

# Symantec Enterprise Vault™

## Introduction and Planning

10.0

# Symantec Enterprise Vault: Introduction and Planning

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: 2012-08-24.

## Legal Notice

Copyright © 2012 Symantec Corporation. All rights reserved.

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

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

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

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

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

Symantec Corporation  
350 Ellis Street, Mountain View, CA 94043

<http://www.symantec.com>

# Technical Support

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

Symantec's support offerings include the following:

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

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

<http://support.symantec.com>

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

## Contacting Technical Support

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

<http://support.symantec.com>

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

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

- Product release level

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

## Licensing and registration

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

<http://support.symantec.com>

## Customer service

Customer service information is available at the following URL:

<http://support.symantec.com>

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

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

## Support agreement resources

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

Asia-Pacific and Japan	<a href="mailto:customercare_apac@symantec.com">customercare_apac@symantec.com</a>
Europe, Middle-East, and Africa	<a href="mailto:semea@symantec.com">semea@symantec.com</a>
North America and Latin America	<a href="mailto:supportsolutions@symantec.com">supportsolutions@symantec.com</a>



# Contents

Technical Support .....	3
Chapter 1      About this guide .....	13
Introducing this guide .....	13
Where to get more information about Enterprise Vault .....	14
“How To” articles on the Symantec Enterprise Support site .....	15
Enterprise Vault training modules .....	16
Comment on the documentation .....	16
Chapter 2      Introduction .....	17
Overview of Enterprise Vault .....	17
How archiving works .....	18
How to access items in archives .....	19
About Compliance Accelerator and Discovery Accelerator .....	22
About Enterprise Vault add-ons .....	23
How Enterprise Vault works .....	28
About single instance storage .....	32
About Enterprise Vault indexing .....	35
About Index Server groups .....	38
About Enterprise Vault Administration Console .....	41
About Enterprise Vault sites, Directory, and Directory database .....	41
About Enterprise Vault tasks .....	43
About Enterprise Vault services .....	46
About the Discovery Search Service .....	51
About the Enterprise Vault Outlook Add-In .....	53
About the Enterprise Vault Client for Mac OS X .....	55
About Microsoft Exchange forms .....	55
About OWA Extensions .....	56
About Enterprise Vault Mobile Search .....	56
About Enterprise Vault extensions for Lotus Notes .....	57
About Enterprise Vault Web access components .....	57
About Enterprise Vault monitoring and reporting .....	59
FIPS 140-2 compliance .....	59

Chapter 3	Enterprise Vault administration .....	61
	About Enterprise Vault administration .....	61
	Administration Console configuration of archiving .....	62
	Administration accounts and roles .....	62
	How to archive PST file contents .....	63
	How to archive NSF file contents .....	63
	How to export archived items .....	64
	Welcome message and other notifications .....	64
	About reporting and monitoring in Enterprise Vault .....	65
	Enterprise Vault Reporting .....	66
	Report mode .....	67
	Event and diagnostic logging .....	67
	System status in the Administration Console .....	68
	Enterprise Vault Operations Manager .....	68
	Automatic monitoring of events and performance .....	69
	Message queue monitoring .....	70
	Enterprise Vault auditing .....	70
	Veritas Backup Reporter 6.6 support for Enterprise Vault .....	71
	How to script management tasks .....	71
	Checklist of day-to-day management tasks .....	72
Chapter 4	Exchange Server archiving .....	75
	About Exchange Server archiving and user mailboxes .....	75
	Exchange Provisioning tasks .....	76
	Exchange Mailbox Archiving tasks .....	76
	Exchange archiving targets .....	77
	Exchange mailbox policies .....	78
	Exchange desktop policies .....	78
	Exchange archiving filters .....	79
	Exchange Server and journal mailbox archiving .....	80
	Exchange Server and journal filtering .....	81
	Compliance Accelerator and Exchange journaling .....	81
	Types of items to archive with Exchange Server archiving .....	81
Chapter 5	Exchange Public Folder archiving .....	83
	Exchange Public Folder tasks, Targets, and Policies .....	83
	How an Exchange Public Folder task archives .....	84
	User access to Exchange Public Folder archives .....	85



Chapter 6	File System Archiving .....	87
	About File System Archiving .....	88
	About File archiving policies .....	88
	About shortcut files with File System Archiving .....	89
	About setting up File System Archiving .....	92
	File System Archiving in a clustered environment .....	95
	The process of File System Archiving .....	97
	How File System Archiving handles older versions of archived files .....	99
	How File System Archiving synchronizes permissions .....	99
	File System Archiving reports .....	99
	How to restore files with File System Archiving .....	100
	About FSAUtility .....	101
	How to back up and scan shortcut files with File System Archiving .....	102
	Pass-through recall for placeholder shortcuts with File System Archiving .....	102
	File Blocking with File System Archiving .....	103
	File Blocking configuration with File System Archiving .....	104
	Retention Folders and File System Archiving .....	105
	FSA Reporting .....	106
Chapter 7	Archiving Microsoft SharePoint™ servers .....	109
	About archiving Microsoft SharePoint servers .....	109
	How to configure SharePoint archiving .....	110
	SharePoint archiving tasks .....	110
	SharePoint archiving targets .....	111
	SharePoint archiving reports .....	112
	SharePoint archiving policies .....	112
	How to access archived SharePoint documents .....	113
	About Enterprise Vault shortcuts in SharePoint .....	113
Chapter 8	Domino mailbox archiving .....	115
	About Domino mailbox archiving and Enterprise Vault .....	115
	Domino provisioning groups .....	117
	Domino mailbox archiving tasks .....	118
	Domino mailbox archiving policies .....	119
	Domino mailbox archiving retention folders .....	119
	Domino mailbox archiving desktop policies .....	120

Chapter 9	Domino Journal archiving .....	121
	About Domino Journal archiving .....	121
	Domino Journal archiving policies .....	121
	Domino journal archiving database considerations .....	122
	How to set up Domino Journal Archiving .....	122
	Support for clustered Domino Journal databases .....	123
Chapter 10	SMTP Archiving .....	125
	Overview of SMTP Archiving .....	125
	SMTP Archiving architecture .....	125
	Setting up SMTP Archiving .....	127
Chapter 11	Enterprise Vault Accelerators .....	129
	About the Enterprise Vault Accelerators .....	129
	Differences between the Enterprise Vault Accelerators .....	130
	About Compliance Accelerator .....	130
	Compliance Accelerator components .....	131
	The Compliance Accelerator client application .....	134
	Compliance Accelerator configuration data .....	136
	About Discovery Accelerator .....	136
	The analytics facility in Discovery Accelerator .....	137
	Discovery Accelerator components .....	138
	Discovery Accelerator client application .....	140
	Discovery Accelerator configuration data .....	142
Chapter 12	Building in resilience .....	143
	About Enterprise Vault and VCS .....	143
	Supported VCS configurations and software .....	143
	About Enterprise Vault and the VCS GenericService agent .....	144
	Typical Enterprise Vault configuration in a VCS cluster .....	144
	About Enterprise Vault and Windows Server Failover Clustering .....	145
	Supported Windows Server Failover Clustering	
	configurations .....	145
	Typical Enterprise Vault configuration in a Windows Server	
	failover cluster .....	146
	About Enterprise Vault building blocks .....	147
	Building blocks and high availability .....	149

