterprise Vault:

- Vault stores, where the archived items are held.
- Indexes.
- SQL Server databases:
  - Enterprise Vault Directory database
  - Vault store databases
  - Vault store group fingerprint databases
  - Monitoring database
  - One or more FSA Reporting databases, if FSA Reporting is configured
- Server cache for temporary files used by Enterprise Vault.
- Shopping baskets, which are used by Enterprise Vault for details of items that are to be restored.

In addition a small amount of local storage is needed on the Enterprise Vault server.

This section gives a basic guide to the Enterprise Vault storage requirements.

For full details of all the supported storage devices and software, see the Enterprise Vault *Compatibility Charts* at <http://www.symantec.com/docs/TECH38537>.

## Storage for vault stores

The Enterprise Vault Storage service computer needs access to storage for the vault stores.

Enterprise Vault is very versatile in its use of storage for the vault stores, and is designed to operate with various types of storage solution provided by third party software and hardware products. Many storage solutions provide high performance archiving and retrieval.

The types may be categorized as follows:

- Local storage
- NTFS (an NTFS volume or a network share that appears on the network as an NTFS volume)
- SAN
- NAS
- CAS (Centera)
- Storage device that supports the Enterprise Vault storage streamer API

The Write Once Read Many (WORM) feature is supported on several devices.

If you plan to create a vault store partition on a storage device that supports the Enterprise Vault storage streamer API, ensure that the appropriate storage device software is installed on the Enterprise Vault storage servers. Install the storage device software on all the Enterprise Vault storage servers that manage the partitions in the vault store group.

One of the most important factors that will determine the performance of Enterprise Vault is the speed of the storage device.

### Preparing WORM storage devices

The information in this section refers specifically to NetApp ONTAP devices with SnapLock. If you plan to use other WORM devices to hold vault store partitions, then we recommend that you configure them in a similar way, if possible.

For details of the required commands, refer to the API documentation for your storage system.

For a list of the WORM devices that can be used for vault store partitions, see the Enterprise Vault *Compatibility Charts* at <http://www.symantec.com/docs/TECH38537>.

On NetApp devices, you can set the default retention period and a maximum retention period for items stored on the device. To ensure that items with the

Enterprise Vault retention period of **Forever** remain locked, you need to configure the following settings explicitly on the storage device:

- Set the default retention period to infinite.
- Set the maximum retention period to infinite.

If either of these is not set, or set to a value other than infinite, then users or third party applications may be able to delete the items after the default or maximum retention period set on the device has expired.

---

**Note:** Enterprise Vault will not expire or delete the items.

---

## Required amount of storage for vault stores

When an item is archived, it is first compressed and then metadata is added to it. As a general rule, the item is compressed to half its original size and the metadata comprises approximately 5 KB. When an item is shared, only the metadata is added.

The following general rules can be used for estimating the amount of storage needed:

- Take the total size of items to be archived and halve it.
- For email items, divide by the average number of recipients.
- Add 5 KB multiplied by the total number of items.

The compression ratio may vary considerably. Office documents tend to compress well. Other document types, such as ZIP files or JPG files, are already compressed and cannot be compressed further. For this reason, you should always overestimate the amount of storage needed.

The above general rule applies to most types of archiving, but care needs to be taken with File System Archiving (FSA). For example, if ZIP files or JPG files are archived, there is no space saving.

For email archiving, growth in the number of mailboxes and the number and size of messages must also be taken into consideration. Because of these extra factors, a more conservative method of estimating storage is to assume that space used by archiving will equal the space used by Exchange Server or Domino Server in storing items.



## Migration of archived data to secondary storage

You can migrate the data that you archive with Enterprise Vault to secondary storage systems. [Table 2-3](#) describes the storage solutions that interoperate with Enterprise Vault to provide integrated data migration.

**Table 2-3** Supported storage solutions

Storage solution	More information
Amazon Simple Storage Service	<a href="http://www.symantec.com/docs/DOC5387">http://www.symantec.com/docs/DOC5387</a>
AT&T Synaptic Storage as a Service	<a href="http://www.symantec.com/docs/DOC5388">http://www.symantec.com/docs/DOC5388</a>
Fujitsu ETERNUS Archive Storage	<a href="http://www.symantec.com/docs/TECH49971">http://www.symantec.com/docs/TECH49971</a>
IBM System Storage DR550	<a href="http://www.symantec.com/docs/TECH49972">http://www.symantec.com/docs/TECH49972</a>
Nirvanix Storage Delivery Network	<a href="http://www.symantec.com/docs/TECH162359">http://www.symantec.com/docs/TECH162359</a>
Rackspace Cloud Files	<a href="http://www.symantec.com/docs/DOC5389">http://www.symantec.com/docs/DOC5389</a>
Symantec Backup Exec	See the <i>Backup Exec Administrator's Guide</i> , which is available from the Symantec Enterprise Support site: <a href="http://www.symantec.com/business/support/index?page=content&amp;key=15047&amp;channel=DOCUMENTATION">http://www.symantec.com/business/support/index?page=content&amp;key=15047&amp;channel=DOCUMENTATION</a>
Symantec NetBackup	For NetBackup 7.0 or later, see the <i>NetBackup for Enterprise Vault Agent Administrator's Guide</i> . This guide is available from the Symantec Enterprise Support site: <a href="http://www.symantec.com/business/support/index?page=landing&amp;key=15145">http://www.symantec.com/business/support/index?page=landing&amp;key=15145</a>  For NetBackup 6.5, see the following white paper on the Symantec Enterprise Support site: <a href="http://www.symantec.com/docs/TECH70427">http://www.symantec.com/docs/TECH70427</a>

The [Compatibility Charts](#) provide the latest information on the secondary storage software that Enterprise Vault supports.

**Caution:** If you use secondary storage that is slow to respond, some Enterprise Vault operations that access this storage will take a long time. For example, both tape and cloud storage can be very slow.

## Storage for Enterprise Vault indexes

The computer hosting the Enterprise Vault Indexing service requires access to adequate storage for the indexes.

Each indexing Service also requires disk space for indexing configuration and reporting data. This is set using **Index metadata location** in the Indexing service properties. If you install Enterprise Vault on a cluster, then the index metadata folder, *Enterprise Vault installation folder\EVIndexing\data\metadata*, must be moved to a shared drive. You will also need to update **Index metadata location** in the Indexing service properties.

Indexes may be placed on local storage, SAN, or NAS. If fast indexing is required or searches across a large number of archives, NAS devices may not be suitable.

File systems that use slow storage media as part of their solution, such as optical disk, are unsuitable for indexes.

If indexes are stored on NetApp devices, and possibly other NAS systems, opportunistic locking must be turned off for volumes that contain indexes. For more information, see the following article on the Symantec Enterprise Support site:

<http://www.symantec.com/docs/TECH45566>

As anti-virus software can potentially change data, it is important to exclude the index locations in your virus checking application. For more information, see the following article on the Symantec Enterprise Support site:

<http://www.symantec.com/docs/TECH48856>

Table 2-4 shows how to calculate the expected sizes of indexes.

**Table 2-4** Index size compared to size of original data

Indexing type	Index size as a proportion of original data size
Brief	4%
Full	12%

The type of data being archived will also affect the size of indexes. Archiving a large number of text or HTML files will produce larger indexes. Archiving a large number of binary files, such as image files, will produce smaller indexes, as the content is not indexed.

There is no sharing of index files.

## Storage requirements for SQL databases

Storage space is required for the following SQL databases:

- Enterprise Vault Directory database
- Vault store databases
- Vault store group fingerprint databases
- Monitoring database
- One or more FSA Reporting databases, if FSA Reporting is configured
- Audit database

### Storage required for the Enterprise Vault Directory database

The directory database has an initial storage requirement of 10 MB for the data device and 25 MB for the transaction log device, making a total initial disk space requirement of 35 MB.

To allow for temporary growth and the transaction logs, it is suggested that you make 5 GB available for the directory database.

### Storage required for the vault store databases

Each vault store database has an initial storage requirement of 100 MB for the data device and 80 MB for the transaction log device, making a total initial disk space requirement of 180 MB for each vault store database.

Ensure that there is adequate space for database devices to grow as data is added. Transaction logs should be limited to an appropriate size for your back-up and maintenance plan.

A basic sizing guide for each vault store database is 250 bytes for each item archived plus 5 GB for static data, transaction logs and temporary data fluctuations.

If you configure a vault store partition on an EMC Centera device, and the partition is enabled for collection, then an additional SQL index may be created for the Saveset table in the associated vault store database. The space required for this index on the SQL Server hosting the relevant vault store database is approximately 27 bytes per row in the Saveset table.

### Storage required for the fingerprint databases

A vault store group's fingerprint database holds the fingerprint, the storage location, and sharing boundary information for each SIS part that is stored in the group's vault stores.

The fingerprint database has an initial storage requirement of 244 MB, made up as follows:

- 132 MB for the primary filegroup
- 1 MB for each of the 32 non-primary filegroups
- 80 MB for the transaction log device

The non-primary filegroups hold the SIS part fingerprints and other information about the SIS parts. If you share items using Enterprise Vault single instance storage, the non-primary filegroups may grow very rapidly in size. Ensure that there is adequate space for the non-primary filegroups to grow as data is added.

The New Vault Store Group wizard provides the following options for the initial configuration of the fingerprint database:

- A default basic configuration, where Enterprise Vault locates the primary filegroup and all the non-primary filegroups on one device.
- An advanced configuration option, where you can specify separate locations for the 32 non-primary SQL filegroups.

To ensure acceptable archiving and retrieval performance, it is important to configure the fingerprint database appropriately for the amount of sharing in the vault store group.

For optimal performance, do as follows:

- Use the advanced configuration option to specify as many locations as possible on the SQL Server, up to the maximum of 32.
- Use a separate device for each location. If you specify more than one location on the same device there is no performance benefit.

---

**Note:** To add or change locations after the fingerprint database is configured is a SQL Server administration task.

---

Limit transaction logs to an appropriate size for your back-up and maintenance plan.

## Storage required for the Monitoring database

The Monitoring database has an initial storage requirement of 100 MB for the data device and 80MB for the transaction log device, making a total initial disk space requirement of 180 MB.

Ensure that there is adequate space for the database to grow as monitoring data is added.

## Storage required for the FSA Reporting databases

If you configure FSA Reporting, Enterprise Vault creates an FSA Reporting database. This database contains the data that the Enterprise Vault File Collector service gathers. This data is used in FSA Reporting's data analysis reports.

You may want to create additional FSA Reporting databases, for example for scalability or to segregate the reporting data.

Each FSA Reporting database has an initial storage requirement of 100 MB for the data device and 80 MB for the transaction log device. The total initial disk space requirement is 180 MB.

Ensure that there is adequate space for each FSA Reporting database to grow as reporting data is added.

A batch file is provided to trim the FSA Reporting database history tables. The batch file retains recent and trend-related information.

See "Maintaining the FSA Reporting databases" in the *Reporting* guide.

## Storage required for the audit database

The audit database is not created until you enable auditing. By default, auditing is disabled.

The initial storage requirement for the audit database is 100 MB for the database and 80 MB for the transaction log.

You can enable auditing for individual Enterprise Vault servers. The auditing events for several Enterprise Vault servers in a site can be written to a single auditing database.

The amount of space required will depend on the number and type of events logged and the level of detail required.

The *Utilities* manual describes how to set up auditing.

Limit transaction logs to an appropriate size for your back-up and maintenance plan. For instructions on how to roll over the audit database, see this Symantec Support document:

<http://www.symantec.com/docs/TECH35746>

## Storage requirements for the Enterprise Vault cache folder

The cache is a folder on the Enterprise Vault server in which Enterprise Vault stores temporary files for the following:

- Indexing service

- File System Archiving (FSA), if the target file server is either a NetApp Filer for which you have configured pass-through recall or an EMC Celerra/VNX device
- Vault Cache clients

You must specify a location for the cache if any of these facilities is configured on the Enterprise Vault server. In the Administration Console, you configure the cache location on the **Cache** tab of the computer properties for the Enterprise Vault server.

Keep the following in mind when you configure the cache location:

- To ensure optimum performance, create the cache folder on fast, locally-attached storage.
- The Vault Service account must have read and write access to the cache folder.
- The major use for the cache is to provide temporary storage for Vault Cache clients. If only a few Enterprise Vault clients use Vault Cache, a location with a minimum of 20 GB of free space is probably sufficient. If many clients use Vault Cache, specify a location with far more free space.
- Anti-virus software can potentially change data in the cache, so it is important to exclude the cache location from virus checking.
- If you have clustered Enterprise Vault with Veritas Cluster Server or Windows Server Failover Clustering, the cache location should be a clustered resource.

## Storage requirements for shopping baskets

Space is required on the Shopping service computer for shopping baskets. These are used by Enterprise Vault for keeping details of items that users request Enterprise Vault to restore.

The amount of space required depends on the extent to which users restore items using the browser search shopping baskets. As a guide, for each shopping basket allow 4 KB for static data plus 1 KB for each item in a basket.

## Local storage requirements for temporary files

A small amount of local storage is needed for temporary files. For example, the local temporary area may be used by the Storage service when processing large files. Local storage is also required for MSMQ files and for Windows system files.

We recommend that you reassign the TEMP system variable to a drive other than the C: drive.

Slow local disks can seriously impact the performance of Enterprise Vault. You are recommended to allocate separate disks for MSMQ files. The disks need to be set up for maximum speed; for example using RAID 1+0 rather than RAID 5.





# Enterprise Vault required software and settings

This chapter includes the following topics:

- [About the Enterprise Vault prerequisite software and settings](#)
- [About the Enterprise Vault Deployment Scanner](#)
- [Basic software requirements for Enterprise Vault](#)
- [Best practice settings for Enterprise Vault servers](#)
- [Preinstallation tasks for Enterprise Vault server](#)

## About the Enterprise Vault prerequisite software and settings

Read this chapter to find out the following:

- Software prerequisites for core Enterprise Vault components.
- Tasks that you need to perform before installing Enterprise Vault.

The Enterprise Vault *Compatibility Charts* at <http://www.symantec.com/docs/TECH38537> contain details of the supported versions of prerequisite software.

There are additional prerequisites for other optional Enterprise Vault components and the different types of archiving. Ensure that you also review the additional prerequisite information for your planned installation, as outlined in later chapters.

There are also prerequisites if you are installing Enterprise Vault in a clustered environment.

## About the Enterprise Vault Deployment Scanner

Before installing Enterprise Vault, you can use Enterprise Vault Deployment Scanner to find out which prerequisites are missing. When you have finished preparing your servers for installation, it is advisable to run Deployment Scanner to check that all the prerequisites have been correctly installed. When you start the Enterprise Vault installer, you are given the option to run the Deployment Scanner before the installation begins.

Enterprise Vault Deployment Scanner is a separate wizard that is supplied on the Enterprise Vault media. When the tool runs, it creates a `Reports` folder in the folder in which it is run, and places a report file in the `Reports` folder.

You can find Deployment Scanner and accompanying documentation in the `Symantec Enterprise Vault\Deployment Scanner` folder on the Enterprise Vault media.

Windows Installer 3.1 is required on your Enterprise Vault servers in order to install Enterprise Vault server components.

## Basic software requirements for Enterprise Vault

This section describes the operating system and software requirements for the core Enterprise Vault services.

There may be additional requirements for the different types of archiving.

If required, the Enterprise Vault Administration Console can be installed on a separate computer.

See “[About the prerequisites for a standalone Enterprise Vault Administration Console](#)” on page 117.

## Required operating system components for Enterprise Vault

Enterprise Vault requires a version of Windows Server to be installed on each Enterprise Vault server. Not all versions of Windows Server are supported and for some versions you need a specific service pack or hotfix.

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

Install Windows with the following options and components:

- NTFS file system.
- Microsoft Message Queuing (MSMQ) services.  
See “[Installing MSMQ](#)” on page 43.

- Internet Information Services (IIS) 7.5 or later.  
See “[Internet Information Services \(IIS\)](#)” on page 44.
- .NET Framework 3.5 SP1 or SP2.  
See “[Microsoft .NET Framework](#)” on page 44.
- Internet Explorer 7.0 or later.
- MSXML.  
See “[MSXML](#)” on page 45.

## Roles-based administration in Enterprise Vault

Roles-based administration uses Microsoft Windows Authorization Manager. Creating and managing roles using the Administration Console requires the Authorization Manager MMC snap-in, which is available on the following:

- Windows Server 2003
- Windows Server 2008
- Windows Vista with the Administration Tools Pack for Windows Server 2003 and Windows Server 2008

You can download the Administration Tools Pack from the following location:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=c16ae515-c8f4-47ef-a1e4-a8dcbacff8e3&DisplayLang=en>

## Installing MSMQ

Enterprise Vault tasks use MSMQ to communicate with the Storage service. If you want to install Enterprise Vault services on more than one computer in the network, you must configure MSMQ on each computer.

Note the following when you install MSMQ:

- Active Directory Integration should not be enabled.
- We recommend that you place MSMQ storage folders on a drive other than the system drive.

### To install MSMQ on Windows Server 2008 R2

- 1 Start Server Manager.
- 2 Click **Features** in the left pane.
- 3 Click **Add Features** in the right pane.

- 4 When the Add Features wizard starts, click **Message Queuing**, and then click **Next**.

The only MSMQ feature that Enterprise Vault requires is **Message Queuing Server**.

- 5 Click **Install**.
- 6 Follow the remaining instructions in the wizard.

## Microsoft .NET Framework

You need to install Microsoft .NET Framework 3.5 SP1 or SP2 on Enterprise Vault servers.

For more details, see the Enterprise Vault *Compatibility Charts* (<http://www.symantec.com/docs/TECH38537>).

If necessary, you can download .NET Framework using the link in the `Links to related software` folder on the Enterprise Vault media.

## Internet Information Services (IIS)

You need IIS 7.5 or later on each Enterprise Vault server.

In IIS, you can configure the level of isolation for particular Web applications. For shopping baskets in the Enterprise Vault Web access application to be created correctly, the application needs to run under the predefined Local System account.

The configuration wizard will automatically set the correct isolation and account settings. You do not need to configure this.

The configuration wizard will create a new Application Pool, EnterpriseVaultAppPool, for the Web access application and assign the Local System account to that pool.

The Enterprise Vault Web Access application is configured in the default Web site in IIS. Although HTTP or HTTPS can be configured for Enterprise Vault client connections to the Web Access application, HTTPS is strongly recommended to ensure the security of transmitted data. To use HTTPS, you must first configure the default Web site in IIS for HTTPS, and install a valid SSL certificate.

## Enterprise Vault prerequisites for IIS on Windows Server 2008 R2

In Windows Server 2008 R2, if you use the Add Roles Wizard to install IIS, you get the default installation, which has a minimum set of role services. Enterprise Vault requires the following IIS-related roles services as a minimum:

Web Server	Common HTTP Features	<ul style="list-style-type: none"> <li>■ Static Content</li> <li>■ Default Document</li> <li>■ Directory Browsing</li> <li>■ HTTP Errors</li> <li>■ HTTP Redirection</li> </ul>
	Application Development	<ul style="list-style-type: none"> <li>■ ASP.NET</li> <li>■ .NET Extensibility</li> <li>■ ASP</li> <li>■ ISAPI Extensions</li> <li>■ ISAPI Filters</li> </ul>
	Health and Diagnostics	<ul style="list-style-type: none"> <li>■ HTTP Logging</li> <li>■ Logging Tools</li> <li>■ Request Monitor</li> <li>■ Tracing</li> </ul>
	Security	<ul style="list-style-type: none"> <li>■ Basic Authentication</li> <li>■ Windows Authentication</li> <li>■ URL Authorization</li> <li>■ Request Filtering</li> <li>■ IP and Domain Restrictions</li> </ul>
	Performance	<ul style="list-style-type: none"> <li>■ Static Content Compression (recommended for performance but not mandatory)</li> </ul>
Management Tools	IIS Management Console	
	IIS Management Scripts and Tools	
	Management Service	

---

**Note:** Windows Server Update Services role is not compatible with Enterprise Vault and should not be installed.

---

## MSXML

All Enterprise Vault server computers require MSXML. MSXML is installed automatically with Internet Explorer 7.0 and later.

If MSXML 6.0 is not present when you install the Enterprise Vault Services component, the Enterprise Vault installer installs it without asking for confirmation.

## Windows PowerShell

Windows PowerShell is a Windows command-line shell that is designed for system administrators. For help using Windows PowerShell, see Microsoft's PowerShell documentation.

PowerShell includes native binary commands called cmdlets. Some Enterprise Vault administration tasks are managed using additional cmdlets that are provided in a PowerShell snap-in. To use these Enterprise Vault cmdlets, you must install PowerShell.

---

**Note:** On Windows Server 2008 R2, you must add the Windows PowerShell feature in Server Manager.

---

To run PowerShell and load the Enterprise Vault snap-in, click **Start > Programs > Enterprise Vault > Enterprise Vault Management Shell**.

The Enterprise Vault PowerShell snap-in is 32-bit and you must run it with the 32-bit version of PowerShell even on 64-bit servers. The **Enterprise Vault Management Shell** shortcut runs the 32-bit version of PowerShell automatically. However, if you run Enterprise Vault cmdlets directly from external scripts such as backup scripts, you must ensure that you call the 32-bit version of PowerShell.

## SQL server software

Enterprise Vault 10.0 supports the following versions of Microsoft SQL Server:

- SQL Server 2005 x86 and x64 editions (Enterprise and Standard): SP3 and SP4
- SQL Server 2008 x64 edition only (Enterprise and Standard): SP2, SP3, R2, and R2 SP1

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

Both Windows Authentication mode and with Mixed Mode Authentication are supported.

The SQL installation must be case-insensitive, as case-sensitive SQL installations are not supported.

The Deployment Scanner performs checks to confirm that SQL Server meets all the requirements for Enterprise Vault.

## SQLXML

SQLXML 4.0 is required on computers on which the Enterprise Vault Services component is installed.

If SQLXML 4.0 is not present when you install the Enterprise Vault Services component, the Enterprise Vault installer automatically installs it without asking for confirmation.

## Microsoft Data Access Components (MDAC)

To enable access to the SQL databases, MDAC 2.6 or later must be installed on Enterprise Vault servers. A suitable version is installed automatically with Windows Server 2008 R2.

If necessary, you can install the software using the link supplied in the `Links to related software` folder on the Enterprise Vault media.

## Net.Tcp port sharing on Index Servers

Enterprise Vault Indexing uses the Windows Net.Tcp Port Sharing Service. If the Net.Tcp Port Sharing Service startup type is set to 'Disabled' the Indexing service automatically changes the startup type to 'Manual' and starts the service.

# Best practice settings for Enterprise Vault servers

The Enterprise Vault best practice settings help to ensure that an Enterprise Vault server performs as well as possible. Some of the settings prevent errors; others improve performance.

During the installation you have the option to set these best practice settings automatically. You do not need to modify these settings manually.

## Message queue cleanup interval: MessageCleanupInterval

Name	MessageCleanupInterval
Location	HKEY_LOCAL_MACHINE \Software \Microsoft \MSMQ \Parameters
Type	DWORD

Best practice setting	1800000 (milliseconds = 30 minutes)
Description	MessageCleanupInterval controls the frequency with which Microsoft Message Queuing (MSMQ) removes old message files. The MSMQ default of 6 hours is too infrequent for Enterprise Vault. A build up of old messag files can eventually bring archiving services to a halt.

## Message queue message storage limit: MachineQuota

Name	MachineQuota
Location	HKEY_LOCAL_MACHINE \Software \Microsoft \MSMQ \Parameters
Type	DWORD
Best practice setting	8388608 (KB = 8 GB)
Description	The default disk quota that is allowed for Microsoft Message Queuing (MSMQ) messages is not sufficient for the Enterprise Vault archiving tasks. If all the space is used, the Enterprise Vault archiving tasks cannot archive items.

## Disable opportunistic locking: OplocksDisabled

Name	OplocksDisabled
Location	HKEY_LOCAL_MACHINE \System \CurrentControlSet \Services \MRXSmb \Parameters
Type	DWORD
Best practice setting	(Hex) 01
Description	Opportunistic locking can result in issues with 32-bit indexes, including index corruption.



## Disable loopback check: DisableLoopbackCheck

Name	DisableLoopbackCheck
Location	HKEY_LOCAL_MACHINE \System \CurrentControlSet \Control \Lsa
Type	DWORD
Best practice setting	00000001 (Decimal)
Description	If DisableLoopbackCheck is not set you may get Access Denied errors in the Administration Console and in some configurations Enterprise Vault services may fail to start.

## Disable strict name checking: DisableStrictNameChecking

Name	DisableStrictNameChecking
Location	HKEY_LOCAL_MACHINE \System \CurrentControlSet \Services \LanmanServer \Parameters
Type	DWORD
Best practice setting	00000001 (Decimal)
Description	Enterprise VaultVault uses DNS Aliases. When a client computer uses an alias name to connect to a Windows server, the client may receive an error message. This problem can occur when the client tries to connect by using a CNAME alias that is created in the DNS zone. The server is not listening on the alias, and so does not accept connections to that name. By disabling strict name checking, this issue is resolved.  <a href="http://support.microsoft.com/default.aspx?scid=kb;en-us;281308#">http://support.microsoft.com/default.aspx?scid=kb;en-us;281308#</a>

## Maximum Outlook attachments and recipients: AttachmentMax and RecipientMax

Names	AttachmentMax RecipientMax
Location	HKEY_CURRENT_USER \Software \Microsoft \Office \version \Outlook \Options \Mail
Type	DWORD
Best practice settings	AttachmentMax: (Hex) FFFFFFFF RecipientMax: (Hex) FFFFFFFF

Description	<p>A Microsoft Outlook issue may cause errors when the Enterprise Vault Storage service computer runs Outlook 2003 SP3 or Outlook 2007 SP1.</p> <p>The issue occurs when an archived item has either of the following:</p> <ul style="list-style-type: none"><li>■ At least 2048 recipients in any of the TO, CC or BCC fields.</li><li>■ At least 2048 attachments.</li></ul> <p>The issue can cause errors whenever Enterprise Vault recalls an archived item. For example, when rebuilding an index.</p> <p>Microsoft has provided hotfixes for this issue, as follows:</p> <p>For Outlook 2003 SP3:</p> <ol style="list-style-type: none"><li>1 Install the following Microsoft hotfix on the Storage service computer: <a href="http://support.microsoft.com/kb/948073">http://support.microsoft.com/kb/948073</a></li><li>2 Set the RecipientMax and AttachmentMax registry entries as described in the following Microsoft Knowledge Base article: <a href="http://support.microsoft.com/kb/948074">http://support.microsoft.com/kb/948074</a>.</li></ol> <p>For Outlook 2007 SP1:</p> <ol style="list-style-type: none"><li>1 Install the following Microsoft hotfix on the Storage service computer: <a href="http://support.microsoft.com/kb/968858">http://support.microsoft.com/kb/968858</a>.</li><li>2 Set the RecipientMax and AttachmentMax registry entries as described in the following Microsoft Knowledge Base article: <a href="http://support.microsoft.com/kb/952295">http://support.microsoft.com/kb/952295</a>.</li></ol>
-------------	---

## TCP/IP maximum ports and TCP timed wait delay

Names	MaxUserPort TcpTimedWaitDelay
Location	HKEY_LOCAL_MACHINE \CurrentControlSet \Services \Tcpip \Parameters
Type	DWORD
Best practice settings	MaxUserPort: (Hex) fffe TcpTimedWaitDelay: (Hex) 78

Description

The default number of ephemeral ports for TCP/IP client connections can be insufficient for Enterprise Vault archiving. If there are too few ports some items are not archived from the server and you may see error messages in Enterprise Vault.

For more information see the following Microsoft article:  
<http://msdn.microsoft.com/en-us/library/aa560610.aspx>

## Preinstallation tasks for Enterprise Vault server

You need to perform the tasks described in this section, irrespective of the types of archiving that you plan to implement.

**Table 3-1** Preinstallation tasks for Enterprise Vault server

Step	Task	See this section for more details
Step 1	Create the Vault Service account.	See “ <a href="#">Creating the Vault Service account</a> ” on page 52.
Step 2	Create a SQL login account.	See “ <a href="#">Creating a SQL login account</a> ” on page 55.
Step 3	Assign the required permissions and roles in the SQL databases.	See “ <a href="#">About assigning permissions and roles in SQL databases</a> ” on page 57.
Step 4	Create Enterprise Vault DNS aliases.	See “ <a href="#">Creating Enterprise Vault DNS aliases</a> ” on page 58.
Step 5	Turn off or reconfigure Windows Firewall in Windows Server 2008.	See “ <a href="#">Turning off or reconfiguring Windows Firewall</a> ” on page 59.
Step 6	Secure the locations for Enterprise Vault index and vault store partition files.	See “ <a href="#">Securing data locations</a> ” on page 59.
Step 7	Read about User Account Control (UAC).	See “ <a href="#">About User Account Control (UAC)</a> ” on page 60.

### Creating the Vault Service account

The Vault Service account is used by Enterprise Vault processes to access the Windows server operating system. The account is shared by all the Enterprise Vault computers in the Enterprise Vault directory. If you are managing multiple Enterprise Vault sites, you can use the same Vault Service account for more than one Enterprise Vault site.

The Vault Service account must be a member of the local Administrators group on each Enterprise Vault computer. The account must be a domain-based Windows security account that belongs to the local Administrators group on all servers in the Enterprise Vault directory. The account password must not be blank. If you create more than one Enterprise Vault site in the same Enterprise Vault directory you must use the same Vault Service account for all sites.

We recommend that you do not make this account a Domain Administrator. It is better to assign required permissions explicitly. This section describes the basic permissions that you need to set for this account. Different types of archiving require additional permissions for the Vault Service account. For details of these, see the section on the type of archiving that you are implementing.

If possible, create the account so that it is in the same domain as the Enterprise Vault computers. If it is necessary for the Vault Service account and the Enterprise Vault computers to be in different domains, create the account so that it is in a domain that is trusted by the Enterprise Vault computers' domain.

Ensure that the Microsoft Message Queue security has been set up to grant the Administrators group access to the Enterprise Vault queues.

You are recommended to be logged in to the Vault Service account when you install Enterprise Vault. You must be logged in to the Vault Service account when you run the Enterprise Vault Configuration wizard.

Some pages of the Configuration wizard require you to specify the locations for SQL Server database files. You can specify the locations explicitly, by entering the path from the perspective of the SQL Server computer. The wizard also provides Browse buttons to let you browse the SQL Server computer to select the locations. However, folder browsing is only available if the Vault Service account has access to the administrative shares on the SQL Server computer. Note that some wizards in the Administration Console provide similar Browse buttons. To use those Browse buttons, the account that you use to run the Administration Console also requires access to the SQL Server's administrative shares.

Unless you assign the SQL system administrator (sysadmin) role to the Vault Service account, you must perform some additional steps before you run the Enterprise Vault Configuration wizard for the first time.

See [“About assigning permissions and roles in SQL databases”](#) on page 57.

During configuration, you are asked to provide the name and password of the Vault Service account. Enterprise Vault automatically grants the account the following advanced user rights:

- Log On As a Service
- Debug programs

- Replace a process-level token

Note that you may need to wait for Active Directory replication to complete. The account cannot be used until the replication is complete.

**To create the Vault Service account**

- 1 On the domain controller, click **Start > All Programs > Administrative Tools > Active Directory Users and Computers**.
- 2 In the left-hand pane of **Active Directory Users and Computers**, double-click the **Domain** container.
- 3 Double-click the **Users** container.
- 4 On the **Action** menu, click **New** and then **User**. The **New Object – User** screen is displayed.
- 5 Complete the **New Object – User** screen and click **Next**. The next screen asks for password details.
- 6 Enter a password and confirm it. You must set a password; the Vault Service account password cannot be blank.

---

**Note:** If you ever change the password of the Vault Service account, and you have installed an add-on such as Enterprise Vault Discovery Collector, then you may also need to change the user account credentials of the Vault Service account in the add-on. See the documentation that accompanies the add-on for more information.

---

- 7 Select the **Password never expires** check box.
- 8 Leave the remaining check boxes clear:
  - **User must change password at logon**
  - **User cannot change password**
  - **Account is disabled**
- 9 If you are using Exchange Server 2003, click **Next** to move to the mailbox server screen and then clear **Create an Exchange mailbox**.
- 10 Click **Next** to move to the summary screen.
- 11 Click **Finish** to create the new user.

**To add the new Vault Service account to the local Administrators group**

- 1 Log on to the Enterprise Vault computer as Administrator.
- 2 In Control Panel, open **Administrative Tools** and start the **Computer Management** console.
- 3 Expand **System Tools** and then **Local Users and Groups**.
- 4 Select **Groups**, and then double-click the **Administrators** group in the right-hand pane.
- 5 Use **Add** to add the Vault Service account to this group.
- 6 Click **OK**.
- 7 Repeat these steps on each computer which will have Enterprise Vault installed.

## Creating a SQL login account

The Vault Service account must have a SQL login account for the SQL Server, with the required permissions.

**To create a SQL login account in SQL 2005**

- 1 Start SQL Server Management Studio.
- 2 In the tree, select **Security>Logins**.
- 3 Right-click **Logins**, and select **New Login**.
- 4 Either type in the Vault Service account as *domain\username* or click **Search** and search for the account. In the search dialog box, ensure that the correct domain is entered in the **Locations** box.
- 5 Select **Windows authentication**.
- 6 In the tree, click **Server roles**.
- 7 Select the check box beside **dbcreator**.
- 8 Click **OK**.
- 9 In the toolbar, click **New Query**.
- 10 Enter the following script:

```
use Master
GRANT VIEW SERVER STATE TO "domain\vsa_account"
GO
```

where *domain\vsa\_account* is the domain and name of the Vault Service account.

- 11 Click **Execute**.
- 12 You can check that the Vault Service account has the dbcreator role as follows:
  - In the tree, select **Security>Server Roles**.
  - In the right-hand pane, double-click the **dbcreator** role.
  - The Vault Service account should be displayed in the membership list.
- 13 You can check that the Vault Service account has VIEW SERVER STATE permission as follows:
  - In the tree, right-click the top level SQL Server object and select **Properties**.
  - Select the **Permissions** page.
  - Under **Logins or roles**, select the Vault Service account and then click **Effective Permissions**. Check that **VIEW SERVER STATE** is included in the list of permissions.

#### To create a SQL login account in SQL 2008

- 1 Start SQL Server Management Studio.
- 2 In the tree, select **Security>Logins**.
- 3 Right-click **Logins**, and select **New Login**.
- 4 Either type in the Vault Service account as *domain\username* or click **Search** and search for the account. In the search dialog box, ensure that the correct domain is entered in the **Locations** box.
- 5 Select **Windows authentication**.
- 6 In the tree, click **Server roles**.
- 7 Select the check box beside **dbcreator**.
- 8 Click **OK**.
- 9 In the toolbar, click **New Query**.
- 10 Enter the following script:

```
use Master
GRANT VIEW SERVER STATE TO "domain\vsa_account"
GRANT ALTER ANY LOGIN TO "domain\vsa_account"
GO
```

where *domain\vsa\_account* is the domain and name of the Vault Service account.

- 11 Click **Execute**.



- 12 You can check that the Vault Service account has the **dbcreator** role as follows:
  - In the tree, select **Security > Server Roles**.
  - In the right-hand pane, double-click the **dbcreator** role.
  - The Vault Service account should be displayed in the membership list.
- 13 You can check that the Vault Service account has VIEW SERVER STATE and ALTER ANY LOGIN permissions as follows:
  - In the tree, right-click the top level SQL Server object and select **Properties**.
  - Select the **Permissions** page.
  - Under **Logins or roles**, select the Vault Service account and then click **Effective Permissions**. Check that **VIEW SERVER STATE** and **ALTER ANY LOGIN** are included in the list of permissions.

## About assigning permissions and roles in SQL databases

Unless you assign the SQL system administrator (sysadmin) role to the Vault Service account, you must perform the following additional steps before you run the Enterprise Vault Configuration wizard for the first time:

- Add the Vault Service account to the msdb system database.
- Grant the Vault Service account Select permissions on the msdb tables sysjobs, sysjobschedules, sysjobservers, and sysjobsteps.
- Assign the database role SQLAgentUserRole to the Vault Service account.

If you do not perform these steps, the following problems occur:

- Enterprise Vault fails to purge the history records from the Monitoring database, so these database records continue to grow.
- Upon completion, the Enterprise Vault Configuration wizard logs an error in the event log with the category 'Monitoring Configuration Utility' and Event ID 41123. The error description begins as follows and then lists the contents of a Purge Job SQL script file:

```
Monitoring Configuration Utility reported error: SQL Error at: --
```

If you run the Enterprise Vault Configuration wizard without performing these additional steps, see the following Enterprise Vault technical note:

<http://www.symantec.com/docs/TECH72170>.

## Assigning permissions and roles in SQL Server 2005/2008 databases

You must add the Vault Service account to the msdb system database, grant the required permissions to the account, and assign the database role SQLAgentUserRole to the account.

### To add the Vault Service account to the msdb system database

- 1 On the SQL Server computer, start SQL Server Management Studio.
- 2 Select the required SQL Server.
- 3 Browse to **Databases > System Databases > msdb > Security > Users**.
- 4 Right-click **Users** and then click **New User**.
- 5 In the **User name** box, enter a new user name.
- 6 In the **Login name** box, enter the domain and the user name of the Vault Service account, in the form *domain\user\_name*.
- 7 Click **OK**.

### To grant the permissions to the Vault Service account

- 1 Right-click the new user that you just created, and then click **Properties**.
- 2 Select the Securables page.
- 3 Add the following msdb tables to the list of securables, and then grant Select permission for them to the Vault Service account:
  - sysjobs
  - sysjobschedules
  - sysjobservers
  - sysjobsteps

### To assign the SQLAgentUserRole to the Vault Service account

- 1 Browse to **Databases > System Databases > msdb > Security > Roles > Database Roles**.
- 2 Right-click **SQLAgentUserRole**, and then click **Properties**.
- 3 On the General page, click **Add**, and then specify the Vault Service account that you have just created.

## Creating Enterprise Vault DNS aliases

It is good practice to create a DNS alias for each Enterprise Vault server computer. You are asked to enter the unqualified alias, for example "evserver1", when you

run the Enterprise Vault Configuration wizard. When you configure Enterprise Vault on the first computer in a site, Enterprise Vault automatically creates a vault site alias using the DNS alias entered for that computer. The vault site alias is used by the Enterprise Vault software to refer to the Enterprise Vault site.

The DNS alias must not contain special characters. As defined in RFC-1034, only the following characters are permitted: [a-z], [A-Z], [0-9], hyphen (-), and period (.). The last character must not be a hyphen or period.

Using an unqualified DNS alias allows future flexibility if you change the computer that is running the Enterprise Vault services.

## Turning off or reconfiguring Windows Firewall

In Windows Server 2008 R2, Windows Firewall is enabled by default. This prevents Distributed COM (DCOM) from working and therefore, because Enterprise Vault requires DCOM, you must either turn off Windows Firewall or configure it appropriately. Enterprise Vault requires dynamic TCP/IP ports for DCOM.

For guidelines on how to configure dynamic port ranges for TCP/IP, see the following article:

<http://support.microsoft.com/kb/929851>

## Securing data locations

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

If you use a network share for Enterprise Vault data, then you must ensure that the Vault Service account has full access to the network share on the remote server. A recommended way to manage access to Enterprise Vault data locations on network shares is to create a domain security group for this purpose. This approach avoids the need to propagate new permissions to all subfolders and files if you change the Vault Service account.

### To secure data locations

- 1 Check the ACL on network shares and folders that you plan to use for index locations and vault store partition folders.

Accounts other than the Vault Service account and local administrators should not have, or inherit, access to these locations.

- 2 If you want to manage access to network shares using a group, create a domain security group in Active Directory, for example EVDataAccess.

- 3** Add the Vault Service account to the new group.
- 4** Grant the new group full access to the network shares and folders that you plan to use for index locations and vault store partitions.

## About User Account Control (UAC)

Symantec recommend that you do not use mapped drives as storage locations. If you use mapped drives, Windows User Account Control (UAC) can prevent Enterprise Vault access to storage locations. We recommend that you use UNC paths instead of mapped drives.

# Additional requirements for Operations Manager

This chapter includes the following topics:

- [About additional requirements for Operations Manager](#)
- [Where and when to install Operations Manager](#)
- [Additional prerequisite software for Operations Manager](#)
- [Additional preinstallation tasks for Operations Manager](#)

## About additional requirements for Operations Manager

Enterprise Vault Operations Manager is a separately installable component. It is a Web application that makes remote monitoring of Enterprise Vault possible from any computer on which Internet Explorer is installed.

## Where and when to install Operations Manager

To use Operations Manager to monitor the Enterprise Vault servers in an Enterprise Vault site, Operations Manager must be installed on at least one Enterprise Vault server in that site.

Operations Manager requires Enterprise Vault Services on the same computer. You can install the Operations Manager component at the same time as installing the Enterprise Vault Services component, or at a later date. You must run the Enterprise Vault configuration wizard to configure the Enterprise Vault Services before you configure Operations Manager.

## Additional prerequisite software for Operations Manager

The computer on which you install Operations Manager requires the following software prerequisite in addition to the core Enterprise Vault prerequisite software and settings:

- Internet Information Services (IIS) must not be locked down.

See [“About the Enterprise Vault prerequisite software and settings”](#) on page 41.

## Additional preinstallation tasks for Operations Manager

In the Active Directory domain, create a Windows user account named, say, "MonitoringUser", for Operations Manager to use when accessing the Enterprise Vault databases. This monitoring user account does not require an Exchange mailbox, and it need not be a member of the Windows Administrators group.

When you create the monitoring user account, note the following:

- Select the **Password Never Expires** option.
- Leave the remaining check boxes clear (**User Must Change Password At Logon**, **User Cannot Change Password**, and **Account Is Disabled**).

# Additional requirements for Enterprise Vault Reporting

This chapter includes the following topics:

- [About the requirements for Enterprise Vault Reporting](#)
- [Where and when to install Enterprise Vault Reporting](#)
- [Prerequisites for Enterprise Vault Reporting](#)
- [Enterprise Vault reports that require monitoring or auditing to be enabled](#)
- [Preparing for the installation of Enterprise Vault Reporting](#)

## About the requirements for Enterprise Vault Reporting

The Enterprise Vault Reporting feature provides enterprise-level reporting for Enterprise Vault servers, using Microsoft SQL Server Reporting Services as the reporting mechanism. Administrators manage report content and view reports using the Reporting Services Report Manager Web application.

Enterprise Vault Reporting is required if you want to use FSA Reporting.

For more information on Enterprise Vault Reporting, see the *Reporting* guide.

## Where and when to install Enterprise Vault Reporting

Typically, the Enterprise Vault Reporting component is installed without any other Enterprise Vault components on a server that runs Microsoft SQL Server

Reporting Services. However, you can include the Reporting component as part of an Enterprise Vault server installation, if the required prerequisites are met.

You can install the Enterprise Vault Reporting component at any time. However, you must not run the Reporting Configuration utility until after you have run the Enterprise Vault Configuration wizard successfully on at least one computer in the site on which Enterprise Vault services are installed.

## Prerequisites for Enterprise Vault Reporting

You can install Enterprise Vault Reporting on a computer that has the following prerequisites:

- Microsoft .NET Framework 3.5 SP1.
- One of the following versions of Microsoft SQL Server Reporting Services:
  - Microsoft SQL Server 2005 Reporting Services, with SP2 or later.
  - Microsoft SQL Server 2008 Reporting Services.
  - Microsoft SQL Server 2008 R2 Reporting Services.
- For Microsoft SQL Server 2005 Reporting Services, ASP.NET 2.0 must be registered with IIS.
- A network connection to the computer or computers that host the Enterprise Vault databases.

If you intend to configure FSA Reporting, you must install the following software on the SQL Server computers that host FSA Reporting databases:

- Microsoft SQLXML 4.0
- Microsoft MSXML 6.0

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

## Enterprise Vault reports that require monitoring or auditing to be enabled

Some of Enterprise Vault Reporting's reports rely on Enterprise Vault monitoring or Enterprise Vault auditing for source data.

The following reports require Enterprise Vault monitoring to be enabled:

- Enterprise Vault Server 24-hour Health Status



- Enterprise Vault Server Seven Day Health Status
- Exchange Server Journal Mailbox Archiving Health
- Exchange Server Journal Mailbox Archiving Trends
- Domino Server Journal Mailbox Archiving Health
- Domino Server Journal Mailbox Archiving Trends

The following reports require Enterprise Vault auditing to be enabled:

- Archived Item Access
- Archived Item Access Trends

If you want to use these reports, you must ensure that Enterprise Vault monitoring or auditing are set up, as required.

---

**Note:** You can set up monitoring and auditing before or after you install and configure Enterprise Vault Reporting. The affected reports do not contain any information until the Monitoring database or the Auditing database contains the relevant data.

---

You can enable monitoring from the Enterprise Vault Configuration wizard.

You can also enable monitoring from the Enterprise Vault Operations Manager Web application, if you have installed the Operations Manager component.

See the section "Configuring the monitoring parameters" in the chapter "Monitoring with Enterprise Vault Operations Manager" in the *Administrator's Guide*.

To set up auditing, you must enable auditing and then configure auditing on the Enterprise Vault servers for which you want to gather information.

See "About auditing" in the *Administrator's Guide*.

## Preparing for the installation of Enterprise Vault Reporting

Before you install the Enterprise Vault Reporting component, you must perform the following steps.

### To prepare for the installation of Enterprise Vault Reporting

- 1 In the Active Directory domain, create a Windows user account named, say, "ReportingUser", for Enterprise Vault Reporting to use when accessing the

Enterprise Vault databases. This reporting user account does not require a mailbox, and it need not be a member of the Windows Administrators group.

When you create the reporting user account:

- Select the **Password Never Expires** option.
  - Leave the remaining check boxes clear (**User Must Change Password At Logon**, **User Cannot Change Password**, and **Account Is Disabled**).
- 2 Give the Vault Service account a "Content manager" role on the Microsoft SQL Server Reporting Services server. Refer to the Microsoft documentation for instructions on how to assign Microsoft SQL Server Reporting Services roles to user accounts.
  - 3 Add the Vault Service account to the Local administrators group on the Microsoft SQL Server Reporting Services server computer.

# Additional requirements for Exchange Server archiving

This chapter includes the following topics:

- [About Exchange Server archiving](#)
- [Preinstallation tasks for all Exchange Server versions](#)
- [Preinstallation tasks for Exchange Server 2010 and 2007](#)
- [Preinstallation tasks for Exchange Server 2003 and 2000](#)
- [Enterprise Vault client access with Exchange Server archiving](#)
- [Prerequisites for OWA](#)
- [Prerequisites for RPC over HTTP](#)
- [Prerequisites for Enterprise Vault Mobile Search](#)

## About Exchange Server archiving

You can archive items from mailboxes and public folders on the following target Exchange servers:

- Exchange 2000 with Service Pack 3
- Exchange Server 2003
- Exchange Server 2007
- Exchange Server 2010 SP1

## Preinstallation tasks for all Exchange Server versions

This section describes the preinstallation tasks that you must complete to support archiving from all versions of Exchange Server:

- [Installing Outlook on the Enterprise Vault server](#)
- [Creating the Enterprise Vault system mailbox](#)
- [Removing the restriction on NSPI connections to a Windows Server 2008 domain controller](#)
- [Creating a user profile and an Outlook profile on the Enterprise Vault server](#)

### Installing Outlook on the Enterprise Vault server

To archive from Exchange Server 2010, you must install the following on the Enterprise Vault server:

- Outlook 2007 SP2 with [hotfix KB2475891](#), or later service pack

To archive from Exchange Server versions prior to Exchange Server 2010, you must install one of the following on the Enterprise Vault server:

- Outlook 2003 SP2 or later service pack
- Outlook 2007 SP2 with [hotfix KB2475891](#), or later service pack

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

Outlook must be the default mail client on the Enterprise Vault server. On startup, the Enterprise Vault Admin service checks that Outlook is configured as the default mail client and, if it is not, configures it as such.

### Creating the Enterprise Vault system mailbox

The Enterprise Vault system mailbox is a mailbox that is used by the Exchange Mailbox, Exchange Journaling, and Exchange Public Folder tasks when connecting to the Exchange Server.

You must create an Enterprise Vault system mailbox on each Exchange Server that you want Enterprise Vault to archive.

---

**Note:** If you use database availability groups (DAGs) in your Exchange Server 2010 environment, you must create each Enterprise Vault system mailbox in a database that is replicated across the DAG.

---

Note also the following requirements:

- The Enterprise Vault tasks require exclusive use of this mailbox, so the mailbox must not be used for any other purpose.
- The mailbox must not be hidden from address lists.
- The account that the Enterprise Vault system mailbox is associated with must not be disabled.

Enterprise Vault prompts you for the name of this mailbox whenever you create an Exchange Server archiving task.

After you create the Enterprise Vault system mailbox, it may take some time for the mailbox to be available. The mailbox must be available before you add an Exchange Server archiving task.

If required, you can make the mailbox available sooner by manually forcing an update of Exchange Server 2003 or 2000.

This is not required on Exchange Server 2010 or 2007.

#### To force a manual update of the Exchange Server (2003 or 2000)

- 1 Click **Start > Programs > Microsoft Exchange > System Manager**.
- 2 In the left-hand pane, double-click the **Recipients** container.
- 3 Click **Recipient Update Services**.
- 4 In the right-hand pane, right-click the **Recipient Update Service** for the domain that contains the Exchange Server computer for which you are adding an archiving task.
- 5 Click **Update Now**.

The mailbox should be available within a minute or two.

## Removing the restriction on NSPI connections to a Windows Server 2008 domain controller

Windows Server 2008 domain controllers restrict NSPI connections to 50 concurrent connections per user. There is no restriction on concurrent NSPI connections in earlier versions of Windows Server operating systems. You must remove this restriction to prevent the failure of Enterprise Vault's Exchange archiving tasks.

### To remove the restriction on concurrent NSPI connections

- 1 On the Windows Server 2008 domain controller, create a new registry DWORD value called “NSPI max sessions per user” under the following registry key:

```
HKEY_LOCAL_MACHINE
\System
\CurrentControlSet
\Services
\NTDS
\Parameters
```

- 2 Set “NSPI max sessions per user” to 0xffffffff.

This sets “NSPI max sessions per user” to its maximum value, which removes the restriction on concurrent NSPI connections by each user. For more information about the restriction, see the following Microsoft Knowledge Base article:

<http://support.microsoft.com/kb/949469>

## Creating a user profile and an Outlook profile on the Enterprise Vault server

Before you install Enterprise Vault, you must:

- Log in to the server using the Vault Service account, to create a Windows user profile
- Create an Outlook profile
- Configure the Outlook profile to connect to an Exchange server mailbox

If you run Exchange archiving tasks under any other service accounts, you must also complete these actions for each service account.

## Preinstallation tasks for Exchange Server 2010 and 2007

This section describes the preinstallation tasks that you must complete to support archiving from Exchange Server 2010 and 2007:

- [Creating a mailbox for the Vault Service account](#)
- [Creating an Exchange Server 2007 Public Folder store](#)
- [Configuring the Exchange 2010 throttling policy on the Vault Service account](#)

- [Granting the Vault Service account Send As permission on the system mailboxes](#)
- [Assigning Exchange Server permissions to the Vault Service account](#)

## Creating a mailbox for the Vault Service account

During the preinstallation tasks for Exchange 2010, you must run a PowerShell script to configure the Exchange 2010 throttling policy on the Vault Service account.

See [“Configuring the Exchange 2010 throttling policy on the Vault Service account”](#) on page 72.

You must specify a mailbox when you run this PowerShell script, so you must first create a mailbox for the Vault Service account.

If you run Exchange 2010 in a cross-forest environment, the Vault Service account must have a linked mailbox in the resource forest.

For example, Exchange might reside in a resource forest called “Resources”, and user accounts in a user forest called “Users”. In this case, the Vault Service account is in the Users forest, and you must ensure it has a linked mailbox in the Resources forest.

## Creating an Exchange Server 2007 Public Folder store

If the target Exchange server is Exchange Server 2007, it must have a Public Folder store created to enable connections from versions of Outlook earlier than Outlook 2007. If you selected the option to support older clients when you installed Exchange Server 2007, a Public Folder store will have been created automatically.

If a Public Folder store does not exist on the target Exchange Server 2007, you must create one manually to enable Outlook 2003 on the Enterprise Vault server to connect to the Exchange server.

### To create a Public Folder store manually

- 1 On the Exchange Server, open the Exchange Management Shell.
- 2 Type the following command:

```
new-publicfolderdatabase -Name "Public Folders" -StorageGroup  
"First Storage Group" -EdbFilePath "C:\Program  
Files\Microsoft\ExchangeServer\Mailbox\First Storage Group\Public  
Folders.edb"
```

- 3 Type the following command to mount the Public Folder database:

```
mount-database -Identity "Public Folders"
```

- 4 You may need to create an Offline Address Book with Public Folder integration enabled if you are using clients prior to Outlook 2007.

## Configuring the Exchange 2010 throttling policy on the Vault Service account

Exchange Server 2010 has a default throttling policy which restricts user accounts to no more than 20 open connections to the server. This restriction on the Vault Service account would cause failures of the Enterprise Vault tasks that run under the account.

To prevent these failures, you must remove the restriction from the Vault Service account when you archive from Exchange Server 2010. Enterprise Vault includes a PowerShell script which creates a new policy and assigns it to the Vault Service account to remove the restriction.

The script must be run against an Exchange 2010 mailbox. If your Vault Service account already has a mailbox on Exchange Server 2007 or earlier, you must first move the mailbox to Exchange 2010.

### To configure the Exchange 2010 throttling policy on the Vault Service account

- 1 Log in to an Exchange Server using an account that is assigned the following management roles:

- Mail Recipients
- Recipient Policies

By default, members of the “Organization Management” role group are assigned these roles.

- 2 On the Enterprise Vault server, locate the script called `SetEVThrottlingPolicy.ps1` and copy it to the Exchange Server.

The Exchange 2010 PowerShell scripts are in the `PowerShellScripts` subfolder of the Enterprise Vault installation folder (for example `C:\Program Files (x86)\Enterprise Vault`).

- 3 On the Exchange Server, open the Exchange Management Shell.



- 4 If you moved an existing Vault Service account mailbox from Exchange 2007 or earlier, update the mailbox using the following command:

```
Set-Mailbox mailbox_name -ApplyMandatoryProperties
```

where:

*mailbox\_name* is the name of the Vault Service account's mailbox. If *mailbox\_name* contains spaces, enclose it in quotation marks.

- 5 Run `SetEVThrottlingPolicy.ps1`.

The syntax for this script is:

```
.\SetEVThrottlingPolicy.ps1 -user domain\user_name
```

where:

*domain* is the Active Directory domain that the Vault Service account belongs to.

*user\_name* is the Vault Service account. If *user\_name* contains spaces, enclose it in quotation marks.

---

**Note:** In cross-forest environment, you must specify the resource domain so that `SetEVThrottlingPolicy.ps1` runs against the Vault Service account's linked mailbox in the resource forest.

See [“Creating a mailbox for the Vault Service account”](#) on page 71.

---

- 6 If you want to force these changes to take effect immediately, restart the Microsoft Exchange RPC Client Access service on each Exchange CAS server.

If you do not restart the service, the changes can take up to two hours to take effect by default.

You can also run `SetEVThrottlingPolicy.ps1` remotely from the Exchange Server under PowerShell 2.0. When you run the script remotely, use the `-server` switch to specify the name of the Exchange 2010 mailbox server.

In this case, the full syntax for this script is:

```
.\SetEVThrottlingPolicy.ps1 -user domain\user_name -server  
exchange_mailbox_server
```

## Granting the Vault Service account Send As permission on the system mailboxes

The Vault Service account requires Send As permission on the Enterprise Vault system mailbox on each Exchange mailbox server. You can set this permission manually on each account, or use the following procedure.

### To grant the Vault Service account Send As permission on a system mailbox

- 1 Log in to the Exchange Server using an account that is assigned the following management role:

- Active Directory Permissions

By default, members of the “Organization Management” role group are assigned this role.

- 2 Open the Exchange Management Shell.
- 3 Run the following command:

```
Add-ADPermission -Identity mailbox_name -User domain\user_name  
-AccessRights ExtendedRight -ExtendedRights "send as"
```

where:

*mailbox\_name* is the Enterprise Vault system mailbox. If *mailbox\_name* contains spaces, enclose it in quotation marks.

*domain* is the Active Directory domain that the Vault Service account belongs to.

*user\_name* is the Vault Service account. If *user\_name* contains spaces, enclose it in quotation marks.

## Assigning Exchange Server permissions to the Vault Service account

For Exchange Server 2010 and Exchange Server 2007, Enterprise Vault includes a PowerShell script which assigns the necessary permissions to the Vault Service account.

Although you must run this script on Exchange Server 2010 or Exchange Server 2007, the script assigns permissions required by all the Exchange versions in your environment, including Exchange Server 2003 and Exchange 2000. However, if your environment contains Exchange servers no later than Exchange Server 2003, you must assign permissions manually.

See [“Assigning permissions on Microsoft Exchange Server 2003 and 2000”](#) on page 77.

See “[Microsoft Exchange permissions assigned to the Vault Service account](#)” on page 75.

### To assign Exchange Server permissions to the Vault Service account

- 1 Log in to the Exchange Server using an account that is assigned the following management roles:

- Active Directory Permissions
- Exchange Servers
- Organization Configuration

By default, members of the “Organization Management” role group are assigned these roles.

- 2 On the Enterprise Vault server, locate the script called `SetEVExchangePermissions.ps1` and copy it to the Exchange Server.

The Exchange 2010 PowerShell scripts are in the `PowerShellScripts` subfolder of the Enterprise Vault installation folder (for example `C:\Program Files (x86)\Enterprise Vault`).

- 3 On the Exchange Server, open the Exchange Management Shell.
- 4 Run `SetEVExchangePermissions.ps1`.

The syntax for this script is:

```
.\SetEVExchangePermissions.ps1 -user domain\user_name
```

where:

*domain* is the Active Directory domain that the Vault Service account belongs to.

*user\_name* is the Vault Service account. If *user\_name* contains spaces, enclose it in quotation marks.

- 5 If you want to force these changes to take effect immediately, restart the Microsoft Exchange Information Store service on each Exchange mailbox server.

### Microsoft Exchange permissions assigned to the Vault Service account

[Table 6-1](#) lists the permissions that `SetEVExchangePermissions.ps1` assigns to the Vault Service account.

**Table 6-1** Permissions assigned to the Vault Service account

Path	Object	Permissions
CN=Configuration, CN=Services, CN=Microsoft Exchange, CN= <i>Organization</i> , CN=Administrative Groups, CN= <i>AdminGroup</i>	CN=Databases and descendant objects.  <i>SetEVExchangePermissions.ps1</i> assigns these permissions if Exchange Server 2010 exists in your environment.	Read  Administer information store  Create named properties in the information store  Open mail send queue  Receive as  Send as  View information store status
	CN=Servers and descendant objects.  <i>SetEVExchangePermissions.ps1</i> assigns these permissions if Exchange Server 2007 or earlier exists in your environment.	Read  Administer information store  Create named properties in the information store  Open mail send queue  Receive as  Send as  View information store status
CN=Configuration, CN=Services, CN=Microsoft Exchange	CN= <i>Organization</i> .	Read
CN=Configuration, CN=Services, CN=Microsoft Exchange, CN= <i>Organization</i>	CN=ELC Folders Container and descendant objects.	Read
	CN=Global Settings and descendant objects.	Read
	CN=Transport Settings.	Read
CN=Configuration, CN=Services, CN=Microsoft Exchange, CN= <i>Organization</i> , CN=Transport Settings	CN=Rules.	Read

**Table 6-1** Permissions assigned to the Vault Service account (*continued*)

Path	Object	Permissions
CN=Configuration, CN=Services, CN=Microsoft Exchange, CN= <i>Organization</i> , CN=Transport Settings, CN=Rules	CN=Journaling and descendant objects.	Read
	CN=JournalingVersioned and descendant objects.  SetEVExchangePermissions.ps1 assigns these permissions if the schema has been updated. This happens if Exchange Server 2010 exists in your environment.	Read

## Preinstallation tasks for Exchange Server 2003 and 2000

This section describes the preinstallation tasks that you must complete to support archiving Exchange Server 2003 and 2000:

- [Assigning permissions on Microsoft Exchange Server 2003 and 2000](#)

### Assigning permissions on Microsoft Exchange Server 2003 and 2000

The Vault Service account needs to be able to access mailboxes on the Exchange servers that Enterprise Vault is to archive. You need to assign permissions explicitly on each Exchange server. If you later add another Exchange server, you need to repeat the procedure on the new server to enable mailbox access for the Vault Service account.

---

**Note:** If you have Exchange Server 2010 or 2007 in your environment, you should already have assigned permissions using the PowerShell script called `SetEVExchangePermissions.ps1`. In this case you do not need to complete the procedures in this section.

See [“Assigning Exchange Server permissions to the Vault Service account”](#) on page 74.

---

#### On Microsoft Exchange Server 2003 and Microsoft Exchange 2000 Server

- 1 Click **Start > Programs > Microsoft Exchange > System Manager**.
- 2 Expand the **Servers** container.
- 3 Right-click your Exchange Server and, on the shortcut menu, click **Properties**.

- 4 Click the **Security** tab.
- 5 Click **Add**.
- 6 Double-click the Vault Service account to add it to the list.
- 7 Click **OK** to go back to the **Security** tab. The Vault Service account has been added to the **Name** list.
- 8 In the **Name** list, click the Vault Service account.
- 9 In the **Permissions** list, make sure that all check boxes in the **Allow** column are selected. Select any check boxes that are not already selected.
- 10 Click **OK**.

### Assigning the permissions at Organization or Administrative Group level

If required, you can add the permissions at the Organization or Administrative Group level in the Exchange hierarchy. This will enable the permissions to be propagated automatically to any new Exchange Servers added below the level at which the permissions are assigned.

**To assign the permissions at Organization or Administrative Group level (Exchange Server 2000 or 2003)**

- 1 Enable the display of the **Security** page by configuring the **ShowSecurityPage** registry setting (see Microsoft Knowledge Base article [883381](#)).
- 2 In the left-hand pane of **Microsoft Exchange, System Manager**, right-click your Exchange Organization or the administrative group that you want, and select **Properties**.
- 3 Select the **Security** tab and set the required permissions for the Vault Service account, as described in the steps for individual Exchange Servers.

## Enterprise Vault client access with Exchange Server archiving

Users can access and manage items in archives using the following client access methods:

- Enterprise Vault Outlook Add-In
- Enterprise Vault Client for Mac OS X
- OWA clients, which require Enterprise Vault Exchange Server extensions for OWA

- Enterprise Vault customized shortcuts
- Enterprise Vault search or Archive Explorer in a browser session

## Prerequisites for the Enterprise Vault Outlook Add-In

The Enterprise Vault Outlook Add-In provides Enterprise Vault user functionality to Outlook users. From within Outlook, users can archive items manually, and view, copy and delete archived items. Outlook users can also start Archive Explorer and Enterprise Vault Search, within Outlook, to access and manage items stored in archives.

Before users can send items to an archive from within their Outlook client, the Outlook Add-In must be installed on their computers. Install the Outlook Add-In on users' computers after you have configured the Enterprise Vault server.

Users' computers must have the following:

- One of the following versions of Windows:
  - Windows XP with Service Pack 3. (Currently, only 32-bit versions of Windows XP are supported.)
  - Windows Vista.
  - Windows 7.
- Internet Explorer 7.0 or later, with JavaScripting enabled. This must be installed, even if it is not used.
- TCP/IP protocol.
- One of the following mail clients:
  - Outlook 2003 SP2 or later
  - Outlook 2007 or later
  - Outlook 2010 or later

Install Internet Explorer before you install the mail client.

- If you plan to enable Vault Cache, Background Intelligent Transfer Service (BITS) 2.0 or later must be installed and enabled on users' computers. This service is used by Microsoft Windows Update and is included in Windows XP SP3, Windows Vista, and Windows 7. If necessary, it can be downloaded from the Microsoft website.
- If you plan to enable Vault Cache, and you have disabled the expansion of PST files on users' computers by setting the registry entry, PstDisableGrow, then you need to request and install the appropriate Outlook hotfix from Microsoft.

Note that the hotfix may already have been installed as part of a Microsoft Update.

For Outlook 2003: <http://support.microsoft.com/?kbid=953671>

For Outlook 2007: <http://support.microsoft.com/?kbid=953925>. This hotfix is not required if Outlook 2007 SP2 or later is installed.

You will also need to configure the registry setting PSTDisableGrowAllowAuthenticcodeOverrides on users' computers, as described in the *Setting up Exchange Server Archiving* manual.

- If you plan to enable the Windows Search plug-in, Windows Search 4.x or later must be available on the desktop computers.  
The Windows Search plug-in also requires the following to be installed on the desktop computers:
  - Outlook 2003, Outlook 2007, or Outlook 2010
  - One of the following:
    - Version 9.0/9.0.n/10.0 of the Enterprise Vault Outlook Add-In or HTTP-Only Outlook Add-In
    - Version 10.0.1 or later of the Enterprise Vault Outlook Add-In

If necessary, you can download Windows Search from the following address:  
<http://www.microsoft.com/windows/desktopsearch/downloads/default.mspx>

## Prerequisites for Enterprise Vault Client for Mac OS X

The Enterprise Vault Client for Mac OS X provides Enterprise Vault functionality to users of Microsoft Entourage and Outlook 2011 for Mac. These users can archive, restore, and delete items, and conduct searches of the items in their archives.

You can install the Enterprise Vault Client for Mac OS X on any computer that meets the following requirements:

- Mac OS X version 10.5 (Leopard), 10.6 (Snow Leopard), or 10.7 (Lion)
- One of the following email clients:
  - Entourage 2008 version 12.1.5 or later
  - Entourage 2008 Web Services Edition
  - Outlook 2011 for Mac version 14.0.0 or later
- Safari version 3.2.1 or later



## OWA clients

Enterprise Vault functionality can be made available in OWA 2003 and later clients by installing Enterprise Vault OWA Extensions on the Exchange Server. Enterprise Vault functionality available with OWA 2000 clients is limited to viewing archived items.

With OWA 2003 and later clients, you can control the functionality available in the premium and basic clients using OWA settings on the Advanced page of the Exchange Desktop Policy properties.

On user desktops, Internet Explorer 7.0 or later is required to support the full functionality available with OWA 2003 and later clients.

You do not need to install the Enterprise Vault Outlook Add-In on user desktop computers.

## Customized shortcuts

If you do not want to install the Enterprise Vault clients on desktop computers, you can configure Enterprise Vault customized shortcuts in the Exchange Mailbox Policy. Using customized shortcuts, users can view an HTML version of archived items, and start Archive Explorer and archive search in a browser session to access and manage the items that are stored in archives.

On Windows computers, Internet Explorer 7.0 or later with JavaScripting enabled must be installed on each user's computer.

On Mac computers, the Safari browser and Entourage and Outlook 2011 for Mac email clients are supported. For details of supported versions, see the Enterprise Vault *Compatibility Charts* at <http://www.symantec.com/docs/TECH38537>.

## Archive search and Archive Explorer in standalone browser

Users can access Enterprise Vault archives using Archive Explorer or archive search in a standalone browser session. The Enterprise Vault Add-In is not required on desktop computers, but you will need to inform users of the URLs to enter in their browser for Archive Explorer and archive search. These will typically take the following format:

- Archive Explorer URL:  
`http://web_server_name/EnterpriseVault/ArchiveExplorerUI.asp`
- Integrated search URL:  
`http://web_server_name/EnterpriseVault/searcho2k.asp`
- Browser search URL:  
`http://web_server_name/EnterpriseVault/search.asp`

where *web\_server\_name* is the name of your Web server.

To use Enterprise Vault browser search or Archive Explorer in a browser session, Internet Explorer 7.0 or later, with JavaScripting enabled, must be installed on each user's desktop computer.

---

**Note:** With Exchange Server Journal archiving, shortcuts are not created in the mailbox. The associated archives can be accessed using archive search, but not Archive Explorer.

---

## Prerequisites for OWA

You can configure OWA access to Enterprise Vault after you have set up your Enterprise Vault server for Exchange Server archiving. The instructions for configuring OWA access to Enterprise Vault assume that you have already configured OWA on Exchange Servers.

To provide OWA 2000 or OWA 2003 access, install Enterprise Vault OWA 2000 or OWA 2003 Extensions on front-end and back-end Exchange Servers. To provide OWA 2007 or 2010 access, install the Enterprise Vault OWA 2007 or 2010 Extensions on the Exchange CAS computers.

All the Exchange Servers on which you install the Enterprise Vault OWA Extensions should be at the same Exchange Server service pack and hotfix level.

When you install the Enterprise Vault OWA Extensions on your Exchange Servers, ensure that you install the same Enterprise Vault release version of the extensions on all the Exchange Servers.

The following are required for accessing Enterprise Vault from OWA clients:

- Enterprise Vault OWA 2010 Extensions require Exchange Server 2010 SP1 or later.
- The following Role Services must be installed for the Web Server (IIS):
  - IIS Management Scripts and Tools
  - IP and Domain Restrictions

In addition, the option IPv4 Address and Domain Restrictions in Feature Delegation must be set to Read/Write. To find this option, open Internet Information Services (IIS) Manager and click the server object in the navigation pane. Open Feature Delegation and ensure that IPv4 Address and Domain Restrictions is included in the listed options.

- When using the Enterprise Vault OWA 2007 Extensions, if the mailboxes being accessed are located on a server which is separate from the CAS computer,

and users are authenticated to OWA using Integrated Windows Authentication (IWA), then it is necessary to configure constrained delegation. Configuring constrained delegation requires a domain functional level of Windows Server 2003 or later.

For more information about domain functional levels, see "Domain and forest functionality" in the Help and Support Center for Windows Server 2003.

Instructions on how to set up constrained delegation are given in the manual *Setting up Exchange Server Archiving*.

- The following are required on each Windows 2003 Server on which you will install the Enterprise Vault OWA 2003 Extensions:
  - Windows Server 2003 Service Pack 2 or later
  - Exchange Server 2003 Service Pack 1 or later
- As Enterprise Vault OWA 2003 Extensions modify OWA control files on Exchange Server 2003, the version of these files must be one that is supported by Enterprise Vault.

See *Exchange Server OWA control file versions* in the [Enterprise Vault Compatibility Charts](#).

Before you install an Exchange Server hotfix that changes the OWA control file version, check in the Compatibility Charts that the version is supported by Enterprise Vault.
- Enterprise Vault OWA 2000 Extensions require at minimum Exchange 2000 SP3.
- If the back-end Exchange 2000 server computer is running Windows 2000, Windows 2000 Service Pack 4 or later is required.
- MSXML is required on Exchange Servers (with the exception of front-end Exchange 2000 servers). MSXML is installed automatically with Internet Explorer 7.0 and later.
- On user desktops, Internet Explorer 7.0 or later is required to support the full functionality available with OWA 2003 and later clients.

The Enterprise Vault buttons are not available in OWA 2000 clients, which means that you can only view archived items. To be able to archive, restore, and delete archived items from your OWA client and have integrated access to Archive Explorer and Search features, you need to use OWA on Exchange Server 2003 or later.

## Prerequisites for RPC over HTTP

This section describes the preinstallation tasks that you must complete to support RPC over HTTP access for Outlook users:

- [Prerequisites for RPC over HTTP with Exchange Server 2003](#)
- [Prerequisites for Outlook Anywhere access to Enterprise Vault](#)

### Prerequisites for RPC over HTTP with Exchange Server 2003

Exchange Server 2003 with the RPC over HTTP Windows component is required on RPC proxy Exchange Servers.

Client computers require Outlook 2003 SP2 or later.

The Enterprise Vault Outlook Add-In is required on desktop computers.

You can configure RPC over HTTP access to Enterprise Vault after you have set up your Enterprise Vault server for Exchange Server archiving and distributed the Outlook Add-In to desktop computers.

You then install and configure Enterprise Vault OWA Extensions on RPC proxy servers and target Exchange Servers. For this reason, the additional prerequisites listed for Enterprise Vault OWA 2003 Extensions are also needed if you are configuring RPC over HTTP access with Exchange Server 2003.

See [“Prerequisites for OWA”](#) on page 82.

See the *Setting up Exchange Server Archiving* manual for instructions on setting up RPC over HTTP access to Enterprise Vault.

The instructions given assume that you have already configured RPC over HTTP on RPC proxy servers and target Exchange Servers. Users' computers must also be set up to use RPC over HTTP access to the Exchange Server.

### Prerequisites for Outlook Anywhere access to Enterprise Vault

In Exchange Server 2007 and 2010 environments, Outlook in RPC over HTTP mode is called Outlook Anywhere. To support Enterprise Vault requests from Outlook Anywhere clients, no Enterprise Vault extensions are required on the Exchange CAS computer. However, you need to configure RPC over HTTP access on the Enterprise Vault server.

Outlook on users' computers needs to be configured to use RPC over HTTP, and the Enterprise Vault Outlook Add-In needs to be installed on users' computers. See the *Setting up Exchange Server Archiving* manual for instructions.

# Prerequisites for Enterprise Vault Mobile Search

This section includes the following topics:

- [Prerequisites for Enterprise Vault Mobile Search in a production environment](#)
- [Hardware requirements for the Enterprise Vault Mobile Search server](#)
- [Windows Server 2003 requirements for Enterprise Vault Mobile Search](#)
- [Windows Server 2008 requirements for Enterprise Vault Mobile Search](#)
- [Enterprise Vault API Runtime required for Enterprise Vault Mobile Search](#)

## About configuring Enterprise Vault Mobile Search

For information about configuring Mobile Search access to Enterprise Vault, see *Setting up Exchange Server Archiving*. The information in *Setting up Exchange Server Archiving* includes the following:

- Preinstallation tasks for Mobile Search
- Step-by-step installation instructions
- Detailed configuration information

## Prerequisites for Enterprise Vault Mobile Search in a production environment

In a production environment, we recommend that you install Mobile Search on a computer that does not have any of the following applications installed:

- Enterprise Vault server
- Microsoft SQL Server
- Microsoft Exchange Server (the target system for Enterprise Vault archiving)
- BlackBerry Enterprise Server

Mobile Search can be installed on the same computer as these applications for pilot or demonstration purposes.

## Hardware requirements for the Enterprise Vault Mobile Search server

[Table 6-2](#) lists recommended minimum requirements for the Mobile Search server in a production environment.

Table 6-2 Mobile Search server hardware

Item	Recommended minimum
Number of CPUs	Two
Processor	Intel Xeon 1.86 GHz
RAM	2 GB
Free disk space on installation volume	100 MB

The minimum RAM requirement is particularly important if users perform large, simultaneous archive searches.

## Windows Server 2003 requirements for Enterprise Vault Mobile Search

You can install Mobile Search on Microsoft Windows Server 2003 SP2.

The computer must be part of a Windows domain.

Install Windows Server 2003 SP2 with the following options and components:

- NTFS file system
- Microsoft .NET Framework 2.0
- Microsoft Internet Information Services (IIS)

Additionally, you must ensure that ASP.NET is allowed in IIS Web Service Extensions.

If you are installing Enterprise Vault on a 64-bit version of Windows Server 2003, you need to switch to the 32-bit version of ASP.NET 2.0. To do this, see the following article in the Microsoft Knowledge Base:

<http://support.microsoft.com/?kbid=894435>

## Windows Server 2008 requirements for Enterprise Vault Mobile Search

You can install Mobile Search on Microsoft Windows Server 2008.

The computer must be part of a Windows domain.

Install Windows Server 2008 with the following options and components:

- NTFS file system
- Microsoft .NET Framework 2.0
- Microsoft Internet Information Services (IIS)

Additionally, you must ensure that ASP.NET is allowed in IIS Web Service Extensions.

For IIS 7.0 on a Mobile Search Web server, we recommend that you add certain role service components to the Web server role.

[Table 6-3](#) lists the role service components that we recommend.

**Table 6-3** Recommended role service components for the Web server role

Role service	Recommended components
Common HTTP features	Static Content Default Document Directory Browsing HTTP Errors
Application Development	ASP.NET .NET Extensibility ISAPI Extension ISAPI Filters
Health and Diagnostics	HTTP Logging Request Monitor
Security	Basic Authentication Request Filtering
Performance	Static Content Compression
Management Tools	IIS Management Console

## Enterprise Vault API Runtime required for Enterprise Vault Mobile Search

The API Runtime is located on the Enterprise Vault release media in the following folder:

`\Symantec Enterprise Vault\API Runtime`

Note the following:

- We recommend that you run Mobile Search on a server that is separate from the Enterprise Vault server. You must install the Enterprise Vault API Runtime before installing Mobile Search.

- You must ensure that the API Runtime version and the Enterprise Vault server version are the same. We recommend the use of version 10.0 or later of the API Runtime and Enterprise Vault server with Mobile Search. However, version 9.0/9.0.*n* of the API Runtime and Enterprise Vault server are also supported with Mobile Search.



# Additional requirements for Domino Server archiving

This chapter includes the following topics:

- [Domino Server archiving prerequisites for all Enterprise Vault servers](#)
- [Prerequisites for Domino mailbox archiving](#)
- [Prerequisites for Domino journaling archiving](#)

## Domino Server archiving prerequisites for all Enterprise Vault servers

For all Domino archiving, you must install the Lotus Notes client on the Enterprise Vault Domino Gateway and on every Enterprise Vault server, as follows:

- Install Lotus Notes 8.5.2 or later client software. For details of the latest supported software versions, see the Enterprise Vault *Compatibility Charts* (<http://www.symantec.com/docs/TECH38537>).
- If you installed the Notes client with the Multi-User Install option, log on as the Windows account that the Enterprise Vault services will use. This is normally the Vault Service account.
- Start the Notes client and complete its configuration wizard. Use the ID file that you want to use for Domino archiving.  
See [“About the user ID for Domino mailbox archiving”](#) on page 94.

## Prerequisites for Domino mailbox archiving

For Domino mailbox archiving, you need to configure the following:

- One or more Enterprise Vault Domino Gateways.  
The Enterprise Vault Domino Gateway is a Domino server that is customized by Enterprise Vault configuration. The Enterprise Vault Domino Gateway provides the interface between Lotus Notes clients and Enterprise Vault. All the major actions on archived data (opening, restoring, deleting and searching) are handled by the Enterprise Vault Domino Gateway.
- One or more Enterprise Vault servers. If necessary, you can use the Enterprise Vault Domino Gateway to run Enterprise Vault services and tasks.
- Target Domino mail servers.
- Enterprise Vault client extensions for Lotus Notes and Domino Web Access.

If you are going to install Enterprise Vault Administration Console on a remote computer, then you must also install Lotus Notes 8.5.2 or later on that computer to manage Domino user archives.

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

## Prerequisite software for Enterprise Vault Domino Gateway

The Enterprise Vault Domino Gateway must be a Windows server that is running the following minimum software versions:

- Enterprise Vault 10.0
- Domino Server 8.5.2 (32-bit version) Fix Pack 2 and Lotus Notes Client 8.5.2

It is best practice for the standard Domino mail templates to be present on the Enterprise Vault Domino Gateway. These templates are required by the Enterprise Vault `EVinstall.nsf` installer.

For details of all supported software versions and the required hotfixes, see the Enterprise Vault *Compatibility Charts* (<http://www.symantec.com/docs/TECH38537>).

You need at least a Domino Messaging server license for each Enterprise Vault Domino Gateway.

## Prerequisite software for target Domino mail servers

Target Domino mail servers that you want to archive must be running Domino Server 7.0.0 or later.

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

## Prerequisites for Enterprise Vault extensions for Lotus Notes clients

Client access to archived items from Lotus Notes or Domino Web Access (DWA) clients is provided through changes to the Lotus Notes and DWA mail templates; no application needs to be installed on user workstations. You install the updated mail templates on target Domino mail servers and DWA servers throughout an organization.

Users who require Enterprise Vault functionality available in their Lotus Notes client must have Lotus Notes Client 7.0.0 or later installed on their workstations.

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

To enable the use of Enterprise Vault integrated search from within Lotus Notes or DWA mail clients, users must have Internet Explorer 7.0 or later installed on their workstations, and it must be set as the default Web browser in Lotus Notes. In addition, you need to configure Single Sign-On for the users on the Enterprise Vault Domino Gateway.

See “[Configuring Single Sign-On on the Enterprise Vault Domino Gateway](#)” on page 93.

## Preinstallation tasks for Domino mailbox archiving

You should have already created the following:

- The Vault Service account
- A SQL login account for the Vault Service account
- DNS aliases for the Enterprise Vault server and site

See “[Preinstallation tasks for Enterprise Vault server](#)” on page 52.

You now need to perform the following tasks to set up Domino server and Lotus Notes on the Enterprise Vault Domino Gateway computer. The following steps must be completed before you install Enterprise Vault on the computer. This ensures that the Enterprise Vault installation program detects that this is a Domino server and will install the extension manager files and other database files.

- Use IBM Domino Administrator client to do the following:
  - Register the Domino server that will run on the Enterprise Vault Domino Gateway computer, and set up the configuration for this server in the Domino Directory.  
See “[Register the Enterprise Vault Domino Gateway](#)” on page 92.
  - Identify or create a user ID for the Domino mailbox archiving.  
See “[About the user ID for Domino mailbox archiving](#)” on page 94.

- Configure the server documents for the Domino mail servers from which Enterprise Vault will archive.  
See [“Configuring the server document for each target Domino mail server”](#) on page 96.
- On the computer that will host the Enterprise Vault Domino Gateway, do the following:
  - Install Domino server binaries and configure the Domino server.  
See [“Install and configure Enterprise Vault Domino Gateway”](#) on page 97.
  - Install Lotus Notes client binaries and hotfix, and configure the client. Use the ID file that you want to use for Domino archiving.  
See [“Domino Server archiving prerequisites for all Enterprise Vault servers”](#) on page 89.

After you have completed these tasks, you can install Enterprise Vault and perform the initial configuration.

See [“Installing Enterprise Vault”](#) on page 127.

You can then complete the configuration of Domino mailbox archiving. See the *Setting up Domino Server Archiving* manual for instructions.

## Register the Enterprise Vault Domino Gateway

There must be at least one Enterprise Vault Domino Gateway for each Domino domain to be archived. In a production environment, the Enterprise Vault Domino Gateway should not be used as a general mail server.

The Enterprise Vault Domino Gateway can be a partitioned Domino server.

Use the IBM Domino Administrator Client to register the Enterprise Vault Domino Gateway, and configure the server document, as described in this section. If you plan to have several Enterprise Vault Domino Gateway computers in your Domino domain, repeat the following tasks for each Enterprise Vault Domino Gateway:

- Configure the Internet port for HTTP on the Enterprise Vault Domino Gateway.
- Configure server security.
- Set up Single Sign-On on the Enterprise Vault Domino Gateway.

### Configuring the Internet port for HTTP on the Enterprise Vault Domino Gateway

Enterprise Vault requires the HTTP task to be configured on the Enterprise Vault Domino Gateway. As IIS and the Domino server HTTP task both use port 80, change the port used by the Domino server.

### To configure the Internet port for HTTP on the Enterprise Vault Domino Gateway

- 1 In the IBM Domino Administrator Client, open the server document for the Enterprise Vault Domino Gateway.
- 2 Select the **Ports** tab and then the **Internet Ports** tab in the subdocument.
- 3 On the **Web** tab, set the TCP/IP port number to something other than 80; for example, 8080.

## Configuring server security for the Enterprise Vault Domino Gateway

Use the IBM Domino Administrator Client to configure the server document. If you plan to have several Enterprise Vault Domino Gateway computers in your Domino domain, repeat the following procedure for each Enterprise Vault Domino Gateway.

### To configure server security for the Enterprise Vault Domino Gateway

- 1 Open the **Security** page of the server document.
- 2 In the **Programmability restrictions Who can** section, ensure that the user who will sign the mail templates is displayed in the field **Sign agents to run on behalf of the invoker of the agent** (Domino versions earlier than 8.5) or **Sign agents or XPages to run on behalf of the invoker** (Domino 8.5).
- 3 Scroll down to **Server Access**.
- 4 Add the user who will create the Enterprise Vault Domino Gateway mail template to **Create master templates**.
- 5 Add the target Domino mail servers to **Trusted servers**.
- 6 Click **Save and Close**.
- 7 Repeat steps 1 through 6 for each Enterprise Vault Domino Gateway.

## Configuring Single Sign-On on the Enterprise Vault Domino Gateway

To enable authentication for the archive search feature, you need to set up Single Sign-On on the Enterprise Vault Domino Gateway.

The following procedure assumes that you are not using Internet Sites documents, if you are then use the procedure outlined in the Lotus Domino documentation.

For more detail on how to configure Single Sign-On using Web Configuration, see the following IBM article:

<https://publib.boulder.ibm.com/infocenter/iserics/v5r4/topic/rzatz/51/sec/secssdom.htm>

### To configure Single Sign-On on the Enterprise Vault Domino Gateway

- 1 In the IBM Domino Administrator Client, go to the **Configuration** tab and select **Server > All Server Documents** view. Select (but do not open) the server document for the Enterprise Vault Domino Gateway.
- 2 Click **Web**, and select **Create Web SSO Configuration** from the drop-down box.
  - In the **Configuration Name** field, change the default name to EVLtpaToken.
  - In the **DNS Domain** field, enter the DNS domain of the participating Domino servers.
  - In the **Domino Server Names** field, add all the Enterprise Vault Domino Gateways. If you want Single Sign-On to cover DWA users, then you also need to add the target Domino mail servers.
  - Click **Keys** and, in the drop-down menu, select **Create Domino SSO Key**. Click **OK**.
  - Save and close the Web SSO Configuration.
- 3 While the server document for the Enterprise Vault Domino Gateway is selected, click **Edit server**.
  - Click the **Internet Protocols** tab and then **Domino Web Engine** sub-tab.
  - Change the **Session Authentication** field to **Multiple Servers (SSO)** and click **OK**.
  - In the **Web SSO Configuration** field, select **EVLtpaToken**.
  - Save and close the server document.