Chapter 13	Planning component installation .....	151
	About planning component installation .....	151
	Prerequisites for Enterprise Vault components when planning installation .....	151
	Factors to consider when planning deployment of Enterprise Vault components .....	152
	Enterprise Vault Directory Service installation planning .....	152
	Where to set up the Enterprise Vault Services and Tasks .....	153
	How to plan installing Exchange Mailbox Archiving Tasks .....	156
	How to plan installing Exchange Journaling Tasks .....	157
	How to plan installing Exchange Public Folder Tasks .....	157
	How to plan installing Domino Journaling and Mailbox Archiving Tasks .....	158
	How to plan installing the Move Archive task .....	158
	How to plan installing the Storage Service .....	158
	How to plan installing the Indexing Service .....	158
	How to plan installing the Shopping Service .....	160
	How to plan installing File System Archiving .....	160
	How to plan installing SharePoint Archiving .....	160
	How to plan installing SMTP Archiving .....	160
	How to plan installing Accelerator Services .....	161
	Enterprise Vault databases and planning their installation .....	161
	Vault store groups and vault stores installation planning .....	163
	Administration Console installation .....	165
	Installation planning for client components .....	165
	Installation planning for Outlook Web Access (OWA) and RPC over HTTP components .....	166
Chapter 14	Planning your archiving strategy .....	167
	About archiving strategies .....	168
	Where to define default settings for the Enterprise Vault Site .....	169
	How to allow users flexibility .....	170
	How to plan the types of items to archive .....	170
	How to define your archiving policy for user mailboxes .....	170
	How to plan enabling mailboxes .....	171
	How to plan controlling the appearance of the desktop .....	172
	How to plan the archiving policy for journal mailboxes .....	172
	How to plan the archiving strategy for Exchange public folders .....	173
	How to plan enabling public folders .....	174
	How to plan an archiving strategy for FSA .....	174
	How to plan a strategy for SharePoint archiving .....	175
	How to plan settings for Retention Categories .....	176

- How to plan the automatic deletion of archived items ..... 177
- How to plan PST migration ..... 177
- How to plan NSF migration ..... 178
- How to plan shared archives ..... 178
- How to plan vault stores and partitions ..... 179
  - How to plan handling safety copies ..... 179
- How to plan single instance storage ..... 180
- About Enterprise Vault reports ..... 180
  - Enterprise Vault Reporting feature ..... 181

Index ..... 183

# About this guide

This chapter includes the following topics:

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

## Introducing this guide

This book gives an introduction to Symantec Enterprise Vault and associated products and explains how to plan your installation.

The book is designed to be read serially. The first part introduces the features and architecture of the various Enterprise Vault components. This gives you the background information you need to plan and set up your Enterprise Vault system. The second part describes the planning decisions that you need to make to set up Enterprise Vault.

To set up Enterprise Vault, you need a working knowledge of the following products:

- Windows 2008 R2 administrative tasks
- Microsoft SQL Server
- Microsoft Message Queue Server
- Microsoft Outlook
- Internet Information Services (IIS)

If you are going to be using Enterprise Vault with Microsoft Exchange Server or Microsoft SharePoint Portal Server, you should also have a working knowledge of these products.

# 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	Includes all the following documentation so that you can search across all files. You can access this file by doing either of the following: <ul style="list-style-type: none"><li>■ On the Windows <b>Start</b> menu, click <b>Start &gt; Programs &gt; Enterprise Vault &gt; Documentation</b>.</li><li>■ In the Administration Console, click <b>Help &gt; Help on Enterprise Vault</b>.</li></ul>
<i>Introduction and Planning</i>	Provides an overview of Enterprise Vault functionality.
<i>Deployment Scanner</i>	Describes how to check the prerequisite software and settings before you install Enterprise Vault.
<i>Installing and Configuring</i>	Provides detailed information on setting up Enterprise Vault.
<i>Upgrade Instructions</i>	Describes how to upgrade an existing Enterprise Vault installation to the latest version.
<i>Setting up Exchange Server Archiving</i>	Describes how to archive items from Microsoft Exchange user mailboxes, journal mailboxes, and public folders.
<i>Setting up Domino Server Archiving</i>	Describes how to archive items from Domino mail files and journal databases.
<i>Setting up File System Archiving</i>	Describes how to archive the files that are held on network file servers.
<i>Setting up SharePoint Server Archiving</i>	Describes how to archive content from Microsoft SharePoint servers.
<i>Setting up SMTP Archiving</i>	Describes how to archive SMTP messages from other messaging servers.
<i>Administrator's Guide</i>	Describes how to perform day-to-day administration, backup, and recovery procedures.

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

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

For the latest information on supported devices and versions of software, see the *Enterprise Vault Compatibility Charts* book, which is available from this address:  
<http://www.symantec.com/docs/TECH38537>

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

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

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

- 1 Type the following in the address bar of your Web browser, and then press **Enter**:  
[http://www.symantec.com/business/support/all\\_products.jsp](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.



# Introduction

This chapter includes the following topics:

- [Overview of Enterprise Vault](#)
- [How Enterprise Vault works](#)
- [FIPS 140-2 compliance](#)

## Overview of Enterprise Vault

Enterprise Vault is a Windows application that enables an organization to store messaging and file system data automatically in centrally-held archives. Using Enterprise Vault clients, users can retrieve selected items easily and quickly when required.

Enterprise Vault can archive any of the following types of data:

- Items in Microsoft Exchange user mailboxes
- Items in Microsoft Exchange journal mailboxes
- Microsoft Exchange Public Folder contents
- Items in Domino mail files
- Items in Domino journal databases
- Files held on network file servers
- Items held on Microsoft SharePoint servers
- Instant Messages and Bloomberg messages
- SMTP messages from other messaging servers

For a full list of the platforms and operating systems from which Enterprise Vault can archive, and the operating systems supported for client access of archived

items, see the *Enterprise Vault Compatibility Charts*, available at the following address on the Symantec Enterprise Vault Support site:

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

## How archiving works

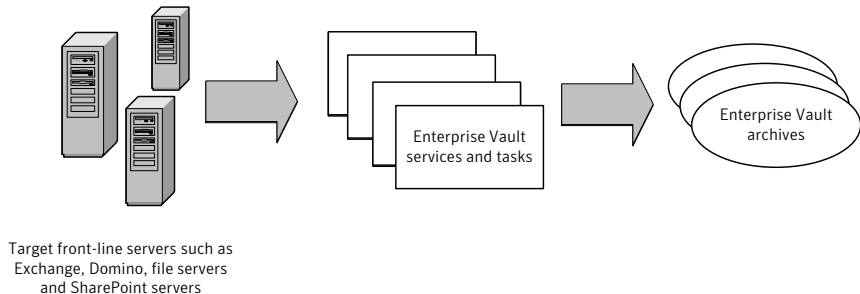
At scheduled times, Enterprise Vault archiving processes check target servers for items to archive. Relevant items are then stored in Enterprise Vault archives.

Archived items are indexed by Enterprise Vault to enable fast searching and retrieval. The administrator can set the level of indexing required.

When an item is archived, it is automatically assigned a Retention Category, which defines how long it must be kept. The administrator can define different Retention Categories for different types of data. As Enterprise Vault monitors the archives, it can then delete items when the retention period expires.

Figure 2-1 describes how Enterprise Vault tasks and services store data in archives.

**Figure 2-1** Enterprise Vault tasks and services store data in archives



The original items can be replaced with shortcuts to the archived copy. In this way primary storage on user computers and servers can be freed up. From the end users' point of view, they will still be able to access the items as before.

A wide range of configuration options allow the administrator to customize and control the archiving process.

Some examples of configuration options are as follows:

- The time and frequency of archiving runs.
- What is to be archived. Some of the attributes that can be used to define whether a file is to be archived are: where the file is located, file age, file type, size.
- Where particular archived items are to be stored.

- Available Retention Categories.
- Required level of indexing.
- Whether shortcuts are to be created and their contents.
- What access users are to be allowed to have to archived items.

## Introduction to PST files and NSF files

In many organizations, PST files have been used to back up Exchange Server mailbox contents. Using Enterprise Vault to archive Exchange Server mailboxes removes the need for these PST files. To ensure that all legacy information is archived, Enterprise Vault includes PST migration tools for importing PST files into Enterprise Vault archives.

Enterprise Vault also includes migration tools to import content from Lotus Domino and Notes NSF files.

## Benefits of archiving

Automatic archiving and archive management provide the following important benefits:

- It ensures that messages and documents are retained for the period of time required by compliance regulations or company policy
- The size of Exchange Server mailboxes and public folders and Domino mail files is easily controlled without the loss of data
- Primary disk space usage is reduced

## How to access items in archives

One of the main drawbacks of conventional archiving applications is the high cost of finding and retrieving items from storage. In Enterprise Vault, item properties and content are indexed to enable fast searching of archived items.

Enterprise Vault can be configured to leave shortcuts to archived items in the original location (Exchange Server mailbox, public folder, PST file, Domino mail file, file system folder or SharePoint server). The shortcuts provide a text or HTML preview of the item. Users can double-click shortcuts to view the original item in its associated application or the contents of the shortcut, depending on how you configure Enterprise Vault. The user can save the item to their local computer or use options in an Enterprise Vault client to restore the item to its original location, depending on permissions, or to a specified location.

With Exchange mailbox archiving only, users may have the option to restore archived items to the current folder. The current folder is the location in the

mailbox that corresponds to the location of the archived item inside the vault. So if the shortcut has been moved from its original folder, the current folder is the folder where the shortcut is now located. If the shortcut has expired, or has been deleted, the current folder is the folder where the shortcut was last located.

With SharePoint archiving, you can restore items from SharePoint document libraries but not social content items.

To enable users to access archives, search for items and manage archived items, the following Enterprise Vault client features are available:

- An integrated archive search. This search can be launched from within mail clients to enable users to perform searches on one or more archives and restore archived items.
- A browser search application. This archive search feature enables users to perform more complex searches. The search is launched in a browser window.

---

**Note:** Both the integrated archive search and the browser search application are primarily designed to let individual users search their own archives. Neither feature is a replacement for the Compliance Accelerator and Discovery Accelerator applications, which let compliance officers and case administrators conduct more sophisticated, enterprise-wide searches.

See [“About Compliance Accelerator and Discovery Accelerator”](#) on page 22.

---

- Enterprise Vault Mobile Search lets users search for and view archived Microsoft Exchange Server emails using a Web browser on a mobile device.
- Archive Explorer. This browser interface presents archive folders in a tree structure that users can browse for required items. Users can manage archived items and also perform searches.
- The Enterprise Vault Outlook Add-In and the Enterprise Vault Client for Mac OS X can be installed on user desktops to enable users to search mailbox archives and manage archived items from within Outlook and Entourage. The Enterprise Vault Outlook Add-In includes the Virtual Vault feature. With Virtual Vault enabled, users can access their archives in the Outlook Navigation Pane. To the user, the archive looks similar to their mailbox or personal folders.
- Enterprise Vault extensions for OWA can be configured on Exchange Servers to enable OWA users to manage archived items in mailboxes and public folders. OWA users do not require the Enterprise Vault Outlook Add-In to be installed on their desktop computers.  
RPC over HTTP connections to Exchange Server mailboxes are also supported by Enterprise Vault. RPC over HTTP users do require the Enterprise Vault Outlook Add-In to be installed on their desktop computers.

- Enterprise Vault extensions for Lotus Notes and Domino Web Access clients.

All the client features except Mobile Search and the Enterprise Vault Client for Mac OS X are currently available in the following languages:

- |                        |             |           |
|------------------------|-------------|-----------|
| ■ Brazilian Portuguese | ■ French    | ■ Korean  |
| ■ Chinese, Simplified  | ■ German    | ■ Polish  |
| ■ Chinese, Traditional | ■ Hebrew    | ■ Russian |
| ■ Danish               | ■ Hungarian | ■ Spanish |
| ■ Dutch                | ■ Italian   | ■ Swedish |
| ■ English              | ■ Japanese  |           |

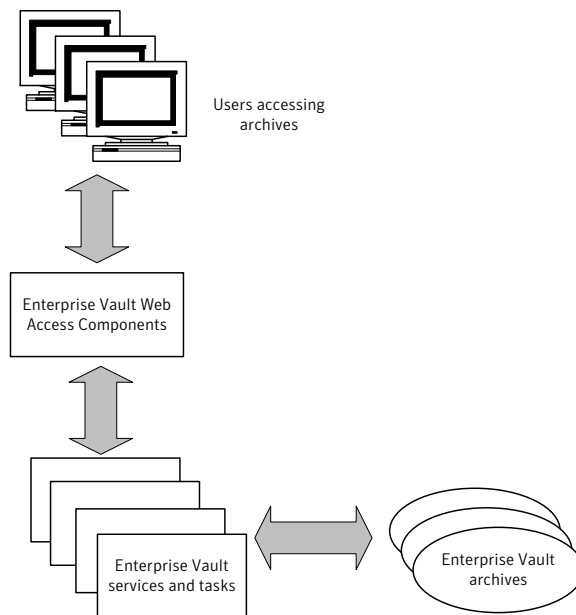
Mobile Search is available in all these languages except for Hebrew. The Enterprise Vault Client for Mac OS X is currently available in English, French, German, Spanish, and Japanese only.

For a full list of the operating systems on which Enterprise Vault client features are supported, including opening shortcuts to archived items, see the *Enterprise Vault Compatibility Charts*, available at the following address on the Symantec Enterprise Support site:

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

Figure 2-2 gives an overview of the process involved when users access Enterprise Vault archives using the Enterprise Vault clients.

**Figure 2-2** How users access stored items



For example, using browser search, a user searches for an item stored in an archive. The web access component passes the request to the Enterprise Vault tasks and services, which perform the search and return a list of the search results to the user. The user then clicks the link to view the required item. Again, this request is passed to Enterprise Vault tasks and services, which return to the user an HTML version of the item or the item in its original format, depending on how the system has been configured.

In addition to searching and viewing items, users can restore items and, if permitted, delete items from archives. Items can be restored to their original location or, in the case of Exchange mailbox archiving only, to their current folder. Items can also be restored to a network share or the user's local computer. Restoring is not applicable to social content from SharePoint as shortcuts are not created for social content.

The administrator can control which functionality is available to users.

## About Compliance Accelerator and Discovery Accelerator

Enterprise Vault also provides applications for compliance monitoring activities and data mining activities, such as legal discovery.

Legislation by regulatory bodies, such as SEC, NYSE and NASD, means that financial and legal organizations are obliged to retain an increasing amount of electronic correspondence and data. Outside the financial services sector, the Sarbanes-Oxley Act of 2002 extends the length of time that corporate data needs to be available for audit. Enterprise Vault enables organizations to capture, store and retrieve the relevant data. The Enterprise Vault Accelerator products, Compliance Accelerator and Discovery Accelerator, provide specialized web tools for capturing, searching and reviewing data that has been archived using Enterprise Vault.