## About the user ID for Domino mailbox archiving

The Domino provisioning and mailbox archiving tasks need to access the user's mail databases to do the following:

- Add hidden views.
- Add or update a hidden Enterprise Vault profile document.
- Change mail items into shortcuts.

To comply with the Domino security model, this access to Domino mail databases needs to be done by an authenticated user using a Lotus Notes ID file. When you configure the server document for target Domino mail servers, you will give this ID at least Editor access and Delete Documents and Create shared folders/views permissions on mail files to be archived.

See [“Granting the Domino archiving user access to all mail files”](#) on page 95.

Later, you specify this ID in the Enterprise Vault Administration Console when you are configuring Domino mailbox archiving. The ID details (including the password) are encrypted and stored in the Enterprise Vault directory database.

Although you can use any user ID file that has the correct level of access, we recommend that you create a generic user account and grant the user the access permissions required.

## Creating the Domino archiving user

Use the user registration tool in the Domino Administrator client to create a generic user account. As the user's person document must contain the Domino domain name, the user must be a Lotus Notes mail user. It is advisable to give the user a sensible generic name, such as Enterprise Vault Domino Archiving.

You can prefix the last name with the special character '&' to ensure that the user is only displayed at the end of the address list; for example, Enterprise Vault Domino &Archiving/*organization*.

---

**Note:** Place the user's ID file and copy it to the Lotus Notes data folder on every Enterprise Vault server that will run the Domino archiving task. You must also copy the ID file to the Lotus Notes data folder on the Enterprise Vault Domino Gateway. The default location for the Lotus Notes data folder is `C:\Program Files\lotus\notes\data`.

---

## Granting the Domino archiving user access to all mail files

The Domino archiving user account needs permissions to all the mail files to be archived. We recommend that you provide **Manager** access to the mail files. The account requires a minimum of **Editor** access with **Delete Documents** and **Create shared folders/views**

---

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

---

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

Repeat the following steps for each target Domino mail server.

### To grant the Domino archiving user access to all mail files

- 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, 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.

## Configuring the server document for each target Domino mail server

When configuring the server document for each of the target Domino mail servers, you will need to do the following:

- The server document for each target Domino mail server must have Enterprise Vault Domino Gateways added as trusted servers.
- The signing ID that will be used to sign the Enterprise Vault client templates also needs to be given the following permissions:
  - **Sign agents to run on behalf of the invoker of the agent** (Domino versions earlier than 8.5)
  - **Sign agents or XPages to run on behalf of the invoker** (Domino 8.5)
  - Create master templates.



- The Domino archiving user needs to be given access to target user mail files.
- Optionally, you may want to enable Single Sign-On for DWA users.  
The main requirement for Single Sign-On is to enable users to use the Enterprise Vault search feature. However, if Single Sign-On is not configured, DWA users will need to re-enter authentication details when opening archived items. To avoid this, you may want to configure Single Sign-On on DWA servers, even if you do not plan to give users access to the Enterprise Vault search feature.  
See [“Configuring Single Sign-On on the Enterprise Vault Domino Gateway”](#) on page 93.

#### To configure the server document for each target Domino mail server

- 1 Open the **Security** page of the server document.
- 2 In the **Programmability restrictions Who can** section, ensure that the user who will sign the mail templates is displayed in the following field:
  - **Sign agents to run on behalf of the invoker of the agent** (Domino versions earlier than 8.5)
  - **Sign agents or XPages to run on behalf of the invoker** (Domino 8.5)
- 3 Scroll down to **Server Access**, and add all the Enterprise Vault Domino Gateways in the domain as trusted servers.
- 4 Add the user who will create the Enterprise Vault mail template to **Create master templates**.
- 5 Click **Save and Close**.
- 6 Repeat the above steps for each Enterprise Vault target Domino mail server.

## Install and configure Enterprise Vault Domino Gateway

Install Domino Server binaries on each Enterprise Vault Domino Gateway computer. Select the Messaging Server option when installing.

You must install the appropriate Domino hotfixes on the Enterprise Vault Domino Gateway.

See [“Prerequisite software for Enterprise Vault Domino Gateway”](#) on page 90.

You must make the Vault Service account into a local administrator on the Enterprise Vault Domino Gateway.

The Domino server on the Enterprise Vault Domino Gateway must run under the Vault Service account. It is best practice to run the Domino server as a service, but be aware that the server console is not displayed when running a service under

an account other than the system account. This is a Microsoft Windows limitation. To see the console, you can connect to it remotely.

If you want to have the server console displayed locally while you are configuring Domino Mailbox archiving, you can run the Domino server as an application as follows:

- Log on to the Enterprise Vault Domino Gateway computer using the Vault Service account.
- In Windows Services console, if the Lotus Domino Server service is running, stop it.
- Disable the Lotus Domino Server service.
- Start the Lotus Domino Server (by double-clicking the desktop icon or running *Domino program directory\nserver.exe*), and select the option to start the server as a regular application. The Domino server configuration starts.

During Domino server configuration, do the following:

- Supply the Domino Server ID that was created when you registered the Domino server on the Enterprise Vault Domino Gateway.
- Select the option **Web Browsers (HTTP Services)** on the Internet Services page to add the HTTP server task.
- For optimum performance, use the **Customize** button to remove all but the minimum server tasks. The following Domino server services are the minimum required on the Enterprise Vault Domino Gateway:
  - Indexer (Update)
  - Administration process (AdminP)
  - Domino web server (HTTP)

---

**Note:** In a production environment, start the Domino Server on the Enterprise Vault Domino Gateway as a service running under the Vault Service account.

---

To ensure that Enterprise Vault can configure user mail files for archiving, and subsequently update the users' mail files with any archiving policy changes, the Domino Directory should replicate frequently to the Enterprise Vault Domino Gateway.

To enable DWA users to open those archived MIME items that are signed or encrypted there must be an SSL connection to the Enterprise Vault Domino Gateway. In this case, you must configure the Enterprise Vault Domino Gateway for SSL. If you do not do this configuration, DWA users receive the following error message:

Unable to complete the current operation.  
SSL is required for secure mail,  
but is not enabled on Domino Server.  
Please notify your administrator.

## Prerequisites for Domino journaling archiving

This section describes the minimum requirements for Domino journaling archiving. For details of the latest supported software versions, see the Enterprise Vault *Compatibility Charts* (<http://www.symantec.com/docs/TECH38537>).

## Prerequisites for Enterprise Vault archiving from Domino Journaling databases

Enterprise Vault will archive from any subfolder of the target Domino server's Data directory. Each subfolder, which must already exist, must be an immediate subfolder of the Data directory, and not lower down the folder structure. Otherwise, the Domino Journaling task fails to find any databases to archive.

By default, Enterprise Vault archives from all Domino Journaling databases that are in the subfolder and use the STDMailJournaling template. You can use a registry value to specify other templates to use. See the *Setting up Domino Server Archiving* manual for instructions.

The normal Enterprise Vault configuration is to retain the original item until the vault store that contains the archived item has been backed up. Enterprise Vault then deletes the original item. The Domino Database Management method must not interfere with this Enterprise Vault process, which means that the Purge and Compact method (specified in the Journaling section of the server configuration document) is unsuitable, because there is the potential to lose items that have, for some reason, not been archived.

Thus, the Domino Journaling database must have its Database Management method set to one of the following in the Journaling section of the server configuration document:

- Periodic Rollover or Size Rollover. The rollover databases must be in the same directory as the initial database in order for them to be archived.
- None. If you select this method the database will continue to grow, so we recommend that you compact the journal directory each night.

Configure Domino Journaling so that the Journaling database is in a subfolder of the server's Data directory. If Domino Journaling is already configured, you may need to move the Journaling database and update the server configuration document.

## **Support for Enterprise Vault archiving from clustered Domino journal databases**

Enterprise Vault can archive from Domino journal databases on Domino Servers that are clustered using Domino application clustering.

To support clustered journal databases, the following requirements must be satisfied:

- Each Domino Server in the cluster should be independently journaling to a local database.
- Mail journaling databases should not be configured to replicate to other Domino servers in the cluster. This includes both cluster replication and scheduled replication.
- Enterprise Vault should be configured to archive from the Domino journal databases on each server in the cluster.

## **Configuring access for Enterprise Vault to Domino domain, server, and Journaling location**

When you configure Enterprise Vault to archive a Domino Journaling location you must supply at least one Lotus Notes ID file. Enterprise Vault requires three levels of access, to domain, server, and journaling location. You can use a different ID file for each level or, for simplicity, a single ID file.

The access levels are as follows:

- Access to the Domino domain. This is provided by the ID file of a user who is enabled for Lotus Mail and whose account is in the same domain as the server. This account must have read access to the Domino Directory.
- Access to the Domino server. This is provided by the ID file of a user who has access to the Domino server and its directories.  
By default, Enterprise Vault will use the same ID file as is used to access the domain.
- Access to the Domino Journaling location. This is provided by the ID file of a user who has Editor, Designer, or Manager access to the journaling databases, and also has the Delete Documents permission. If the database is encrypted, this ID file must be the one that was used to encrypt the database.  
By default, Enterprise Vault will use the same ID file as is used to access the server. If you do not specify a file for server access, Enterprise Vault will use the same ID file as is used to access the domain.

### To configure access for Enterprise Vault

- ◆ Place the user's ID file and copy it to the Lotus Notes data folder on every Enterprise Vault server that will run a Domino Journaling task. The default location for the Lotus Notes data folder is `C:\Program Files\lotus\notes\data`.

## Domino mailing list groups

To ensure the expansion of Domino mailing list groups when using Enterprise Vault Compliance Accelerator Journaling Connector, it is important that you set the Mail Domain field explicitly when configuring Domino mailing list groups.

## Client access for Domino journal archiving

Domino Server journal archives can be searched using Enterprise Vault browser search. These archives cannot be accessed using Archive Explorer.

To use Enterprise Vault browser search, Internet Explorer 7.0 or later, with Java scripting enabled, must be installed on the user's desktop computer.



# Additional prerequisites for File System Archiving (FSA)

This chapter includes the following topics:

- [About the prerequisites for FSA](#)
- [Enterprise Vault server requirements for FSA](#)
- [About FSA shortcuts](#)
- [About the FSA Agent](#)
- [Preparing file servers for FSA](#)
- [Client requirements for FSA](#)

## About the prerequisites for FSA

For full details of all the supported versions of prerequisite products, see the [Enterprise Vault Compatibility Charts](#). This document also provides full details of the target platforms, operating systems and protocols that Enterprise Vault supports for FSA, and lists the operating systems supported for client access of archived items, including opening Internet and placeholder shortcuts to archived items.

## Enterprise Vault server requirements for FSA

An Enterprise Vault Storage service is required on the Enterprise Vault server that hosts FSA.

Internet Explorer 7.0 or later is required on the Enterprise Vault server computer that hosts FSA.

If you are implementing FSA but not Exchange Server archiving, you do not need to install Outlook on the Enterprise Vault server. However, Outlook is required on the Enterprise Vault server if you want to access any files that Enterprise Vault archived before Enterprise Vault 7.0.

Note also that if FSA archives `.MSG` files then Enterprise Vault indexing of these files is restricted unless Outlook is installed on the Enterprise Vault server that archives from the file server. For example, Enterprise Vault can index the content of Outlook messages, but not the message subjects or attachments. If you want the full indexing functionality, install Outlook on the Enterprise Vault server.

If you archive Outlook `.MSG` files from a file server and Outlook is not present on the Enterprise Vault server, Enterprise Vault generates a warning message in the Enterprise Vault event log. If you do not want to receive these warning messages you can prevent them by setting a registry value. To prevent the messages, add a `DWORD` registry value named `WarnForMissingOutlook` with a value of 0 to the following registry key on the Enterprise Vault server:

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

## About FSA shortcuts

When a file is archived, Enterprise Vault can optionally leave one of the following types of shortcut in its place:

- A placeholder shortcut. This is a special file that appears exactly as the original file but, when opened, forces Enterprise Vault to fetch the archived file. A Placeholder service needs to be configured to create these shortcuts.
- An internet (URL) shortcut. This is a `.url` text file containing a hypertext link to the archived file. The Placeholder service is not required to create these shortcuts.

Enterprise Vault cannot create placeholders for certain legacy files. This is particularly true of files that have extended attributes because they were previously stored in an HPFS (OS/2) file system.

Check in the [Enterprise Vault Compatibility Charts](#) that users' operating systems are supported for client access of archived items, including opening internet and placeholder shortcuts.



## Placeholder shortcut requirements

Enterprise Vault supports the creation of placeholder shortcuts on the following file system types:

- NTFS.

The FSA Agent must be installed on each Windows file server to provide the Enterprise Vault Placeholder service.

See “[About the FSA Agent](#)” on page 105.

Each disk on which placeholder shortcuts are required must be an NTFS device; it is not sufficient to use a non-NTFS device that appears on the network as an NTFS device.

The Enterprise Vault server uses CIFS when accessing the file system, for example, to archive files.

- NetApp Filer with Data ONTAP 7.2 or later.

To use the pass-through recall option, the NetApp filer must have Data ONTAP 7.3 or later.

The FSA Agent is not required. The Enterprise Vault server runs an equivalent process to the Placeholder service, and accesses the NetApp Filer using CIFS.

- EMC Celerra/VNX.

The FSA Agent is not required. The Enterprise Vault server runs an equivalent process to the Placeholder service, and accesses the EMC Celerra/VNX file system using CIFS.

Before installing and configuring FSA, ensure that the target file system that you want to archive is supported.

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

## About the FSA Agent

For Windows file servers, the FSA Agent must be installed on a target file server if you want to do any of the following:

- Use placeholder shortcuts.
- Implement File Blocking.
- Gather data for FSA Reporting.

In an environment where Windows file servers are grouped in a cluster, the FSA Agent must be installed on each cluster node.

---

**Note:** File Blocking and FSA Reporting are not supported on computers that run a Server Core installation of Windows. For details of supported operating systems see the Enterprise Vault *Compatibility Charts*, at <http://www.symantec.com/docs/TECH38537>.

---

Prerequisites and instructions for installing the FSA Agent are included in *Setting up File System Archiving*.

For non-Windows file servers the FSA Agent is used only in the following circumstances:

- To implement File Blocking on NetApp file servers you must configure a Windows server in the Administration Console as a file server, and install the FSA Agent on the Windows server to provide a File Blocking agent server for the NetApp file server.  
See the *Setting up File System Archiving* guide.
- To implement FSA Reporting on non-Windows file servers you must configure an FSA Reporting proxy server to gather the FSA Reporting data. If you configure an FSA Reporting proxy server that is not an Enterprise Vault server, the proxy server must have the FSA Agent installed.  
See the *Reporting* guide.

## Preparing file servers for FSA

You can configure and manage file servers in Enterprise Vault with the Vault Service account or an account that belongs to a suitable administrator role. The predefined administrator roles that permit FSA administration are the File Server Administrator and the Power Administrator.

See "Managing administrator security" in the *Administrator's Guide*.

The account that you use must have local administrator rights on the computer on which you run the Administration Console.

For Windows file servers, give the following access rights to the Vault Service account and to any other account that is to administer the file server:

- Local administrator rights on the file server
- Full control on any share that is configured as a target volume

Optionally, the account also requires browse permissions on the target folders, and on any folders in the paths to the target folders. If these optional permissions are not set, the administrator is unable to browse in the Administration Console for the target folder, and so must specify the path by typing it in.

Before configuring a NetApp file server for archiving you must set up the required administrative permissions on the file server.

For instructions on how to prepare a NetApp file server or EMC Celerra/VNX device, see *Setting up File System Archiving*.

## Client requirements for FSA

The following client access to archived items is available with FSA:

- If shortcuts are created in the item's original location, users can access an archived item simply by double-clicking the shortcut on the file server.
- If shortcuts are not created, users can access the archived items in the archives using archive search or Archive Explorer.

To use Enterprise Vault browser search or Archive Explorer, Internet Explorer 7.0 or later, with JavaScripting enabled, must be installed on each user's desktop computer.



# Additional prerequisites for SharePoint Server archiving

This chapter includes the following topics:

- [About the Enterprise Vault server requirements for SharePoint Server archiving](#)
- [Prerequisites for SharePoint Servers](#)

## About the Enterprise Vault server requirements for SharePoint Server archiving

Internet Explorer 7.0 or later is required on the server that hosts the Enterprise Vault Storage service.

If you are implementing SharePoint Server archiving but not Exchange Server archiving, you do not need to install Outlook on the Enterprise Vault server. However, Outlook is required on the Enterprise Vault server if you want to access any files that Enterprise Vault archived before Enterprise Vault 7.0.

## Prerequisites for SharePoint Servers

The prerequisite software and settings for the SharePoint Servers are as follows:

- The version of Microsoft SharePoint products must be at least one of the following:
  - Microsoft Windows SharePoint Services 3.0 (WSS 3.0)
  - Microsoft Office SharePoint Server 2007 (MOSS 2007)
  - SharePoint Server 2010

■ **SharePoint Foundation 2010**

- Ensure that the Vault Service account has local administrator permissions on the SharePoint Server computer.
- The account under which the Enterprise Vault SharePoint task runs (typically the Vault Service account) must have full access to target site collections and their content. When archiving from SharePoint 3.0 sites, the account must have Site Collection Administrator privileges on the target SharePoint site collections.
- SharePoint Servers must be running either Windows Server 2003 with Service Pack 2 or later, or Windows Server 2008 with Service Pack 1 or later. If Windows Server 2008 with Service Pack 1 is installed, you must also install the following mandatory hotfix for IIS:

<http://support.microsoft.com/kb/949516>

Note the following:

- The hotfix that Microsoft provides for Windows Vista is the hotfix to use for Windows Server 2008.
- By default the Microsoft Web page presents a hotfix download that matches the operating system of the computer that you are using. On the download page, choose the option to show hotfixes for all platforms and languages so that you can select the correct version of the hotfix.
- If you install in a server farm, you must install the Enterprise Vault components on all the front-end Web servers.
- The Enterprise Vault SharePoint components require the Enterprise Vault SharePoint HttpModule. The Enterprise Vault Setup program automatically installs the Enterprise Vault HttpModule when you choose to install the Enterprise Vault SharePoint component.
- The DCOM port (135) must be open on the target SharePoint system.
- If Enterprise Vault and SharePoint run on separate computers, we recommend that you do not install Backup Exec on the same computer as the Enterprise Vault Microsoft SharePoint Components.
- You must use host names in the URL when adding SharePoint targets.

For full details of all the supported versions of prerequisite products, see the Enterprise Vault *Compatibility Charts* at

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

## About SharePoint security certificates

The certificate used by the SharePoint virtual server or Web Application must have the same name as the SharePoint URL. For example, if the SharePoint URL is `https://sharepoint`, then the name of the certificate used when issuing a certificate request must be `sharepoint`.

If the names do not match, Enterprise Vault will not be able to validate the SharePoint site when you try to configure it in the Administration Console.





# Additional prerequisites for SMTP archiving

This chapter includes the following topics:

- [About the prerequisites for SMTP archiving](#)
- [Microsoft SMTP Server computer requirements](#)
- [EML file holding area and Enterprise Vault server requirements](#)
- [Client access for SMTP archiving](#)

## About the prerequisites for SMTP archiving

There are additional prerequisites for the Enterprise Vault SMTP Archiving. These include requirements for the Microsoft SMTP Server, and also for the EML file holding area.

Ensure that you use supported versions of prerequisite products.

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

## Microsoft SMTP Server computer requirements

As part of configuring SMTP archiving, you must set up a Microsoft SMTP Server to receive a copy of each SMTP message that you want Enterprise Vault to archive.

Note the following:

- Although you can install the Microsoft SMTP Server on the same computer as Enterprise Vault, it is more common to install it on a separate computer.

- Enterprise Vault stores all the messages that you send to SMTP archiving; it does not perform any filtering. For this reason, only SMTP messages should be sent to the Microsoft SMTP Server, and not Exchange MAPI messages. We recommend that you do not run Microsoft Exchange Server on this computer.
- We recommend that you locate the holding area for the EML files locally on the Microsoft SMTP Server computer.  
See [“EML file holding area and Enterprise Vault server requirements”](#) on page 114.

The following software versions are required on the Microsoft SMTP Server computer:

- Windows Server 2008 R2 x64 edition (using WOW64). The SMTP Server is not installed by default. Add the SMTP Server using the **Features Summary** area of the Server Manager tool in Windows Server 2008.
- Internet Information Services (IIS) 7.5 or later, with the IIS 6 Management Compatibility component.

The computer on which you install the SMTP archiving components must be enabled for IPv4 network connections. SMTP archiving components do not support IPv6 network connections.

You must configure a Microsoft SMTP virtual server in IIS. For more information, see the *Setting up SMTP Archiving* manual.

## EML file holding area and Enterprise Vault server requirements

Enterprise Vault uses File System Archiving (FSA) to archive the files from the EML file holding area. This means that:

- The holding area computer must satisfy the FSA prerequisites for a file server.
- The Enterprise Vault server must satisfy the prerequisites for FSA.

See [“About the prerequisites for FSA”](#) on page 103.

You do not need to install Outlook on the Enterprise Vault server unless you are also implementing Exchange Server archiving.

Internet Explorer 7.0 or later is required on the computer that hosts the Enterprise Vault Storage Service; typically this is the Enterprise Vault server computer.

## Client access for SMTP archiving

Users can find and retrieve archived SMTP messages using Enterprise Vault browser search or Archive Explorer, which they can run from a browser.

To view messages in their original format, users must have Outlook Express installed.

To use Enterprise Vault browser search or Archive Explorer, Internet Explorer 7.0 or later, with Java scripting enabled, must be installed on the user's desktop computer.



# Additional requirements for a standalone Enterprise Vault Administration Console

This chapter includes the following topics:

- [About the prerequisites for a standalone Enterprise Vault Administration Console](#)

## About the prerequisites for a standalone Enterprise Vault Administration Console

If required, the Enterprise Vault Administration Console can be installed on a separate computer that has the following prerequisite software:

- One of the following versions of Windows:
  - Windows Vista SP1 or later.
  - Windows 7.
  - Windows Server 2008 R2.
- MDAC 2.6 or later. A suitable version is installed automatically with Windows Server 2008 R2 (which changes the name of MDAC to Windows Data Access Component, or Windows DAC).
- Microsoft .NET Framework 3.5 SP1 or SP2.

- On Windows Server 2008 R2: IIS 7.5.
- On Windows Vista and Windows 7: The Administration Tools Pack. You can download the Administration Tools Pack from the following locations:
  - Windows Vista:  
<http://www.microsoft.com/downloads/en/details.aspx?FamilyID=9ff6e897-23ce-4a36-b7fc-d52065de9960>
  - Windows 7:  
<http://www.microsoft.com/downloads/en/details.aspx?FamilyID=7d2f6ad7-656b-4313-a005-4e344e43997d>

If Enterprise Vault is configured to archive Exchange servers, you also require one of the following versions of Microsoft Outlook on the remote Administration Console computer:

- Outlook 2003 SP2
- Outlook 2007 SP2
- Outlook 2010

## Additional requirements for the Discovery Search Service

This chapter includes the following topics:

- [About additional requirements for the Discovery Search Service](#)
- [Additional prerequisite software for Discovery Search Service](#)

### About additional requirements for the Discovery Search Service

The Discovery Search Service provides the means through which third-party client applications can search across all the archives in an Enterprise Vault installation. In this release, the service is available for use with the Clearwell eDiscovery platform only.

You monitor the activities of the Discovery Search Service by using the Enterprise Vault Operations Manager. If you have yet to configure Operations Manager, it is best to do so before you configure the Discovery Search Service.

### Additional prerequisite software for Discovery Search Service

To use the Discovery Search Service to search across all archives in an Enterprise Vault installation, you must install it on at least one Enterprise Vault server in the site.

You must also ensure that the Windows Communication Foundation (WCF) Activation features are enabled on the Enterprise Vault server.

**To enable the WCF Activation features**

- 1** On the **Start** menu of your Enterprise Vault server, click **Start > Administrative Tools > Server Manager**.
- 2** In the **Server Manager** pane, click **Features**.
- 3** In the right pane, click **Add Features**.
- 4** In the first page of the Add Features Wizard, expand the **.NET Framework 3.5.1 Features** entry and then expand the **WCF Activation** entry.
- 5** Ensure that both **HTTP Activation** and **Non-HTTP Activation** are checked, and then click **Next**.
- 6** Click **Install** and then, on the **Installation Results** page, click **Close**.



# Installing Enterprise Vault

- [Chapter 13. Licenses and license keys](#)
- [Chapter 14. Installing Enterprise Vault](#)
- [Chapter 15. Postinstallation tasks](#)
- [Chapter 16. Uninstalling Enterprise Vault](#)



# Licenses and license keys

This chapter includes the following topics:

- [Overview of Enterprise Vault licensing](#)
- [Obtaining license keys for Enterprise Vault](#)
- [Installing Enterprise Vault license key files](#)
- [Replacing Enterprise Vault licenses and installing additional licenses](#)

## Overview of Enterprise Vault licensing

Enterprise Vault uses the Enterprise Licensing System (ELS). To run the associated Enterprise Vault services, you must install a license key file that covers the Enterprise Vault features that you want to implement.

The following types of Enterprise Vault license are available:

- **Production license.** This license comprises a product base license and any additional feature licenses. When the license file is installed, the functionality of Enterprise Vault depends on the feature licenses that you have purchased. Production licenses generally do not have an expiry date.
- **Trialware license.** With this 30 day license, the full functionality of Enterprise Vault is available, but the functionality is time-limited, as defined by the key. When the license expires, the software continues to run in restricted, read-only mode, which allows archived items to be viewed and retrieved, but no items can be archived. Enterprise Vault tasks will not start, and you cannot migrate the contents of personal folder (PST) files to Enterprise Vault.
- **Temporary licenses.** Temporary licenses are available for 10 day to 90 day duration.  
When the license expires, the software continues to run in restricted, read-only mode, which allows archived items to be viewed and retrieved, but no items

can be archived. Enterprise Vault tasks will not start, and you cannot migrate the contents of personal folder (PST) files to Enterprise Vault.

## Obtaining license keys for Enterprise Vault

For information on how to purchase Enterprise Vault licenses, see Symantec Enterprise Vault Licensing Information at the following address on the Symantec Web site:

[http://www.symantec.com/enterprise/products/licensing.jsp?pcid=1018&pvid=322\\_1](http://www.symantec.com/enterprise/products/licensing.jsp?pcid=1018&pvid=322_1)

The following Enterprise Vault features, which are mentioned in this guide, require licenses:

- Enterprise Vault core services
- Exchange Server mailbox archiving
- Exchange Server journal archiving
- Domino Server mailbox archiving
- Domino Server journal archiving
- Exchange Server public folder archiving
- Migrating PST files
- NSF migration wizard
- SharePoint Server archiving
- Archive Explorer
- Vault Cache
- File System Archiving (FSA)
- SMTP archiving
- Policy Manager (EVPm)
- Custom filters and properties
- Migrating collected Enterprise Vault files

Note that other Enterprise Vault tools and features that are not mentioned in this guide may also need licenses.

After you have purchased licenses and received your License Certificate, Voucher Document, or Upgrade Notification, you need go to the Symantec Licensing Portal at the following address to register and generate your license key file.

<https://licensing.symantec.com/acctmgmt/index.jsp>

You will need the serial number on the license document or notification in order to generate a Symantec Licensing Portal account.

When you have generated a license key file, you download a zipped and digitally-signed ELS license file. The ELS license file has a unique name and the extension `.slf`. Each license file can contain the license keys for several Enterprise Vault features.

For information about generating license key files, contact Symantec Customer Care at the following address:

<http://support.symantec.com>

## Installing Enterprise Vault license key files

Save this file in a temporary location on each Enterprise Vault server computer.

The Enterprise Vault installation wizard prompts for the location of your ELS license file, and copies the file to the top-level Enterprise Vault folder (for example `C:\Program Files (x86)\Enterprise Vault`). When the Enterprise Vault Admin service is started, it installs the licenses and writes a license information report message to the event log.

You can continue Enterprise Vault installation without an ELS license file, but Enterprise Vault will operate in restricted, read-only mode until you obtain and install a new ELS license.

## Replacing Enterprise Vault licenses and installing additional licenses

Follow the instructions in this section if you have already installed Enterprise Vault and subsequently want to install additional license files or replace existing license files.

### To replace a license or install an additional license

- 1 Place the new `.slf` license file in the Enterprise Vault folder (for example `C:\Program Files (x86)\Enterprise Vault`).
- 2 Restart the Enterprise Vault Admin service to install the licenses. The Admin service writes a license information report message to the event log.
- 3 For a multi-server Enterprise Vault deployment, you must repeat the steps on each Enterprise Vault server.



# Installing Enterprise Vault

This chapter includes the following topics:

- [Installing Enterprise Vault](#)

## Installing Enterprise Vault

---

**Caution:** Before you install Enterprise Vault, check that all the prerequisites for your planned installation have been fulfilled.

Run the Deployment Scanner on the computers on which you plan to install Enterprise Vault.

See [“About the Enterprise Vault Deployment Scanner”](#) on page 42.

---

Perform the following steps to install the required Enterprise Vault components.

Note that the Enterprise Vault installer automatically installs the following software without asking for confirmation:

- Microsoft Visual C++ 2005 and 2008 Redistributable Packages
- Microsoft MSXML 6.0 and SQLXML 4.0, if you install the Enterprise Vault Services component

### To install Enterprise Vault

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

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

- 4 In the right pane of the Install Launcher click **View ReadMeFirst** under Enterprise Vault. Read the ReadMeFirst before you continue with the installation.
- 5 In the list in the left pane of the **Symantec Enterprise Vault Install Launcher** window, click **Enterprise Vault**.
- 6 Click **Server Installation**.
- 7 In the right pane, click **Installation on first server in new site**.
- 8 Click **Install**. The Enterprise Vault installation wizard starts.
- 9 Install the required Enterprise Vault components for this computer.

The core components for an Enterprise Vault server are as follows:

- **Enterprise Vault Services.**  
Installs all the core Enterprise Vault services. After the installation, you must configure the services before using them. This is done when you run the Enterprise Vault configuration wizard.  
See [“About configuring Enterprise Vault”](#) on page 145.
- **Administration Console.**  
Installs the Administration Console. This is a snap-in to the Microsoft Management Console (MMC) that enables you to manage Enterprise Vault. This component also installs the Enterprise Vault configuration wizard, and the PST Migrator and NSF Migrator wizards.  
If you want to install a standalone Administration Console on a remote system, then select this component only.

A number of other components can be installed as required. Before installing the selected components, the installer checks that the prerequisites are met.

- **SMTP Archiving Components, Exchange Server Extensions, and Microsoft SharePoint components** are usually installed on computers other than the Enterprise Vault server. For details, see the appropriate section elsewhere in this manual.
- **The Enterprise Vault Operations Manager component** is a Web application that enables you to monitor Enterprise Vault servers remotely from a computer on which Internet Explorer is installed.  
Enterprise Vault Operations Manager must be installed on at least one Enterprise Vault server in a site if you want to monitor the Enterprise Vault servers in that site.
- **The Enterprise Vault Reporting component** provides enterprise-level reporting for Enterprise Vault servers, using Microsoft SQL Server Reporting Services as the reporting mechanism. Administrators manage



report content and view reports using the Reporting Services Report Manager Web application.

Enterprise Vault Reporting is required if you want to use FSA Reporting. Enterprise Vault Reporting requires Microsoft SQL Server Reporting Services (SSRS) as a prerequisite.

Enterprise Vault Reporting can be installed on an Enterprise Vault server, but is more typically installed on a separate server that is running SSRS. For more information about installing and configuring Enterprise Vault Reporting, see the *Reporting* guide.

- 10** If Lotus Domino is installed, the installation lists the Domino partitions that are available. The installation installs the Enterprise Vault Domino Gateway software in each partition that you select.
- 11** Setup automatically scans the computer to determine whether it meets the Enterprise Vault prerequisites and generates a report. If the computer does not meet all the requirements Setup gives you the option to view a report of the findings.
- 12** Setup checks that the computer is configured to use Enterprise Vault best practice settings.
- 13** At the end of installation, you may be instructed to restart your computer. The installation continues after you have restarted the computer. There is a confirmation message that informs you that the installation is complete.



# Postinstallation tasks

This chapter includes the following topics:

- [Default security for the Enterprise Vault Web Access application](#)
- [Customizing security for the Enterprise Vault Web Access application](#)
- [Customizing security for the Web Access application on client computers](#)

## Default security for the Enterprise Vault Web Access application

The Enterprise Vault Web Access application is located in the IIS virtual directory **EnterpriseVault** in the default Web site. Although HTTP over TCP port 80 is the default setting for Enterprise Vault client connections to the Web Access application, HTTPS is recommended to ensure the security of transmitted data. To use HTTPS, you must first configure the default Web site in IIS for HTTPS, and install a valid SSL certificate.

---

**Warning:** If you use HTTP, ensure that your network is secure. HTTP communication between Enterprise Vault clients and the Enterprise Vault Web Access application is unencrypted, and therefore vulnerable to interception on the network.

---

Both Basic authentication and Integrated Windows authentication are configured automatically.

The authentication that is automatically set up affects users when they log in to the Web Access application, as follows:

- A user logging in with a browser that supports Integrated Windows Authentication, such as Internet Explorer, must supply domain name and username separately:

Username: *username*

Password: *password*

Domain: *domain*

This domain can never be defaulted.

An Internet Explorer user with suitably-customized browser settings does not need to supply logon details manually because the logon is automatic; Internet Explorer automatically uses the details of the account to which the user is currently logged on.

See [“Customizing security for the Web Access application on client computers”](#) on page 135.

- A user logging in to the Web Access application with a browser that does not support Integrated Windows Authentication must supply both domain name and username in response to a single username prompt:

Username: *domain\username*

Password: *password*

It is possible for you to set up a default domain.

See [“Customizing authentication for the Enterprise Vault Web Access application”](#) on page 134.

## Customizing security for the Enterprise Vault Web Access application

You can change the port or protocol that is used to access the Web Access application. For example, it is recommended that connections to the application use HTTPS.

See [“Customizing the port or protocol for the Enterprise Vault Web Access application”](#) on page 133.

You can also customize the amount of information that users need to provide when logging on to the Web Access application.

See [“Customizing authentication for the Enterprise Vault Web Access application”](#) on page 134.

## Customizing the port or protocol for the Enterprise Vault Web Access application

You can change the port or protocol that is used to access the Enterprise Vault Web Access application. For example, it is recommended that you configure HTTPS for client connections to the Web Access application.

If you are configuring HTTPS for access to the Enterprise Vault Web Access application, you must first configure the default Web site in IIS for HTTPS, and install a valid SSL certificate.

---

**Warning:** If you use HTTP, ensure that your network is secure. HTTP communication between Enterprise Vault clients and the Enterprise Vault Web Access application is unencrypted, and therefore vulnerable to interception on the network.

---

If you change the port after items have been archived, existing shortcuts will no longer work. Shortcuts in Outlook and Lotus Notes can be updated with the new protocol or port information using Synchronize mailboxes in the Enterprise Vault Administration Console, but customized shortcuts, FSA shortcuts and SharePoint shortcuts cannot be updated.

Before you change the Web Access application port or protocol in Enterprise Vault, you must first make the required changes to the default Web site in IIS for each server in the Enterprise Vault site. Bear in mind that changing the protocol or port for the default Web site will affect all virtual directories in the Web site, including the `FSAReporting` virtual directory.

When you have made the necessary changes in IIS, change the Web Access application port or protocol settings on the **General** tab of the Site properties in the Administration Console.

If the Enterprise Vault site uses FSA Reporting, you must then perform some additional steps. Otherwise the status of FSA Reporting is shown as Off in the Administration Console. Perform the following steps on each Enterprise Vault server and on each file server in the Site.

### Additional steps for FSA Reporting after you change the port or protocol

- 1 Log on as the FSA Reporting user. The FSA Reporting user is the Windows user account that you specified for FSA Reporting to use when you ran the FSA Reporting Configuration wizard.
- 2 Open Internet Explorer and select **Tools > Internet Options**.
- 3 If you chose to use an SSL port, click the **Advanced** tab and under **Security** make sure that **Check for server certificate revocation** is not selected.

- 4 Click the **Security** tab and select the **Local intranet** zone. Then click **Custom Level** to display the Security Settings. Under **User Authentication**, make sure that **Prompt for user name and password** is not selected.
- 5 Repeat steps 1 to 4 on each Enterprise Vault server and on each file server in the Site.

## Customizing authentication for the Enterprise Vault Web Access application

The standard security for the Web Access application means that users must provide domain name, user name, and password whenever they start the Web Access application.

You can set up various levels of automatic authentication for the users. If none of these methods is acceptable to you, the default authentication enables users to log on by supplying domain, username, and password.

### Using a default domain with basic authentication

With only Basic authentication configured, users must provide a domain name when logging on to the Web Access application. For example, a user in domain myDomain with a username of Rogers must specify myDomain\Rogers when logging on to the Web Access application.

It is possible for IIS and Enterprise Vault to use a default domain for Basic authentication. In this case, users in the default domain do not need to specify a domain name when starting the Web Access application. Users in other domains must still specify a domain name.

### Setting up a default domain in IIS

You can set up IIS so that it uses a default domain for Basic authentication. How you do this depends on the version of IIS that you have installed.

Note that the default domain does not work unless you also define it for the Web Access application.

See [“Setting up a default domain in the Web Access application”](#) on page 135.

#### To set up a default domain in IIS 7

- 1 Start Internet Information Services (IIS) Manager.
- 2 Expand the Sites container for the Enterprise Vault Web Access application computer.
- 3 Click the **EnterpriseVault** folder.
- 4 Double-click **Authentication** in the **IIS** area at the right.

- 5 Ensure that **Anonymous Authentication** is disabled and **Basic Authentication** is enabled.
- 6 To set the default domain, do the following:
  - Right-click **Basic Authentication**, and then click **Edit**.
  - Enter the name of the domain that contains the majority of the user accounts that will be using the Web Access application.
  - Click **OK**.

### Setting up a default domain in the Web Access application

Note that the default domain does not work unless you also define it in IIS.

See [“Setting up a default domain in IIS”](#) on page 134.

**To set up the Web Access application so that it uses the same default authorization domain as you have set up in IIS**

- 1 Use a text editor to create an initialization file called `WebApp.ini`, containing the following line:

```
Domain=DomainName
```

where *DomainName* is the name of the domain that you have specified in IIS for Basic authentication. Note that entries in this file are case-sensitive.

For example, to use a domain called "myDomain", the line to use is as follows:

```
Domain=myDomain
```

- 2 Save the file in the Enterprise Vault program folder, for example `C:\Program Files (x86)\Enterprise Vault`, on the computer that runs the Web Access application.

## Customizing security for the Web Access application on client computers

On user computers, you can configure Internet Explorer so that users are automatically logged on to the Web Access application, without receiving a logon prompt. Essentially, you must configure Internet Explorer so that it trusts the Web Access application computer.

For this to work, you must also be using the Integrated Windows Authentication.

To make Internet Explorer log on automatically, you may need to modify the Internet Explorer Internet Options on each client computer. The settings are

saved in the Windows registry, so you can save them for rollout to many client computers.

There are many possible ways for you to configure Internet Explorer security, some of which may not be acceptable to you. The following methods are described here:

- Using the proxy bypass list
- Explicitly naming the Web Access application computer

See the Internet Explorer help if you need more information on configuring browser security.

On Windows computers that comply with Federal Desktop Core Configuration (FDCC), you cannot change local intranet zone settings in Internet Explorer. However, you can publish the Enterprise Vault server details to users' computers by modifying the relevant FDCC GPO. Users can then perform Enterprise Vault operations without being prompted for authentication each time.

See [“Publishing Enterprise Vault server details to FDCC-compliant computers”](#) on page 137.

## Configuring Internet Explorer to use the proxy bypass list

Note that you must be using a proxy server before you can use the proxy bypass list.

### To configure Internet Explorer to use the proxy bypass list

- 1 In Internet Explorer, click **Tools** and then **Internet Options**.
- 2 Click the **Security** tab and then click the **Local Intranet** zone.
- 3 Click **Sites** and then select **Include all sites that bypass the proxy server**.
- 4 Click **OK**.
- 5 Click **Custom Level**.
- 6 Under **Logon**, select **Automatic logon only in Intranet zone**.
- 7 Click **OK**.
- 8 Click the **Connections** tab, and click **LAN Settings**.
- 9 Check that a proxy server is being used.



- 10 If either of the **Automatic configuration** settings is selected, you must make sure that the Web Access application computer is in the automatic configuration exceptions list.
- 11 If neither of the **Automatic configuration** settings is selected, click **Use a proxy server** and then **Advanced**. If there is no existing entry that includes the Web Access application computer, specify the Web Access application computer in the **Exceptions** list.

## Configuring Internet Explorer to trust the Web Access application computer

This section describes how to add the Web Access application computer to the Internet Explorer local intranet zone. Once you have set up the security, users will not need to log on to search archives or to view or restore archived items.

It is possible to configure users' desktops so that they automatically add the Web Access application computer to the Internet Explorer local intranet zone. You configure this using the advanced Outlook settings in the Exchange Desktop policy. See the *Administrator's Guide* for more details.

### To configure Internet Explorer to trust the Web Access application computer

- 1 In Internet Explorer, click **Tools** and then click **Internet Options**.
- 2 Click the **Security** tab and then click the **Local Intranet** zone.
- 3 Click **Custom Level**.
- 4 Under **Logon**, select **Automatic logon only in Intranet zone** and then click **OK**.
- 5 Click **Sites** and then **Advanced**.
- 6 In the **Add this Web site to the zone** box, enter the fully-qualified domain name of the Web Access application computer and then click **Add**. For example, **vault.company.com**.
- 7 In the **Add this Web site to the zone** box, enter the computer name, without the DNS domain, of the Web Access application computer, and then click **Add**.
- 8 Click **OK**.

## Publishing Enterprise Vault server details to FDCC-compliant computers

If you have applied Federal Desktop Core Configuration (FDCC) Group policy objects (GPO) to Windows computers, users cannot change local intranet zone settings. This restriction is because the mandatory FDCC group policy, "Security

**Zones:** Use only machine settings", ignores all user-based settings on the local intranet zone in Internet Explorer. As a result, users need to enter authentication credentials each time they access Enterprise Vault. For example, users would be prompted for credentials when they archive, or retrieve an item, or open Archive Explorer.

This section describes how to add the Enterprise Vault server details to the FDCC Internet Explorer GPO. When the GPO is refreshed, the Enterprise Vault server details are added to the local intranet zone on users' computers. You must ensure that the Enterprise Vault server details are correct, because settings in the GPO take precedence over user settings.