Compliance Accelerator provides a capture and review system for monitoring employee messages to ensure compliance with industry regulations or company policy. A random sample of journaled messages (inbound and outbound) can be captured daily and reviewed by compliance officers using the Compliance Accelerator Web interface. In addition, compliance administrators can run regular searches to find messages that meet certain criteria, for example, messages that contain unacceptable language.

Discovery Accelerator is specially tailored for performing enterprise-wide searches to find archived items relating to a legal case. Using the Discovery Accelerator Web interface, case administrators can run searches for relevant data. Case reviewers can then review the items returned by the searches and produce the required items in a format suitable for presenting as evidence.

## About Enterprise Vault add-ons

An increasing number of storage management applications are being integrated with Enterprise Vault to manage the collection and migration of archived data. For details of these integrations and instructions on what you need to configure to use the products with Enterprise Vault, see the following article on the Symantec Enterprise Support site:

<http://www.symantec.com/docs/TECH49714>

Extensions are partner solutions for archiving additional content with Enterprise Vault such as Unix file systems, text messages, social media content, and web pages. See the Enterprise Vault Partner Portal for extensions provided by authorized partners in the Symantec Technology Enabled Program (STEP):

<http://go.symantec.com/archive-everything>

You can also go to the Enterprise Vault Partner Portal from the **Extensions** page in the Enterprise Vault Administration Console.

The Enterprise Vault media contains applications that integrate with Enterprise Vault to provide additional functionality.

## Introduction to Adapter for Secure Messaging and Rights Management

The Enterprise Vault Adapter for Secure Messaging and Rights Management removes the protection, or encryption, from email messages and attachments as they enter Enterprise Vault. Specifically, the Exchange Journal copy of a protected email message is decrypted by the Adapter.

Protection is also removed from supported documents and other email messages that are attached to protected email messages.

The Adapter stores certain parameters, or metadata, about the protection in the archive. You can later search the archive and tailor your query based on these parameters.

In addition to Microsoft Rights Management Services (RMS) and Active Directory Rights Management Services (AD RMS), the Enterprise Vault Adapter for Secure Messaging and Rights Management works with the following security services:

- **Liquid Machines Document Control:** provides encryption and rights-management of documents. In addition, it extends RMS and AD RMS protection beyond Office 2003 and Office 2007 to Office XP and Office 2000, as well as to leading desktop and enterprise applications, such as Adobe Acrobat, Adobe Reader, and Microsoft Visio.
- **PGP:** a point-to-point technology that enables senders to encrypt data to send to specific recipients. It is not a rights management system and does not use permissions. PGP provides for data confidentiality and integrity using encryption and digital signatures.

The Adapter can be configured to search the contents of Zip archives for protected data. The examination can include further recursion to any depth, in the case of a Zip archive within another Zip archive. Any protected file found inside a Zip archive is decompressed and unprotected. The result is recompressed and reinserted into a reconstituted form of the Zip archive.

Full documentation on how to install and configure the software is included with the software.

## Introduction to EnCase® Ingest Connector

The EnCase Ingest Connector is a utility that ingests files from forensic evidence files into archives, so that they can be searched using Discovery Accelerator, or to designated disk locations.

The EnCase Ingest Connector ingests files from Logical Evidence Files, EnCase images, and data definition (DD) images. Using the EnCase Ingest Connector, you



can copy individual files or select sets of files based on metadata (for example, file name, file name extension, or creation, modification and last accessed dates).

Full documentation on how to install and configure the software is included with the software.

## Introduction to IM Manager

Symantec IM Manager is a software proxy for securing, managing, and logging IM messages for public and enterprise IM protocols. It delivers real-time threat protection, management, and compliance for your organization's IM activity through the following features:

- **Threat protection.** Symantec IM Manager security features enable you to protect your corporate network against external threats such as IM viruses, worms, and malicious URLs.
- **Management.** Symantec IM Manager management features enable you to define the corporate policies and rules to which your IM users must adhere.
- **Compliance.** Symantec IM Manager compliance features help you to enforce regulatory requirements.

Enterprise Vault IM Archiving Option delivers the compliance features necessary to log and archive Instant Messages to Enterprise Vault. For security features a full license of IM Manager is required – contact your local Symantec representative for upgrade options, if desired.

Full documentation on how to install and configure the software is included with the software.

## Introduction to Enterprise Vault Discovery Collector

Enterprise Vault Discovery Collector addresses your eDiscovery needs during the identification phase and collection phase of eDiscovery. It supports a more active approach to eDiscovery by letting you identify and index potentially relevant sources of data in your enterprise. This allows for targeted analysis during the identification phase when you are trying to understand and identify the data that you need to collect for an active legal case.

Discovery Collector provides a number of features that are specifically designed to support active eDiscovery, including the following:

- The ability to identify and search all non-archived data using keyword or attribute searches.
- Simple generation of query analysis reports and data topology maps. Each query analysis report provides information on the data sources for all the

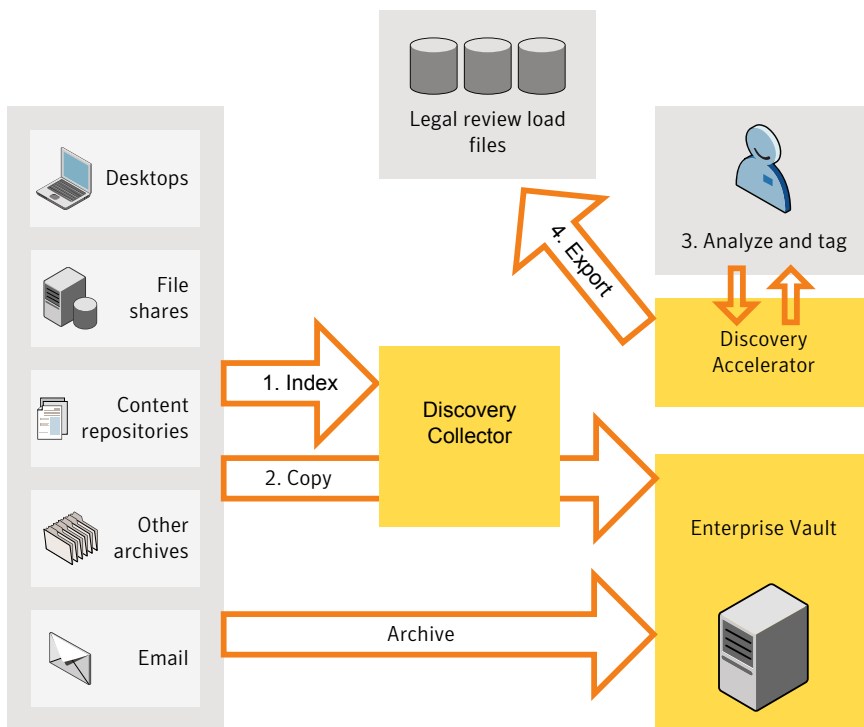
responsive objects, custodian information, the number of responsive documents and their estimated total size to produce, and more.

- The ability to export data in standard file formats that are compatible with common legal review tools. These formats include Concordance, Summation Enterprise, and EDRM XML.
- Automated collection into Enterprise Vault of all the data that the legal team has identified. This collection process also creates detailed audit trails that you can use to demonstrate a repeatable process and assert a chain of custody.

Figure 2-3 shows the Discovery Collector workflow. The data that Discovery Collector identifies and collects is stored in Enterprise Vault for analysis and review by Discovery Accelerator. When this process has completed, Discovery Collector can export the data in an appropriate load-file format for your external counsel's review platform.

The Discovery Collector is available from Symantec FileConnect (<https://fileconnect.symantec.com>).

**Figure 2-3** Enterprise Vault Discovery Collector workflow



Full documentation on how to install and configure the software is included with the software.

## Introduction to Enterprise Vault Data Classification Services

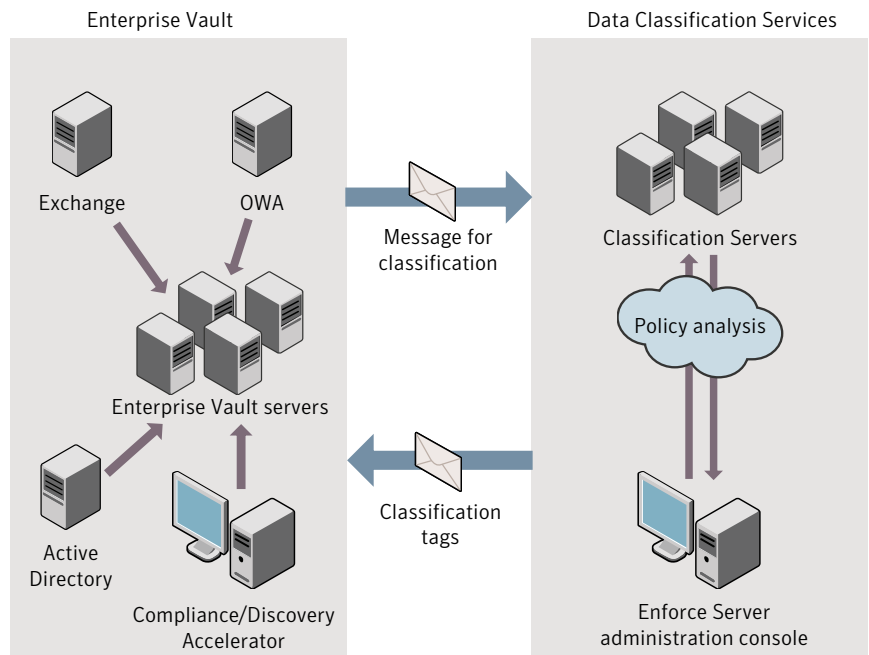
Data Classification Services uses various components of Symantec Enterprise Vault and Symantec Data Loss Prevention to automate the classification of Microsoft Exchange messages that are managed in Enterprise Vault. After Data Classification Services has applied classification tags to the messages, users of applications like Compliance Accelerator and Discovery Accelerator can use the tags to filter messages when they conduct searches and reviews.

The Data Classification Services components are available from Symantec FileConnect (<https://fileconnect.symantec.com>).

You create the required classification policies by using the Enforce Server administration console that comes with Data Loss Prevention. You can create new policies from scratch, or you can base them on any of the templates that accompany Data Classification Services.

[Figure 2-4](#) shows the key components in a Data Classification Services environment.

**Figure 2-4** How Enterprise Vault and Data Classification Services interact



The capabilities that Data Classification Services provides supersede those that Automatic Classification Engine (ACE) provided in earlier versions of Enterprise Vault. You cannot configure Enterprise Vault to work simultaneously with both ACE and Data Classification Services.

For more information on Enterprise Vault Data Classification Services, see the *Implementation Guide*. This guide is available from the following page of the Symantec Enterprise Support site:

<http://www.symantec.com/docs/DOC4121>

## How Enterprise Vault works

This section introduces the Enterprise Vault components and gives an overview of the basic archiving and retrieval processes. A fuller description of how Enterprise Vault archives different types of data is given in later chapters. Enterprise Vault is packaged as a number of components, which you can select at installation time.

The core Enterprise Vault components include the following:

- The Enterprise Vault Server component comprising services and tasks for performing the main archiving, indexing, storing and restoring functions.
- The Enterprise Vault Administration Console for configuring and managing services, tasks, indexes, and archives.
- Active Server Page (ASP) web access components for enabling users to access items in archives.

The following additional components are provided for Exchange Server archiving:

- Enterprise Vault Outlook Add-In for enabling users to access archived items from within their Outlook client.
- Enterprise Vault Client for Mac OS X for enabling Microsoft Entourage or Outlook 2011 for Mac users to access archived items.
- Outlook Web Access (OWA) Extensions for enabling users to access archived items from within their OWA client.
- Enterprise Vault Mobile Search for enabling mobile device users to search for and view Microsoft Exchange Server emails that Enterprise Vault has archived.

The following additional components are provided for Domino Server archiving:

- Enterprise Vault extensions for Lotus Notes and DWA clients.

The following, additional components are provided for file system archiving, SharePoint archiving and SMTP message archiving:

- The FSA Agent, which provides the FSA services on Windows file servers for the creation of placeholder shortcuts, for File Blocking, and for FSA Reporting.
- Microsoft SharePoint components for archiving and restoring documents on SharePoint servers. Optional Enterprise Vault web parts provide archive search features for SharePoint users.
- SMTP archiving components for processing messages from third-party SMTP messaging servers

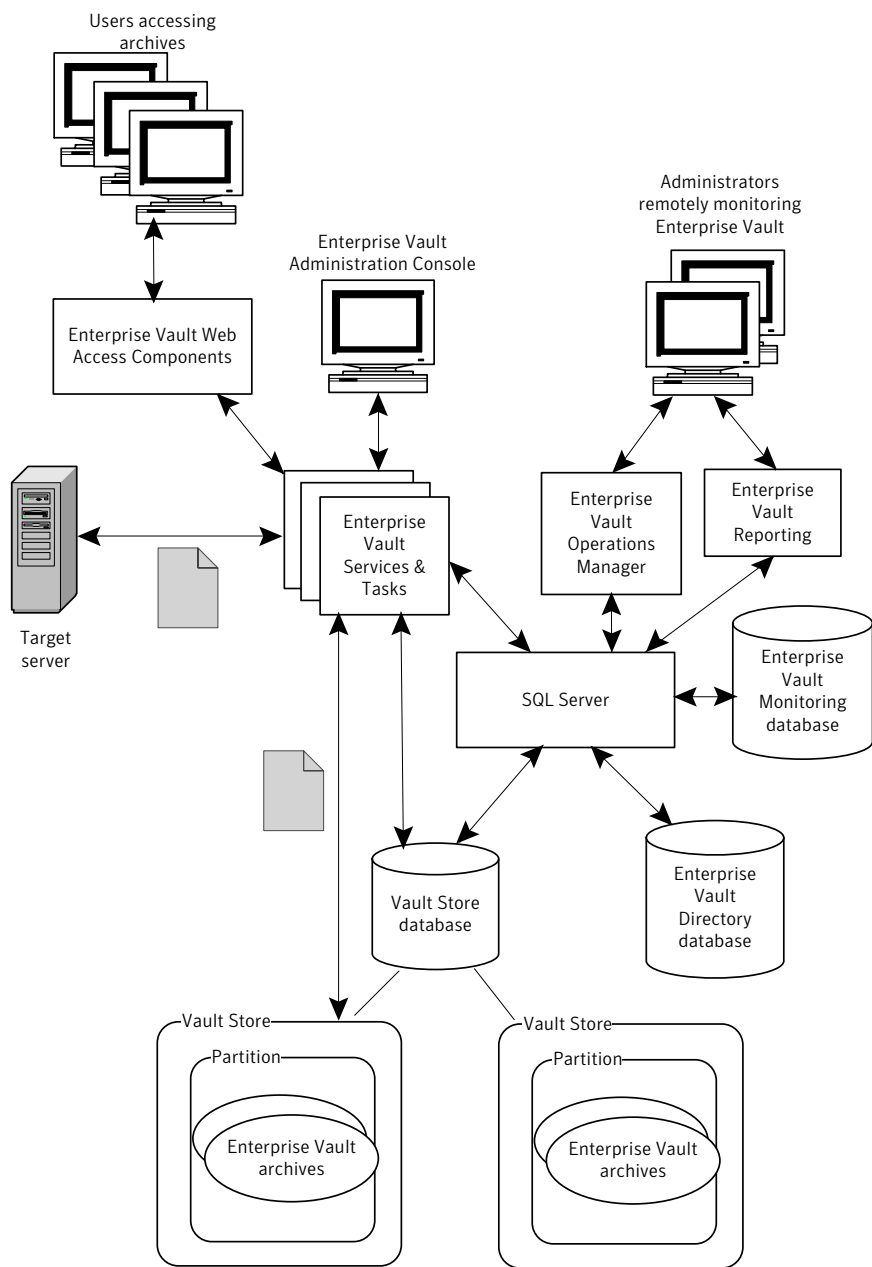
The following optional components provide enhanced management and reporting facilities:

- Enterprise Vault Operations Manager is a Web application that makes remote monitoring of the status of Enterprise Vault possible from any computer on which Internet Explorer is installed.
- Enterprise Vault Reporting provides enterprise-level reporting, using Microsoft SQL Server Reporting Services.

Once installed and configured, the Enterprise Vault Server comprises a combination of Windows services and tasks, Microsoft SQL Server databases and Active Server Page (ASP) web access components. Services, tasks and archives are configured using the Enterprise Vault Administration Console, which is a snap-in to the Microsoft Management Console (MMC).

[Figure 2-5](#) shows the main components in an installed Enterprise Vault system. The target server in the diagram is a server from which items are to be archived. The illustration omits the components involved in single instance storage, which are described separately.

Figure 2-5 Illustration of an installed Enterprise Vault system



The Windows services and tasks perform background tasks such as scanning target servers for items to be archived, storing the items in archives, indexing item attributes and content and retrieving items from archives.

The Enterprise Vault Directory database and Vault Store database are SQL databases that hold Enterprise Vault configuration data and information about the archives.

The Enterprise Vault Monitoring database is a SQL database that holds monitoring data for use by the Enterprise Vault Operations Manager and Enterprise Vault Reporting components. A Monitoring agent on each Enterprise Vault server monitors the status of the Enterprise Vault services and archiving tasks, and the values of performance counters for vault stores, disk, memory, and processors. The agents collect data every few minutes and record it in the Enterprise Vault Monitoring database.

The first time that you configure a file server target for FSA Reporting, Enterprise Vault creates an FSA Reporting database (not shown in the figure). The FSA Reporting database holds the scan data that FSA Reporting gathers from the file server. When you configure another file server target for FSA Reporting, you can assign the file server to an existing FSA Reporting database, or create another database. Multiple FSA Reporting databases can provide scalability if you obtain FSA Reporting data for many file servers.

The Active Server Page web access components run on an IIS server and enable users to view, search and restore archived items using Enterprise Vault web client interfaces.

The physical organization of the components will depend on the requirements of your site. The various Enterprise Vault services and tasks can reside on one computer or be distributed over several computers. In a pilot system, for example, all the Enterprise Vault services, SQL server, IIS server and target server for archiving can, in most cases, reside on one computer.

The archives themselves can reside on your preferred storage system, for example, SAN, NAS, NTFS, WORM. You can also use certain storage devices that support the Enterprise Vault storage streamer API. Older archives can be moved off to more economic media for long term storage. An increasing number of products can be used to provide long-term storage solutions for Enterprise Vault archives.

These products include the following:

- Symantec NetBackup™
- Symantec Backup Exec™
- Amazon Simple Storage Service™
- AT&T Synaptic Storage as a Service

- Nirvanix Storage Delivery Network™
- Rackspace Cloud Files™
- IBM System Storage™ DR550
- FUJITSU ETERNUS® Archive Storage

The use of Hierarchical Storage Management (HSM) is also supported.

For details of supported software and storage devices, see the Enterprise Vault *Compatibility Charts*.

Enterprise Vault organizes the archives in entities called vault stores. Vault stores contain one or more Enterprise Vault partitions. A partition can reside on any of the supported storage media.

In each vault store, there can be only one open partition, and this is the partition in which Enterprise Vault archives data. When you want to switch archiving to another partition, such as when the disk that hosts the open partition is nearly full, you can use the Administration Console to close this partition and open another. You can also use Enterprise Vault's partition rollover feature to manage the automatic rollover from one partition to another.

On NTFS volumes, Enterprise Vault automatically uses NTFS file security. Although some elements of Enterprise Vault can be set up on FAT volumes (for example, the indexes) there will be no file security.

## About 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. However, it can increase the network traffic between the Enterprise Vault servers and the storage devices that host the partitions.

Enterprise Vault single instance storage works on the following principles:

- Vault stores are grouped within vault store groups. A vault store group forms the outer boundary for sharing with single instance storage.
- Each vault store is assigned a sharing level, which is one of "Share within group", "Share within vault store" or "No sharing".
- Enterprise Vault archives an item using single instance storage if the target vault store has a sharing level of "Share within vault store" or "Share within group".
- A vault store's sharing level determines the vault store's sharing boundary, as follows:



- If a vault store's sharing level is "Share within group", its sharing boundary includes all the vault stores in the group that have this sharing level.
- If a vault store's sharing level is "Share within vault store", its sharing boundary contains only the vault store.
- If a vault store's sharing level is "No sharing", the vault store has no sharing boundary. Enterprise Vault does not perform single instance storage for the vault store.
- Enterprise Vault 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.
- Enterprise Vault stores each SIS part only once within the target vault store's sharing boundary. 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.
- Enterprise Vault 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.

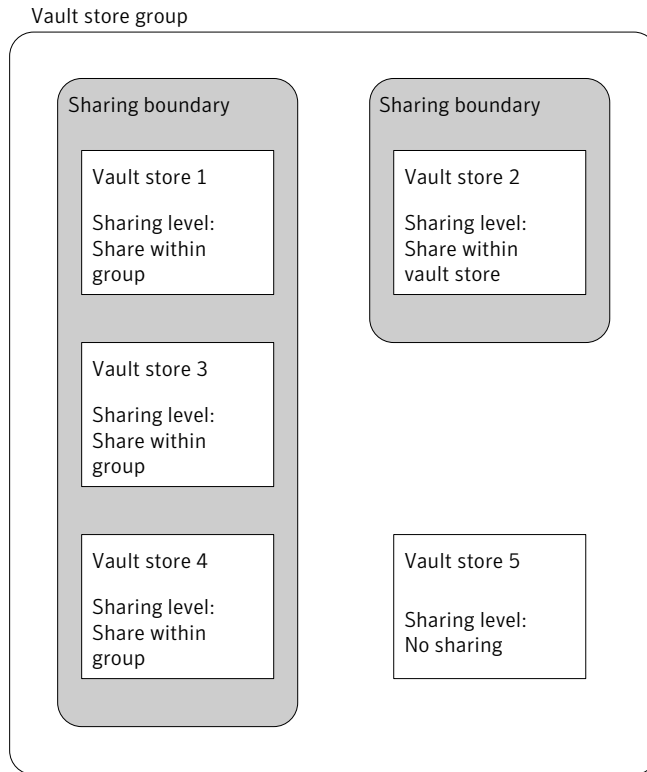
Figure 2-6 shows an example vault store group that contains five vault stores:

- 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 items 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 items it archives to the 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.