#### To publish Enterprise Vault server details to FDCC-compliant computers

- 1 Log on to the domain controller computer using an administrator account with permission to modify and publish GPOs.
- 2 Open the Group Policy Object Editor.
- 3 Select the FDCC group policy object that applies Internet Explorer settings to the Windows XP and Vista computers.
- 4 In the Group Policy Object Editor, navigate to the following section:  
**Computer Configuration > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Security Page**
- 5 Right-click **Site to Zone Assignment List**, and select **Properties**.
- 6 Select **Enabled**, if it is not already selected, and then click **Show** to enter the required zone assignments.
- 7 Click **Add**.
- 8 In the box **Enter the name of the item to be added**, type the name of the Enterprise Vault server.

In the box **Enter the value of the item to be added**, type **1**.

This maps the server name to the intranet zone.

In the same way, add all the Enterprise Vault server names to the list and map them to the intranet zone. The list should include all Enterprise Vault server aliases. For an Enterprise Vault server that has the name SRV1 and the alias EVSERVER1, you would add the following to the site to zone assignment list:

**Value Name: evserver1.mycorp.local**

**Value: 1**

**Value Name: srv1**

**Value: 1**

- 9 When you have finished adding Enterprise Vault server names to the list, click **OK**.
- 10 On the Site to Zone Assignment List Properties page, click **Apply**.
- 11 When the policy is next refreshed, the changes to the GPO are applied to the Windows XP and Vista computers.
- 12 On one of the users' computers, you can verify that the Enterprise Vault server names have been added to the local intranet sites:
  - Log on to the computer as a standard user.
  - Open Internet Explorer.
  - Click **Tools > Internet options > Security > Local Intranet > Sites > Advanced**.
  - The Enterprise Vault server names should be listed in the Web sites.

## Enabling remote access to the Enterprise Vault Web Access application computer

You may need to grant users of the Enterprise Vault Web Access application access to the IIS computer, using the local IIS computer accounts database, not the domain accounts database.

---

**Note:** If the IIS computer is a domain controller, there is no local accounts database, only a domain accounts database. If you continue with these instructions when the IIS computer is a domain controller, you will make changes to the security access of the domain accounts database. This will affect all computers within the domain, not just the IIS computer. If you do not want to affect the whole domain, you should ensure that you run IIS on a non-domain controller.

---

### To enable remote access to the Web Access application computer

- 1 Click **Start > Programs > Administrative Tools > Local Security Policy**.
- 2 In the Local Security Policy window, expand the **Local Policies** container.
- 3 Click **User Rights Assignment**.
- 4 Set up Basic authentication access by following the steps below in the order listed:
  - In the right-hand pane, right-click **Allow log on locally** and then, on the shortcut menu, click **Properties**.

- Check that the **Users** group appears in the **Local Security Setting** list.
- 5 Set up Integrated Windows Authentication access by following the steps below in the order listed:
  - With **User Rights Assignment** still selected in the left pane of the Local Security Policy window, right-click **Access this computer from the network** in the right pane and then, on the shortcut menu, click **Properties**.

- Check that the **Users** group appears in the **Local Security Setting** list.  
If you do not want to add the **Users** group, see the other options below.

By default, the Users group includes Domain Users. If the Users group does not include Domain Users, or if some Web Access application users are in a different domain, you must do one of the following:

- Add the Web Access application users to the **Users** group.
- Add the Web Access application users to some other group and then grant the access right to that group.
- Grant the access right to each Web Access application user's account.

The Enterprise Vault Web Access application is now set up and ready to be used by users in the same domain as IIS.

# Uninstalling Enterprise Vault

This chapter includes the following topics:

- [Uninstalling Enterprise Vault](#)
- [Reinstalling Enterprise Vault](#)

## Uninstalling Enterprise Vault

Note the following before you proceed:

- If you uninstall Enterprise Vault on the primary Enterprise Vault server that is associated with the Directory database, the Directory database will also be removed.
- If you uninstall Enterprise Vault on a secondary Enterprise Vault server, the Directory database will not be removed.
- If you are uninstalling Enterprise Vault on a secondary Enterprise Vault server, and you want to preserve the Directory database, first backup the database and then close down the primary Enterprise Vault server computer, before uninstalling Enterprise Vault on the secondary Enterprise Vault server computer.
- If an Enterprise Vault service has data associated with it, you cannot use the Enterprise Vault Administration Console to remove that service.
- The uninstaller does not remove the following software components, which are automatically installed as part of the Enterprise Vault installation process:
  - Microsoft Visual C++ 2005 and 2008 Redistributable Packages
  - MSXML 6.0

■ SQLXML 4.0

**To uninstall Enterprise Vault**

- 1 From the Windows Control Panel, select **Add/Remove Programs**.
- 2 From the list of programs, select **Enterprise Vault**, and then click **Add/Remove**.

You are asked to confirm that you want to remove Enterprise Vault from your system.

- 3 Click **Yes**.

The uninstaller stops Enterprise Vault services that are still running. It then removes all Enterprise Vault Services and Enterprise Vault software from your system. The uninstaller does not delete data.

## Reinstalling Enterprise Vault

If you want to reinstall Enterprise Vault on the computer, perform the following steps.

**To reinstall Enterprise Vault**

- 1 Re-run the Setup program. You do not have to select the same installation folder for Enterprise Vault that you previously selected.
- 2 Run the Enterprise Vault configuration wizard. When this program prompts you for a Directory Computer, give the same name as for the previous installation. The configuration wizard automatically creates the same services as the computer had before.

If you do not want to reinstall Enterprise Vault, delete the Enterprise Vault data manually.

# Configuring Enterprise Vault

- [Chapter 17. About configuring Enterprise Vault](#)
- [Chapter 18. Running the Enterprise Vault configuration wizard](#)
- [Chapter 19. Running the Enterprise Vault Getting Started wizard](#)
- [Chapter 20. Configuring Enterprise Vault Operations Manager](#)
- [Chapter 21. Configuring the Discovery Search Service](#)





# About configuring Enterprise Vault

This chapter includes the following topics:

- [About configuring Enterprise Vault](#)

## About configuring Enterprise Vault

On completion of the Enterprise Vault installation program, you may need to run one or more configuration programs, depending on which Enterprise Vault components you installed.

If you have upgraded from an earlier version of Enterprise Vault, follow the Enterprise Vault upgrade instructions for your new version.

For a new Enterprise Vault installation, do as follows:

- If you installed the Enterprise Vault Services component, run the Enterprise Vault configuration wizard before you run any other configuration programs. See [“When to run the Enterprise Vault configuration wizard”](#) on page 147.
- If you installed the Enterprise Vault Operations Manager component, configure Enterprise Vault Operations Manager. See [“When to run the Enterprise Vault Operations Manager Configuration utility”](#) on page 169.
- If you installed the Discovery Search Service, run its configuration utility. See [“Running the Discovery Search Service Configuration utility”](#) on page 173.
- If you installed the Enterprise Vault Reporting component, configure Enterprise Vault Reporting. See the chapter “Configuring Enterprise Vault Reporting” in the *Reporting* guide.

- If you installed only the Administration Console component, you do not need to run any configuration program.
- If you installed components for specific archiving implementations such as Exchange, Domino, SharePoint, or SMTP, you may need to perform separate configuration steps for those components. See the relevant section elsewhere in this manual.

# Running the Enterprise Vault configuration wizard

This chapter includes the following topics:

- [When to run the Enterprise Vault configuration wizard](#)
- [What the Enterprise Vault configuration wizard does](#)
- [Running the Enterprise Vault configuration wizard](#)
- [Troubleshooting configuration of the Enterprise Vault Monitoring database](#)

## When to run the Enterprise Vault configuration wizard

Run the Enterprise Vault configuration wizard either immediately after installation (after restarting your computer if prompted), or after performing the postinstallation tasks for the Web access application.

Note the following:

- If you run the configuration wizard immediately after the installation, remember that there are some additional tasks that you need to do before users can use Enterprise Vault.  
See [“About configuring Enterprise Vault”](#) on page 145.
- If you exit from the configuration wizard before configuration is complete, you can run the configuration wizard again and have the option to delete the Directory database. Once you have successfully completed the configuration wizard, you cannot run it again on the same computer.

## What the Enterprise Vault configuration wizard does

The configuration wizard lets you do the following:

- Select which SQL Server you want to use for the Enterprise Vault Directory database
- Create the Enterprise Vault Directory database
- Create the Enterprise Vault Monitoring database
- Create an Enterprise Vault site
- Add the computer to the site
- Select the Enterprise Vault services you want to run on the computer
- Choose the storage areas to use for Enterprise Vault data

Some tasks, such as adding a service or assigning storage areas for the data, can also be done using the Enterprise Vault Administration Console. However, the following tasks can only be done using the configuration wizard:

- Creating a new Enterprise Vault Directory
- Creating a new Enterprise Vault site
- Adding a new Enterprise Vault server

## Running the Enterprise Vault configuration wizard

---

**Note:** These instructions apply to a non-clustered environment. If you are configuring Enterprise Vault in a Veritas Cluster Server or Windows Server Failover Clustering environment, see instead the appropriate clustering section in this manual.

---

You may be starting the configuration wizard after restarting your computer or after completing the Installation Program.

Follow the instructions below to run the configuration wizard on the first Enterprise Vault server in your site. When you are using the configuration wizard to configure Enterprise Vault on subsequent computers, refer to the online Help if you are unsure about how to proceed.

Before you run the configuration wizard, make sure that you have assigned the required SQL Server permissions and roles to the Vault Service account.

See [“About assigning permissions and roles in SQL databases”](#) on page 57.

If during the running of the configuration wizard you receive an error related to the configuring of the Enterprise Vault Monitoring database, complete the configuration wizard and then refer to the troubleshooting information for the Monitoring database.

See [“Troubleshooting configuration of the Enterprise Vault Monitoring database”](#) on page 151.

### To run the Enterprise Vault configuration wizard

**1 Click **Start > Programs > Enterprise Vault > Enterprise Vault Configuration**.**

The Configuration wizard starts. The first screen asks whether you want to create a new Enterprise Vault Directory database.

**2 Click **Yes** and then **Next**.**

The wizard asks you to select the language you want Enterprise Vault to use when populating the default settings in the Administration Console.

**3 Select the required language and then **Next**.**

The wizard asks for details of an account for Enterprise Vault services to use.

**4 Enter the details of the Vault Service account that you created earlier.**

See [“Creating the Vault Service account”](#) on page 52.

You must use the format *domain\_name\username* when you specify the account. Alternatively, browse for the Vault Service account.

Enter the password for the Vault Service account and confirm it.

**5 Click **Next**.**

A warning message is displayed if the account you are using does not have sufficient privileges to validate the password to the Vault Service account. Click **Yes** to continue.

A message tells you that the Vault Service account has been added to the local Administrators group. Click **OK** to close the message.

A second message notifies you that the account will be given the advanced user rights, **Log On As a Service**, **Debug programs**, and **Replace a process-level token**. Click **OK** to close the message.

The configuration wizard creates the Directory service and then the next screen asks for the location of the SQL Server that you want to use for the Directory database.

**6 Enter the location of the SQL Server that you want to use. Alternatively, click **Browse** to browse for the SQL Server. You can specify a SQL Server instance if required.**

**7 Click Next.**

The wizard shows the default locations for the Directory database files and transaction log.

**8 Change the locations if necessary.**

If you have specified that SQL Server is on a remote computer, the paths for the data file and transaction log file must be valid on that remote computer.

**9 Click Next.**

The wizard creates the Directory database. The next screen asks for the location of the SQL Server that you want to use for the Monitoring database.

**10 Enter the location of the SQL Server that you want to use. You can specify a SQL Server instance if required.**

**11 Click Next.**

The next screen shows default locations on the SQL server for the Monitoring database files and transaction log.

**12 Change the locations if necessary.**

If you have specified that SQL Server is on a remote computer, the paths for the data file and transaction log file must be valid on that remote computer.

Do not specify paths that are on the root of a file system, such as C: or C:\.

**13 Click Next.**

The wizard creates the Monitoring database.

The next screen asks for details of the new Enterprise Vault site.

**14 Enter a name and description for the new Enterprise Vault site.**

**15 Click Next.**

The next screen asks for a DNS alias for current computer.

The value you enter must be an unqualified DNS alias for this computer, for example, "evserver1". A fully-qualified DNS name (for example, "evserver1.mycompany.local") is not permitted.

If this is the first computer added to the site, the DNS alias entered will automatically be used as the vault site alias.

See ["Creating Enterprise Vault DNS aliases"](#) on page 58.

**16 Enter a DNS alias for the current computer and click Next.**

- 17 Click **Next** to add the computer to the Enterprise Vault site.

An information screen lists software that is installed on your computer. Based on this list, the wizard automatically selects Enterprise Vault services to add to your computer.
- 18 Click **Next**. The list shows the services that will be added to your computer.
- 19 Check the list of services. You can add or remove services as required, as follows:
  - To remove a service, click the service to select it and then click **Remove**.
  - To add a service, click **Add** and then select the service you require.
- 20 Click **Next**. An information page lists the services that the wizard will create.
- 21 Click **Next** to create the services.
- 22 The final screen of the wizard gives you the following options:
  - **Run the Enterprise Vault Getting Started Wizard**. Choose this option to set up archiving as quickly as possible. The wizard provides both express and custom options for maximum flexibility.
  - **Run the Enterprise Vault Administration Console**. Choose this option if you are already familiar with the Administration Console and familiar with setting up archiving.
  - **Just close this wizard**. Choose this option to close the Configuration Wizard. You can then use the Enterprise Vault Start menu options to run the Enterprise Vault Getting Started Wizard or the Administration Console.
- 23 Click **Finish** to exit from the configuration wizard.

---

**Note:** Remember that you can run the configuration wizard successfully only once on a computer. If you exit the configuration wizard after successfully configuring Enterprise Vault, you cannot run the wizard again. To do any further setup or management of the Enterprise Vault components, other than that related to Enterprise Vault Operations Manager or Enterprise Vault Reporting, you must use the Administration Console.

---

## Troubleshooting configuration of the Enterprise Vault Monitoring database

If while running the configuration wizard you receive errors indicating that the configuration of the Enterprise Vault Monitoring database has failed, complete

the configuration wizard and then run the Monitoring Configuration utility to configure the Monitoring database and the Monitoring agents manually.

For information on how to do this, see the following technical note on the Symantec Support Web site:

<http://www.symantec.com/docs/TECH50809>

The technical note also describes how to troubleshoot issues with Monitoring agents.



# Running the Enterprise Vault Getting Started wizard

This chapter includes the following topics:

- [What the Enterprise Vault Getting Started wizard does](#)
- [Preparing to run the Enterprise Vault Getting Started wizard](#)
- [Running the Enterprise Vault Getting Started wizard](#)
- [About the express and custom modes of the Enterprise Vault Getting Started wizard](#)
- [Planning for the Enterprise Vault Getting Started wizard](#)

## What the Enterprise Vault Getting Started wizard does

The Enterprise Vault Getting Started Wizard enables you to configure archiving as quickly as possible.

The wizard helps you do the following, as appropriate:

- Create archiving policies for Exchange Server, Domino, and File System Archiving.
- Set up storage locations.
- Configure indexing.
- Create retention categories.

You can choose to run sections of the wizard in express mode or in custom mode, as follows:

- In express mode, the wizard does not ask many questions. Instead, it applies as many default settings as possible. Later, you can use the Administration Console to make changes to the settings, if required.
- In custom mode, you have the flexibility to change the default settings.

---

**Note:** In express mode, the Getting Started wizard asks you to specify a local disk. The wizard then configures Enterprise Vault to use that disk for all storage. If you want to configure remote storage or a different local storage configuration, you must select custom mode for storage configuration.

---

## Preparing to run the Enterprise Vault Getting Started wizard

The Getting Started wizard checks the Enterprise Vault license keys to determine which options to present to you. Before you run the Getting Started wizard you must have installed your license keys.

See [“Overview of Enterprise Vault licensing”](#) on page 123.

You can run the Enterprise Vault Deployment Scanner to create a report that shows whether the Enterprise Vault prerequisite configuration is correct.

See the *Deployment Scanner* manual in the `Documentation` folder of the Enterprise Vault media.

**To run the Deployment Scanner from within the Enterprise Vault Getting Started wizard**

- ◆ On the **Before You Begin** page, click **Run Deployment Scanner**.

## Running the Enterprise Vault Getting Started wizard

You can run the Getting Started wizard immediately after you complete the Configuration wizard as part of a new installation of Enterprise Vault.

If you exit from the Getting Started wizard before the end of the wizard, you can run the wizard again. When you have successfully completed the Getting Started wizard, you can run it again later on the same computer but some options may not be available. You can also run the Getting Started wizard on other computers in the site.

### To run the Enterprise Vault Getting Started wizard

- ◆ Do one of the following:
  - Select the **Run the Enterprise Vault Getting Started Wizard** option on the last page of the Configuration wizard.
  - On the Windows **Start** menu, click **All Programs > Enterprise Vault > Enterprise Vault Getting Started Wizard**.

## About the express and custom modes of the Enterprise Vault Getting Started wizard

The Getting Started wizard enables you to select express mode or custom mode to perform the following:

- Indexing configuration
- Storage configuration
- Policy definition
- Exchange target configuration
- Domino target configuration
- File Server target configuration

In express mode, the wizard does not ask many questions. Instead, the wizard applies default settings so that you can configure Enterprise Vault as quickly as possible. Later, you can use the Administration Console to make changes to the settings, if required.

In custom mode, you can make any changes you require but it can take a long time to go through all the options. You may prefer to accept the default options and then make changes in the Administration Console.

There is a planning sheet that lists the Getting Started wizard's express-mode choices. You can use the sheet to record your own requirements and then later use the Administration Console to make the required changes.

See [“Planning for the Enterprise Vault Getting Started wizard”](#) on page 163.

## About indexing configuration with the Enterprise Vault Getting Started wizard

In express mode the Enterprise Vault Getting Started wizard automatically configures Indexing services to use local Storage services. The Getting Started

wizard does not create an Index Server group and does not add the current server to any existing Index Server group.

If you want to add the current server to an Index Server group, select **Custom** mode for **Indexing Configuration**. Custom mode enables you to create an Index Server group and to add the server to the Index Server group.

### Automatic indexing configuration in express mode

This section lists the settings that the Enterprise Vault Getting Started wizard automatically configures when you choose express mode for Indexing Configuration.

[Table 19-1](#) shows the Vault Store Group settings that the wizard creates in express mode.

**Table 19-1** Indexing settings in express mode

Item	Description
Indexing level	'Full'. Indexes the metadata and content of archived items.
Preview length	'128 characters'.
Create previews of attachments	'Off'. Enterprise Vault does not create previews of attachments. These previews cannot be viewed in Enterprise Vault 10.0.
Delete indexing subtasks after	'7 days'. Enterprise Vault deletes indexing subtasks after this amount of time has elapsed since the tasks finished. If all of a task's subtasks are deleted, the task is itself deleted.
Index server location in Administration Console	The Administration Console shows the new Index server under <b>Indexing</b> , in the <b>Ungrouped Servers</b> container.

## About storage configuration with the Enterprise Vault Getting Started wizard

In express mode, the Enterprise Vault Getting Started wizard configures all storage locally on the server.

See [“About setting up storage for Enterprise Vault archives”](#) on page 193.

The wizard sets up the following:

- A vault store group
- A vault store
- A vault store partition
- The Enterprise Vault server cache
- Indexes
- Shopping baskets (if a Shopping service is present)

Select the custom option for storage configuration if you want to do any of the following:

- Configure remote storage.
- Use a different SQL Server for vault stores from the one that you specified in the configuration program.
- Configure the structure of the vault store group's fingerprint database.

If you create an open vault store partition on the first server in the site, storage configuration may appear to be optional when you run the Enterprise Vault Getting Started wizard on subsequent servers in the site. However, you must configure an Enterprise Vault server cache on each Enterprise Vault server that has an Indexing service. Similarly, you must configure a shopping basket area on each server that has a Shopping service.

When a vault store partition is configured on another server, you can configure the Enterprise Vault server cache or shopping location in one of the following ways:

- Select **Indexing Configuration** and **Express** mode. This lets you set the location for both the Enterprise Vault server cache and the shopping location.
- Select **Storage Configuration** and **Custom** mode. This lets you set the server cache location.

## Storage configuration information you must supply in express mode

For the express storage configuration, you must specify which volume to use to store Enterprise Vault data. This information is used when Enterprise Vault creates the following storage locations:

- Cache location: <volume>\EVStorage\Cache
- Index locations: <volume>\EVStorage\Index
- Shopping location: <volume>\EVStorage\Cache\Shopping

**Note:** As antivirus software can potentially change data, it is important to exclude the cache and index locations in your virus checking application.

### Automatic storage configuration in express mode

This section lists the settings that the Enterprise Vault Getting Started wizard automatically configures when you choose express mode for Storage Configuration.

[Table 19-2](#) shows the Vault Store Group settings that the wizard creates in express mode.

**Table 19-2** Vault Store Group settings in express mode

Item	Description
Name	"Express Vault Store Group". If the name already exists a number is appended to make the name unique. For example, "Express Vault Store Group_1".
Description	The same as the Vault Store Group name.
SQL Server name for fingerprint database	The same SQL Server as was specified in the Configuration program for the Enterprise Vault Directory database.
Folder for all fingerprint database filegroups.	The default database folder for the Enterprise Vault Directory computer.
Folder for fingerprint database log	The default log folder for the Enterprise Vault Directory computer.

[Table 19-3](#) shows the Vault Store settings that the wizard creates in express mode.

**Table 19-3** Vault Store settings in express mode

Item	Description
Name	"Express Vault Store". If the name already exists a number is appended to make the name unique. For example, "Express Vault Store_1".
Description	The same as the vault store name.
SQL Server	The same SQL Server as was specified in the Configuration program for the Enterprise Vault Directory database.

**Table 19-3** Vault Store settings in express mode (*continued*)

Item	Description
Sharing	Set to 'Share within Vault Store'.
Remove safety copy	Set to 'After backup (immediate for Journaling)'.
Limit archive usage	Set to 'Use Site setting'.

[Table 19-4](#) shows the Vault Store partition settings that the wizard creates in express mode.

**Table 19-4** Vault Store partition settings in express mode

Item	Description
Name	"Express Vault Store Ptn1". If the name already exists a number is appended to make the name unique. For example, "Express Vault Ptn2".
Description	Partition of Vault Store [ <i>Vault_store_name</i> ]
State	Open.
Device type	NTFS volume.
Data deduplication	Destination device does not perform data deduplication.
Data compression	Destination device does not perform data compression.
Partition rollover	Not enabled.
How to check that items have been secured	Use the archive attribute.
Use collection files	Not enabled.
Migrate files	Not enabled.

## About policy definition with the Enterprise Vault Getting Started wizard

A policy defines which documents are to be archived and how they are to be archived.

Enterprise Vault creates policies automatically. The Getting Started wizard uses the default Enterprise Vault policies. The default policies in express mode and custom mode are the same.

You can use the Administration Console to modify all policy settings later, if required.

## About Exchange target configuration with the Enterprise Vault Getting Started wizard

If you choose to configure Exchange Server targets, the Getting Started wizard searches the network for instances of Exchange Server. You can then select the Exchange Server computers for which you want to configure archiving.

For the Exchange Server that you select you must do the following:

- Specify whether to configure mailbox archiving or journal archiving, or both.
- If you choose to configure mailbox archiving you must specify a system mailbox on that server that Enterprise Vault can use to log on.
- If you choose to configure journal archiving you must specify which journal mailboxes to archive and specify the journal archive to use for each mailbox. The wizard enables you to create new archives, if required.

[Table 19-5](#) shows the Exchange provisioning group settings that the wizard creates in express mode.

**Table 19-5** Exchange provisioning group settings in express mode

Item	Description
Provisioning group name	'Express Provisioning Group'. If you have selected 'Storage configuration' the provisioning group uses a new vault store that the wizard creates. If you have not selected 'Storage configuration', the wizard uses an existing vault store.
Provisioning group scope	'Whole Exchange Server organization'
Desktop policy	'Default Exchange Desktop Policy'
Mailbox policy	'Default Exchange Mailbox Policy'
PST migration policy	'Default Exchange PST migration Policy'
Default retention category	'Default Retention Category'



## About Domino target configuration with the Enterprise Vault Getting Started wizard

If you choose to configure Domino targets, the Getting Started wizard searches the network for Domino servers. You can then select the Domino servers for which you want to configure archiving. For each Domino server you can specify whether to configure mailbox archiving or journal archiving, or both. The Getting Started wizard then configures archiving appropriately.

For the express Domino configuration you must provide the following:

- ID file name. Enterprise Vault uses the ID file as the default ID file for all Enterprise Vault operations that require an ID file. The wizard lists Domino ID files that are in the Lotus Notes data folder, which by default is `C:\Program Files\lotus\notes\data`.  
You must place the ID file that you want to use in the data folder so that you can select it in the wizard.
- ID file password. The password for the ID file.
- The names of the Domino servers for which you want to configure mailbox archiving.
- The names of the Domino servers for which you want to configure journal archiving.
- The retention category to use when archiving from a Domino target.

[Table 19-6](#) shows the Domino provisioning group settings that the wizard creates in express mode.

**Table 19-6** Domino provisioning group settings in express mode

Item	Description
Provisioning group name	'Express Provisioning Group'. If the name already exists a number is appended to make the name unique. For example, "Express Provisioning Group_1".
Vault store	If you have selected 'Storage configuration' the provisioning group uses a new vault store that the wizard creates. If you have not selected 'Storage configuration', the wizard selects an existing vault store.
Provisioning group scope	'All Organizational Units'

**Table 19-6** Domino provisioning group settings in express mode *(continued)*

Item	Description
Desktop policy	'Default Domino Desktop Policy' If this policy is not available the wizard selects the first policy that is available, alphabetically.
Mailbox policy	'Default Domino Mailbox Policy'. If this policy is not available the wizard selects the first policy that is available, alphabetically.
Default retention category	'Default Retention Category'

**Table 19-7** Vault Store settings in express mode

Item	Description
Name	The Vault store that was created in the current run of the wizard, if any. If the wizard did not create a vault store the first vault store with an open partition is used.
Description	The same description as for the vault store name.
SQL Server	The same SQL Server as was specified in the Configuration program for the Enterprise Vault Directory database.
Sharing	Set to 'Share within Vault Store'.
Remove safety copy	Set to 'After backup (immediate for Journaling)'.
Limit archive usage	Set to 'Use Site setting'.

## About file target configuration with the Enterprise Vault Getting Started wizard

The Getting Started wizard enables you to configure archiving for the file servers that you specify.

You can install the Enterprise Vault FSA Agent on each Windows file server if required. You need to install the FSA agent if you require placeholder shortcuts, File Blocking, or need to obtain data for FSA Reporting.

---

**Note:** File Blocking and FSA Reporting are not supported on computers that run a Server Core installation of Windows. For details of supported operating systems see the Enterprise Vault *Compatibility Charts*, at <http://www.symantec.com/docs/TECH38537>.

---

## Planning for the Enterprise Vault Getting Started wizard

This section lists the choices that the Getting Started wizard makes automatically when you run it in Express mode. In Express mode, the Getting Started wizard does not ask many questions. Instead, the wizard applies as many default settings as possible. Later, you can use the Administration Console to make changes to the settings, if required.

[Table 19-8](#) shows the Indexing settings that the wizard creates in Express mode.

**Table 19-8** Indexing settings in Express mode

Item	Wizard's value	Administration Console possible values	Your choice
Indexing level	Full	Brief or Full	
Preview length	128 characters	128 or 1000	
Create previews of attachments	Off	Off or On	
Delete indexing subtasks after	7 days	Edit as required	

[Table 19-9](#) shows the Vault Store Group settings that the wizard creates in Express mode.

**Table 19-9** Vault Store Group settings in Express mode

Item	Wizard's value	Administration Console possible values	Your choice
Name	"Express Vault Store Group". If the name already exists a number is appended to make the name unique. For example, "Express Vault Store Group_1".	Edit as required.	
Description	The same as the Vault Store Group name.	Edit as required.	
SQL Server for fingerprint database	The same SQL Server as was specified in the Configuration program for the Enterprise Vault Directory database.	Cannot change.	
Folder for all fingerprint database filegroups	The default database folder for the Enterprise Vault Directory computer.	Cannot change.	
Folder for fingerprint database log	The default log folder for the Enterprise Vault Directory computer.	Cannot be changed.	

**Table 19-10** shows the Vault Store settings that the wizard creates in Express mode.

**Table 19-10** Vault Store settings in Express mode

Item	Wizard's value	Administration Console possible values	Your choice
Name	"Express Vault Store". If the name already exists a number is appended to make the name unique. For example, "Express Vault Store_1".	Edit as required.	
Description	The same as the vault store name.	Edit as required.	

**Table 19-10** Vault Store settings in Express mode (*continued*)

Item	Wizard's value	Administration Console possible values	Your choice
SQL Server	The same SQL Server as was specified in the Configuration program for the Enterprise Vault Directory database.	Can be changed to another SQL Server.	
Sharing	'Share within Vault Store'.	'No sharing'; 'Share within Vault Store'; 'Share within group'.	
Remove safety copies	'After backup (immediate for Journaling)'.	'Never'; 'After backup'; 'After backup (immediate for Journaling)'; 'Immediately after archive'.	
Limit archive usage	'Use Site setting'.	'Disabled'; 'Enabled'; 'Use Site setting'.	

[Table 19-11](#) shows the Vault Store partition settings that the wizard creates in Express mode.

**Table 19-11** Vault Store partition settings in Express mode

Item	Wizard's value	Administration Console possible values	Your choice
Name	"Express Vault Store Ptn1". If the name already exists a number is appended to make the name unique. For example, "Express Vault Ptn2".	Edit as required.	
Description	Partition of Vault Store [ <i>Vault_store_name</i> ]	Edit as required.	
State	Open.	'Closed'; 'Open'; 'Ready'.	
Device type	NTFS volume.	Cannot change.	

Table 19-11 Vault Store partition settings in Express mode (continued)

Item	Wizard's value	Administration Console possible values	Your choice
Data deduplication	Destination device does not perform data deduplication.	Device performs data deduplication; Device does not perform data deduplication.	
Data compression	Destination device does not perform data compression.	Device performs data compression; Device does not perform data compression.	
Partition rollover	Not enabled.	'Not Enabled'; 'Enabled based on volume'; 'Enabled based on time'; 'Enabled based on time or volume'.	
How to check that items have been secured	Use the archive attribute.	'Use the archive attribute'; 'Check for a trigger file'.	
Use collection files	Not enabled.	Use collection files; Do not use collection files.	
Migrate files	Not enabled.	Enabled; Not enabled.	

Table 19-12 shows the Exchange provisioning group settings that the wizard creates in Express mode.

**Table 19-12** Exchange provisioning group settings in Express mode

Item	Wizard's value	Administration Console possible values	Your choice
Provisioning group name	'Express Provisioning Group'. If you have selected 'Storage configuration' the provisioning group uses a new vault store that the wizard creates. If you have not selected 'Storage configuration', the wizard uses an existing vault store.	Edit as required.	
Provisioning group scope	'Whole Exchange Organization'	'Windows group'; 'Windows user'; 'Distribution group'; 'Organizational Unit'; 'LDAP query'; 'Whole Exchange Organization'.	
Desktop policy	'Default Exchange Desktop Policy'	Edit as required.	
Mailbox policy	'Default Exchange Mailbox Policy'	Edit as required.	
PST migration policy	'Default Exchange PST migration Policy'	Edit as required.	
Default retention category	'Default Retention Category'	Edit as required.	

[Table 19-13](#) shows the Domino provisioning group settings that the wizard creates in Express mode.

**Table 19-13** Domino provisioning group settings in Express mode

Item	Wizard's value	Administration Console possible values	Your choice
Provisioning group name	'Express Provisioning Group'. If the name already exists a number is appended to make the name unique. For example, "Express Provisioning Group_1".	Edit as required.	
Vault store	If you have selected 'Storage configuration' the provisioning group uses a new vault store that the wizard creates. If you have not selected 'Storage configuration', the wizard selects an existing vault store.	Edit as required.	
Provisioning group scope	'All Organizational Units'	'Directory Group'; 'Mailbox'; 'Organizational Unit'; 'Corporate Hierarchy'.	
Desktop policy	'Default Domino Desktop Policy'. If this policy is not available the wizard selects the first policy that is available, alphabetically.	Edit as required.	
Mailbox policy	'Default Domino Mailbox Policy'. If this policy is not available the wizard selects the first policy that is available, alphabetically.	Edit as required.	
Default retention category	'Default Retention Category'	Edit as required.	



# Configuring Enterprise Vault Operations Manager

This chapter includes the following topics:

- [When to run the Enterprise Vault Operations Manager Configuration utility](#)
- [Running the Enterprise Vault Operations Manager Configuration utility](#)
- [Accessing Enterprise Vault Operations Manager](#)
- [Troubleshooting Enterprise Vault Operations Manager](#)

## When to run the Enterprise Vault Operations Manager Configuration utility

Run the Enterprise Vault Operations Manager Configuration utility after installing Operations Manager on a server, but only after the server has been successfully configured using the Enterprise Vault configuration wizard.

You can rerun the Operations Manager Configuration utility if the configuration fails for some reason and you need to repeat it.

You can also rerun the utility if you need to change the details of the monitoring user account. In this case, be sure to rerun the utility on all servers on which Operations Manager is installed.

---

**Note:** You must also re-run the Operations Manager Configuration utility after you enable or disable the Windows policy setting for FIPS-compliant algorithms on a server on which the Operations Manager is configured.

---

## Running the Enterprise Vault Operations Manager Configuration utility

Run the Operations Manager Configuration utility to configure the Operations Manager for the first time or to update the configuration, for example to change the details of the monitoring user account.

To run the Enterprise Vault Operations Manager Configuration utility

- 1 Ensure you are logged in under the Vault Service account.
- 2 Click **Start > Programs > Enterprise Vault > Operations Manager Web App Configuration**.

The Operations Manager Configuration utility starts.

- 3 Provide the details of the monitoring user account you have created for Operations Manager to run under.

Enter the Active Directory domain, the user name, and the password for the monitoring user account.

- 4 Click **Configure** to run the utility.

The utility gives the account the required permissions, and adds the user to the EnterpriseVaultDirectory database as the monitoring user.

- 5 When the utility has finished, click **OK** on the displayed dialog to quit the utility.

---

**Note:** If you ran this utility to update the details of the monitoring user account, remember to rerun the utility on any other Enterprise Vault server with Operations Manager installed.

---

You can now try accessing Operations Manager to confirm that it has been successfully configured.

## Accessing Enterprise Vault Operations Manager

If you have installed the Enterprise Vault Operations Manager Web application on at least one Enterprise Vault server in an Enterprise Vault site, you can use it to monitor the site's Enterprise Vault servers.

After configuring Operations Manager, try accessing it to confirm the configuration has been successful.

### To access Enterprise Vault Operations Manager

- 1 Enter the following URL in Internet Explorer:

`http://host_ipaddress/MonitoringWebApp/default.aspx`

where *host\_ipaddress* is the IP address of the computer hosting an Enterprise Vault server on which the Enterprise Vault Operations Manager Web application feature is installed.

Alternatively, if you are accessing Operations Manager from the computer on which it is installed, you can use the following URL, which does not require the next step:

`http://localhost/MonitoringWebApp/default.aspx`

- 2 In the **Connect to <IP Address>** dialog box, enter the user name and password of an account in the host computer's domain (use the format *domain\account*). Then click **OK**.

---

**Note:** Any user other than the Vault Service account must be assigned to a suitable role to access Operations Manager. Users can view only the tabs and tables in Operations Manager that are applicable to the role to which they are assigned.

See "Roles-based administration" in the *Administrator's Guide*.

---

If the user credentials are valid, Operations Manager displays its Site Summary page.

## Troubleshooting Enterprise Vault Operations Manager

If you see an error page when attempting to access Enterprise Vault Operations Manager, ensure that you have done the following and then try to access the application again:

- Confirm that you have satisfied all the preinstallation steps.  
See "[About additional requirements for Operations Manager](#)" on page 61.
- Check that IIS is not locked down.
- Ensure that Integrated Windows Authentication is enabled for the default Web site in IIS, and then restart IIS.

If this does not solve the problem, see the following technical note on the Symantec Support Web site:

<http://www.symantec.com/docs/TECH51287>

The technical note provides detailed troubleshooting information related to installing and using Operations Manager.

# Configuring the Discovery Search Service

This chapter includes the following topics:

- [Running the Discovery Search Service Configuration utility](#)
- [Manually configuring a request endpoint for the Discovery Search Service](#)
- [Manually configuring a result endpoint for the Discovery Search Service](#)
- [Setting up the Discovery Search Service web applications to require secure \(HTTPS\) connections](#)

## Running the Discovery Search Service Configuration utility

Run the Discovery Search Service Configuration utility to configure the service for the first time or update an existing configuration. You use the configuration utility to do the following:

- Create a SQL Server database in which to store search metadata information. This information includes the Enterprise Vault sites, index services, vault stores, vaults, and index volumes in which you may conduct searches, and details of those searches. It also includes search results information, such as the number of hits for an index volume and the location of the search results.
- Configure *request endpoints* to which your client search application submits all of its search requests.
- If you move the Discovery Search Service database from one SQL Server computer to another, notify the Enterprise Vault Directory database of the change that you have made.

- Nominate a folder on each of your Enterprise Vault index servers in which to store the results of your searches in XML format.

You monitor the activities of the Discovery Search Service by using the Enterprise Vault Operations Manager. If you have yet to configure Operations Manager, it is best to do so before you configure the Discovery Search Service.

#### To run the Discovery Search Service Configuration utility

- 1 Log on as the Vault Service account to the Enterprise Vault server where you have installed the Discovery Search Service components.
- 2 Do one of the following:
  - In the left pane of the Vault Administration Console, right-click **Discovery Search Service** and then click **Configure**.
  - In Windows Explorer, navigate to the Enterprise Vault program folder (for example, C:\Program Files (x86)\Enterprise Vault) and then double-click `DSSConfiguration.exe`.

The Discovery Search Service Configuration utility starts.

- 3 When the first page of the utility appears, click **Next** to proceed to the next page.
- 4 Choose the operation that you want to perform, and then click **Next**.

The online Help that accompanies the utility provides instructions on how to complete each step.

## Manually configuring a request endpoint for the Discovery Search Service

The Discovery Search Service configuration utility can set up a request endpoint automatically, provided that you choose to use the default port number for the endpoint. If you prefer not to do this, you must configure the endpoint manually.

#### To configure a request endpoint for Discovery Search Service manually

- 1 Start Internet Information Services (IIS) Manager.
- 2 Perform the following steps to create an application pool for the request endpoint:
  - In the left pane of IIS Manager, expand the server node and then click **Application Pools**.
  - In the **Actions** pane at the right of the **Application Pools** page, click **Add Application Pool**.

- Set the following in the **Add Application Pool** dialog box, and then click **OK**.

<b>Name</b>	EVDSSRequestAppPool
<b>.NET Framework version</b>	.NET Framework v2.0. <i>nnnnn</i>
<b>Managed pipeline mode</b>	Integrated
<b>Start application pool immediately</b>	Checked

- 3 In the left pane of IIS Manager, expand the server node and then expand the **Sites** node.
- 4 Right-click the **Default Web Site** node and then click **Add Application**.
- 5 Set the following in the **Add Application** dialog box, and then click **OK**.

<b>Alias</b>	DSSRequestEndPoint
<b>Application pool</b>	EVDSSRequestAppPool
<b>Physical path</b>	<i>DSS_installation_folder</i> \RequestEndPoint. For example: C:\Program Files (x86)\Enterprise Vault\RequestEndPoint

- 6 In the left pane of IIS Manager, right-click the **DSSRequestEndPoint** node and then click **Switch to Features View**.
- 7 In the **Features View** pane, double-click **Authentication**.
- 8 In the **Authentication** page, make sure that all the authentication modes except **Anonymous Authentication** are disabled. You must enable **Anonymous Authentication**.
- 9 Switch back to content view for the DSSRequestEndPoint node.
- 10 In the **/DSSRequestEndPoint Content** page, right-click `RequestService.svc` and then click **Browse**.
- 11 Make sure that no errors occur and that you can launch the service successfully.

# Manually configuring a result endpoint for the Discovery Search Service

Just as you can manually configure a request endpoint, you can also manually configure a result endpoint.

To configure the result endpoint for Discovery Search Service manually

- 1
- Start Internet Information Services (IIS) Manager.
- 2
- Perform the following steps to create an application pool for the request endpoint:
  - In the left pane of IIS Manager, expand the server node and then click **Application Pools**.
  - In the **Actions** pane at the right of the **Application Pools** page, click **Add Application Pool**.
  - Set the following in the **Add Application Pool** dialog box, and then click **OK**.

Name:	EVDSSResultAppPool
.NET Framework version:	.NET Framework v2.0. <i>nnnnn</i>
Managed pipeline mode:	Integrated
Start application pool immediately:	Checked

- 3
- In the left pane of IIS Manager, expand the server node and then expand the **Sites** node.
- 4
- Right-click the **Default Web Site** node and then click **Add Application**.
- 5
- Set the following in the **Add Application** dialog box, and then click **OK**.

Alias:	DSSResultEndPoint
Application pool:	EVDSSResultAppPool
Physical path:	<i>DSS_installation_folder</i> \ResultEndpoint. For example: C:\Program Files (x86)\Enterprise Vault\ResultEndpoint

- 6
- In the left pane of IIS Manager, right-click the **DSSResultEndPoint** node and then click **Switch to Features View**.



- 7 In the **Features View** pane, double-click **Authentication**.
- 8 In the **Authentication** page, make sure that all the authentication modes except **Anonymous Authentication** are disabled. You must enable **Anonymous Authentication**.
- 9 Switch back to content view for the DSSResultEndPoint node.
- 10 In the **/DSSResultEndPoint Content** page, right-click `ResultService.svc` and then click **Browse**.
- 11 Make sure that no errors occur and that you can launch the service successfully.

## Setting up the Discovery Search Service web applications to require secure (HTTPS) connections

You can set up the Request Endpoint and Result Endpoint web applications to require communications over a secure (HTTPS) connection.

### To set up the Request Endpoint web application to require secure (HTTPS) connections

- 1 In the left pane of the Enterprise Vault Administration Console, expand the tree view until the **Discovery Search Service** node is visible.
- 2 Click **Discovery Search Service**.
- 3 In the right pane, right-click **Request Endpoint** and then click **Configure**.
- 4 Follow the on-screen instructions to enable SSL and set the appropriate port.
- 5 Use the facilities in Internet Information Services (IIS) Manager to enable SSL for the DSSRequestEndpoint web application. This application is under the Default Web Site.

See the IIS documentation for guidelines on how to enable SSL.