**Figure 2-6** Sharing boundaries in a vault store group



Single instance storage can save storage space in a number of ways:

- If you use separate vault stores for journaling and mailbox archiving, Enterprise Vault can share the SIS parts between the vault stores, provided that they are in the same sharing boundary.
- If a number of separate messages with the same large 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 large 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.

---

**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.

---

## About Enterprise Vault indexing

To provide fast and efficient searching of archived data, Enterprise Vault indexes items as they are archived. An index is created for each archive. As items are added to or deleted from the archive, associated index documents are added to or deleted from the index. When a user performs a search for an item in an archive, Enterprise Vault searches the index, not the actual archive.

In Enterprise Vault you can set the required level of indexing. If required, different levels can be set for different groups of users. Two levels of indexing are available: brief and full:

- **Brief indexing.** This level enables users to search on attributes of an archived item such as author, subject, recipients, created date, file extension, retention category and so on. With brief indexing, the content of the item is not indexed.
- **Full indexing.** This level enables users to search as for brief indexing, and also provides content searching.

The more information that is indexed, the more disk space is required for the index. [Table 2-1](#) shows the estimated size of an index as a percentage of the size of the unarchived item for the different indexing levels.

**Table 2-1** Estimated size of index data

Indexing level	Estimated size of index
Brief	4%
Full	12%

At Enterprise Vault 10.0 a new 64-bit search engine was introduced. A 64-bit index is created for the items that are indexed using Enterprise Vault 10.0 or later releases. The indexes that were created using earlier releases of Enterprise Vault

were 32-bit indexes. When a search is performed on an archive that has both 32-bit and 64-bit indexes, Enterprise Vault automatically searches across both 32-bit and 64-bit indexes. An update tool is provided in the Enterprise Vault Administration Console to upgrade 32-bit indexes to 64-bit, if required. For details of this tool, see *Managing indexes* in the *Administrator's Guide*.

The Enterprise Vault Indexing service manages the various tasks that create, update, and search indexes. It interoperates closely with the Storage service to index items as they are stored, or later, and find items for the Storage service to retrieve. The Storage service converts items to HTML or text, if possible, and this converted content is then used to index the item. As Enterprise Vault does not index the content of items that cannot be converted to text or HTML, it is not possible to search on the content of such items. For example, the content of binary files cannot be converted, or searched. However, Enterprise Vault does index the attributes of items it cannot convert, so that items can still be found in the archive.

You do not have to install the Indexing Service on every Enterprise Vault server. For example, in larger deployments of Enterprise Vault the Indexing and Storage services can be located on more powerful computers to optimize search and retrieve performance. Associated Storage and Indexing services can reside on different computers. To ensure good performance, the connection between such computers must be fast.

From Enterprise Vault 10.0 Enterprise Vault servers that perform indexing can be grouped together in Index Server groups to provide scalability and load balancing.

See [“About Index Server groups”](#) on page 38.

## About index volumes

The index for an archive comprises one or more sequential index volumes. Each index volume contains index documents for the items that are stored in the archive.

Typically, a user mailbox index requires only one or two volumes. Indexes for larger archives, such as file system archives and journal archives, are likely to have multiple volumes.

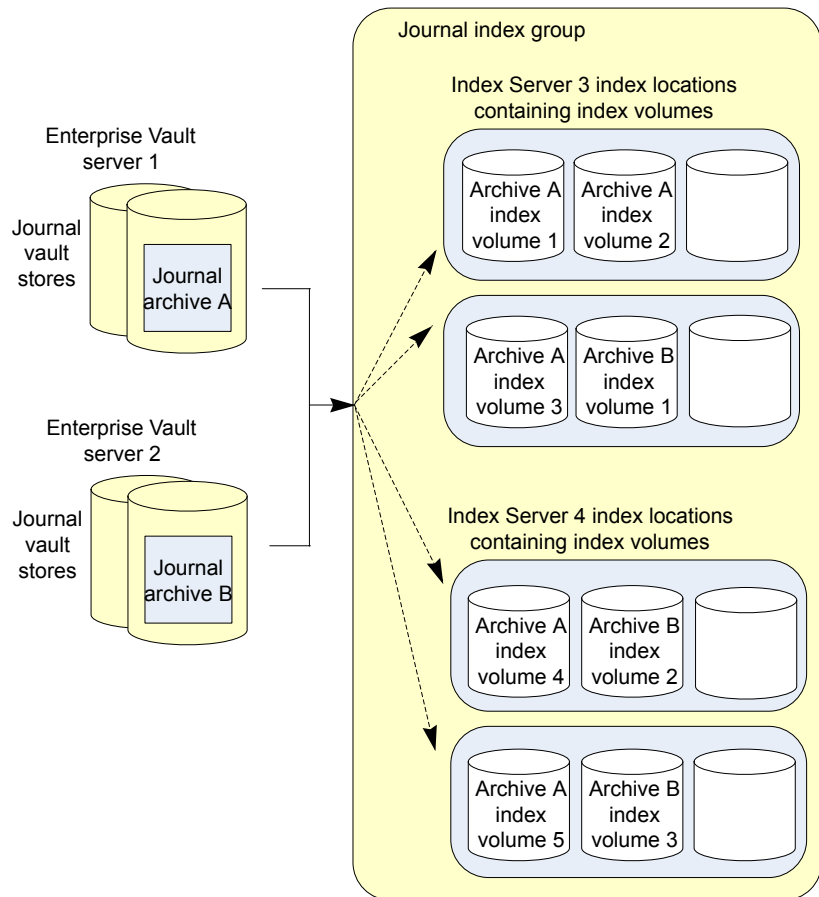
When an index volume is full, the Index Server automatically creates a new index volume. The location that is selected for new index volumes depends on whether the vault store is managed by a single Index Server or an Index Server group. If the vault store is indexed by an Index Server group, the index volumes for an archive may be distributed across multiple Index Servers and locations, as shown in [Figure 2-7](#). In general, when the index for a mailbox rolls over, the existing Index Server is used, if possible. The index location is selected using a round robin algorithm, to balance the load across all index locations. For larger archives, such

as journal archives, new volumes are distributed evenly across the Index Servers and index locations.

The Enterprise Vault Administration Console includes tools for managing index volumes.

See [“About managing indexes and index volumes”](#) on page 37.