- 6 In Windows Explorer, browse to the folder `EV_installation_folder\RequestEndpoint` (typically `C:\Program Files (x86)\Enterprise Vault\RequestEndpoint`).
- 7 Open the `Web.config` file in a plain-text editor such as Windows Notepad.
- 8 Make the following changes to the file:
  - Find the following key, and change the `REPBindingWithoutSSL` value to `REPBindingWithSSL`:

```
<service behaviorConfiguration="SearchBehavior"
  name="Symantec.EnterpriseVault.DSS.RequestEndpoint.RequestService">
  <endpoint address="" binding="wsHttpBinding"
    bindingConfiguration="REPBindingWithoutSSL"
```

- Find the following key, and change the `REPMonitoringBindingWithoutSSL` value to `REPMonitoringBindingWithSSL`:

```
<service behaviorConfiguration="MonitoringBehavior"
  name="Symantec.EnterpriseVault.DSS.RequestEndpoint.MonitoringService">
  <endpoint address="" binding="wsHttpBinding"
    bindingConfiguration="REPMonitoringBindingWithoutSSL"
```

- Find the following keys, and change both of the `httpGetEnabled` attributes to `httpsGetEnabled`:

```
<behavior name="SearchBehavior">
  <serviceMetadata httpGetEnabled="true"/>
  ...
<behavior name="MonitoringBehavior">
  <serviceMetadata httpGetEnabled="true"/>
```

#### To set up the Result Endpoint web application to require secure (HTTPS) connections

- 1 In the left pane of the Enterprise Vault Administration Console, expand the tree view until the **Discovery Search Service** node is visible.
- 2 Right-click **Discovery Search Service** and then click **Properties**.
- 3 Click the **Settings** tab to bring it to the front.
- 4 Set **Enable SSL on Result Endpoint** to **On**, and **Result Endpoint port** to the appropriate port.
- 5 Use the facilities in Internet Information Services (IIS) Manager to enable SSL for the DSSResultEndpoint web application. This application is under the Default Web Site.

See the IIS documentation for guidelines on how to enable SSL.

- 6 In Windows Explorer, browse to the folder `EV_installation_folder\ResultEndpoint` (typically `C:\Program Files (x86)\Enterprise Vault\ResultEndpoint`).
- 7 Open the `Web.config` file in a plain-text editor such as Windows Notepad.
- 8 Make the following changes to the file:

- Find the following key, and change the `ResultBindingWithoutSSL` value to `ResultBindingWithSSL`:

```
<service behaviorConfiguration="RestBehaviour"
  name="Symantec.EnterpriseVault.DSS.ResultEndpoint.ResultService">
  <endpoint address="" behaviorConfiguration="webHttp"
    binding="webHttpBinding"
    bindingConfiguration="ResultBindingWithoutSSL"
```

- Find the following key, and change the `httpGetEnabled` attribute to `httpsGetEnabled`:

```
<behavior name="RestBehaviour">
  <serviceMetadata httpGetEnabled="true"/>
```



## Initial Enterprise Vault setup

- [Chapter 22. Initial Enterprise Vault setup](#)
- [Chapter 23. Setting up storage](#)
- [Chapter 24. Adding index locations](#)
- [Chapter 25. Setting up Index Server groups](#)
- [Chapter 26. Reviewing the default settings for the site](#)



# Initial Enterprise Vault setup

This chapter includes the following topics:

- [License keys](#)
- [Using the Enterprise Vault Administration Console](#)
- [Adding core Enterprise Vault services with the Administration Console](#)
- [Creating Enterprise Vault retention categories](#)
- [Performance issues when an Enterprise Vault server has no Internet connection](#)

## License keys

At the end of the configuration wizard you were asked to start the Enterprise Vault services. These services will not start until you have installed the appropriate license keys.

## Using the Enterprise Vault Administration Console

The Enterprise Vault Administration Console is a snap-in for Microsoft Management Console (MMC). MMC provides a common framework for administrative tools that gives them all a similar look and feel. It is possible to customize an MMC snap-in so that it includes the exact functionality needed by a particular administrator.

The Administration Console enables you to manage the Enterprise Vault sites, services, archiving tasks, policies and targets.

If people are using separate administration consoles at the same time to make changes to Enterprise Vault, the changes made by one person are not necessarily shown in the other consoles. You are recommended to avoid using multiple consoles simultaneously when managing Enterprise Vault. If you do use multiple consoles, press F5 to refresh the Administration Console display before you make any changes.

## Starting the Enterprise Vault Administration Console

To use the Administration Console initially, you should log in as the Vault Service account. You can then assign roles to other administrators, to enable them to perform the required Enterprise Vault management tasks using the Administration Console.

### To start the Enterprise Vault Administration Console

- 1 On the Windows **Start** menu, click **Programs > Enterprise Vault > Administration Console**.
- 2 On the **Connect** dialog, enter the name or IP address of any server in the Enterprise Vault site that is running the Directory service. You can enter the IP address in IPv4 or IPv6 format.

MMC starts and loads the Administration Console snap-in.

The first time the Administration Console is used there is a dialog box that shows the new features in this release. There may also be a dialog box that enables you to opt in to Enterprise Vault Product Improvement. The Product Improvement feature in Enterprise Vault helps Symantec to improve the quality of Enterprise Vault.

The left pane of the main Administration Console shows you the hierarchy of components that make up your Enterprise Vault site. The right pane shows you the contents of whatever you select in the hierarchy.

### To get help

- ◆ Do one of the following:
  - To access online help for Enterprise Vault, click **Help > Help on Enterprise Vault**. This online help includes Enterprise Vault manuals.
  - To find out more about MMC, click **Help > Help on MMC** in the MMC window. The MMC help appears.

### To refresh the screen

- ◆ Press F5 to force a refresh at any time.



## About administration roles in the Enterprise Vault Administration Console

Enterprise Vault provides the following mechanisms that you can use to control the access administrators have to the Administration Console:

- **Roles-based administration.** Many administrative tasks do not require all the permissions that are associated with the Vault Service account. Roles-based administration enables you to provide individual Enterprise Vault administrators with exactly the permissions required to perform their individual administrative tasks.

You can assign individuals or groups to roles that match their responsibilities and they are then able to perform the tasks that are included in those roles. Because the permissions are associated with roles, rather than with individual administrators, you can control the role permissions without having to edit the permissions for each administrator.

- **Admin permissions.** You can grant or deny access to the following containers in the Administration Console tree:
  - File Server
  - Exchange Server
  - SharePoint Virtual Server
  - Enterprise Vault Server

You can control access by assigning roles, or by using admin permissions, or both.

When you install Enterprise Vault for the first time, only the Vault Service account can access the Administration Console. You can restrict the tasks administrators can perform by assigning roles and you can further restrict access by using admin permissions to restrict administrators to managing specific Administration Console containers.

Roles-based administration enables you to use Microsoft Authorization Manager to configure the various administrator roles. All such configuration is performed using the Vault Service account.

See [“Roles-based administration in Enterprise Vault”](#) on page 43.

For instructions on setting up roles-based administration, see the *Administrator's Guide*.

## Adding core Enterprise Vault services with the Administration Console

Use the Administration Console to add the following core Enterprise Vault services:

- Indexing service
- Storage service
- Shopping service
- Task Controller service

When creating services, you may be prompted for the password of the Vault Service account.

Ensure that the index storage location is on an accessible device to which the Vault Service account has write access.

When you add archiving tasks, such as Exchange Mailbox or File System archiving tasks, they run under the control of the Task Controller service. If you stop the Task Controller service, all tasks running under the control of this service also stop.

The same instructions can be repeated to add each of these services.

### To add a core Enterprise Vault service with the Administration Console

- 1 In the left pane, expand the Enterprise Vault site hierarchy until the **Enterprise Vault Servers** container is visible.
- 2 Expand the **Enterprise Vault Servers** container.
- 3 Expand the computer to which you want to add a service.
- 4 Right-click **Services** and, on the shortcut menu, click **New** and then **Service**.  
The **Add Service** dialog box appears, listing the services you can add.
- 5 Click the service that you want to add.
- 6 Click **Add**.

## Creating Enterprise Vault retention categories

You may have decided during planning that you wanted more retention categories than the ones predefined in Enterprise Vault. If this is the case, you must create your own retention categories. Alternatively, you can edit the predefined retention categories to suit your needs.

If you configure Enterprise Vault to archive from Exchange managed folders, it can automatically synchronize managed content settings to managed folder retention categories. Enterprise Vault creates managed folder retention categories automatically. For more information, see the *Administrator's Guide*.

#### To create an Enterprise Vault retention category

- 1 In the left pane of the Administration Console, expand Enterprise Vault, then **Directory**, then the site name, and then **Policies**.
- 2 Right-click **Retention Categories**.
- 3 From the shortcut menu, select **New > Retention Category**.  
The **New Retention Category** wizard starts.
- 4 Work through the wizard. Click **Help** on any of the wizard screens if you need more information.

## About the properties of Enterprise Vault retention categories

By assigning an Enterprise Vault retention category to items at the time they are archived, it is possible to categorize stored items. This categorization makes it easier to retrieve items because it is possible to search by category.

A retention category also specifies the minimum amount of time after its last modification date that an item must be retained. This length of time is the retention period. For mail messages, the retention period is the time since the message was received. For documents, it is the time since the document was last modified.

With Exchange Server archiving, users can select retention categories for mailbox folders or items so that, when archiving occurs, items are stored with the appropriate retention category.

If you later modify a retention category, the changes are retrospective. For example, if you have a retention category called Customer Accounts with a retention period of 5 years and you change the retention period to 10 years, items that have been already archived with the Customer Accounts retention category are retained for a minimum of 10 years.

Enterprise Vault can automatically delete expired items. See the *Administrator's Guide* for more details.

---

**Note:** You cannot delete retention categories. You can rename them as required and you can hide them from users.

---

A retention category has the following properties:

Name	<p>You can modify the retention category name as needed. The new name is used immediately, so users of the Web access application must search using the new name to find items stored with this retention category.</p>
Description	<p>(Required) This is a description of the retention category. Make sure that the description you give here is meaningful to users.</p>
Retention period	<p>This is the minimum amount of time to retain an item that has been archived using this retention category.</p> <p>You can choose whether the period runs from the date the item was last modified or from the date that the item was archived.</p> <p>If you choose to archive by last modified date, Enterprise Vault calculates the date as follows:</p> <ul style="list-style-type: none"> <li>■ For mail messages, the date is the date that the message was received.</li> <li>■ For documents, the date is the date the document was last modified.</li> </ul>
Retain items forever	<p>Select this if you want items never to expire.</p> <p>If you plan to store items indefinitely on a WORM storage device, then ensure that the retention settings on the device are correctly configured.</p> <p>See <a href="#">“Preparing WORM storage devices”</a> on page 31.</p>
Prevent deletion of archived items in this category	<p>Select this to prevent users deleting items that have been archived using this retention category. This protection applies during the retention period, and also after the retention period has expired. In other words, while this option remains selected, users can never delete items that have been stored using this retention category.</p> <p>This setting affects only those items that are stored in archives. It does not affect items that are still on archiving target servers.</p>

Hide this category from users	<p>Check this to prevent users using this category when archiving new items. The category is still available to users when they are searching for items that have already been archived.</p> <p>Enterprise Vault does not allow the site default retention category to be hidden from users. If you hide the site default retention category, Enterprise Vault automatically chooses another retention category and makes it the site default.</p>
Lock this Retention Category	To prevent unintentional changes, check this to lock all the retention category settings.
Base expiry on	<p>Select one of the following:</p> <ul style="list-style-type: none"> <li>■ Inherit from Site settings. The retention period is inherited from the Site default retention category settings.</li> <li>■ Modified date. The retention period is based on the date when the item was last modified. For mail messages, a retention period that is based on the Modified date is the time since the message was sent or received. For documents, it is the time since the document was last modified.</li> <li>■ Archived date. The retention period is the time since the item was archived.</li> </ul>
Administrative Note	For your notes. Edit this text as necessary. This text is visible only to Enterprise Vault administrators.

## Performance issues when an Enterprise Vault server has no Internet connection

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 with a VeriSign certificate. 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 install Enterprise Vault.

- When you start the Administration Console.
- When users access Web applications such as Archive Explorer or the integrated search.

If you use Enterprise Vault on a server without an Internet connection, you can prevent the Windows check for digital certificates that have been revoked. You can use the following methods to prevent certificate revocation checks:

- You can use `.config` files to prevent the checks for individual processes.
- You can use Internet Explorer settings to prevent the checks for all processes that run under a particular account. If you choose this method, you must change the Internet Explorer settings on each Enterprise Vault server for every account that runs an Enterprise Vault service.

#### To turn off certificate revocation checking Enterprise Vault per process

- 1 Use a plain-text editor such as Windows Notepad to create a configuration file that contains the following lines:

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

- 2 Save the file as `No_Connection.config` in any convenient location, such as `C:\`.

- 3 Copy the `No_Connection.config` file to the following names and locations:

- To file `w3wp.exe.config` in the same folder as `w3wp.exe`. For example:  
`%windir%\system32\inetsrv`  
 This turns off checks by all web applications on the server.
- On a 32-bit Windows system: To file `mmc.exe.config` in the same folder as `mmc.exe`.  
 For example: `%windir%\System32\mmc.exe.config`  
 On a 64-bit Windows system: To file `mmc.exe.config` in the same folder as `mmc.exe`. For example:  
`%windir%\SysWOW64\mmc.exe.config`  
 This turns off checks by the Enterprise Vault System Status MMC snapin.
- To file `RegAsm.exe.config` in the same folder as `RegAsm.exe`. For example:  
`%windir%\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe.config`

This turns off checks by the self-registration routines in the Enterprise Vault installer.

- To file `InstallUtil.exe.config` in the same folder as `InstallUtil.exe`.  
For example:

`%windir%\Microsoft.NET\Framework\v2.0.50727\InstallUtil.exe.config`

This turns off checks by the self-installation routines in the Enterprise Vault installer.

If the Enterprise Vault server gains Internet access in the future, delete the files to enable signature checking again.

For more information on the `generatePublisherEvidence` element, see the following article on the Microsoft Web site:

<http://msdn.microsoft.com/en-us/library/bb629393.aspx>

There is an alternative method that you can use to turn off certificate revocation checking. This alternative method is specific to the Vault Service account and any other accounts that you use to run Enterprise Vault services. There is no requirement for you to use this alternative method.

#### **To turn off certificate revocation checking for a particular user account**

- 1 Log on to the Enterprise Vault server as an account that runs Enterprise Vault services on that server. This account is typically the Vault Service account.
- 2 In Windows Control Panel, double-click **Internet Options**.
- 3 In the **Internet Properties** dialog box, click the **Advanced** tab.
- 4 In the **Security** section, uncheck **Check for publisher's certificate revocation**.
- 5 Click **OK**.

**Performance issues when an Enterprise Vault server has no Internet connection**



# Setting up storage

This chapter includes the following topics:

- [About setting up storage for Enterprise Vault archives](#)
- [About Enterprise Vault single instance storage](#)
- [Developing a suitable sharing regime for Enterprise Vault single instance storage](#)
- [Creating vault store groups](#)
- [About creating vault stores](#)
- [Creating vault store partitions](#)
- [Configuring sharing for a vault store group](#)

## About setting up storage for Enterprise Vault archives

Before you set up storage for your archives, consider whether you want to use Enterprise Vault's optimized single instance storage. Single instance storage can greatly reduce your storage requirements by sharing the common parts of archived items. However, it can increase the network traffic between the Enterprise Vault servers and the storage devices that host the partitions.

If you intend to use single instance storage, you need to decide on a sharing regime that is appropriate for your requirements and compatible with your network connection speeds.

- See [“About Enterprise Vault single instance storage”](#) on page 194.
- See [“Developing a suitable sharing regime for Enterprise Vault single instance storage”](#) on page 201.

---

**Note:** A new vault store group is configured by default to use Enterprise Vault single instance storage. The only exception is the Default Upgrade Group that Enterprise Vault created if you previously upgraded to Enterprise Vault 8.0.

---

For Enterprise Vault to be able to create archives, you must create a vault store group that contains a vault store and at least one vault store partition:

- A vault store group is a container for vault stores. It defines the outer boundary for sharing items in Enterprise Vault single instance storage.  
See [“Creating vault store groups”](#) on page 203.
- A vault store is a logical entity to which an Enterprise Vault Storage service archives items. Each vault store has its own vault store database. The vault store database holds information about the archives in the vault store and all the items that are stored in each archive.  
See [“About creating vault stores”](#) on page 204.
- A vault store partition is a physical location where Enterprise Vault stores archived data. Each vault store must contain at least one partition. Partitions can be placed on different physical disks and on various types of storage medium. As the data in a vault store grows, you can create more partitions to provide additional capacity. You can configure the partitions so that archiving rolls over from one partition to another when certain criteria are met.  
See [“Creating vault store partitions”](#) on page 208.

To configure Enterprise Vault single instance storage for a vault store group, you must run the Configure Sharing wizard on the group.

See [“Configuring sharing for a vault store group”](#) on page 215.

## About Enterprise Vault single instance storage

Enterprise Vault's optimized single instance storage can provide a significant reduction in the storage space that is required for archived items. Enterprise Vault identifies the shareable parts (SIS parts) of an item, such as a message attachment or the contents of a document. It stores each SIS part separately, and only once within a sharing boundary. A sharing boundary can include one or more vault stores within a vault store group. When Enterprise Vault identifies a SIS part that it has already stored in the target vault store's sharing boundary, it references the stored SIS part file instead of archiving the SIS part again.

Enterprise Vault applies a minimum size threshold for SIS parts. The size threshold enables Enterprise Vault to balance the likely storage savings against the resources that are required to create, archive, and retrieve the SIS parts.

Enterprise Vault single instance storage can save storage space in a number of ways:

- Enterprise Vault shares the SIS parts between all the vault stores within a sharing boundary. For example, if you use separate vault stores for journaling and mailbox archiving, Enterprise Vault can share the SIS parts between the vault stores.
- If a number of separate messages with the same attachment are sent to multiple recipients, Enterprise Vault stores the attachment only once within a sharing boundary.
- Enterprise Vault identifies a SIS part from the content, not the file name. If two messages both have the same file attachment, Enterprise Vault can share the attachments, even if they have different file names.
- Enterprise Vault can share the identical SIS parts that result from different types of archiving, such as an Exchange message attachment that is also stored as a file on a file server.

A new vault store uses single instance storage by default, and shares only the SIS parts of items that are archived within itself. You can run the Configure Sharing wizard on a vault store group to extend sharing between vault stores, or to turn off Enterprise Vault single instance storage if you want.

---

**Note:** Enterprise Vault single instance storage is not performed when items are stored to partitions that are hosted on EMC Centera devices. Enterprise Vault provides a separate device-level sharing option to take advantage of the sharing capabilities of EMC Centera devices.

See [“About EMC Centera device-level sharing”](#) on page 200.

---

For more information on Enterprise Vault single instance storage, see the following topics:

- See [“About sharing levels and sharing boundaries”](#) on page 196.
- See [“How Enterprise Vault single instance storage works”](#) on page 198.
- See [“About the fingerprint database”](#) on page 199.
- See [“Deletion of SIS parts”](#) on page 199.
- See [“Requirements for Enterprise Vault single instance storage”](#) on page 200.
- See [“Developing a suitable sharing regime for Enterprise Vault single instance storage”](#) on page 201.

## About sharing levels and sharing boundaries

When you configure sharing for a vault store group, you set a sharing level for each vault store in the group. The sharing levels determine the boundaries for single instance storage sharing in the group.

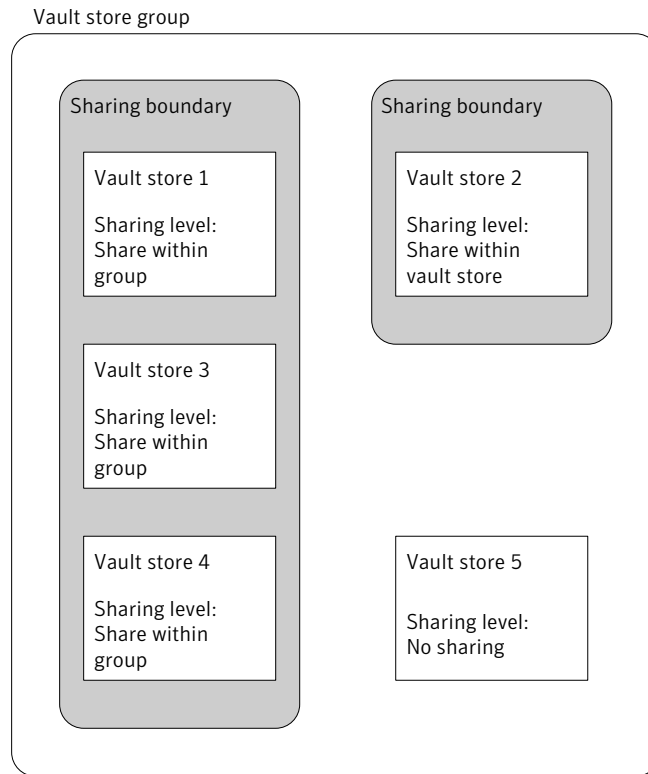
**Table 23-1** Vault store sharing levels

Vault store's sharing level	Effect on sharing
Share within group	The vault store shares SIS parts with all the other vault stores in the vault store group that have this sharing level.
Share within vault store	The vault store shares SIS parts only within itself.
No sharing	Enterprise Vault does not perform single instance storage for this vault store.

A vault store group can therefore contain one or more sharing boundaries. Each sharing boundary contains one or more vault stores that share the SIS parts that result from Enterprise Vault single instance storage.

[Figure 23-1](#) shows an example vault store group that contains five vault stores:

**Figure 23-1** Sharing boundaries in a vault store group



- Vault stores 1, 3, and 4 all have the sharing level "Share within group". These vault stores are within the same sharing boundary. Enterprise Vault shares SIS parts across the three vault stores for the items that it archives to these vault stores.
- Vault store 2 has the sharing level "Share within vault store", so it has its own sharing boundary. Enterprise Vault shares SIS parts within the vault store for the items that it archives to this vault store.
- Vault store 5 has the sharing level "No sharing". The vault store is not included in any sharing boundary. Enterprise Vault does not perform Enterprise Vault single instance storage on the items that it archives to this vault store.

Note that a vault store group can have only one sharing boundary that contains multiple vault stores. For example, in [Figure 23-1](#), you cannot configure two new vault stores to share SIS parts across each other and not with the existing vault stores. You can instead create the new vault stores in another vault store group.

Enterprise Vault assigns a sharing level of "Share within vault store" to new vault stores.

To change the sharing level for a vault store, run the Configure Sharing wizard on the vault store group after you have created a partition for the vault store.

## How Enterprise Vault single instance storage works

Enterprise Vault archives an item using single instance storage if both of the following conditions apply:

- The target vault store has a sharing level of "Share within vault store" or "Share within group".
- The current open partition is not hosted on an EMC Centera device.

Enterprise Vault archives an item for single instance storage as follows:

- It identifies the parts of an item that are suitable for sharing, such as large message attachments. These parts are referred to as SIS parts. Enterprise Vault uses a minimum size threshold for SIS parts, to balance the likely storage savings against the resources that are required to create, archive, and retrieve them.
- It generates a digital fingerprint to each SIS part. The fingerprint is a cryptographic, hash-based identifier that is determined by the contents of the SIS part.
- For each SIS part, Enterprise Vault accesses the vault store group's fingerprint database to determine whether a SIS part with the same fingerprint is already stored within the vault store's sharing boundary. A SIS part with the same fingerprint indicates an identical SIS part.
  - If an identical SIS part is not already stored within the sharing boundary, Enterprise Vault stores the SIS part and saves the SIS part's fingerprint information in the fingerprint database.
  - If an identical SIS part is already stored within the sharing boundary, Enterprise Vault references the stored SIS part. It does not store the SIS part again.
- It stores the remainder of the item (the item minus any SIS parts) as the residual saveset file. The residual saveset file holds Enterprise Vault metadata about the item and unique information about it, such as the file name if it is a document or attachment, and follow up flags if it is a message.

When Enterprise Vault receives a request to restore an archived item, it reconstitutes the item from the item's residual saveset file and SIS part files.

If an item's target vault store has a sharing level of "no sharing" or the target partition is hosted on an EMC Centera device, then Enterprise Vault does not use single instance storage. It archives the item with its Enterprise Vault metadata as a single saveset file.

## About the fingerprint database

A vault store group's fingerprint database holds information about each SIS part that is stored in the vault store group. The information includes the SIS part's digital fingerprint, the name of the partition in which the SIS part is stored, and in which sharing boundary the SIS part is shared.

When you create a vault store group, Enterprise Vault creates a fingerprint database for that vault store group.

---

**Note:** To add or change locations after the fingerprint database is configured is a SQL Server administration task. See your Microsoft SQL Server documentation for details.

---

The New Vault Store Group wizard provides the following options for configuring the fingerprint database's SQL filegroups:

- A basic configuration, where Enterprise Vault locates the primary filegroup and all the non-primary filegroups on one device.
- An option to configure additional locations for the 32 non-primary filegroups. The non-primary filegroups store fingerprint information for archived items and so they can grow rapidly when you use single instance storage. For best performance you need to spread the non-primary filegroups across multiple locations.

For optimal performance, do as follows:

- Select the option to configure additional locations for the non-primary filegroups.
- Specify as many locations as possible for the non-primary filegroups on the SQL Server, up to the maximum of 32.
- Specify a separate device for each location. If you specify more than one location on the same device there is no performance benefit.

## Deletion of SIS parts

The fingerprint database for each vault store group records the number of references to each SIS part that are present in the group's vault stores.

As users delete archived items, the number of references to a SIS part decreases. On the deletion of an item, if the number of references to a SIS part falls to 0 then Enterprise Vault checks whether the group's vault stores contain any references to the SIS part. Provided that no references remain, Enterprise Vault deletes the SIS part. If any references remain, Enterprise Vault retains the SIS part and generates an error in the Enterprise Vault event log.

---

**Note:** If you use collections, unreferenced SIS parts may remain in a CAB file for some time before they are deleted.

See [“About collections and migration”](#) on page 210.

---

## Requirements for Enterprise Vault single instance storage

Enterprise Vault single instance storage places some additional requirements on a system, as follows:

- Storage space for the fingerprint database. When you use Enterprise Vault single instance storage the fingerprint database may grow very rapidly. To ensure acceptable archiving and retrieval performance, it is important to configure the fingerprint database appropriately for the amount of sharing in the vault store group.

See [“Creating vault store groups”](#) on page 203.

- Network connectivity requirements. An Enterprise Vault server communicates with the following computers when it stores or retrieves items using Enterprise Vault single instance storage:

- The computers that host the vault store partitions for the vault stores that are within the vault store's sharing boundary.

- The computer that hosts the vault store group's fingerprint database.

Network connection speeds must be fast enough across these connections to provide acceptable storage and retrieval times.

See [“Developing a suitable sharing regime for Enterprise Vault single instance storage”](#) on page 201.

## About EMC Centera device-level sharing

You can configure a partition for an EMC Centera device to take advantage of the Centera's device-level sharing, if required. Enterprise Vault then stores the shareable parts of a saveset as separate data blobs, so that the Centera device is able to share them.



The New Partition wizard includes an option to enable device-level sharing when you create a partition and specify an EMC Centera device.

See [“Creating vault store partitions”](#) on page 208.

You can also enable device-level sharing from the General tab of the partition properties.

Partitions for EMC Centera do not take part in Enterprise Vault single instance storage sharing. If you create a partition for EMC Centera in a vault store that is configured for sharing, the partition is ignored for the purposes of Enterprise Vault single instance storage sharing.

## About sharing partitions on storage devices that support the Enterprise Vault storage streamer API

You can create vault store partitions on storage devices that support the Enterprise Vault storage streamer API. The appropriate storage device software must be installed on the Enterprise Vault server that hosts the Enterprise Vault Storage service for the partition.

To support sharing within the vault store group, the storage device software must also be installed on each Enterprise Vault storage server that manages a partition in the same vault store group.

## Developing a suitable sharing regime for Enterprise Vault single instance storage

If you use Enterprise Vault single instance storage, you need to create a sharing regime that meets your organization's data sharing requirements and which is appropriate for your network connection speeds.

Consider what sort of sharing regime you require before you start archiving. There are limits to what you can change:

- You can change a vault store's sharing level, but the change does not act retrospectively. For example, if you change a vault store's sharing level from 'share within group' to 'share within vault store', any items already shared within the vault store group remain so.
- You cannot move a vault store to another vault store group unless all of the following circumstances apply:
  - You previously upgraded to Enterprise Vault 8.0.
  - The vault store is one that Enterprise Vault upgraded to Enterprise Vault 8.0, or one that you created in the Default Upgrade Group.

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

When deciding how to set up single instance storage, consider the following:

- You may need to keep parts of your organization separated with information barriers, also known as "Chinese walls". For example, a datacenter may be required by law or by company policy to keep information separate between its investment, retail, and mergers and acquisitions groups, to avoid conflicts of interest.

You may want to create a separate vault store group for each organizational group in which information must be isolated.

- Network connectivity between the appropriate computers must be sufficient to provide acceptable storage and retrieval times. As a minimum we recommend that you limit single instance storage to an environment in which the connections support the expected response time of a 100 Mbps switched Ethernet LAN.

The Enterprise Vault server whose Storage service manages a vault store must have adequate connectivity with the following:

- The computers that host the vault store partitions for the vault stores that are within the vault store's sharing boundary.
- The computer that hosts the vault store group's fingerprint database.

The slower the connection speeds between these computers, the longer it takes Enterprise Vault to archive and retrieve the shared items.

If your organization spans several widely-dispersed geographical locations it may be appropriate to create separate vault store groups for each location. Remember to locate the fingerprint databases locally.

Enterprise Vault provides a connectivity test to estimate connection speeds across sample network connections. The relevant wizards prompt you to run the connectivity test when you create a new vault store group or partition, or when you configure sharing. The connectivity test can help you create a sharing regime with an acceptable level of performance. To assess performance, the connectivity test measures the average round-trip time for a number of `ping` requests. If you have disabled `ping` in your environment, use your own tools to decide if the performance is acceptable. We recommend a round-trip time of one millisecond or less.

If the test results indicate poor connectivity, consider modifying the sharing boundaries or changing the location of your computers to improve connection speeds. If you are willing to accept poorer performance, you can choose to accept poor connectivity test results.

- When you create a vault store group, configure its fingerprint database appropriately for the projected sharing requirements.  
See ["Creating vault store groups"](#) on page 203.

# Creating vault store groups

Vault stores are grouped within vault store groups. If you use Enterprise Vault single instance storage, a vault store group forms an outer boundary for the sharing of SIS parts.

Before you start creating vault store groups and vault stores, consider what sort of sharing regime is compatible with your organization's structure and network connection speeds.

See [“Developing a suitable sharing regime for Enterprise Vault single instance storage”](#) on page 201.

You can create a vault store group using the New Vault Store Group wizard, as follows.

## To create a vault store group

- 1 In the left pane of the Administration Console, expand the Enterprise Vault site hierarchy until **Vault Store Groups** is visible.
- 2 Right-click **Vault Store Groups** and then click **New > Vault Store Group**.  
The New Vault Store Group wizard starts.
- 3 Work through the wizard. You need to provide the following information:
  - A name for the Vault Store Group.
  - The SQL server that is to host and manage the group's fingerprint database.
  - The locations for the fingerprint database's SQL filegroups.

The New Vault Store Group wizard provides the following options for configuring the filegroups:

- A basic configuration, where Enterprise Vault locates the primary filegroup and all the non-primary filegroups on one device.
- An option to configure additional locations for the 32 non-primary filegroups. The non-primary filegroups can grow rapidly in size when you use single instance storage. For best performance, spread the non-primary filegroups across multiple locations.

For optimal performance do as follows:

- Select the option **Configure additional locations for non-primary filegroups**.
- Specify as many locations as possible for the non-primary filegroups on the SQL Server, up to the maximum of 32.

- Specify a separate device for each location. If you specify more than one location on the same device there is no performance benefit.

---

**Note:** To add or change locations after the fingerprint database is configured is a SQL Server administration task. See your Microsoft SQL Server documentation for details.

---

When the vault store group has been created, the New Vault Store wizard takes you through the steps to create a vault store.

See [“About creating vault stores”](#) on page 204.

## About creating vault stores

When you create a vault store, you must specify an Enterprise Vault Storage service to manage it, and a location for the SQL vault store database.

The vault store database holds information about the archives in the vault store and all the items that are stored in each archive. For example, when an archived item has been backed up, this fact is reflected in the information that is held in the vault store database.

## About Enterprise Vault safety copies

Enterprise Vault can be configured to retain archived items until the vault store partition in which they are archived has been backed up. During the time between archiving and removal, the original items are treated as safety copies by Enterprise Vault. When the vault store partition has been backed up, Enterprise Vault can remove the safety copies.

The removal of safety copies takes place when the storage service is started, or when backup mode is cleared from the vault store. Enterprise Vault also creates shortcuts and placeholders at this time if it is configured to do so.

### Choosing when to remove Enterprise Vault safety copies

During the creation of each vault store, you must choose from the following settings to control how Enterprise Vault manages safety copies:

- **Never.** Enterprise Vault does not remove safety copies, even after the original items have been backed up.
- **After backup.** Enterprise Vault does not remove safety copies until the partition that contains the archived items has been backed up.

- **After backup (immediate for journaling).** This option is the same as the **After backup** option except for journal items, which are removed immediately after they are archived.
- **Immediately after archiving.** All original items are removed immediately after they are archived.

## Checking that the partition has been backed up before Enterprise Vault removes safety copies

If you selected the **After backup** option or the **After backup (immediate for journaling)** option during the creation of a vault store, Enterprise Vault must check that each partition has been backed up before it removes safety copies.

Enterprise Vault check that each partition has been backed up based on one of the following:

- The archive attribute of the files on the partition. You can use archive attributes to determine whether a partition has been backed up only if your backup software resets the archive attributes after backup.
- A trigger file mechanism. If your backup software does not reset the archive attribute on the files it backs up, you must use this mechanism.

You must choose which method to use for each partition when you create it using the **New Partition** wizard.

## Using the archive attribute to determine whether a partition has been backed up

The **Use the archive attribute** option requires your backup software to reset the archive attribute on the files in vault store partitions after they have been secured. If your backup software does not reset the archive attribute, you must use the trigger file mechanism.

When Enterprise Vault creates a file in a vault store partition, the file's archive attribute is set. Until the archive attribute is cleared, Enterprise Vault considers that the file is not backed up, and the corresponding safety copies are not removed. However, when your backup software clears the archive attribute, Enterprise Vault considers that the file is backed up, and is free to remove the safety copy. If appropriate, shortcuts to the archived items are created at the same time the safety copy is removed.

---

**Note:** Some WORM devices do not allow the archive attribute to be changed. These devices are incompatible with the **Use the archive attribute** option.

---

## Using the trigger file mechanism to determine whether a partition has been backed up

Some backup software clears the archive bit on files after backing them up. This attribute is visible as the **File is ready for archiving** option in each file's properties.

However, some backup software and other methods of securing data do not clear this attribute. In this case you must use the trigger file mechanism to indicate that data on each partition is secure.

The use of trigger file mechanism would be necessary in the following examples:

- You take snapshots of the partition to secure its data.
- You use backup software that does not clear the archive bit, such as Tivoli Storage Manager (TSM).
- You take differential backups, which clear the archive bit only when a full backup occurs.

---

**Note:** You must ensure that your backup scripts do not create a trigger file unless the backup has completed successfully.

---

The **Check for a trigger file** option determines whether the files in a vault store partition have been secured by checking for a trigger file called `IgnoreArchiveBitTrigger.txt`. At each backup, your backup software or script must place a newly created `IgnoreArchiveBitTrigger.txt` in the root of the partition to show that a backup has taken place.

For example, if you have a vault store called "Sales", and you have placed its partitions in `E:\EVStorage`, you might have a partition folder called `E:\EVStorage\Sales Ptn1`. In this case, your backup software or script must place `IgnoreArchiveBitTrigger.txt` in `E:\EVStorage\Sales Ptn1` to indicate that it has backed up the partition.

---

**Note:** It is essential that your backup script creates a new `IgnoreArchiveBitTrigger.txt` file when it backs up a partition. It is not sufficient to rename another file because its file creation date does not match the time of the backup.

---

For example, you can use the following command in your backup script to create a new file:

```
echo "Enterprise Vault trigger file" > "E:\EVStorage\Sales  
Ptn1\IgnoreArchiveBitTrigger.txt"
```

When Enterprise Vault finds `IgnoreArchiveBitTrigger.txt`, all the partition's saveset files that were created before the creation of `IgnoreArchiveBitTrigger.txt` are considered backed up. Enterprise Vault is then free to remove the safety copies that correspond with the secured saveset files, and to create shortcuts if appropriate.

If Enterprise Vault does not find `IgnoreArchiveBitTrigger.txt`, it considers that the partition is not backed up, and safety copies are not removed.

When Enterprise Vault has completed the removal of safety copies, it renames `IgnoreArchiveBitTrigger.txt` with a `.old` extension to show that the file has been processed and that the relevant files on the partition are secure.

At the next backup, your backup software creates a new `IgnoreArchiveBitTrigger.txt`.

Enterprise Vault checks partitions for a trigger file when the storage service starts and when backup mode is cleared from a vault store. Additionally, if you set a scan interval for the partition, Enterprise Vault checks the partition at intervals determined by the value you set.

Although you cannot use the trigger file mechanism on Centera partitions, Enterprise Vault queries the Centera API to determine whether or not a partition has been replicated. Enterprise Vault checks Centera partitions when the storage service starts, and when backup mode is cleared from a vault store.

Additionally, if you set a scan interval for the Centera partition, Enterprise Vault checks the partition at intervals determined by the value you set.

## Creating a vault store

You can create a vault store using the New Vault Store wizard.

### To create a vault store

- 1 If you created a vault store group using the New Vault Store Group wizard, the New Vault Store wizard starts automatically. Go to step 5.
- 2 In the left pane of the Administration Console, expand the Enterprise Vault site hierarchy until **Vault Store Groups** is visible.
- 3 Expand the **Vault Store Groups** container to show the existing vault store groups.

- 4 Right-click the vault store group in which you want to create the vault store, and then click **New > Vault Store**.

The New Vault Store wizard starts.

- 5 The New Vault Store wizard takes you through the steps to create a vault store.

You need to provide the following information:

- The name of the computer that hosts the Storage Service that the vault store is to use. The wizard requests this information only if the Enterprise Vault site contains more than one computer with a Storage Service.
- The name of the vault store. The name can contain letters, numbers, and spaces.
- The SQL server that is to create and manage the vault store database, and the locations for the database files.
- When safety copies of items are to be removed, and how Enterprise Vault checks that partitions have been backed up.  
See [“About Enterprise Vault safety copies”](#) on page 204.

---

**Note:** Enterprise Vault assigns a sharing level of "Share within vault store" to new vault stores. An exception to this rule applies to the Default Upgrade Group, which Enterprise Vault created if you previously upgraded to Enterprise Vault 8.0. If you do not configure sharing for the Default Upgrade Group, Enterprise Vault assigns a sharing level of "No sharing" to new vault stores in that group.

To change the sharing level for a vault store, run the Configure Sharing wizard on the vault store group after you have created a partition for the vault store.

---

When the vault store has been created, the New Partition wizard takes you through the steps to create a partition for the vault store.

See [“Creating vault store partitions”](#) on page 208.

## Creating vault store partitions

Vault store partitions can be placed on different physical disks and on various types of storage medium. For example, you can create partitions on local NTFS volumes, NetApp filers, EMC Centera devices, or streamer storage devices. For a full list of supported devices, see the Enterprise Vault *Compatibility Charts* at <http://www.symantec.com/docs/TECH38537>.

When deciding on the location for a partition, do not choose the location of an existing partition, or a location that includes any folders that are associated with



an existing partition. Take particular care to avoid the overlap of partition folders when using network shares or mount points. You may suffer data loss if a folder is associated with more than one partition.

Enterprise Vault assumes that the partition root path is empty. Do not use the root path to hold files or folders other than those that Enterprise Vault creates.

If you plan to store items indefinitely on a WORM storage device, then ensure that the retention settings on the device are correctly configured.

See [“Preparing WORM storage devices”](#) on page 31.

If you plan to create a vault store partition on a storage device that supports the Enterprise Vault storage streamer API, then ensure that the appropriate storage device software is installed on the Enterprise Vault storage servers. Install the storage device software on all the Enterprise Vault storage servers that manage the partitions in the vault store group.

## Initial states of vault store partitions

As the data in a vault store grows, you can create more partitions to provide additional capacity. Each vault store can contain only one open partition and Enterprise Vault archives data into this partition while it remains open.

There are two approaches to the management of open vault store partitions:

- You can manually change the open partition in a vault store. For example, when the disk that hosts the open partition reaches capacity, you can close the partition and open a partition on another disk.
- The automatic partition rollover feature which lets you configure partitions such that archiving rolls over from one partition to another when certain criteria are met. For example, you can configure a partition to roll over when the disk that hosts the open partition has only 5% free space. You can also configure partitions to roll over on a date that you set. For more information, see the *Administrator's Guide*.

To support both these features, during the creation of partitions, you can choose any one of these initial states:

- Select **Closed** to create a closed partition. If there is an existing open partition, it is not affected by this choice. You can open the new partition at any time by editing its properties.  
See [“About closed Enterprise Vault partitions”](#) on page 210.
- Select **Open** to create an open partition. Each vault store can have only one open partition. If there is an existing open partition in the vault store, it is automatically closed and items are archived to this new partition.

- Select **Ready** to create a new partition that is available for partition rollover.

## About closed Enterprise Vault partitions

When a partition is closed, Enterprise Vault stops writing new information to it. Enterprise Vault may still modify the items that are on the closed partition.

---

**Note:** A closed partition can increase in size and needs to be backed up.

---

Enterprise Vault modifies a closed partition for the following reasons:

- **Deletion.** Enterprise Vault modifies the partition if users delete items from their archives.
- **Storage Expiry.** Enterprise Vault deletes items from archives when their Retention Periods expire.
- **Collections.** The Enterprise Vault Collector continues to run on a closed partition.  
Collections are required on closed partitions because the collection process removes the temporary files that are created when users view archived items.
- **Pending Items.** Items that are in a pending state before the partition is closed result in writes to the closed partition.

If a closed partition is likely to be modified, we recommend that you continue to perform regular backups of the closed partition

If a closed partition is never modified, you do not need to perform regular backups. You can perform a final backup of the partition and then remove the partition from your backup routine.

## About collections and migration

Where vault store partitions are held on non-WORM devices other than EMC Centera, you can configure and schedule the collection and migration of the files that are stored in the partition.

Collection involves collecting multiple small files into much larger collection files (.cab files). Collection may give you a significant improvement in backup times. Collection is not recommended on devices that perform deduplication, as it causes loss of deduplication.

Migration involves moving the collection files onto longer term storage devices. For example, you may want to migrate older collections to cheaper, slower storage.

If you choose to use collection files you can configure the collection criteria, and optionally provide details of how and when to migrate the collection files to

secondary storage. See the Administration Console help for details on setting these options.

---

**Note:** When you use collections, an unreferenced item may remain in a `.cab` file for some time before it is deleted. Enterprise Vault compacts a `.cab` file and deletes the unreferenced items when the ratio of unreferenced items reaches a fixed level.

---

Other storage devices have been integrated with Enterprise Vault to enable the migration of data files. Supported devices are listed in the Enterprise Vault *Compatibility Charts* (<http://www.symantec.com/docs/TECH38537>).

For instructions on how to configure migration to the supported storage devices, see the migration articles on the Symantec support knowledge base.

## Collections on EMC Centera devices

Collections are handled differently on EMC Centera devices, as follows:

- Centera collection clips are used instead of CAB files.
- Savesets are collected as soon as they are archived, not according to a schedule.
- A collection clip and the savesets that it contains are not deleted until there are no references to any of the savesets in the clip.

To ensure optimal archiving performance when vault store partitions on Centera devices are enabled for collection, an additional index, `IX_Collection_Saveset_Partition`, can be created for the Saveset table in the associated vault store database. If the index does not exist, Enterprise Vault creates it automatically when the Storage service starts provided the following conditions are satisfied:

- At least one Centera vault store partition is open and enabled for collection.
- The number of records in the Saveset table is less than, or equal to 1,000,000.

The space required for this index on the SQL Server hosting the relevant vault store database is approximately 27 bytes per row in the Saveset table.

## Creating a vault store partition

You can create a vault store partition using the New Partition wizard.

In an environment that uses Enterprise Vault single instance storage, the network connection speeds must be adequate to support sharing. If you intend to use single instance storage in the vault store, run the connectivity test when the New Partition wizard prompts you. The connectivity test helps to determine whether the connection speeds are adequate for sharing.

See [“Developing a suitable sharing regime for Enterprise Vault single instance storage”](#) on page 201.

#### To create a vault store partition

- 1 If you created a vault store using the New Vault Store wizard, the New Partition wizard starts automatically. Go to step 6.
- 2 In the left pane of the Administration Console, expand the Enterprise Vault site hierarchy until **Vault Store Groups** is visible.
- 3 Expand the **Vault Store Groups** container to show the existing vault store groups.
- 4 Expand the vault store group that contains the vault store for which you want to create the partition.
- 5 Right-click the vault store in which you want to create the partition, and then click **New > Partition**.

The New Partition wizard starts.

- 6 The New Partition wizard takes you through the steps to create a partition.

You need to provide the following information:

- The partition name and description.
- Whether the new partition should be created closed, open or ready. There can only be one open partition. If you create an open partition, any existing open partition is closed.
- The type of device on which the partition is to be created. Select the required type of storage device from the drop-down list. The additional information that you need to provide depends on which device type you select. For help with the options, see the Administration Console help for the wizard pages.
- The location on the device for the new partition. The location can be entered as a UNC path or a path that starts with a drive letter. For a network location, enter the full UNC path rather than a mapped network drive path.

---

**Note:** Do not specify the location of an existing partition, or a location that includes any folders that are associated with an existing partition. Take particular care to avoid the overlap of partition folders when using network shares or mount points. You may suffer data loss if any folder is associated with more than one partition.

The Storage service does not start if it detects that two partitions share the same path.

Enterprise Vault assumes that the partition root path is empty. Do not use the root path to hold files or folders other than those that Enterprise Vault creates.

---

The Storage service creates a network share for a partition if you specify the storage type as **NTFS Volume** and you specify a local path such as `H:\...` as the location. The Storage services on remote Enterprise Vault servers use the partition network share when they require access to the data on the partition.

See [“Partition network shares for NTFS partitions with local paths”](#) on page 214.

If you specify a UNC path that includes an administrative share, such as `\\server\H$\partitionlocation`, then administrative shares must always be enabled. If you disable the server's administrative shares, Enterprise Vault is unable to access the partition.

- The storage settings that are used by the storage device. Enterprise Vault uses this information to help optimize data storage. For more details, see the Administration Console help for the wizard pages.

With the exception of the storage mode, you can change the storage settings later from the Volume tab of the partition's properties.

If you change the storage settings on the device at a later date, you must update the related storage settings on the **Volume** tab of the partition's properties to reflect the new behavior.

- For partitions on EMC Centera devices, whether to enable device-level sharing.
- Partition rollover criteria if you choose to enable the feature for this partition.

Although you can create ready partitions on EMC Centera devices, you cannot enable onward rollover from a Centera-hosted partition.
- Whether to use Security ACLs. This option does not apply to Centera devices. It is usual to create a vault store partition with security ACLs on

the folders in the partition. Some optical devices, however, do not allow Enterprise Vault to add the ACLs.

See “[Securing data locations](#)” on page 59.

- How to check whether items have been secured.
- Whether to use file collection software. If you choose to use collection files you can configure the collection criteria, and optionally provide details of how and when to migrate the collection files to secondary storage.

## Partition network shares for NTFS partitions with local paths

The Storage service creates a network share for a partition if you specify the storage type as **NTFS Volume** and you specify a local path; for example a path that begins `C:\...` or `H:\...`. The Storage services on remote Enterprise Vault servers use the partition network share when they require access to the data on the partition.

---

**Note:** Enterprise Vault does not create a partition network share if you specify the partition's location with a UNC path.

---

A benefit of using partition network shares is that, each time a Storage service starts, it verifies its local partition network shares. If the verification of a share fails, the Storage service attempts to create a new partition network share.

A partition network share has a UNC path with the following format:

```
\\server\EVPartitionnumber$
```

where *server* is the Enterprise Vault server on which the partition is located, and *number* is a unique hexadecimal number.

The Storage service creates the partition network share regardless of the vault store's sharing level. The Storage service grants access only to the Vault Service account, which has full access rights.

If the Storage service cannot create a partition network share, either for the first time or when verification fails, the Storage service does not start. Enterprise Vault logs an error in the event log with the following description:

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

The most likely cause is that Enterprise Vault cannot access the root path of the partition for one of the following reasons:

- A drive is offline.

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

If you see this error event, use Windows Explorer to check whether you can access the local paths to the local NTFS partitions.

## Configuring sharing for a vault store group

To change the sharing levels for the vault stores in a vault store group, you must run the Configure Sharing wizard on the vault store group.

---

**Note:** You can rerun the Configure Sharing wizard at any time, but changes you make to the vault store sharing levels do not act retrospectively.

---

See [“Developing a suitable sharing regime for Enterprise Vault single instance storage”](#) on page 201.

### To configure sharing for a vault store group

- 1 In the left pane of the Administration Console, expand the Enterprise Vault site hierarchy until **Vault Store Groups** is visible.
- 2 Expand the **Vault Store Groups** container to show the existing vault store groups.
- 3 Right-click the vault store group for which you want to configure sharing, and on the shortcut menu click **Properties**.
- 4 Click the **Sharing** tab.

The Sharing tab lists the vault stores in the vault store group, and their current sharing levels.

- 5 Click **Configure Sharing**.

The Configure Sharing wizard starts.

- 6 In the special case of the Default Upgrade Group, Enterprise Vault helps you to configure a fingerprint database for the group, if one does not exist already.
- 7 The Configure Sharing wizard takes you through the steps to configure the sharing levels for the vault stores in the vault store group.

If you change one or more vault store sharing levels to **Share within vault store** or **Share within group**, the wizard prompts you to run a connectivity test before the wizard makes any changes. The connectivity test helps to

determine whether the network connectivity is sufficient to support the sharing configuration you have selected.

The wizard makes no changes until you click **Finish** on the final page of the wizard.

If the connectivity test shows poor results you may want to do one of the following:

- Click **Back**, modify the vault store sharing levels and rerun the connectivity test.
- Click **Cancel** to discard your changes.

For more information on the connectivity test, see the Administration Console help for the Configure Sharing wizard.



# Adding index locations

This chapter includes the following topics:

- [About Enterprise Vault index locations](#)
- [Creating an Enterprise Vault index location](#)

## About Enterprise Vault index locations

Enterprise Vault automatically creates an index for each archive. The size of an index depends on the amount of data that has been indexed in the archive and the level of indexing you choose. Full indexing requires approximately 12% of the space that is used by the original data.

In order to store indexes you must create one or more index locations for Enterprise Vault to use.

---

**Note:** If you ran the Getting Started Wizard then you have already created some index locations. You can create more index locations as necessary.

---

---

**Note:** Because anti-virus software can potentially change data, it is important to exclude the index locations in your virus checking application.

---

## Creating an Enterprise Vault index location

The local Administrators group must have full access to the folders that you use for index locations and the files in them. Unless your policies dictate otherwise, these files and folders should not be accessible by anyone else.

See [“Securing data locations”](#) on page 59.

**To create an index location**

- 1** In the left pane of the Administration Console, expand the Enterprise Vault site hierarchy until the **Enterprise Vault Servers** container is visible.
- 2** Expand the **Enterprise Vault Servers** container.
- 3** Right-click the server that runs the Indexing service for which you want to add an index location
- 4** In the right pane, right-click the Indexing service and, on the shortcut menu, click **Properties**.
- 5** Click the **Index Locations** tab.
- 6** Click **Add**. Enter the password to the Vault Service account if you are prompted to do so.
- 7** In the **Choose Folder** dialog, select the folder that you want to use as an index location.

Click **Help** if you need help to select or create the location.

When you create a new index location, Enterprise Vault creates eight new subfolders in the folder you select. These subfolders are called `index1`, `index2`, and so on. Enterprise Vault uses these subfolders to store the indexes.

# Setting up Index Server groups

This chapter includes the following topics:

- [About Index Server groups](#)
- [Do I need to create Index Server groups?](#)
- [Creating an Index Server group](#)
- [Adding an Index Server to an Index Server group](#)
- [Removing an Index Server from an Index Server group](#)
- [Assigning a vault store to an Index Server group](#)
- [Unassigning a vault store from an Index Server group](#)
- [Assigning a vault store to a different indexer](#)

## About Index Server groups

An Index Server is an Enterprise Vault server that has the Enterprise Vault Indexing service installed. An Index Server can be a member of an Index Server group, or it can be ungrouped.

The Index Servers in an Index Server group do the following:

- Index the vault stores that are associated with the Index Server group.
- Respond to search queries.

An Index Server group allocates new index volumes to different servers in the group. Index volumes that belong to journal archives are allocated to different servers in the group.

By default, Enterprise Vault attempts to allocate mailbox index volumes to the server in the Index Server group that has the Storage service that hosts the mailbox archive. If the mailbox is not hosted on an Index Server that is in the Index Server group then any Index Server in the Index Server group may be used.

- When you place the Storage service and Indexing service on separate servers the communication between these services results in an increase in network traffic.

**Note:** If the network cannot cope with the extra demands there is no benefit from Index Server groups.

- Index Server groups provide Indexing services for large or distributed Enterprise Vault environments. In a distributed environment, some Enterprise Vault servers may host Storage services, while others host Indexing services.

See the section "About Enterprise Vault indexing" in the *Introduction and Planning* manual.

There is a best practices whitepaper for Enterprise Vault indexing.

See <http://www.symantec.com/docs/DOC4250>

## Do I need to create Index Server groups?

Table 25-1 lists various the considerations that determine whether you would benefit from Index Server groups:

Table 25-1 Index Server group considerations

In your Enterprise Vault environment	For details
Do you have more than one Enterprise Vault server	See “Do you have more than one Enterprise Vault server?” on page 221.
Do you use or plan to use journal archiving or File System Archiving?	See “Do you use or plan to use journal archiving or File System Archiving?” on page 221.
Do you use or plan to use Compliance Accelerator or Discovery Accelerator?	See “Do you use or plan to use Compliance Accelerator or Discovery Accelerator?” on page 222.
If you currently use Enterprise Vault is the distribution of server loads uneven?	See “Is the server loading evenly distributed across existing Enterprise Vault servers?” on page 222.

**Table 25-1** Index Server group considerations (*continued*)

In your Enterprise Vault environment	For details
Are there more than approximately 5,000 mailbox archives per Enterprise Vault server	See <a href="#">“Are there more than approximately 5,000 mailbox archives per Enterprise Vault server?”</a> on page 223.

If you answer "No" to all or most of the questions, it is unlikely that your environment can benefit from Index Server groups.

## Do you have more than one Enterprise Vault server?

If you have a single Enterprise Vault server that has acceptable performance there is no benefit from Index Server groups. If you intend to add other servers then you may benefit from Index Server groups.

If you have several Enterprise Vault servers you can group some servers with Indexing services into one or more Index Server groups.

The benefit depends on whether you have some servers that are underused and others that cannot cope with the indexing demand or the archiving demand.

For example, suppose you have three servers, one dedicated to Exchange Journal archives and two dedicated to mailbox archives. In this case it can be beneficial to put all the servers into an Index Server group. The grouping enables you to distribute journal archive index volumes between all three servers. The effect of this distribution is to increase search performance for Discovery Accelerator applications.

## Do you use or plan to use journal archiving or File System Archiving?

If you use journal archiving or FSA archiving, it can be beneficial to do either or both of the following:

- Group some servers with Indexing services into Index Server groups to distribute the indexing load.
- Add new servers to an Index Server group that is dedicated to indexing the vault stores that contain the Journal archives and FSA archives.

This configuration would also improve search performance because it distributes the large index volumes between servers.

## Do you use or plan to use Compliance Accelerator or Discovery Accelerator?

If you use Compliance Accelerator or Discovery Accelerator, it can be beneficial to do the following:

- Group some servers with Indexing services into Index Server groups to distribute the search load.
- Arrange the vault stores so that the archives are split by archive type. For example, use specific vault stores for journal archives. You can then assign a vault store that contains a specific archive type to an Index Server group.
- Add new servers to an Index Server group that is dedicated to indexing the vault stores that contain those archives that Compliance Accelerator or Discovery Accelerator search.

This configuration distributes large index volumes between separate servers. Search performance is improved because there is now parallel execution of queries across multiple servers.

## Is the server loading evenly distributed across existing Enterprise Vault servers?

An Enterprise Vault server can be overloaded because both the Archiving tasks and Indexing tasks and Storage services all share resources. You may have some servers that are underused while others are short of memory and of CPU capacity.

It can be beneficial to do the following:

- Add new servers to an Index Server group that is dedicated to indexing and searching some or all vault stores.
- Arrange the vault stores so that archives are split by type. For example, use specific vault stores for journal archives. You can then assign a vault store that contains a specific archive type to an Index Server group.

This change has the following advantages:

- Indexing CPU and memory requirements are shared between Index Servers.
- The indexing load is removed from the servers that run the Archiving tasks and Storage tasks.
- The performance of indexing and searching are improved because there are dedicated resources on separate servers.

## Are there more than approximately 5,000 mailbox archives per Enterprise Vault server?

Indexing and searching may overload an Enterprise Vault server that has a large number of mailbox archives.

It can be beneficial to add new servers to an Index Server group that is dedicated to indexing those vault stores that contain mailbox archives.

This configuration distributes those index volumes that are associated with new mailbox archives between the servers in the Index Server group. This distribution enables separate servers to process concurrent queries of many archives.

An Enterprise Vault server can be overloaded by searching too many index volumes. If users find that many searches timeout, an index group may improve the search times. If some other problem is the cause of the unsatisfactory search performance, Index Server groups are unlikely to improve performance. For example, Index Server groups cannot improve performance if IIS is overloaded.

You can add new servers to an Index Server group that is dedicated to indexing and searching those vault stores that contain mailbox archives.

This change has the following advantages:

- Improved indexing performance because the index volumes are distributed between several servers.
- Improved search performance because concurrent queries to many archives are distributed between several servers.

## Creating an Index Server group

Do not create the first Index Server group before you are sure that Index Server groups will benefit your Enterprise Vault site.

See [“About Index Server groups”](#) on page 219.

See [“Do I need to create Index Server groups?”](#) on page 220.

### To create an Index Server group

- 1 In the Administration Console expand the Enterprise Vault container.
- 2 Expand the **Directory** container.
- 3 Expand the Enterprise Vault site.
- 4 Expand the **Indexing** container.

- 5 Right-click **Index Server Groups** and on the shortcut menu click **New** and then **Index Server Group**.

The **New Index Server Group** wizard starts. If there is only one Index Server in the Site there is a message that explains that there may be no benefit from an Index Server group. Click **Continue** if you are sure that you want to create an Index Server group.

- 6 The wizard introduction page refers you to documentation for information about Index Server groups.

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

Click **Next** to go the **Name and Description** page.

- 7 Enter a **Name** for the Index Server group and optionally a **Description**. You can change the **Name** and **Description** at any time.

Click **Next**

- 8 Select the Index Servers that you want to add to the new Index Server group. There is no requirement for you to add the Index Servers now. You can add Index Servers later, as required.

Click **Next**.

- 9 If you have chosen to add Index Servers to the new Index Server group you can now choose to associate vault stores with the new Index Server group.

When you add an Index Server to an Index Server group, its associated vault stores are not included automatically. Enterprise Vault does not index those vault stores unless you associate them with an Index Server group. If you want those vault stores to be indexed by the new Index Server group, select **All Vault Stores that are currently indexed by the servers you have chosen to add to the new index server**.

Click **Next**.

- 10 Click **Next**. The page shows the details that you have entered.

- 11 Click **Create Index Server Group**. The wizard creates the new Index Server group and shows a summary page.

- 12 Click **Close** to close the wizard.

If you did not add an Index Server to the new Index Server group you can edit the properties of the Index Server group to do so.

See [“Adding an Index Server to an Index Server group”](#) on page 225.



# Adding an Index Server to an Index Server group

You can add an Index Server to an Index Server group at any time. You cannot remove the Index Server from the Index Server group once it has indexed data as a member of the Index Server group.

---

**Note:** When you add an Index Server to an Index Server group, its associated vault stores are not included automatically. Use the Vault Stores tab in an Index Server group's properties to associate those vault stores with that Index Server group.

---

## To add an Index Server to an Index Server group

- 1 In the Administration Console expand the Enterprise Vault container.
- 2 Expand the **Directory** container.
- 3 Expand the Enterprise Vault site.
- 4 Expand the **Indexing** container.
- 5 Expand **Index Server Groups**.
- 6 Right-click the group to which you want to add an Index Server and click **Properties**.
- 7 In the Index Server group properties, click the **Index Servers** tab. The list shows the Index Servers that are already in the group.
- 8 Click **Add**. The list shows the Index Servers that can be added to an Index Server group.
- 9 Click the Index Server that you want to add to the Index Server group.

You can run a connectivity test to check network performance. The test helps you to determine whether the network provides acceptable performance within the Index Server group. The test determines the response time for ping requests between the Index Server and a vault store that is associated with the Index Server group.

To run the connectivity test:

- Click **Connectivity Test**. The dialog expands to show the **Connectivity Test** section.
- Click **Run Test**.

The test may take a few seconds to run. The list shows a summary of the results. To see the complete details, click **Report**.

- 10 When you have selected the Index Servers that you want to add, click **OK**. A prompt asks whether you are sure that you want to continue. You cannot remove the Index Server from the Index Server group once it has indexed data as a member of the Index Server group. Click **Yes** to continue.

You can also remove an Index Server from an Index Server group.

See [“Removing an Index Server from an Index Server group”](#) on page 226.

## Removing an Index Server from an Index Server group

You can remove an Index Server from an Index Server group subject to the following limitations:

- You cannot remove an Index Server from an Index Server group once it has indexed data as a member of the Index Server group
- You cannot remove an Index Server that is associated with an incomplete indexing task.

### To remove an Index Server from an Index Server group

- 1 In the Administration Console expand the Enterprise Vault container.
- 2 Expand the **Directory** container.
- 3 Expand the Enterprise Vault site.
- 4 Expand the **Indexing** container.
- 5 Expand **Index Server Groups**.
- 6 Right-click the group from which you want to remove an Index Server and click **Properties**.
- 7 In the Index Server group properties, click the **Index Servers** tab. The list shows the Index Servers that are already in the group.
- 8 Click the Index Server that you want to remove from the Index Server group.
- 9 Click **Remove**.

In response to the confirmation prompt, click **Yes**.

## Assigning a vault store to an Index Server group

When you add an Index Server to an Index Server group, its associated vault stores are not included automatically. Enterprise Vault does not index those vault stores until you assign them to an Index Server or Index Server group.

### To add a vault store to an Index Server group

- 1 In the Administration Console expand the Enterprise Vault container.
- 2 Expand the **Directory** container.
- 3 Expand the Enterprise Vault site.
- 4 Expand the **Indexing** container.
- 5 Expand **Index Server Groups**.
- 6 Right-click the group to which you want to add an Index Server and click **Properties**.
- 7 In the Index Server group properties, click the **Vault Stores** tab. The list shows the vault stores that are already assigned to the Index Server group.
- 8 Click **Add**. The list shows the vault stores that can be added to an Index Server group as follows:
  - Vault stores that Enterprise Vault does not index. These are likely to be vault stores that were associated with an Index Server that has been added to an Index Server group.
  - Vault stores that are currently indexed by an Index Server that is not in an Index Server group.
- 9 Select the vault stores that you to associate with the Index Server group.
- 10 You can run a connectivity test to check network performance. The test helps you to determine whether the network provides acceptable performance within the Index Server group. The test determines the response time for ping requests between a vault store and an Index Server that is in the Index Server group.

To run the connectivity test:

  - Click **Connectivity Test**. The dialog expands to show the **Connectivity Test** section.
  - Click **Run Test**.

The test may take a few seconds to run. The list shows a summary of the results. To see the complete details, click **Report**.
- 11 When you have selected the Index Servers that you want to add, click **OK**

You can also unassign a vault store from an Index Server group.

See [“Unassigning a vault store from an Index Server group”](#) on page 228.

## Unassigning a vault store from an Index Server group

You can unassign a vault store from an Index Server group subject to the following limitations:

- You cannot unassign a vault store from Index Server group once data in the vault store has been indexed by a member of the Index Server group
- You cannot unassign a vault store that is associated with an incomplete indexing task.

**To unassign a vault store from an Index Server group**

- 1 In the Administration Console expand the Enterprise Vault container.
- 2 Expand the **Directory** container.
- 3 Expand the Enterprise Vault site.
- 4 Expand the **Indexing** container.
- 5 Expand **Index Server Groups**.
- 6 Right-click the group to which you want to add an Index Server and click **Properties**.
- 7 In the Index Server group properties, click the **Vault Stores** tab. The list shows the vault stores that are assigned to the Index Server group.
- 8 Click the vault store that you want to unassign from the Index Server group.
- 9 Click **Remove**.
- 10 Click **Yes**.

## Assigning a vault store to a different indexer

You can reassign a vault store to a different indexer as follows:

- You can reassign to an Index Server group a vault store that is not already assigned to an Index Server group.
- You can reassign a vault store from one Index Server group to another Index Server group provided that the current Index Server group has not indexed anything in that vault store.

**To assign a vault store to a different indexer**

- 1** In the Administration Console expand the Enterprise Vault container.
- 2** Expand the **Directory** container.
- 3** Expand the Enterprise Vault site.
- 4** Expand the **Vault Store Groups** container.
- 5** Expand the vault store group that contains the vault store that you want to modify.
- 6** Right-click the vault store that you want to assign to a different indexer and click **Properties**.
- 7** In the vault store properties click the **Indexers** tab.

The Indexer section shows whether the vault store is currently indexed by a single Index Server, by an Index Server group, or is not indexed.

- 8** Click **Change**.

The list shows the Index Server groups to which you can assign the vault store.

- 9** Click the Index Server group to which you want to assign the vault store.
- 10** You can run a connectivity test to check network performance. The test helps you to determine whether the network provides acceptable performance within the Index Server group. The test determines the response time for ping requests between the vault store and an Index Server that is in the Index Server group.

To run the connectivity test:

- Click **Connectivity Test**. The dialog expands to show the **Connectivity Test** section.
- Click **Run Test**.

The test may take a few seconds to run. The list shows a summary of the results. To see the complete details, click **Report**.

- 11** When you have selected the new Index Server group, click **OK**.
- 12** Click **OK** to close the vault store properties.

You can also unassign a vault store from an Index Server group.

See [“Unassigning a vault store from an Index Server group”](#) on page 228.



# Reviewing the default settings for the site

This chapter includes the following topics:

- [Reviewing the default settings for the Enterprise Vault site](#)

## Reviewing the default settings for the Enterprise Vault site

Check the default settings configured in the Enterprise Vault site properties.

### To review the default settings for the Enterprise Vault site

- 1 In the Administration Console, expand the contents of the left pane until the Enterprise Vault site is visible.
- 2 Right-click the Enterprise Vault site and then, on the shortcut menu, click **Properties**.

Alternatively, select the site and click the **Review site properties** button on the toolbar.

- 3 Click **Help** on any of the Site Properties screens for further information.
- 4 Site properties include the following settings. Note that you can override some of these at a lower level. For example, you can override the site archiving schedule for a particular task by setting the schedule in the task properties. The indexing level can also be set at policy and archive level and the default retention category can be set at policy level (and at Provisioning Group level for Exchange Server mailbox archiving).

General	<ul style="list-style-type: none"> <li>■ The vault site alias and description.</li> <li>■ The protocol and port to use for the Web Access application.</li> <li>■ A system message for users of the Web Access application, if required.</li> <li>■ PST holding area details.</li> <li>■ A note for administrators, if required.</li> </ul>
Archive Settings	<ul style="list-style-type: none"> <li>■ The default retention category.</li> <li>■ The default indexing level for the site.</li> <li>■ Whether users can delete items from their archives.</li> <li>■ Whether users can recover the archived items that they have deleted.</li> <li>■ The length of time for which the deleted items remain available for recovery.</li> <li>■ The length of time for which to retain the transaction history for archives.</li> </ul>
Storage Expiry	<ul style="list-style-type: none"> <li>■ The schedule for running storage expiry to delete from archives any items that are older than the retention period assigned.</li> </ul>
Archive Usage Limit	<ul style="list-style-type: none"> <li>■ If required, you can set limits on the size of archives.</li> </ul>
Site Schedule	<ul style="list-style-type: none"> <li>■ The schedule for running automatic, background archiving.</li> </ul>
Monitoring	<ul style="list-style-type: none"> <li>■ Performance counters for monitoring Enterprise Vault.</li> </ul>

- 5 Click **Help** on any of the site properties screens for further information.

## Setting the archiving schedule for the Enterprise Vault site

Each archiving task or service runs according to a schedule that you define. The possible schedules for each task are as follows:

- The default schedule, which is the one that you set in the site properties. This schedule applies to all archiving tasks in your Enterprise Vault site.
- The task's own schedule, which is the one that you set by editing its properties. You edit this schedule if you want to provide specific settings for that task, overriding those in the site properties.



### To set the archiving schedule for the Enterprise Vault site

- 1 In the left pane of the Administration Console, expand the Enterprise Vault site hierarchy until the name of the site is visible.
- 2 Right-click the site name and then click **Properties**.
- 3 Click the **Site Schedule** tab.
- 4 Modify the schedule as required. The online help gives detailed instructions on using the schedule page.

## About the Web Access application settings

In the Administration Console, on the General page of site properties, the protocol and port for accessing the Enterprise Vault Web Access application can be set.

The default URL for the Web Access application is set to `/EnterpriseVault`, which is the name of the virtual directory in IIS for the Web Access application. When a client contacts the Web Access application to access an archive, Enterprise Vault creates the full URL dynamically.

In a default configuration, the Web Access application is accessed using HTTP over port 80. The full URL for the Web Access application is then:

`http://FQDN/EnterpriseVault`

where *FQDN* is the fully qualified domain name of the Enterprise Vault server that hosts the Storage service for the user's archive.

If your IIS computer requires a different port or secured connections, then you can set the required values using the options **Use TCP Port** or **Use HTTPS on SSL Port**.

---

**Note:** If you change the protocol or port that is used to access the Web Access application after items have been archived, existing shortcuts will no longer work.

---

See [“Customizing security for the Enterprise Vault Web Access application”](#) on page 132.



# Clustering Enterprise Vault with Veritas Cluster Server

- [Chapter 27. Introducing clustering with VCS](#)
- [Chapter 28. Installing and configuring Veritas Storage Foundation HA for Windows](#)
- [Chapter 29. Configuring the VCS service group for Enterprise Vault](#)
- [Chapter 30. Running the Enterprise Vault Configuration wizard](#)
- [Chapter 31. Implementing an SFW HA-VVR disaster recovery solution with Enterprise Vault](#)
- [Chapter 32. Troubleshooting clustering with VCS](#)



# Introducing clustering with VCS

This chapter includes the following topics:

- [Supported VCS configurations and software](#)
- [About Enterprise Vault and the VCS GenericService agent](#)
- [Typical Enterprise Vault configuration in a VCS cluster](#)
- [Order in which to install and configure the components in a VCS environment](#)

## Supported VCS configurations and software

Both active/passive and N+1 configurations are supported, but active/active configurations are not.

In an active/passive configuration, a dedicated spare server is available for each Enterprise Vault server, ready and waiting for the primary server to go down. In an N+1 configuration, there is a computer for each Enterprise Vault server and then one or more spare servers waiting for any of the active servers to fail over.

The following software must be installed:

- Veritas Storage Foundation HA for Windows, version 5.1 SP2 or later.
- Enterprise Vault.
- Windows Server 2008 R2.

Neither Compliance Accelerator nor Discovery Accelerator must be installed on any server in the planned cluster. These products are not supported within a cluster. However, an unclustered Compliance Accelerator or Discovery Accelerator can reference a clustered Enterprise Vault virtual server.

## About Enterprise Vault and the VCS GenericService agent

The VCS GenericService agent brings online the following Enterprise Vault services, monitors their status, and takes them offline:

- Admin service
- Directory service
- Indexing service
- Shopping service
- Storage service
- Task Controller service

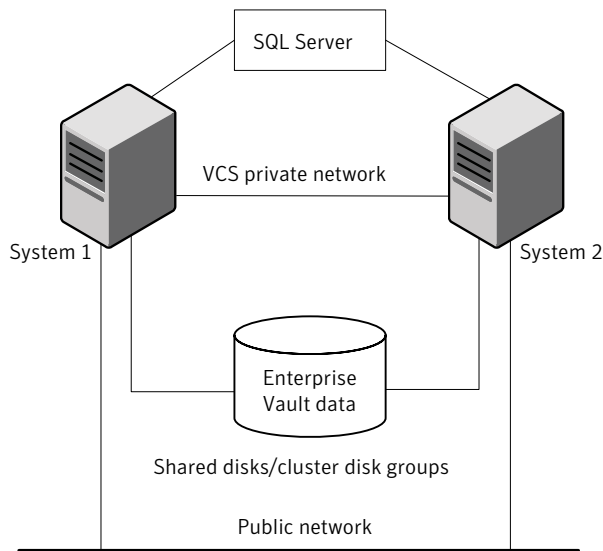
See the *Veritas Cluster Server Bundled Agents Reference Guide* for detailed information on the GenericService agent, including the resource type definitions, attribute definitions, and sample configurations.

The GenericService agent detects an application failure if a configured service is not running. When this happens, the Enterprise Vault service group is failed over to the next available system in the service group's system list, and the services are started on the new system. This ensures continuous availability for the data that Enterprise Vault is managing and archiving.

## Typical Enterprise Vault configuration in a VCS cluster

[Figure 27-1](#) illustrates a typical configuration.

**Figure 27-1** Active/passive failover configuration



Here, the volumes for the Enterprise Vault services data are configured in a cluster disk group on shared storage. The Enterprise Vault virtual server is configured on the active node (System 1). If System 1 fails, System 2 becomes the active node, and the Enterprise Vault virtual server comes online on System 2.

## Order in which to install and configure the components in a VCS environment

The order in which you install and configure the various components in a VCS environment is important.

### To install and configure the components in a VCS environment

- 1 Install all the prerequisite VCS components on each of the cluster nodes.
- 2 Complete the installation and configuration of Veritas Storage Foundation HA for Windows.  
As part of the installation process, take care to install the Enterprise Vault Cluster Setup wizard.
- 3 Configure the disk groups and volumes.
- 4 Run the Enterprise Vault Cluster Setup wizard to configure the Enterprise Vault service group.

- 5** Test that the nodes in the cluster fail over correctly.
- 6** Install the Enterprise Vault server components on all the nodes in the cluster.
- 7** Run the Enterprise Vault Configuration wizard to configure the primary Enterprise Vault cluster node.
- 8** Optionally, run the Enterprise Vault Getting Started wizard to set up Enterprise Vault.
- 9** Install and configure the failover Enterprise Vault cluster nodes.
- 10** Test that the nodes in the cluster still fail over correctly.



# Installing and configuring Veritas Storage Foundation HA for Windows

This chapter includes the following topics:

- [Installing and configuring Veritas Storage Foundation HA for Windows with Enterprise Vault](#)
- [Managing disk groups and volumes in a Veritas Storage Foundation HA environment](#)

## Installing and configuring Veritas Storage Foundation HA for Windows with Enterprise Vault

Except where noted, you can get detailed instructions on how to perform the steps outlined in this section from the *Veritas Storage Foundation and High Availability Solutions Guide*.

**To install and configure Veritas Storage Foundation HA for Windows with Enterprise Vault**

- 1 On each node that is to be a part of the cluster, install all the prerequisite components for Veritas Storage Foundation HA for Windows (SFW HA) 5.1 SP2 or later.

There are several stages to this process. For each node, you must do the following:

- Review the product installation requirements, disk space requirements, and requirements for SFW HA.

- Configure the network and storage.
  - Install SFW HA. As part of this process, take care to install the Enterprise Vault Cluster Setup wizard.
- 2 Run the VCS Configuration wizard to configure the cluster.
  - 3 Configure the disk group and volumes from the first node. You can use the Veritas Enterprise Administrator or equivalent disk management software to do this.

You must create shared volumes to store the following:

- Indexing service data
- Shopping service data
- Vault store partitions
- PST holding folders
- EMC Centera staging areas

For performance reasons, we recommend that you create separate volumes for the following:

- Microsoft Message Queue (MSMQ) data
- Registry replication data
- Indexing service data
- Vault store partitions

See [“Managing disk groups and volumes in a Veritas Storage Foundation HA environment”](#) on page 243.

- 4 Mount the volumes on the system where you will configure the Enterprise Vault service group.
- 5 Run the Enterprise Vault Cluster Setup wizard to configure the Enterprise Vault service group.

See [“About configuring the VCS service group for Enterprise Vault”](#) on page 245.

- 6 Test that the nodes in the cluster fail over correctly.
- 7 Install Enterprise Vault on all systems in the cluster.
- 8 Run the Enterprise Vault Configuration wizard to create the Enterprise Vault services and resources.
- 9 Verify the cluster configuration and test the failover capability.

# Managing disk groups and volumes in a Veritas Storage Foundation HA environment

This section describes how to perform the following activities:

- Importing a dynamic disk group.
- Mounting a shared volume.
- Unmounting a volume and deporting a disk group.

While you set up an SFW HA environment, keep the following points in mind:

- You must mount the volumes on the system where you will configure the Enterprise Vault service resource group.
- When a disk group is initially created, it is imported on the node where it is created.
- A disk group can be imported on one node only at a time.
- To move a disk group from one node to another, unmount the volumes in the group, deport the group from its current node, import it to a new node, and mount the volumes.

## To import a dynamic disk group

- 1 Start the Veritas Enterprise Administrator.
- 2 Right-click a disk name in the dynamic disk group or the dynamic disk group name in the tree view, and then click **Import Dynamic Disk Group** on the context menu.
- 3 Follow the on-screen instructions.

## To mount a volume

- 1 If you have yet to do so, open the Veritas Enterprise Administrator and import the dynamic disk group.
- 2 Right-click the volume, and then click **File System > Change Drive Letter and Path**.
- 3 In the Drive Letter and Paths dialog box, click **Add**.

- 4 Select one of the following options, depending on whether you want to assign a drive letter to the volume or mount it as a folder.

To assign a drive letter.	Click <b>Assign a Drive Letter</b> , and then choose the required letter.
---------------------------	---

To mount the volume as a folder.	Click <b>Mount as an empty NTFS folder</b> , and then click <b>Browse</b> to locate an empty folder on the shared disk.
----------------------------------	---

- 5 Click **OK**.

**To unmount a volume and deport the dynamic disk group**

- 1 In the Veritas Enterprise Administrator, right-click the volume and then click **File System > Change Drive Letter and Path**.
- 2 In the Drive Letter and Paths dialog box, click **Remove**.
- 3 Click **OK**.
- 4 Right-click the disk, and then click **Deport Dynamic Group**.
- 5 Click **Yes** to confirm that you want to deport the disk group.

# Configuring the VCS service group for Enterprise Vault

This chapter includes the following topics:

- [About configuring the VCS service group for Enterprise Vault](#)
- [Before you configure the VCS service group for Enterprise Vault](#)
- [Creating a VCS service group for Enterprise Vault](#)
- [Modifying an existing VCS service group](#)
- [Deleting a VCS service group](#)

## About configuring the VCS service group for Enterprise Vault

In VCS, a service group represents a virtual server. Each service group contains a set of resources, which you can bring online or offline when a group fails over to another node in the cluster. You can arrange a combination of these resources to make a complete Enterprise Vault server.

These resources include the following:

- GenericService resources
- IP address
- Computer name (Lanman resource)
- Microsoft Message Queue (MSMQ resource)
- Disk/storage (MountV and DiskGroup resources)
- NIC

Before you can configure Enterprise Vault in a cluster, you must configure a service group to represent the Enterprise Vault server. VCS provides several ways to configure a service group, including the Enterprise Vault Cluster Setup wizard. You can also use Cluster Manager (Java Console or Web Console) or the command line.

We recommend that Enterprise Vault cluster groups contain resources related to Enterprise Vault only.

## Before you configure the VCS service group for Enterprise Vault

Before you configure an Enterprise Vault service group, do the following:

- Verify your DNS server settings. You must ensure that a static DNS entry maps the virtual IP address with the virtual server name (which will be the same as the Enterprise Vault server name).

Note that the Enterprise Vault Cluster Setup wizard does not support service groups that contain multiple IP address or computer name (Lanman) resources.

- Verify that the Veritas Command Server service is running on all systems in the cluster.
- Verify that the Veritas High Availability Daemon (HAD) is running on the system from where you will run the Enterprise Vault Cluster Setup wizard.
- Ensure that you have Cluster Administrator privileges. You must also be a Local Administrator on the node where you run the wizard.
- Verify that Microsoft Message Queue (MSMQ) is installed locally on each node.
- Mount the shared volumes that you have created to store the following:
  - Indexing service data
  - Shopping service data
  - Vault store partitions
  - PST holding folders
  - EMC Centera staging areas

Unmount the volumes from other nodes in the cluster.

# Creating a VCS service group for Enterprise Vault

As part of the process of installing Veritas Storage Foundation HA for Windows, you installed the Enterprise Vault Cluster Setup wizard. This wizard lets you create a VCS service group for Enterprise Vault.

## To create a VCS service group for Enterprise Vault

- 1 On the Windows **Start** menu, click **All Programs > Symantec > Veritas Cluster Server > Configuration Tools > Enterprise Vault Cluster Setup Wizard**.
- 2 Review the information in the Welcome page, and then click **Next** to display the Wizard Options page.
- 3 Click **Create service group**, and then click **Next** to display the Service Group Configuration page.
- 4 In the **Service Group Name** box, type a name for the group, such as EVGRP1.
- 5 Move to the **Systems in Priority Order** box those systems on which you want to configure the service group.

If you want to change the priority of the systems in the **Systems in Priority Order** box, click a system and then click the up-arrow or down-arrow button.

- 6 Click **Next** to validate the configuration and display the Virtual Server Configuration page.
- 7 Complete the fields by following these steps in the order listed:
  - In the **Virtual Server Name** box, type the server name that you mapped to the virtual IP address when you set up the static DNS entry.
  - In the **Virtual IP address** box, type the address that you mapped to the virtual server. This should be in the same subnet as the current computer, but it should not currently be in use on the network.
  - Enter the subnet mask for the subnet to which the virtual IP address belongs.
  - For each system in the cluster, select the public network adapter name. The wizard lists all the TCP/IP-enabled adapters on the system, including the private network adapters if they are TCP/IP enabled. Be sure to select the adapters to assign to the public network, and not those assigned to the private network.
  - Click **Advanced** to specify details for the Lanman resource. You must select the distinguished name of the organizational unit for the virtual server. By default, the Lanman resource adds the virtual server to the default container Computers.

The user account for VCS Helper service must have adequate privileges on the specified container to create and update computer accounts.

- 8 In the Virtual Server Configuration page, click **Next** to display the MSMQ and RegRep Directory Details page.

This page enables you to virtualize the MSMQ resource so that it can be accessed using its virtual name. This resource also ensures that the queue state is maintained after failover.

- 9 Complete the fields as follows:

- In the **MSMQ Directory** field, enter the path to the required directory.
- In the **Replication Directory** field, enter the path to the registry replication directory. The replication data contains a list of the registry keys to replicate.

We recommend that you configure the MSMQ and replication directories on different volumes. A volume is available for selection only if you have configured it on the shared disk.

- 10 Click **Next** to display the Storage Location Details page.

This page lets you select the volumes that you want to configure for Enterprise Vault services.

The available volumes do not include those that you selected in the previous page of the wizard, when specifying the storage locations for MSMQ and registry replication.

- 11 In the Available Volumes box, select each volume on which you have configured the services and then click the right-arrow button to move it to the Selected Volumes box. You must select the volumes that you configured for each of the following:

- Indexing service data
- Shopping service data
- Vault store partitions
- PST holding folders
- EMC Centera staging areas

- 12 Click **Next** to display the Service Group Summary page.

- 13 Review your configuration. If you want to modify an attribute name for any reason, follow these steps in the order listed:

- Click the resource, and then click the attribute that you want to modify.
- Click the **Edit** icon at the end of the table row.



- In the Edit Attribute dialog box, enter the attribute values.
- Click **OK**.
- Repeat the procedure for each resource and attribute.

**14** Click **Next** to display the Completion page.

**15** Click **Bring the service group online**, and then click **Finish**.

When you have finished adding the service group, check that it can fail over between nodes without error.

# Modifying an existing VCS service group

[Table 29-1](#) lists the items that you can modify in a service group.

**Table 29-1** Modifiable service group items

Item	Notes
System list	You can add nodes to or remove them from the cluster. If you want to remove a node, make sure that it is not the active one.
Volumes	You can add or remove volumes. If you remove a volume on which an Enterprise Vault service is configured, the service ceases to be highly available and is not monitored.
Virtual IP	You can change the virtual IP address if the service group is offline. You cannot change the virtual server name, which is fixed when you create the service group.

You can modify an Enterprise Vault service group in several ways, including the Enterprise Vault Cluster Setup wizard, Cluster Manager (both Java Console and Web Console), and the command line. The following steps describe how to modify the service group with the Enterprise Vault Cluster Setup wizard.

Before you proceed, note the following:

- You must run the wizard from a node on which the service group is online. You can then use the wizard to add resources to or remove them from the configuration.
- You must take the service group partially offline to change the resource attributes. However, the MountV and VMDg resources for the service group should be online on the node where you run the wizard and offline on all other nodes. Mount all the volumes created to store Storage service data (vault stores), registry replication information, Shopping service data, Indexing data and MSMQ data.

- If you want to modify the system list or volumes, the service group must be online.
- Do not modify an existing VCS service group that contains an operational Enterprise Vault server.

**To modify an existing VCS service group**

- 1 Start the Enterprise Vault Cluster Setup wizard.
- 2 Review the information in the Welcome page, and then click **Next** to display the Wizard Options page.
- 3 Click **Modify service group**, and then click **Next**.
- 4 Follow the instructions to modify the service group.

Note that if you add a system to an online service group, any resources with local attributes may briefly have a status of UNKNOWN. After you add the new node to the group, run the Enterprise Vault Configuration wizard on this node to configure the Enterprise Vault services for it.

## Deleting a VCS service group

Follow the steps below to delete a service group with the Enterprise Vault Cluster Setup wizard.

**To delete a VCS service group**

- 1 Start the Enterprise Vault Cluster Setup wizard.
- 2 Review the information in the Welcome page, and then click **Next** to display the Wizard Options page.
- 3 Click **Delete service group**, and then click **Next**.
- 4 In the Service Group Summary page, click **Next**.
- 5 When the wizard prompts you to confirm that you want to delete the service group, click **Yes**.
- 6 Click **Finish**.

# Running the Enterprise Vault Configuration wizard

This chapter includes the following topics:

- [Before you run the Enterprise Vault Configuration wizard](#)
- [Setting up Enterprise Vault in an active/passive VCS configuration](#)
- [About setting up Enterprise Vault in a VCS N+1 configuration](#)

## Before you run the Enterprise Vault Configuration wizard

The Enterprise Vault Configuration Wizard provides options for setting up Enterprise Vault in a VCS cluster.

Before you run the Enterprise Vault Configuration wizard, ensure the following:

- The Enterprise Vault service group exists and is online on the first node in the cluster.  
See [“About configuring the VCS service group for Enterprise Vault”](#) on page 245.
- You have installed SFW HA 5.1 SP2 or later.
- For SFW HA 6.0 or later, you have applied the hotfix that is available from the following page of the Symantec Enterprise Support site:  
<http://www.symantec.com/docs/TECH178773>

# Setting up Enterprise Vault in an active/passive VCS configuration

As well as describing how to set up cluster support in a first-time installation of Enterprise Vault, this section describes how to upgrade an existing, standard installation of Enterprise Vault to a clustered environment.

## Adding VCS cluster support in a first-time Enterprise Vault installation

You must run the Enterprise Vault Configuration wizard on each node of the cluster. On the first node, choose the option to create a new Enterprise Vault server with cluster support. On each additional node, choose the option to add it as a failover node for an existing clustered server.

### To create a new Enterprise Vault server with cluster support

- 1 On the Windows **Start** menu, click **All Programs > Enterprise Vault > Enterprise Vault Configuration**.

The first page of the wizard appears.

- 2 Click **Create a new Enterprise Vault server with cluster support**, and then click **Next**.
- 3 Follow the on-screen instructions.

Note the following important points as you proceed through the wizard:

- When the wizard prompts you for the computer DNS alias, enter an unqualified DNS alias that points to the virtual server name.
- Take care to review the storage locations for the Indexing and Shopping services, when the wizard prompts you to do so.
- When the wizard prompts you to select the data locations, specify a server cache location that is on a shared drive in the cluster.

- 4 In the Finish page, ensure that **Bring all the resources online** is unchecked, and then click **Finish**.
- 5 Follow the steps below to set the path to the index metadata folder, which must be on a shared drive in the cluster. The index metadata folder is the folder in which Enterprise Vault stores indexing configuration data and reporting data.

- Use the Cluster Manager console to bring the Enterprise Vault Directory service and Admin service online.
- In the left pane of the Enterprise Vault Administration Console, browse to **Enterprise Vault Servers > EVServer.domain.local > Services**.

- In the right pane, right-click **Enterprise Vault Indexing Service**, and then click **Properties**.
  - On the **General** tab of the Service Properties dialog box, set the **Index metadata location** path to that of the shared drive in the cluster (for example, `V:\indexmetadata`).
  - Click **OK** to save the change that you have made.
  - Use the Cluster Manager console to bring the Enterprise Vault Indexing service online
- 6 After you have configured the server on the first node, run the wizard from each additional node that you want to configure as a failover node.

Note that the path to the Enterprise Vault program folder must be the same on all nodes in the cluster; for example, `C:\Program Files (x86)\Enterprise Vault`. If the path varies from one node to another, problems can occur during failover.

#### To add a failover node for an existing clustered server

- 1 Ensure that the Enterprise Vault service group is online on a different node in the cluster. The service group must not be online on the node that you are configuring. The node that you are configuring must be a possible failover node for the resources.
- 2 On the Windows **Start** menu, click **All Programs > Enterprise Vault > Enterprise Vault Configuration**.
- 3 Click **Add this node as a failover node for an existing clustered server**, and then click **Next**.
- 4 Follow the on-screen instructions.

When the wizard prompts you for the name of the service group to which you want to add the node, select the name of the service group that you chose for the first node.
- 5 In the summary page, review the information, and then click **Next**.

The wizard informs you that it will create the Enterprise Vault service group on the new node.
- 6 In the Finish page, click **Finish** to exit the wizard.
- 7 Check that you can bring the resources online on the failover node. You can do this with Cluster Explorer, by clicking **Switch To** on the context menu.

## Troubleshooting configuration of the Monitoring database

If during the running of the Enterprise Vault configuration wizard you receive errors indicating that configuring of the Enterprise Vault Monitoring database has failed, complete the configuration wizard and then run the Monitoring Configuration Utility to configure the Monitoring database and the Monitoring agents manually.

For information on how to do this, see the following Enterprise Vault technical note on the Symantec Support Web site:

<http://www.symantec.com/docs/TECH50809>

The technical note also describes how to troubleshoot issues with Monitoring agents.

## Upgrading an existing Enterprise Vault installation to a VCS cluster

If you have an existing Enterprise Vault installation on a single, unclustered server, you can convert it to a failover cluster. To be eligible for conversion to a cluster, the existing Enterprise Vault installation must meet the following conditions:

- Enterprise Vault should already be configured in a non-clustered configuration, and it must not already be part of a cluster.
- Enterprise Vault servers must be configured using DNS aliases rather than standard address records.
- The Enterprise Vault server must have a full set of Indexing, Shopping, Task Controller, and Storage services.
- Neither Compliance Accelerator nor Discovery Accelerator must be installed on any server in the planned cluster. These products are not supported within a cluster. However, an unclustered Compliance Accelerator or Discovery Accelerator can reference a clustered Enterprise Vault virtual server.

### To upgrade an existing Enterprise Vault installation to a VCS cluster

- 1 Check that your setup meets the requirements for the Enterprise Vault service group.  
[See “Before you configure the VCS service group for Enterprise Vault”](#) on page 246.
- 2 Run the Enterprise Vault Cluster Setup wizard to create an Enterprise Vault service group and add to the group the server that you are going to configure.
- 3 Ensure that the following items are all on highly-available shared storage devices.

- Indexing service data
- Shopping service data
- Vault store partitions
- PST holding folders
- EMC Centera staging areas

If they are not, correct the locations in the Enterprise Vault Directory database and then move the associated data to the new locations.

See [“Moving Enterprise Vault data to highly-available locations”](#) on page 255.

- 4 On the Windows **Start** menu, click **All Programs > Enterprise Vault > Convert to Cluster**.
- 5 Read the introductory information, and then click **Next**.
- 6 When the following page appears, check **All locations are highly available storage devices**, and then click **Next**.
- 7 If the wizard detects that there are messages in the Enterprise Vault MSMQ queues, choose whether to proceed with the conversion without migrating them to the clustered MSMQ queues.  
  
Wait until the queues have cleared and then rerun the Convert to Cluster wizard. Any messages that are still in the queues are ignored in the new cluster. To accelerate the process of clearing the queues, stop the Task Controller service and ensure that File System Archiving is not performing an archiving run.
- 8 When the wizard prompts you to choose a service group in which to create the cluster resources for each Enterprise Vault service, select the group that you created earlier.
- 9 Click **Next** to create the cluster resources, and then review the list of actions that the wizard has carried out.
- 10 Click **Finish** to close the wizard.
- 11 Using the DNS snap-in to the Microsoft Management Console (MMC), change the computer name alias to point to the virtual server name rather than the local name.
- 12 Use Veritas Cluster Manager to bring the resources in the cluster online.

## Moving Enterprise Vault data to highly-available locations

In outline, the procedure for moving the data to highly-available locations is as follows:

- Stop the Indexing, Shopping, Storage, and Task Controller services.
- Make a backup copy of the Enterprise Vault Directory database and data files.
- Use the Vault Administration Console or run a SQL query against the Enterprise Vault directory to move the data, as described below.

IndexRootPathEntry  
[IndexRootPath]

- Move the contents of this location to a highly available location.
- Update the database using SQL to point at the new location.

The SQL to view the current location is as follows:

```
SELECT *
FROM IndexRootPathEntry
WHERE (IndexRootPathEntryId = '<ID FROM
LOG FILE>')
```

The SQL to update the location is as follows:

```
UPDATE IndexRootPathEntry
SET IndexRootPath = '<THE NEW LOCATION>'
WHERE (IndexRootPathEntryId = '<ID FROM
LOG FILE>')
```

PartitionEntry  
[AccountName]

- Move the pool entry authorization (.pea) file to a highly available location.
- Use the Vault Administration Console to view the properties of the EMC Centera partition and then, on the **Connection** tab, edit the **Pool Entry Authorization File Location** box to point at the new location.



- PartitionEntry [PartitionRoot Path]
- Move the contents of this location to a highly available location.
  - Update the database using SQL to point at the new location.

The SQL to view the current location is as follows:

```
SELECT *
FROM PartitionEntry
WHERE (PartitionEntryId = '<ID FROM LOG
FILE>')
```

The SQL to update the location is as follows:

```
UPDATE PartitionEntry
SET PartitionRootPath = '<THE NEW
LOCATION>'
WHERE (PartitionEntryId = '<ID FROM LOG
FILE>')
```

- PartitionEntry/Locations [SecondaryLocation]
- Move the secondary storage files to a highly available location.
  - Update the database using SQL to point at the new location.

The SQL to view the current location is as follows:

```
SELECT *
FROM PartitionEntry
INNER JOIN Locations ON
PartitionEntry.SecondaryLocation =
Locations.LocationIdentity
WHERE (PartitionEntry.PartitionEntryId =
'<ID FROM LOG FILE>')
```

The SQL to update the location is as follows:

```
UPDATE Locations
SET Location = '<NEW LOCATION>'
WHERE LocationIdentity =
(SELECT SecondaryLocation FROM PartitionEntry
WHERE PartitionEntryId = '<ID FROM LOG
FILE>')
```

- PartitionEntry [StagingRoot Path]
- Move the contents of this location to a highly available location.
- Update the database using SQL to point at the new location.

The SQL to view the current location is as follows:

```
SELECT *
FROM PartitionEntry
WHERE (PartitionEntryId = '<ID FROM LOG
FILE>')
```

The SQL to update the location is as follows:

```
UPDATE PartitionEntry
SET StagingRootPath = '<THE NEW LOCATION>'
WHERE (PartitionEntryId = '<ID FROM LOG
FILE>')
```

- PSTMigratorTask [Migration Directory]
- 1

Move the contents of the location to a highly available location.
- 2

Use the Vault Administration Console to view the properties of the PST Migrator Task and update the Temporary files folder.

- ShoppingServiceEntry [ShoppingRootPath]
- Move the contents of this location to a highly available location.
- Use the Vault Administration Console to edit the Shopping service location to the new highly available location.

- SiteEntry [PSTHolding Directory]
- Move the contents of the location to a highly available location.
- Use the Vault Administration Console to view the site properties and update the PST Holding Folder property to point at the new location.

# About setting up Enterprise Vault in a VCS N+1 configuration

As a cheaper alternative to setting up an active/passive cluster, you can set up Enterprise Vault in a VCS N+1 configuration. Here, the cluster contains any number of Enterprise Vault servers and a single spare node.

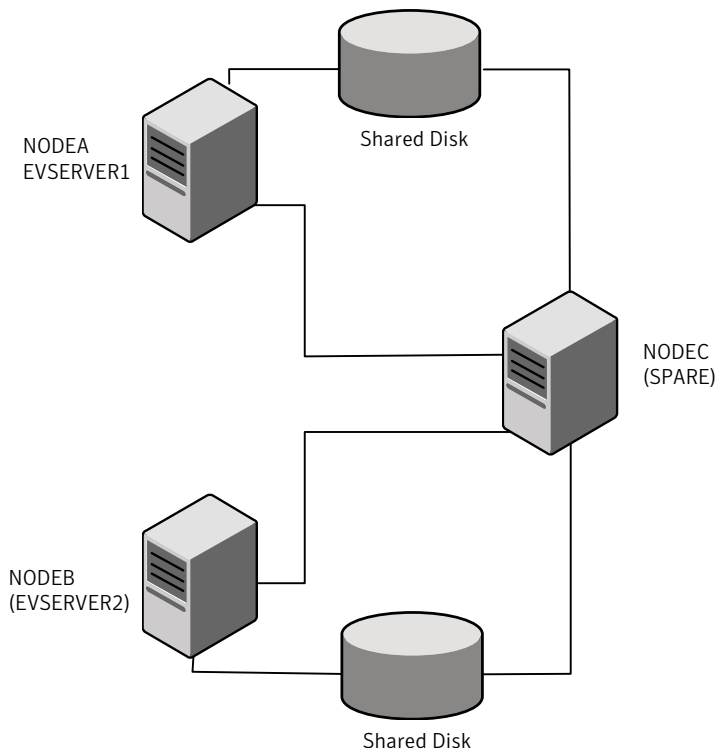
There are two basic types of N+1 configuration. For example, in a cluster that contains two Enterprise Vault servers, you can choose between these configuration types:

- The clustered Enterprise Vault servers run on two nodes, and there is a shared spare node.
- The two Enterprise Vault servers are configured to run on any of the three nodes in the cluster.

## Configuring two Enterprise Vault server nodes and a spare node in a VCS N+1 cluster

[Figure 30-1](#) illustrates a configuration in which there is a spare node in addition to the two nodes on which the Enterprise Vault servers are running. Remember that a cluster can contain many Enterprise Vault servers, depending on the number of available nodes.

**Figure 30-1** Three-node VCS cluster with two Enterprise Vault server nodes and a spare node



You configure the service group for EVSERVER1 to run on both NODEA and NODEC, and the service group for EVSERVER2 to run on both NODEB and NODEC. EVSERVER1 and EVSERVER2 are both virtual computer names from the service group.

**To configure two Enterprise Vault server nodes and a spare node in a VCS N+1 cluster**

- 1
- Mount the volumes on the system where you will configure the Enterprise Vault service group.
- See [“Managing disk groups and volumes in a Veritas Storage Foundation HA environment”](#) on page 243.
- 2
- On either NODEA or NODEC, run the Enterprise Vault Cluster Setup wizard and create a service group called EVSERVER1 for these two nodes.
- 3
- On either NODEB or NODEC, run the Enterprise Vault Cluster Setup wizard and create a service group called EVSERVER2 for these two nodes.
- 4
- Take the actions described below on NODEA and NODEB, depending on whether you are performing a first-time installation of Enterprise Vault or upgrading an existing installation.

Node	New installation	Upgrade installation
NODEA	Run the Enterprise Vault Configuration wizard. Choose to configure a new Enterprise Vault server with cluster group for EVSERVER1.	Run the Convert to Cluster wizard. Choose to create the service resources in the EVSERVER1 service group.
NODEB	Run the Enterprise Vault Configuration wizard. Choose to configure a new Enterprise Vault server with cluster group for EVSERVER2.	Run the Convert to Cluster wizard. Choose to create the service resources in the EVSERVER2 service group.

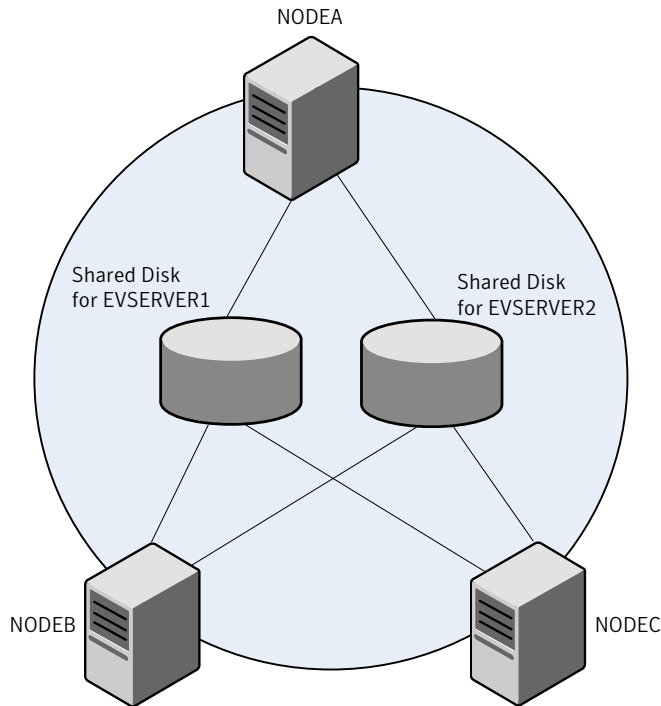
- 5
- On NODEC, run the Enterprise Vault Configuration wizard and choose to add this node as a failover node for an existing clustered server. Select either service group.

When you bring the service groups online on NODEA and NODEB, Cluster Explorer may falsely indicate a problem with the GenericService resources (their icons in the left pane may have question marks). This is because VCS assumes that each resource is simultaneously online on two nodes. You can ignore this situation.

## Configuring two Enterprise Vault servers to run on any of the three nodes in a VCS cluster

Figure 30-2 illustrates a configuration in which the two Enterprise Vault servers are configured to run on any of three nodes in a VCS cluster. This has the advantage that if NODEB fails, the server moves to NODEC. NODEB can then be brought back online and act as a failover server for EVSERVER1 and EVSERVER2.

**Figure 30-2** Three-node VCS cluster with two Enterprise Vault servers



**To configure two Enterprise Vault servers to run on any of the three nodes in a VCS cluster**

- 1 Mount the volumes on the system where you will configure the Enterprise Vault service group.

See [“Managing disk groups and volumes in a Veritas Storage Foundation HA environment”](#) on page 243.

- 2 With the Enterprise Vault Cluster Setup wizard, create a service group for EVSERVER1 that contains nodes NODEA, NODEB, and NODEC.

- 3
- With the Enterprise Vault Cluster Setup wizard, create a service group for EVSERVER2 that contains nodes NODEA, NODEB, and NODEC.
- 4
- Take the actions described below on NODEA and NODEB, depending on whether you are performing a first-time installation of Enterprise Vault or upgrading an existing installation.

Node	New installation	Upgrade installation
NODEA	Run the Enterprise Vault Configuration wizard. Choose to configure a new Enterprise Vault server with cluster group for EVSERVER1.	Run the Convert to Cluster wizard. Choose to create the service resources in the EVSERVER1 service group.
NODEB	Run the Enterprise Vault Configuration wizard. Choose to configure a new Enterprise Vault server with cluster group for EVSERVER2.	Run the Convert to Cluster wizard. Choose to create the service resources in the EVSERVER2 service group.

- 5
- On NODEC, run the Enterprise Vault Configuration wizard and choose to add this node as a failover node for an existing clustered server. Select either service group.

Notice that the only difference in configuration between this option and option 1 is that, when you create the service groups, you must select all the nodes rather than a subset of the nodes.

You can take a similar approach if you require your system to have more than one spare server (N+2, N+3, N+4, and so on). In each case, you must configure a node for each Enterprise Vault server and then add the spare nodes as failover nodes.

## Disallowing two Enterprise Vault servers on the same node in a VCS cluster

You cannot run multiple Enterprise Vault service groups on the same node in an active/active cluster configuration. When configuring the cluster in an N+x configuration, you can stop this from happening by setting the Limits and Prerequisites attributes for every node.

For more information on these steps, see the *Veritas Cluster Server Administrator's Guide*.

**To disallow two Enterprise Vault servers on the same node in a VCS cluster**

- 1 Use Veritas Cluster Manager to log on to the cluster.
- 2 Click anywhere in the Cluster Monitor panel to open Cluster Explorer.
- 3 For each node in the cluster, perform the following steps in the order listed:
  - In the configuration tree at the left, click the node whose attributes you want to edit.
  - In the View panel, click the **Properties** tab.
  - Click **Show all attributes** to open the Attributes View dialog box.
  - Find the Limits attribute.
  - Click the **Edit** icon at the right of the row.
  - In the Edit Attribute dialog box, add a key called EnterpriseVault and give it a value of 1.
  - Click **OK** to close the dialog box and return to the Attributes View dialog box.
  - Repeat for the Prerequisites attribute on each Enterprise Vault service group.

When both the Limits and Prerequisites attributes have a key called EnterpriseVault with a value of 1, two Enterprise Vault servers cannot run on the same node.





# Implementing an SFW HA-VVR disaster recovery solution with Enterprise Vault

This chapter includes the following topics:

- [About installing and configuring SFW HA-VVR with Enterprise Vault](#)
- [Overview of the steps for installing and configuring SFW HA-VVR](#)
- [Setting up the VCS cluster on the primary site](#)
- [Setting up the VCS cluster on the secondary site](#)
- [Adding the VVR components for replication](#)
- [Adding the GCO components for wide-area recovery](#)

## About installing and configuring SFW HA-VVR with Enterprise Vault

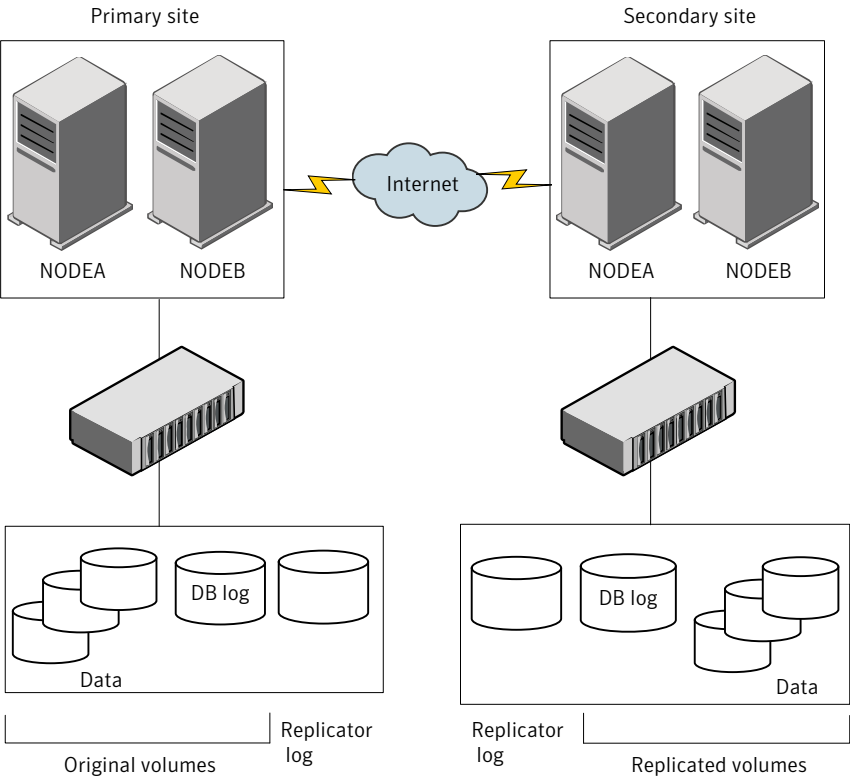
The procedure for installing and configuring SFW HA-VVR with Enterprise Vault is similar to the procedure that the *Veritas Storage Foundation and High Availability Solutions Guide* describes.

In this scenario, there is a source host on the primary site and a destination host on the secondary site. The application data is stored on the primary site and replicated to the secondary site by using the Veritas Volume Replicator (VVR).

The primary site provides data and services during normal operation. If a disaster occurs on the primary site and its data is destroyed, a secondary host can take over the role of the primary host to make the data accessible. The application can be restarted on that host.

Figure 31-1 shows an SFW HA-VVR configuration.

Figure 31-1 SFW HA-VVR configuration



This example has one disk group on each site for the application. Note that a VVR replicator log is needed on each site. If there are multiple disk groups, an additional replicator log is required for each one.

# Overview of the steps for installing and configuring SFW HA-VVR

Table 31-1 lists the tasks that you must perform to install and configure SFW HA-VVR.

Table 31-1            Installing and configuring SFW HA-VVR

Step	Task	See this section for more details
Step 1	Set up the VCS cluster on the primary site.	See “Setting up the VCS cluster on the primary site” on page 267.
Step 2	Set up the VCS cluster on the secondary site.	See “Setting up the VCS cluster on the secondary site” on page 268.
Step 3	Add the VVR components for replication.	See “Adding the VVR components for replication” on page 269.
Step 4	Add the Global Cluster Option (GCO) components for wide-area recovery.	See “Adding the GCO components for wide-area recovery” on page 269.

## Setting up the VCS cluster on the primary site

Complete the following steps to set up the cluster on the primary site. Except where noted, you can obtain more information on how to perform these steps from the *Veritas Storage Foundation and High Availability Solutions Guide*.

To set up the VCS cluster on the primary site

- 1    Install SFW HA 5.1 SP2 or later on each node that is to be a part of the cluster on the primary site.  

There are several stages to this process:

  - Review the product installation requirements, disk space requirements, and requirements for SFW HA.
  - Install Windows and configure the network settings.
  - Install SFW HA on the primary site. Be sure to select the VVR and GCO options during the installation.
  - Using the VVR Security Service Configuration wizard, configure the Veritas Volume Replicator Security Service (VxSAS).
- 2    Configure the cluster by running the VCS Configuration wizard.
- 3    Install Enterprise Vault.

- 4 Configure the disk group and volumes. You must create shared volumes to store the following:
  - Indexing service data
  - Shopping service data
  - Vault store partitions
  - PST holding folders
  - EMC Centera staging areas

We also recommend that you create separate volumes to store the MSMQ and registry replication data.
- 5 Configure the VCS service group at the primary site.

See [“About configuring the VCS service group for Enterprise Vault”](#) on page 245.
- 6 Verify the cluster configuration, and test the failover capability.

## Setting up the VCS cluster on the secondary site

The process of setting up a cluster on the secondary site is similar to that on the primary site. Except where noted, you can obtain more information on how to perform these steps from the *Veritas Storage Foundation and High Availability Solutions Guide*.

### To set up the VCS cluster on the secondary site

- 1 Create a parallel environment on the secondary site.
- 2 Configure the cluster by running the VCS Configuration wizard.
- 3 Install Enterprise Vault.
- 4 Configure the disk groups and volumes on the secondary site.

The disk group and volume setup on the secondary site must be identical to that on the primary site. The disks, disk groups, and volumes must be the same sizes, have the same names, and must be of the same type.
- 5 Configure the VCS service group at the secondary site, taking care to specify the same service group name that you specified on the primary site.
- 6 Verify the cluster configuration, and test the failover capability.

## Adding the VVR components for replication

This section provides information on configuring the VVR components for replication. You can obtain more information on how to perform these steps from the *Veritas Storage Foundation and High Availability Solutions Guide*.

### To add the VVR components for replication

- 1 Create a replicator log volume at each site.
- 2 Set up the replicated data sets for VVR on the hosts for the primary and secondary sites. Note that the Setup Replicated Data Set wizard lets you configure replicated data sets for both sites.
- 3 Create the VVR RVG service group.

You must run the Volume Replicator Agent Configuration wizard from the system that contains the application service group.

## Adding the GCO components for wide-area recovery

You require the Global Cluster Option (GCO) components to manage global clustering for wide-area disaster recovery. For information on how to perform the steps below, see the *Veritas Storage Foundation and High Availability Solutions Guide*.

### To add the GCO components for wide-area recovery

- 1 Ensure that your environment meets the requirements for global cluster operations.
- 2 Link clusters by adding a remote cluster.
- 3 Convert the local service group to a global group.
- 4 Perform additional global cluster administration tasks.



# Troubleshooting clustering with VCS

This chapter includes the following topics:

- [VCS logging](#)
- [Enterprise Vault Cluster Setup wizard error messages](#)
- [Viewing the clustered message queues for an Enterprise Vault virtual server](#)

## VCS logging

VCS generates two error message logs: the engine logs and the agent logs. Log file names are appended by letters, where A indicates the first log file, B the second, C the third, and so on; for example, `agent_A.txt`.

The agent log is located at `%VCS_HOME%\log` (typically `c:\Program Files\Veritas\cluster server\log`). The format of agent log messages is as follows:

*Timestamp Mnemonic Severity Message\_ID Message\_Text*

where:

<i>Timestamp</i>	Shows the date and time when the message was logged.
<i>Mnemonic</i>	Identifies the product (for example, VCS).
<i>Severity</i>	Indicates the severity of the error, which can be CRITICAL, ERROR, WARNING, NOTICE, or INFO. CRITICAL messages are the most severe, whereas INFO messages are the least severe.

*Message\_ID*

Is the unique numeric ID of the error message. The prefix V-16 denotes VCS.

*Message\_Text*

Is the message generated by VCS.

For example, a typical agent log message looks like this:

```
2006/01/24 11:04:17 VCS ERROR V-16-10051-6026 GenericService:
CLSEV1-EnterpriseVaultAdminService:monitor:
The LanmanResName attribute has not been configured.
```

# Enterprise Vault Cluster Setup wizard error messages

[Table 32-1](#) describes some messages that you may see when you run the Enterprise Vault Cluster Setup wizard.

**Table 32-1** Enterprise Vault Cluster Setup wizard error messages

Message	Explanation
Access Denied. You must have Administrator privileges to run the wizard.	Only users who are members of the local administrator's group can run this wizard.
VCS not running on the local machine. Either the service has not been started or it is in a stale state.	Verify that the VCS service has started and is running on the local machine.
MSMQ is not configured properly.	<div>The wizard verifies that MSMQ is installed and configured on all the nodes. The error message is shown if MSMQ is not installed on one node or the configuration is different.</div> <div>To resolve the problem, verify that MSMQ has been installed and configured before proceeding with the Enterprise Vault Cluster Setup wizard.</div>
The required resource type MSMQ is not installed on this system.	The wizard verifies that the MSMQ resource type is installed on the system. This resource type is installed with the 4.3 MP1.



# Viewing the clustered message queues for an Enterprise Vault virtual server

In a clustered Enterprise Vault installation, the Computer Management snap-in does not show Enterprise Vault message queues by default. It shows only queues for the local computer.

## To view the clustered message queues for an Enterprise Vault virtual server

- 1 Ensure the Enterprise Vault virtual server is online on the node you want to view the queues from.
- 2 Open a Command Prompt window and change to the Enterprise Vault installation folder (for example, C:\Program Files (x86)\Enterprise Vault).

- 3 Enter the following command:

```
ClusterCompMgmt
```

This launches the Computer Management snap-in with the environment variables set so that it displays the clustered message queues.

- 4 Expand **Services and Applications**, and then expand **Message Queuing**. The Enterprise Vault virtual server queues are listed under **Private Queues**.



# Clustering Enterprise Vault with Windows Server Failover Clustering

- [Chapter 33. Introducing clustering with Windows Server Failover Clustering](#)
- [Chapter 34. Preparing to cluster with Windows Server Failover Clustering](#)
- [Chapter 35. Configuring Enterprise Vault in a Windows Server failover cluster](#)
- [Chapter 36. Troubleshooting clustering with Windows Server Failover Clustering](#)



# Introducing clustering with Windows Server Failover Clustering

This chapter includes the following topics:

- [About clustering Enterprise Vault with Windows Server Failover Clustering](#)
- [Supported Windows Server Failover Clustering configurations](#)
- [Required software and restrictions on clustering Enterprise Vault with Windows Server Failover Clustering](#)
- [Typical Enterprise Vault configuration in a Windows Server failover cluster](#)
- [Control of Enterprise Vault services in a Windows Server failover cluster](#)

## About clustering Enterprise Vault with Windows Server Failover Clustering

You can cluster Enterprise Vault in a Windows Server failover cluster to provide a high availability solution for Enterprise Vault. If you are setting up Enterprise Vault in an environment where Microsoft Exchange and SQL server are clustered, you may want to cluster Enterprise Vault to ensure that you can meet your service level agreements, recovery times, and recovery point objectives.

High availability is provided by creating an Enterprise Vault cluster server that can fail over between physical nodes in the cluster. When Enterprise Vault services are running on a cluster server they operate with virtual IP addresses, a virtual computer name, virtual Microsoft Message Queues, and highly available shared

disks. When a failure occurs, the cluster software can move the cluster server's resources to a different physical node in the cluster.

To cluster Enterprise Vault in a failover cluster, you need a working knowledge of Windows Server Failover Clustering. See your Microsoft documentation for detailed information.

## Supported Windows Server Failover Clustering configurations

An Enterprise Vault cluster consists of:

- One or more primary nodes, each normally hosting an Enterprise Vault cluster server.
- One or more failover nodes: standbys that can take over the job of hosting an Enterprise Vault cluster server if a primary node fails.

Enterprise Vault does not permit "active/active" cluster configurations. That is, only one Enterprise Vault cluster server can run on a clustered node at any one time. You can configure Enterprise Vault in any operation mode that adheres to this restriction, such as:

- An active/passive failover pair: a primary node with a dedicated failover node.
- N+1 (hot standby server): two or more primary nodes share a single failover node. Only one node failure can be accommodated at any one time.
- N+M: an extension of the hot standby concept with N primary nodes and M failover nodes. Only M node failures can be accommodated at one time.
- N+M *any-to-any*: identical to N+M, except that there is no need to fail back to the original node after a failover. When the original node becomes available again, it can operate as a failover node.

## Required software and restrictions on clustering Enterprise Vault with Windows Server Failover Clustering

You must install Windows Server 2008 R2 on each primary and failover node.

Note the following restrictions:

- Neither Compliance Accelerator nor Discovery Accelerator must be installed on any server in the planned cluster. These products are not supported within

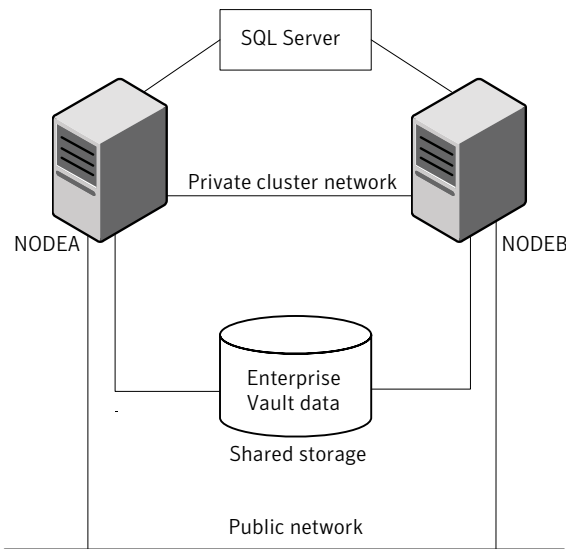
a cluster. However, an unclustered Compliance Accelerator or Discovery Accelerator can reference an Enterprise Vault cluster server.

- The Enterprise Vault Configuration wizard does not support cluster services that contain multiple client access point resources or IP address resources.
- We recommend that Enterprise Vault clusters contain only resources related to Enterprise Vault.

## Typical Enterprise Vault configuration in a Windows Server failover cluster

Figure 33-1 illustrates a typical configuration.

**Figure 33-1** Enterprise Vault in an active/passive failover pair configuration



In this example:

- NODEA and NODEB are the two Enterprise Vault nodes in the failover cluster. NODEA is the primary node. NODEB is the failover node.
- The SQL server and Microsoft Exchange may also be configured in the cluster: this does not affect Enterprise Vault.
- The volumes for the Enterprise Vault services data are configured on shared storage.

- The Enterprise Vault cluster server is configured on the primary node, NODEA. If NODEA fails, the cluster server's resources fail over to NODEB, and the cluster server comes online on NODEB.

## Control of Enterprise Vault services in a Windows Server failover cluster

Whether you configure Enterprise Vault as a server with cluster support, or as a failover node for an existing clustered server, the Configuration wizard installs the following set of Enterprise Vault services on the node:

- Directory service
- Indexing service
- Shopping service
- Storage service
- Task Controller service

An Admin service is already present from when Enterprise Vault was installed. The presence of this set of services is mandatory on each node, to ensure a common configuration on all nodes in the cluster. You cannot remove Enterprise Vault services in a clustered configuration.

The Configuration wizard sets the Enterprise Vault services to manual startup, to enable the cluster software to start and stop them as required.

---

**Note:** In a clustered configuration, you cannot start or stop services using the Administration Console or the EVService utility. If you stop a service using Windows Service Control manager, the cluster software assumes this is due to a system failure, and will restart the service or initiate a failover. To start or stop Enterprise Vault services safely, use only Failover Cluster Manager.

---

See [“Starting and stopping Enterprise Vault services in a Windows Server Failover Clustering environment”](#) on page 311.

## About cluster services and Enterprise Vault service resources in a Windows Server failover cluster

Before configuring an Enterprise Vault server as a server with cluster support, you must create a cluster service, which will become the Enterprise Vault cluster server. The Enterprise Vault Configuration wizard adds the following Enterprise



Vault service resources to the cluster service, to control and monitor the equivalent Enterprise Vault services on the active node:

- Admin service resource
- Directory service resource
- Indexing service resource
- Shopping service resource
- Storage service resource
- Task Controller service resource

The Configuration wizard also adds one more resource to the cluster service: an Enterprise Vault Server Instance resource. All the other Enterprise Vault resources in the cluster service are configured to be dependent on this resource, directly or indirectly. Its purpose is to prevent failovers to nodes already running Enterprise Vault, avoiding an active/active operation mode.

## What happens at failover in a Windows Server failover cluster

If an active node fails, the Enterprise Vault cluster server attempts to fail over to the next available node in the cluster service's preferred node list, assuming all the resources have that node as a possible owner. The Server Instance resource fails over first, provided the failover node is not already running an Enterprise Vault cluster server. The remaining resources then fail over in order of dependency. The resources start the Enterprise Vault services on the failover node, ensuring continuing availability for the data that Enterprise Vault is managing and archiving.



# Preparing to cluster with Windows Server Failover Clustering

This chapter includes the following topics:

- [Preparing to cluster Enterprise Vault with Windows Server Failover Clustering](#)
- [Setting up the shared disks and volumes for a Windows Server failover cluster](#)
- [Setting up the Enterprise Vault cluster services for a Windows Server failover cluster](#)

## Preparing to cluster Enterprise Vault with Windows Server Failover Clustering

The following procedure outlines the preparations that you must take before you can cluster a new or existing Enterprise Vault installation in a failover cluster. See your Microsoft documentation for detailed information.

### To prepare to cluster Enterprise Vault with Windows Server Failover Clustering

- 1 Decide on the operation mode for your cluster, including:
  - The number of primary nodes (each normally hosting an Enterprise Vault cluster server).
  - The number of failover nodes.

- Which nodes are to be the preferred owners of each cluster server.
- 2 Ensure that your setup meets the requirements.  
See [“Required software and restrictions on clustering Enterprise Vault with Windows Server Failover Clustering”](#) on page 278.
- 3 Set up the shared disks and volumes for the cluster.  
See [“Setting up the shared disks and volumes for a Windows Server failover cluster”](#) on page 284.
- 4 Use Failover Cluster Manager to create the cluster and to add the primary and failover nodes.
- 5 Set up a cluster service, including the prerequisite resources, for each Enterprise Vault cluster server you require.  
See [“Setting up the Enterprise Vault cluster services for a Windows Server failover cluster”](#) on page 285.

## Setting up the shared disks and volumes for a Windows Server failover cluster

You must set up shared storage and volumes for the cluster, ready to accept the shared data. Each Enterprise Vault cluster server requires one or more volumes in which to store the following:

- MSMQ data
- Indexing service data
- Storage service data (vault store partitions)
- Shopping service data
- PST holding folders
- EMC Centera staging areas

It is good practice for MSMQ data, Indexing service data, and Storage service data to each have a separate storage device resource. Placing them on the same drives may result in degraded performance.

For example, if you are setting up two Enterprise Vault cluster servers, EVSERVER1 and EVSERVER2, you might allocate the shared storage for the cluster as follows:

Cluster	■ Volume H: Quorum data
---------	-------------------------

- EVServer1

- Volume I: MSMQ data
  - Volume J: Indexing service data
  - Volume K: Vault store data
  - Volume L: PST holding folders, Shopping service data, EMC Centera staging areas
- EVServer2

- Volume I: MSMQ data
  - Volume J: Indexing service data
  - Volume K: Vault store data
  - Volume L: PST holding folders, Shopping service data, EMC Centera staging areas

Note the following when setting up the shared disks and volumes:

- You must configure the storage for different cluster services on different storage devices, as only one server can connect to a storage device at a time.
- Configure shared disks and volumes such that the required nodes will be able to access the clustered disk resources on failover. For example, in a 2+1 configuration, the failover node must have access to the quorum data volume, plus all the volumes that the cluster servers use.

# Setting up the Enterprise Vault cluster services for a Windows Server failover cluster

You must create and configure a cluster service for each cluster server that the cluster is to support. For example, for an N+M cluster, you require N cluster services. We recommend that Enterprise Vault clusters contain only resources related to Enterprise Vault.

**Note:** The Enterprise Vault Configuration wizard does not support cluster services that contain multiple client access point resources or IP address resources.

**Table 34-1** Prerequisite resources for Enterprise Vault cluster services

Resource type	Dependencies	Parameters	Comment
Storage Device or Volume Manager Disk Group	None	Specify the required disk volume.	Configure one disk resource for each volume you have set up for use by this cluster server.

Table 34-1

Prerequisite resources for Enterprise Vault cluster services

(continued)

Resource type	Dependencies	Parameters	Comment
Client Access Point	IP Address resource	<div><div>■ Use the cluster service name as the client access point.</div><div>■ We recommend that you check <b>DNS Registration Must Succeed</b>.</div><div>■ Check <b>Enable Kerberos Authentication</b>. This is required by the Message Queuing resource.</div></div>	Configure one client access point resource.
Message Queuing	<div><div>■ The Storage Device resource for this cluster server's MSMQ data</div><div>■ The Client Access Point resource</div></div>	None	Configure one message queuing resource.

### To set up the Enterprise Vault cluster services for a Windows Server failover cluster

- 1 Use Failover Cluster Manager to create and name the cluster service.

---

**Note:** When Failover Cluster Manager prompts you to select the service or application that you want to configure for high availability, select **Other Server**.

---

- 2 In the Properties of the cluster service, specify the nodes that are to be the preferred owners of this cluster service. List the nodes in the preferred order, according to your chosen operation mode.
- 3 Add the prerequisite resources to the cluster service. Add one resource of each resource type listed in the table, except where noted. We recommend you use the following naming format for the resources:

*service\_name-resource\_type*

For example, if you named a cluster service EV1 and you are adding a Storage Device resource, name the resource EV1-StorageDevice. Later, the Enterprise Vault Configuration wizard adds Enterprise Vault service resources to the cluster service using this naming format.

Specify the required nodes as possible owners for each resource, according to your chosen operation mode.

When you have finished setting up the cluster service, check that it can fail over between nodes without error.





# Configuring Enterprise Vault in a Windows Server failover cluster

This chapter includes the following topics:

- [About configuring Enterprise Vault in a Windows Server failover cluster](#)
- [Setting up a new Enterprise Vault installation with Windows Server Failover Clustering support](#)
- [Converting an existing Enterprise Vault installation to a Windows Server failover cluster](#)
- [Modifying an existing Enterprise Vault cluster](#)

## About configuring Enterprise Vault in a Windows Server failover cluster

This chapter describes:

- Setting up a new Enterprise Vault installation with cluster support.
- Converting an existing Enterprise Vault installation to a cluster.
- Modifying an existing Enterprise Vault cluster to add another Enterprise Vault clustered server or failover node, or to add more shared storage.

Before proceeding, you must have performed the preparatory steps for clustering.

See [“Preparing to cluster Enterprise Vault with Windows Server Failover Clustering”](#) on page 283.

# Setting up a new Enterprise Vault installation with Windows Server Failover Clustering support

This section describes how to set up a first-time Enterprise Vault installation as a cluster.

---

**Note:** If during the running of the Enterprise Vault Configuration wizard you receive an error that is related to the configuring of the Enterprise Vault Monitoring database, complete the wizard and refer to [Troubleshooting configuration of the Enterprise Vault Monitoring database](#).

---

## To set up a new Enterprise Vault installation with Windows Server Failover Clustering support

- 1 Install Enterprise Vault on all the nodes that are to run Enterprise Vault, both primary and failover, but do not run the Enterprise Vault Configuration wizard on any node at this stage.

---

**Caution:** The Enterprise Vault installation folder on all nodes should be the same. For example, if you install Enterprise Vault in the C:\Program Files (x86)\Enterprise Vault folder on the primary node, you must install it in the C:\Program Files (x86)\Enterprise Vault folder on the failover node. If you do not do this, you may experience problems when you configure Enterprise Vault on the failover node.

---

- 2 Configure the Enterprise Vault servers that are to act as clustered servers.  
See [“Configuring a new Enterprise Vault server with Windows Server Failover Clustering support”](#) on page 290.
- 3 Configure Enterprise Vault on the nodes that are to act as failover nodes.  
See [“Configuring a failover node in a Windows Server failover cluster”](#) on page 295.
- 4 Test the cluster to ensure the failovers work as planned.

## Configuring a new Enterprise Vault server with Windows Server Failover Clustering support

Perform one of the following procedures on a newly installed Enterprise Vault server to configure it as an Enterprise Vault server with cluster support. Choose the appropriate procedure depending on which of the following you want to do:

- Create an Enterprise Vault Directory on the Enterprise Vault server. This is mandatory for the first Enterprise Vault server you configure. The Directory is a container for Enterprise Vault Sites, which define common settings for Enterprise Vault servers. Every Enterprise Vault server must belong to just one Site. The configuration process creates a new Site in the new Directory and adds the Enterprise Vault server to that Site. It also creates a Directory database on the SQL server you specify.
- Join an Enterprise Vault Directory on another Enterprise Vault server. You can add the Enterprise Vault server to an existing Enterprise Vault Site in the Directory, or create a new Site in the Directory and add the Enterprise Vault server to that.

Follow this procedure if you want to create a new Enterprise Vault Directory. You must use this procedure if there is no existing Directory.

#### **To configure a server with a new Directory**

- 1 Use Failover Cluster Manager to ensure that a suitable cluster service that you prepared earlier is online on the Enterprise Vault server node.
- 2 On the node's Windows **Start** menu, click **All Programs > Enterprise Vault > Enterprise Vault Configuration**. The first page of the Enterprise Vault Configuration wizard appears.
- 3 Click **Create a new Enterprise Vault server with Cluster support**, and then click **Next**.
- 4 The wizard lists the cluster services that are currently online on this node. Select the prepared cluster service, and then click **Next**.
- 5 On the next Wizard page you can choose whether to create a new Vault Directory or to use an existing Vault Directory. Select **Yes** to create a new Vault Directory on this computer. This creates a new Enterprise Vault site. Click **Next**.
- 6 Select the language you want Enterprise Vault to use when populating the default settings in the Administration Console. Then click **Next**.
- 7 The wizard asks for details of the Vault Service account. This is the account you created earlier as part of the preinstallation tasks for Enterprise Vault. Use the format *domain\_name\username*. Alternatively, click the ... button and browse for the account.

Enter the password details and then click **Next**.

The wizard then displays a couple of messages relating to the Vault Service account having been granted user rights on the computer, and the creation of the Directory Service.

- 8 When prompted, enter the location of the SQL Server to use for the Enterprise Vault Directory database and click **Next**.
- 9 The wizard prompts you to enter the locations for the Enterprise Vault Directory database and transaction log. For performance reasons it is good practice to place these on separate disks. If default locations are shown, change them if they are incorrect. If you specified a SQL server on a remote computer, the paths must be valid paths on that computer, such as `\\DC\C$\Program Files\Microsoft SQL Server\MSSQL\Data.`  
Then click **Next**.
- 10 When prompted, enter the location of the SQL Server to use for the Enterprise Vault Monitoring database. Leave **Start Monitoring immediately** selected to begin monitoring as soon as the configuration is complete on this Enterprise Vault server. Then click **Next**.
- 11 The wizard prompts you to enter the locations for the Enterprise Vault Monitoring database and transaction log. For performance reasons it is good practice to place these on separate disks. If default locations are shown, change them if they are incorrect. If you specified a SQL server on a remote computer, the paths must be valid paths on that computer.  
Then click **Next**.
- 12 The wizard then prompts you for a name and description for the new Vault Site.  
**A Vault Site alias** is created automatically. This is the client access point for the cluster service that you selected in step 4.
- 13 Click **Next** to continue.
- 14 The wizard confirms the Enterprise Vault Site and Enterprise Vault Directory computer you have selected. It prompts you to specify the **Computer Alias** for the computer you are currently configuring.  
Enter the client access point for the Enterprise Vault cluster service that you selected in step 4, and click **Next** to update the Enterprise Vault Directory.
- 15 There is a prompt that asks whether you are sure that you do not want to use a DNS alias. Click **Yes** and then click **Next** again on the wizard page.
- 16 The wizard lists the Enterprise Vault services that are to be added to this computer. Click **Next** to add the services.
- 17 The wizard lists the Enterprise Vault services that it has now added. Note that in a cluster configuration you are not allowed to add or remove services. Click **Next** to continue.

- 18 The wizard shows a summary of the services it has added. Click **Next** to continue.
- 19 The Configuration wizard indicates that it needs to create cluster resources for each of the Enterprise Vault services.
- 20 The final wizard page displays a list of the actions the wizard has performed, and the results. Select **Run the Enterprise Vault Administration Console** and then click **Finish** to exit the wizard.

---

**Note:** Do not select the option to run the Getting Started wizard.

---

- 21 Follow the steps below to set the path to the index metadata folder, which must be on a shared drive in the cluster. The index metadata folder is the folder in which Enterprise Vault stores indexing configuration data and reporting data.
  - Bring the Enterprise Vault Directory service and Admin service online.
  - In the left pane of the Enterprise Vault Administration Console, browse to **Enterprise Vault Servers > EVServer.domain.local > Services**.
  - In the right pane, right-click **Enterprise Vault Indexing Service**, and then click **Properties**.
  - On the **General** tab of the Service Properties dialog box, set the **Index metadata location** path to that of the shared drive in the cluster.
  - Click **OK** to save the change that you have made, and then restart the Indexing service.

Follow this procedure if you want to join an existing Directory. The existing Directory does not need to be in the cluster.

#### To configure a server and join an existing Directory

- 1 Use Failover Cluster Manager to ensure that a suitable cluster service that you prepared earlier is online on the Enterprise Vault server node.
- 2 On the node's Windows **Start** menu, click **All Programs > Enterprise Vault > Enterprise Vault Configuration**. The first page of the Enterprise Vault Configuration wizard appears.
- 3 Click **Create a new Enterprise Vault server with Cluster support**, and then click **Next**.
- 4 The wizard lists the cluster services that are currently online on this node. Select the prepared cluster service, and then click **Next**.

- 5 On the next wizard page, select **No** to join an Enterprise Vault Directory on another Enterprise Vault server, and specify the DNS alias for the remote Enterprise Vault server.  
  
Click **Next** and continue.
- 6 On the next wizard page, do one of the following:
  - Select the option to create a new Vault Site in the remote Enterprise Vault Directory.
  - Click **Next** and continue from step 7.
  - Or select the option to join an existing Vault Site in the remote Enterprise Vault Directory, and select a Vault Site from the list displayed.
  - Then click **Next** and continue from step 10.
- 7 The wizard prompts you for a name and description for the new Vault Site.
- 8 The vault site alias, which is created automatically when the first Enterprise Vault server is added to the site, will be the DNS alias for the remote Enterprise Vault server you specified in step 6.
- 9 Click **Next** to continue.
- 10 The wizard confirms the Enterprise Vault Site and Enterprise Vault Directory computer you have selected. It prompts you to specify the **DNS Alias** for the computer you are currently configuring.
- 11 Enter the client access point of the Enterprise Vault cluster service.
- 12 Click **Next** to update the Enterprise Vault Directory.
- 13 The wizard lists the Enterprise Vault services that are to be added to this computer. Click **Next** to add the services.
- 14 The wizard lists the Enterprise Vault services that it has now added, giving you the option to check their properties. Note that in a cluster configuration you are not allowed to add or remove services. Click **Next** to continue.
- 15 The wizard displays the storage locations for the Indexing and Shopping services. These locations default to the first disk resource in the selected cluster service. If the locations are suitable, click **Next**. If you want to specify different storage locations, click **Back** and edit the properties of the service. The wizard displays a warning if you try to modify these to a local location such as `E:\Shopping`.
- 16 The Configuration wizard indicates that it needs to create cluster resources for each of the Enterprise Vault services.

- 17 The final wizard page displays a list of the actions the wizard has performed, and the results. Click **Finish** to exit the wizard.
- 18 Follow the steps below to set the path to the index metadata folder, which must be on a shared drive in the cluster. The index metadata folder is the folder in which Enterprise Vault stores indexing configuration data and reporting data.
  - Bring the Enterprise Vault Directory service and Admin service online.
  - In the left pane of the Enterprise Vault Administration Console, browse to **Enterprise Vault Servers > EVServer.domain.local > Services**.
  - In the right pane, right-click **Enterprise Vault Indexing Service**, and then click **Properties**.
  - On the **General** tab of the Service Properties dialog box, set the **Index metadata location** path to that of the shared drive in the cluster.
  - Click **OK** to save the change that you have made, and then restart the Indexing service.

## Configuring a failover node in a Windows Server failover cluster

Perform this procedure on the nodes that are to act as failover nodes.

### To configure a failover node in a Windows Server failover cluster

- 1 Ensure that the Enterprise Vault cluster service is online on a different node in the cluster. The cluster service must not be online on the node that you are configuring. The node that you are configuring must be a possible failover node for the resources.
- 2 On the node's Windows **Start** menu, click **All Programs > Enterprise Vault > Enterprise Vault Configuration**. The first page of the Enterprise Vault Configuration wizard appears.
- 3 Click **Configure the node as a failover node for an existing clustered server**, and then click **Next**.
- 4 The wizard prompts you for the name of the Enterprise Vault cluster service for which you want to add the node as a failover node.  
 Select the Enterprise Vault cluster service that is configured to fail over to this node and then click **Next**.
- 5 On the next wizard page, enter the password for the Vault Service account, and then click **Next**.

- 6 The next wizard page lists the actions the wizard will take if you proceed. To continue click **Next**, then click and then click **OK** to confirm the actions taken.
- 7 The final wizard page displays a list of the actions the wizard has performed, and the results. Click **Finish** to exit the wizard.

## Troubleshooting configuration of the Enterprise Vault Monitoring database

If during the running of the Enterprise Vault Configuration wizard you receive errors indicating that configuring the Enterprise Vault Monitoring database has failed, complete the configuration wizard and then run the Monitoring Configuration Utility to configure the Monitoring database and the Monitoring agents manually.

For information on how to do this, see the following Enterprise Vault technical note on the Symantec Support Web site:

<http://www.symantec.com/docs/TECH50809>

The technical note also describes how to troubleshoot issues with Monitoring agents.

## Examples of Enterprise Vault installations in various Windows Server Failover Clustering modes

These examples describe how to set up first-time installations of Enterprise Vault in various cluster operation modes.

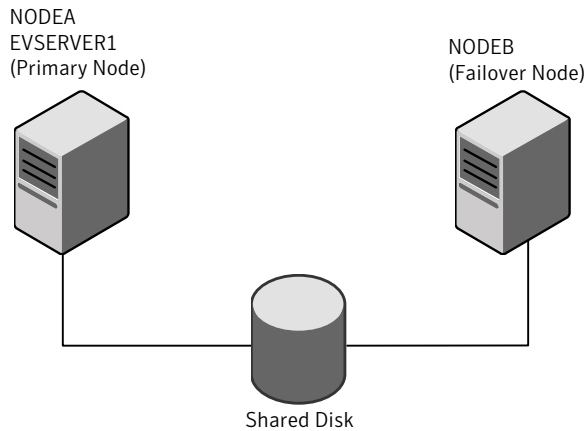
### Clustering Enterprise Vault in an active/passive failover configuration

This example describes setting up a new Enterprise Vault installation of an "active/passive" failover pair.

**Figure 35-1** illustrates a single failover pair, consisting of a primary node, NODEA, running the Enterprise Vault cluster server EVSERVER1, plus a dedicated failover node, NODEB.



**Figure 35-1** Failover pair configuration



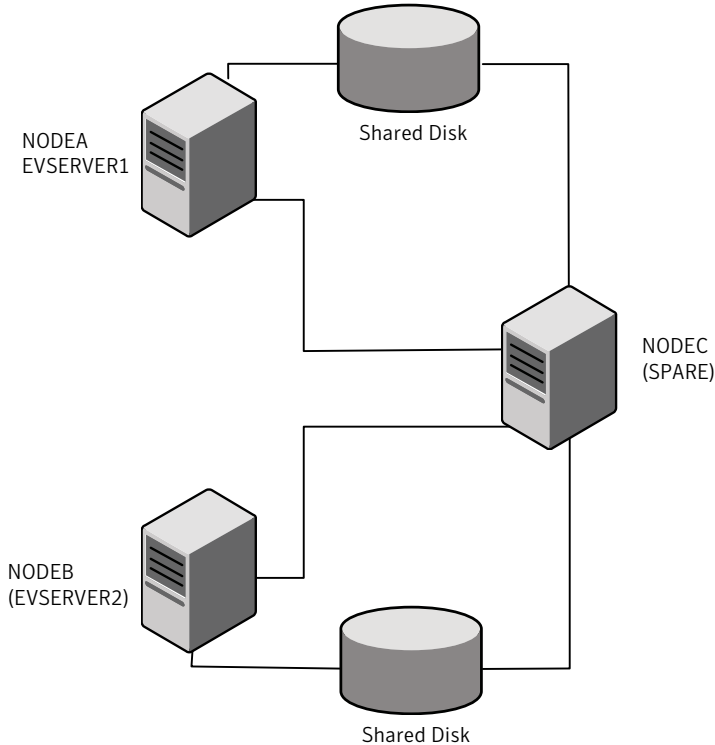
#### To cluster Enterprise Vault in an active/passive failover configuration

- 1 Prepare for clustering Enterprise Vault as follows:
  - Create a node for the primary server (NODEA).
  - Create a node for the failover server (NODEB).
  - Create a cluster service EVSERVER1 for the cluster server, with the preferred owners set to NODEA followed by NODEB.
  - Add the prerequisite resources to cluster service, ensuring that they have NODEA and NODEB as their possible owners.
  - Create a DNS entry for the cluster server.
- 2 Install Enterprise Vault on NODEA and NODEB, without running the Enterprise Vault Configuration wizard.
- 3 On NODEA, run the Enterprise Vault Configuration wizard and choose to configure a new Enterprise Vault server with cluster support. Select EVSERVER1 as the cluster service in which to create the Enterprise Vault service resources. A Vault Site alias will be created automatically.
- 4 On NODEB, run the Enterprise Vault Configuration wizard and choose to configure a failover node for an existing clustered server. Select EVSERVER1 as the cluster service for which you want to add this node as a failover node.
- 5 Test the failover from NODEA to NODEB.

## Clustering Enterprise Vault in a 2+1 configuration without "any-to-any" support

Figure 35-2 illustrates a configuration in which there is a single spare node in addition to the two nodes on which the Enterprise Vault servers are running.

**Figure 35-2** 2+1 configuration without "any-to-any" support



If either NODEA or NODEB fails, the virtual Enterprise Vault server running on that node can fail over to NODEC. This is not an "any-to-any" configuration so if a node fails the resources must be moved back after the node is recovered, in order to return to high availability.

**To cluster Enterprise Vault in a 2+1 configuration without "any-to-any" support**

- 1 Prepare for clustering as follows:
  - Add three nodes to the cluster (NODEA, NODEB, NODEC).
  - Create two cluster services (EVSERVER1, EVSERVER2), and add the prerequisite resources to each service.

- Configure the services and resources so that the following nodes are the preferred owners, in the order shown:

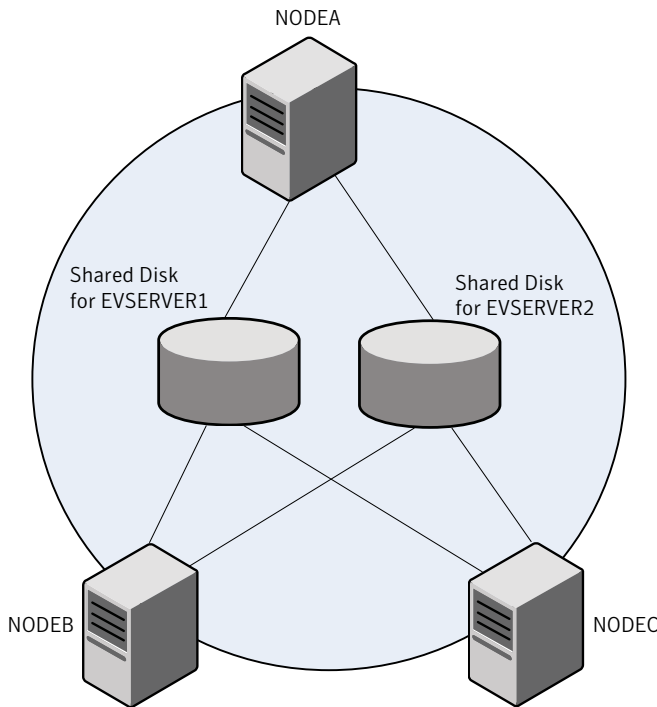
EVSERVER1	NODEA, NODEC
EVSERVER2	NODEB, NODEC

- Create DNS entries for the cluster servers EVSERVER1 and EVSERVER2.
- 2 Install Enterprise Vault on NODEA, NODEB, and NODEC, but do not run the Enterprise Vault Configuration wizard.
  - 3 On NODEA, run the Enterprise Vault Configuration wizard and choose to configure a new Enterprise Vault server with cluster support. Select EVSERVER1 as the cluster service in which to create the Enterprise Vault service resources. A Vault Site alias will be created automatically using the cluster server alias.
  - 4 On NODEB, run the Enterprise Vault Configuration wizard and choose to configure a new Enterprise Vault server with cluster support. Select EVSERVER2 as the cluster service in which to create the Enterprise Vault service resources. A Vault Site alias will be created automatically using the cluster server alias.
  - 5 On NODEC, run the Enterprise Vault Configuration wizard, and choose to configure a failover node for the existing clustered server. Select either EVSERVER1 or EVSERVER2 as the cluster service. This node will be configured as a failover node for both EVSERVER1 and EVSERVER2.
  - 6 Test the cluster to confirm that if NODEA fails, the EVSERVER1 resources fail over successfully to NODEC. Then return the EVSERVER1 resources to NODEA and confirm that if NODEB fails, the EVSERVER2 resources fail over successfully to NODEC.

## Clustering Enterprise Vault in a 2+1 "any-to-any" configuration

This second option for a 2+1 operation mode involves configuring the Enterprise Vault cluster servers EVSERVER1 and EVSERVER2 to run on any of the three nodes. This has the advantage that, for example, if NODEA fails and EVSERVER1 fails over to NODEC, you can bring NODEA back online to act as the failover node for EVSERVER1 and EVSERVER2.

**Figure 35-3** 2+1 "any-to-any" configuration



You can extend the setup process for an N+M configuration with any number of primary and failover nodes, up to the total of eight clustered nodes supported by Windows Server Failover Clustering.

**To cluster Enterprise Vault in a 2+1 "any-to-any" configuration**

**1** Prepare for clustering as follows:

- Add three nodes to the cluster (NODEA, NODEB, NODEC).
- Create two cluster services (EVSERVER1, EVSERVER2), and add the prerequisite resources to each service.
- Configure the services and resources so that the following nodes are the preferred owners, in the order shown:

EVSERVER1	NODEA, NODEC, NODEB
-----------	---------------------

EVSERVER2      NODEB, NODEC, NODEA

- 2 Follow steps 2 to 5 of the 2+1 configuration without "any-to-any" support. See ["Clustering Enterprise Vault in a 2+1 configuration without "any-to-any" support"](#) on page 298.
- 3 Test the cluster to confirm that if an active node fails, the cluster server fails over to the appropriate node.
- 4 For example, if you have configured the preferred owners of the cluster services as suggested in step 1:
  - Confirm that if NODEA fails, EVSERVER1 fails over successfully to NODEC.
  - Then bring NODEA back online as the spare node and confirm that if NODEB fails, EVSERVER2 fails over to NODEA.

## Converting an existing Enterprise Vault installation to a Windows Server failover cluster

If you have an existing Enterprise Vault installation on a single, unclustered server, you can convert it to a failover cluster. To be eligible for conversion to a cluster, the existing Enterprise Vault installation must meet the following conditions:

- Enterprise Vault should already be configured in a non-clustered configuration, and it must not already be part of a cluster.
- Enterprise Vault must be configured using DNS aliases rather than fully qualified node names.
- The Enterprise Vault server must have a full set of Indexing, Shopping, Task Controller, and Storage services.
- Neither Compliance Accelerator nor Discovery Accelerator must be installed on any server in the planned cluster. These products are not supported within a cluster. However, an unclustered Compliance Accelerator or Discovery Accelerator can reference an Enterprise Vault cluster server.

You can cluster an existing Enterprise Vault installation in any of the operation modes previously described. Note that:

- You can configure a combination of new and existing Enterprise Vault servers as cluster servers, if required.
- You must perform a new installation of Enterprise Vault on the nodes that are to act as failover nodes.

**To convert an existing Enterprise Vault installation to a Windows Server failover cluster**

- 1 Prepare for clustering.  
See [“Preparing to cluster Enterprise Vault with Windows Server Failover Clustering”](#) on page 283.
- 2 Install Enterprise Vault on the failover nodes and, if required, on any additional primary nodes you are adding to the existing installation. Do not run the Enterprise Vault Configuration wizard on any node at this stage. For instructions on installing Enterprise Vault, see Sections I and II of this manual.
- 3 Convert your existing Enterprise Vault servers to servers with cluster support.  
See [“Converting an existing Enterprise Vault server to a server with Windows Server Failover Clustering support”](#) on page 302.
- 4 If you are adding any new Enterprise Vault servers, configure the new Enterprise Vault servers as servers with cluster support.  
See [“Configuring a new Enterprise Vault server with Windows Server Failover Clustering support”](#) on page 290.
- 5 Configure Enterprise Vault on the failover nodes.  
See [“Configuring a failover node in a Windows Server failover cluster”](#) on page 295.
- 6 Test the cluster to ensure the failovers work as planned.

## Converting an existing Enterprise Vault server to a server with Windows Server Failover Clustering support

This section describes how to convert an existing Enterprise Vault server to a server with cluster support, including moving data to highly available locations.

**To convert an existing Enterprise Vault server to a server with Windows Server Failover Clustering support**

- 1 Ensure that the following items are all on highly available shared storage devices:
  - Indexing service data
  - Shopping service data
  - Vault store partitions
  - PST holding folders
  - EMC Centera staging areas

If they are not, correct the locations in the Enterprise Vault Directory database and then move the associated data to the new locations.

See [“Moving Enterprise Vault data to highly available locations”](#) on page 304.

- 2 Use Failover Cluster Manager to ensure that a suitable cluster service you prepared earlier is online on the Enterprise Vault server node.
- 3 On the Windows Start menu, click **All Programs > Enterprise Vault > Convert to Cluster**. The first page of the Enterprise Vault Convert to Cluster wizard appears. Click **Next** to continue.
- 4 The wizard makes a number of checks relating to the suitability of the installation for conversion to a cluster. It then displays a warning reminder that when the wizard has successfully completed you must update the DNS alias or Hosts file entry that is currently pointing at the physical node, so that it points at the cluster server name.
- 5 The wizard then displays a list of the current file locations for the Enterprise Vault services and partitions. You must confirm that these locations are all on highly available shared storage devices before continuing. Either select the check box to confirm high-availability, and click **Next** to continue, or click **Cancel** to exit from the wizard and move the required data to highly available locations before running the wizard again.
- 6 If the wizard detects that there are messages in the Enterprise Vault MSMQ queues, it displays a page indicating the name of each queue and the number of messages on it. The wizard cannot move these messages to the clustered message queues due to permissions constraints. We recommend you cancel from the wizard and leave the services running in a non-clustered environment until Enterprise Vault has cleared the message queues. You can then re-run the Convert to Cluster wizard. If you continue without doing this, the messages remain on the node-specific queues and are not processed. If you want to continue without clearing the queues, select the **Continue converting configuration to a cluster** check box and click **Next**.
- 7 The wizard lists the cluster services that are currently online on this node. Select the required cluster service, and then click **Next**.
- 8 The wizard creates the necessary resources, updates the Enterprise Vault services to manual startup, and updates the Directory database tables to remove the local computer name from the computer entry table and the message queue names. The final wizard page displays a list of the actions the wizard has performed, and the results. Click **Finish** to exit the wizard.
- 9 If you have not already done so, manually update the DNS alias to point at the cluster server name rather than the local node name.
- 10 Bring the cluster server resources online using Failover Cluster Manager.

## Moving Enterprise Vault data to highly available locations

In outline, the procedure for moving the Enterprise Vault data to highly available locations is as follows:

- Stop the Indexing, Shopping, Storage, and Task Controller services.
- Make a backup copy of the Enterprise Vault Directory database and data files.
- Use the Enterprise Vault Administration Console or run a SQL query against the Enterprise Vault Directory to move the data, as described below.

IndexRootPathEntry  
[IndexRootPath]

- Move the contents of this location to a highly available location.
- Update the database using SQL to point at the new location.

The SQL to view the current location is as follows:

```
SELECT *
FROM IndexRootPathEntry
WHERE (IndexRootPathEntryId = '<ID FROM
LOG FILE>')
```

The SQL to update the location is as follows:

```
UPDATE IndexRootPathEntry
SET IndexRootPath = '<THE NEW LOCATION>'
WHERE (IndexRootPathEntryId = '<ID FROM
LOG FILE>')
```

PartitionEntry  
[AccountName]

- Move the pool entry authorization (.pea) file to a highly available location.
- Use the Enterprise Vault Administration Console to view the properties of the EMC Centera partition and then, on the **Connection** tab, edit the **Pool Entry Authorization File Location** box to point at the new location.



PartitionEntry  
 [PartitionRootPath]

- Move the contents of this location to a highly available location.
- Update the database using SQL to point at the new location.

The SQL to view the current location is as follows:

```
SELECT *
FROM PartitionEntry
WHERE (PartitionEntryId = '<ID FROM LOG
FILE>')
```

The SQL to update the location is as follows:

```
UPDATE PartitionEntry
SET PartitionRootPath = '<THE NEW
LOCATION>'
WHERE (PartitionEntryId = '<ID FROM LOG
FILE>')
```

PartitionEntry/Locations  
 [SecondaryLocation]

- Move the secondary storage files to a highly available location.
- Update the database using SQL to point at the new location.

The SQL to view the current location is as follows:

```
SELECT *
FROM PartitionEntry
INNER JOIN Locations ON
PartitionEntry.SecondaryLocation =
Locations.LocationIdentity
WHERE (PartitionEntry.PartitionEntryId =
'<ID FROM LOG FILE>')
```

The SQL to update the location is as follows:

```
UPDATE Locations
SET Location = '<NEW LOCATION>'
WHERE LocationIdentity =
(SELECT SecondaryLocation FROM
PartitionEntry
WHERE PartitionEntryId = '<ID FROM LOG
FILE>')
```

PartitionEntry  
[StagingRootPath]

- Move the contents of this location to a highly available location.
- Update the database using SQL to point at the new location.

The SQL to view the current location is as follows:

```
SELECT *
FROM PartitionEntry
WHERE (PartitionEntryId = '<ID FROM LOG
FILE>')
```

The SQL to update the location is as follows:

```
UPDATE PartitionEntry
SET StagingRootPath = '<THE NEW LOCATION>'
WHERE (PartitionEntryId = '<ID FROM LOG
FILE>')
```

PSTMigratorTask  
[MigrationDirectory]

- Move the contents of the location to a highly available location.
- Use the Enterprise Vault Administration Console to view the properties of the PST Migrator Task and update the Temporary files folder.

ShoppingServiceEntry  
[ShoppingRootPath]

- Move the contents of this location to a highly available location.
- Use the Enterprise Vault Administration Console to edit the Shopping service location to the new highly available location.

SiteEntry  
[PSTHoldingDirectory]

- Move the contents of the location to a highly available location.
- Use the Enterprise Vault Administration Console to view the site properties and update the PST Holding Folder property to point at the new location.

# Modifying an existing Enterprise Vault cluster

This section describes how to modify an existing Enterprise Vault cluster to do the following:

- Add a node to host a new Enterprise Vault cluster server or to act as a failover node.
- Add shared storage for a cluster server.

## Adding a node to an existing Windows Server failover cluster

You may want to add a node to an existing Enterprise Vault cluster to host a new Enterprise Vault cluster server or to act as a failover node.

### To add a node to an existing Windows Server failover cluster

- 1 Share the required disk volumes on the new node.
- 2 Use Failover Cluster Manager to add the node to the cluster.
- 3 If you are adding a new Enterprise Vault cluster server, prepare a new cluster service and add the prerequisite resources.

See [“Setting up the Enterprise Vault cluster services for a Windows Server failover cluster”](#) on page 285.

- 4 Specify the new node as a possible owner of all resources in all the cluster services that are required to run on it.
- 5 Add the new node at a suitable position in the preferred owners list of any cluster service that is required to run on it.
- 6 Install Enterprise Vault on the node.
- 7 Run the Enterprise Vault Configuration wizard and choose either **Create a new Enterprise Vault server with Cluster support** or **Configure the node as a failover node for an existing clustered server**, as required.
- 8 Test the modified cluster to confirm that failovers to or from the new node work as planned.

## Adding shared storage to an existing Windows Server failover cluster for an Enterprise Vault cluster server

You may want to add shared storage to an existing Enterprise Vault cluster to provide more storage for an Enterprise Vault cluster server.

### To add shared storage to an existing Windows Server failover cluster for an Enterprise Vault cluster server

- 1 Set up the additional shared disks and volumes, sharing the volumes on the nodes that require access to them.
- 2 For the cluster server that is to use the new storage:
  - Add a Storage Device resource to the cluster service for each new volume. Make the Storage Device resource dependent on the Enterprise Vault **Server Instance** resource.
  - Change the Properties of the **Admin Service resource** to add a dependency on each new Storage Device resource.

- 3** Specify the required nodes as possible owners for the new Storage Device resources, according to your cluster operation mode.
- 4** Test the modified cluster to confirm that the Enterprise Vault cluster server can access the new shared storage successfully before and after failover.

# Troubleshooting clustering with Windows Server Failover Clustering

This chapter includes the following topics:

- [About this chapter](#)
- [Enterprise Vault event messages and the failover cluster log](#)
- [Resource ownership and dependencies when configuring Enterprise Vault in a failover clustered environment](#)
- [Registry replication on failover clustered nodes](#)
- [Viewing the clustered message queues for an Enterprise Vault cluster server](#)
- [Starting and stopping Enterprise Vault services in a Windows Server Failover Clustering environment](#)

## About this chapter

This chapter describes how to troubleshoot problems with Enterprise Vault in a Windows Server failover cluster.

---

**Note:** For information on backing up and recovering a clustered Enterprise Vault environment, see the *Administrator's Guide*.

---

## Enterprise Vault event messages and the failover cluster log

There are no specific Enterprise Vault event messages for clustering, but Enterprise Vault continues to write messages to the standard Application and Enterprise Vault event logs, so check these for errors.

If any failover cluster resources fail to come online, check the event logs and also the cluster log text file, typically `C:\WINDOWS\Cluster\cluster.log`.

To see the operations related to Enterprise Vault, search for "Enterprise Vault".

## Resource ownership and dependencies when configuring Enterprise Vault in a failover clustered environment

Resource ownership must be set up correctly to avoid problems when configuring Enterprise Vault in a cluster. The Configuration wizard only lists a cluster service for selection if every resource in it has the node on which you are running the wizard listed as a possible owner.

Resource ownership and resource dependencies must also be set up correctly to ensure failovers work as planned.

See [Table 34-1](#) on page 285.

The Enterprise Vault Configuration wizard sets up the dependencies for the Enterprise Vault service resources and the Server Instance resource when it adds them to the cluster service.

If you add a shared disk to an existing cluster you must ensure you set up the disk resource and dependencies correctly.

See [“Adding shared storage to an existing Windows Server failover cluster for an Enterprise Vault cluster server”](#) on page 307.

## Registry replication on failover clustered nodes

As part of configuring the cluster server, the Configuration wizard sets up a registry checkpoint on the Admin service resource, to provide the required registry replication on the clustered nodes.

If you suspect problems with registry entries related to an Enterprise Vault cluster server, view the checkpoint to confirm it is set up correctly. Enter the following command using the Windows command line utility `cluster`:

```
cluster resource EnterpriseVaultAdminService /check
```

where *EnterpriseVaultAdminService* is the name of the Admin service resource, for example EVSERVER1-EnterpriseVaultAdminService.

## Viewing the clustered message queues for an Enterprise Vault cluster server

In a clustered Enterprise Vault installation, the Computer Management snap-in does not show Enterprise Vault message queues by default. It shows only queues for the local computer.

### To view the clustered message queues for an Enterprise Vault cluster server

- 1 Ensure the Enterprise Vault cluster server is online on the node you want to view the queues from.
- 2 Open a Command Prompt window and change to the Enterprise Vault installation folder (for example, C:\Program Files (x86)\Enterprise Vault).
- 3 Enter the following command:

```
ClusterCompMgmt
```

This launches the Computer Management snap-in with the environment variables set so that it displays the clustered message queues.

- 4 Expand **Services and Applications**, and then expand **Message Queuing**. The Enterprise Vault cluster server queues are listed under **Private Queues**.

## Starting and stopping Enterprise Vault services in a Windows Server Failover Clustering environment

In a clustered environment, the clustering software must have control of the Enterprise Vault services. To allow this, the Enterprise Vault Configuration wizard sets the startup of these services to manual. Do not attempt to change the startup to automatic.

If a service starts or stops outside of the control of the cluster software, the cluster software assumes that this is due to a change in system condition. For example,

if a service stops, the cluster software assumes a failure and tries to restart the service or initiate a failover.

You should not attempt to start or stop Enterprise Vault services, except through the cluster software in one of the following ways:

- Use Failover Cluster Manager to bring the associated service resource online or offline.
- Use the Windows command-line utility `cluster`. For the syntax of this command, open a Command Prompt window and enter:

```
cluster /?
```

For more details, see the following article on the Microsoft Web site:

<http://technet2.microsoft.com/WindowsServer/en/library/8da99e1e-619f-4deb-acf0-cd8d61ac2ed01033.mspx>

To help prevent the starting and stopping of services by other means, Enterprise Vault behaves as follows in a clustered configuration:

- The Enterprise Vault Administration Console buttons for starting and stopping services are unavailable.
- You cannot start or stop services using the EVService utility. However, you can continue to use EVService to control tasks.
- Enterprise Vault blocks attempts to start Enterprise Vault services using the Windows Service Control Manager, and logs an event message. However, Enterprise Vault cannot block the stopping of services using Windows Service Control Manager, so be careful to avoid this.



# Index

## A

- About safety copies 204
- Active/passive failover configuration 238
- Admin permissions 185
- Administration Console
  - Using 183
- Agent configuration
  - modifying 249
- Assigning administrator roles 185
- Authorization Manager 185

## B

- Backup Exec 33

## C

- Clearwell eDiscovery platform 119
- Client computer
  - customizing security 136
- Client for Mac OS X 80
- Clustering
  - Veritas Cluster Server 237
  - Windows Server Failover Clustering 277
- Collection 210
  - on EMC Centera 211
- computer
  - adding new 148
- Configuration
  - modifying using wizard 249
  - typical setup 238
- Configuration Program 183
- configuration wizard 147
- Configuration wizards
  - Exchange Server Configuration 247
- Configurations
  - active/passive failover 238
- Configure sharing 215
- Connectivity test
  - when adding server to Index Server group 225
  - when associating vault store with Index Server group 227

- Connectivity test *(continued)*
  - when changing indexer 229

## D

- Default domain
  - with basic authentication 134
- Device-level sharing
  - EMC Centera 200
- Discovery Search Service
  - additional requirements for 119
  - manually configuring a request endpoint 174
  - manually configuring a result endpoint 176
  - prerequisite software for 119
  - requiring HTTPS connections 177
  - running the Configuration utility 173
- DNS alias 59
- Domino Journaling
  - configuring access for Enterprise Vault 100
  - configuring the journaling databases 99
  - Database Management 99

## E

- EMC Centera
  - device-level sharing 200
- EMC Centera devices
  - Collections 211
- Enterprise Vault
  - configuring 145
  - hardware requirements 27
  - installing 127, 141
  - network requirements 30
  - running on a virtual server 28
  - storage requirements 30
- Enterprise Vault Client for Mac OS X 80
- Enterprise Vault Operations Manager
  - accessing 170
  - configuring 169
  - requirements 61
- Enterprise Vault Reporting
  - prerequisites 64
  - reporting user account 65

Enterprise Vault Reporting *(continued)*  
 requirements 63

Enterprise Vault site  
 creating new 148

Exchange  
 supported versions 67

Exchange agent  
 about 238  
 configuring using wizard 247  
 supported services 238  
 troubleshooting 271  
 typical setup 238

Exchange archiving  
 preinstallation tasks 68, 70, 77

Exchange cluster  
 active/passive setup 238

Exchange cluster configuration  
 Active/Passive failover 238

Exchange Service agent 238

Exchange service group  
 modifying 249

## F

FDCC compliant computers  
 configuring 138

File System Archiving  
 accounts for managing 106  
 file server preparation 106  
 FSA Agent 105  
 prerequisites 103  
 requirements 103  
 shortcuts 104

Fingerprint database 199

Fingerprint Databases  
 disk space requirements 35

FIPS compliance  
 re-running the Operations Manager  
 Configuration utility 169

FSA Agent 105

FSA Reporting  
 prerequisites 64

FSA Reporting database  
 disk space requirements 37

Fujitsu ETERNUS 33

## H

Hardware requirements for Enterprise Vault  
 server 27

Hardware requirements for SQL server 29  
 HTTPS support 233

## I

IBM System Storage DR550 33

Index Server  
 grouped and ungrouped 219

Index Server group  
 adding a server 225  
 creating 223  
 do I need to create? 220

Index Server groups  
 about 219

Index volume  
 and Index Server group 220

Indexer  
 assigning vault store 228

Internet Explorer  
 for users 79

## L

License keys 123  
 obtaining 124

Licenses 123

## M

Mac OS X client 80

Mapped drive  
 and User Account Control (UAC) 60

MDAC version 47

Microsoft Authorization Manager 185

Migration 210  
 of archived data 33

Mobile Search  
 configuring 85  
 hardware requirements 85  
 operating system for 86  
 preinstallation tasks 85  
 prerequisites 85  
 Web server role 87

Monitoring database  
 disk space requirements 36  
 troubleshooting 152

MSMQ  
 Installing 43

MSXML 45

## N

- Net.Tcp port sharing 47
- NetBackup 33
- Network requirements for Enterprise Vault server 30
- Nirvanix Storage Delivery Network 33

## O

- Operations Manager
  - accessing 170
  - configuring 169
  - requirements 61
- Outlook Add-In 79
  - requirements 79
- Outlook versions
  - for users 79
- OWA client support 81

## P

- Partition
  - creating 208, 211
  - network shares (NTFS) 214
- Partition network shares 214
- Partition states 209
- Port sharing
  - using Net.Tcp port sharing service 47
- Production license defined 123
- PstDisableGrow 79

## R

- Reporting
  - requirements 63
- Reporting user account
  - setting up 65
- Request endpoint for Discovery Search Service
  - configuring 173
  - manually configuring 174
  - requiring HTTPS connections 177
- Result endpoint for Discovery Search Service
  - manually configuring 176
  - requiring HTTPS connections 177
- Retention Category
  - creating new 186
- Roles
  - assigning administrator 185
- Roles-based administration 185

## S

- Safari browser support 81
- Safety copies
  - archive attribute 205
  - removal 204
  - trigger file mechanism 206
- Saveset files 198
- Securing index and archive data 59
- Security
  - on client computers 136
- security
  - for Web Access application [security Web] 131
- Service group
  - modifying 249
- Services
  - configuring 151
- Sharing levels 196
- Sharing regime 201
- Shortcuts
  - File System Archiving 104
- Single instance storage
  - about 194
  - developing a suitable sharing regime 201
  - how it works 198
  - requirements 200
  - sharing boundaries 196
  - sharing levels 196
- SIS parts
  - and fingerprint database 199
  - definition 198
  - deletion 199
- SMTP Archiving
  - MAPI messages 114
- SQL login
  - for Vault Service account 55
- SQL server
  - hardware requirements 29
- SQLXML 47
- Storage
  - setting up 193
- Storage requirements for Enterprise Vault server 30
- Storage streamer API devices
  - sharing partitions 201
- Supported services 238
- Supported versions 237
- Symantec Backup Exec 33
- Symantec NetBackup 33

**T**

- TCP/IP
  - required on client computers 79
- Temporary license
  - defined 123
- Tivoli Storage Manager 33
- Trialware license
  - defined 123
- Troubleshooting
  - Exchange service agent 272
- troubleshooting information 271

**U**

- UAC (User Account Control) 60
- Ungrouped Index Server
  - adding to Index Server group 225
- User Account Control (UAC) 60

**V**

- Vault Directory
  - creating new 148
- Vault Directory Database
  - disk space requirements 35
- Vault Service account
  - requirements 53
  - SQL login 55
- Vault Site alias
  - creating 59
- Vault store
  - assign to different indexer 228
  - creating 204
- Vault Store Database
  - disk space requirements 35
- Vault store group
  - configure sharing for 215
  - creating 203
- Vault Stores
  - Overview 194, 204
- VCS 237
- Veritas Cluster Server 237

**W**

- WCF Activation 119
- Web Access application
  - application pool 44
  - basic authentication 134
  - customizing security for 132
  - https support 233
- Web Access application *(continued)*
  - setting up security 131
  - specifying a port 233
- Windows Communication Foundation Activation. *See* WCF Activation
- Windows PowerShell 46
- Windows Search 80
- Windows Server Failover Clustering 277
  - configuring 289
- Wizards
  - Exchange Server Configuration 247