**Figure 2-7** Spread of index volumes in an Index Server group



## About managing indexes and index volumes

You use the Enterprise Vault Administration Console to manage Index Servers, Index Server groups, and index locations. The Administration Console also includes a range of tools for managing indexes and index volumes. Tasks that you can perform using indexing tools include the following:

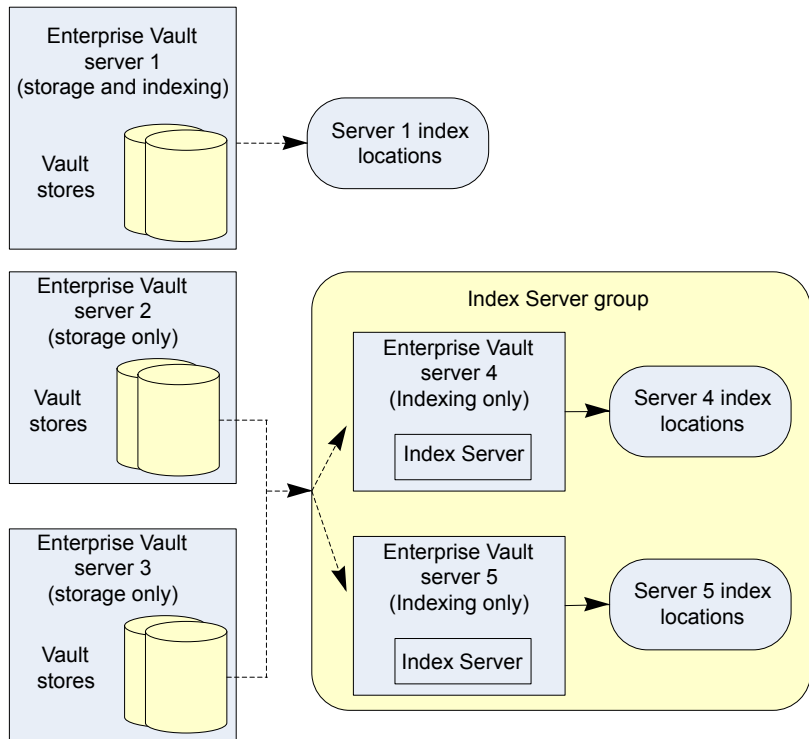
- Browse and manage the index volumes that are associated with an archive.
- Verify the integrity of indexes, and report any archived items that are not indexed or not deleted from the index.
- Synchronize indexes to ensure that they are up to date.
- Rebuild indexes from scratch.
- Change the location of index volumes.
- Upgrade archive indexes from 32-bit to 64-bit indexes.
- Monitor and manage the various indexing tasks.

Additional management functions are provided by PowerShell commands. For example, there are PowerShell commands that enable you to list the Index Servers that are assigned to index locations, and manage the backup mode for a vault store or index location.

For details of the tools, see *Managing indexes* in the *Administrator's Guide*.

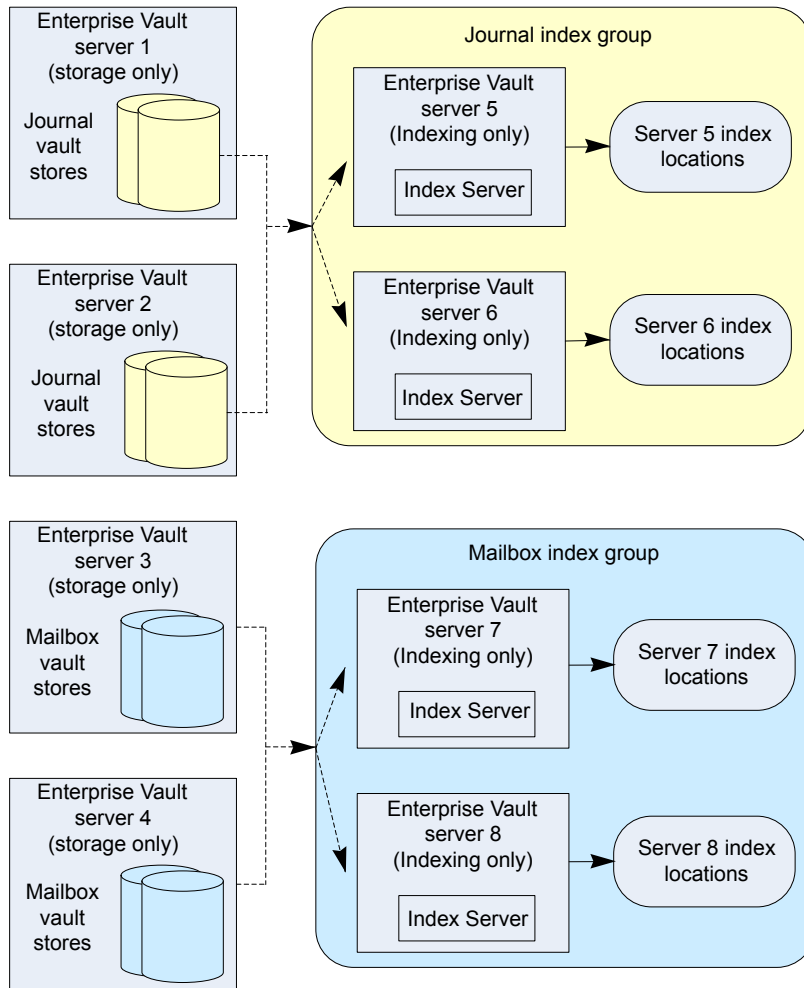
## About Index Server groups

An Index Server is an Enterprise Vault server that has the Enterprise Vault Indexing service installed. An Index Server can be added to an Index Server group, or *ungrouped*. In [Figure 2-8](#) The Index Server group includes Enterprise Vault servers 4 and 5. Enterprise Vault server 1 is an ungrouped Index Server. An Index Server can only be ungrouped if the server has both the Storage and Indexing services installed.

**Figure 2-8** Ungrouped Index Server

Index Server groups provide load-balanced indexing services for large or distributed Enterprise Vault environments. In a distributed environment, some Enterprise Vault servers may host Storage services, while others host Indexing services. An example of this environment is shown in [Figure 2-9](#).

**Figure 2-9** Index Server groups in a distributed environment



For archives to be indexed, the vault store to which they belong must be associated with an Index Server or an Index Server group. An Index Server creates indexes in index locations, and each Index Server has one or more index locations assigned to it. The Index Servers in a group share the task of indexing the items that are stored in the archives in the vault stores assigned to the group.

You use the Enterprise Vault Administration Console to perform the following tasks:

- Create Index Server groups, and add Index Servers to each group.



- Assign physical index locations to each Index Server.
- Assign each vault store to either a standalone Index Server, or an Index Server group.

## About Enterprise Vault Administration Console

The Enterprise Vault Directory and all the various entities in Enterprise Vault sites are configured using the Enterprise Vault Administration Console, which is a snap-in to the Microsoft Management Console (MMC).

The Enterprise Vault Administration Console is currently available in English, Japanese and Simplified Chinese.

In the left-hand pane, a tree structure displays site entities including the following:

- Archives
- Vault stores and partitions
- Enterprise Vault servers and the Enterprise Vault services and tasks running on each server
- Index Servers and Index Server groups
- Targets for archiving (For example, Exchange Servers and mailboxes, Domino Servers and mail files, volumes and folders on file systems and SharePoint site collections).
- Policies for defining which items are to be archived and the archiving actions to be taken
- Retention Categories available
- Target computers and files for PST migration using the Locate and Migrate feature

New entities can be created and the properties of existing entities can be viewed or changed using right click options in both the tree and the right hand pane.

Using the wide range of options in the Enterprise Vault Administration Console, the administrator can configure and manage archiving within an enterprise and define the functionality that is to be available to users in the various client interfaces.

## About Enterprise Vault sites, Directory, and Directory database

During its initial configuration, each Enterprise Vault server must join an Enterprise Vault site. A site comprises one or more Enterprise Vault servers running one or more Enterprise Vault services and tasks to archive items from

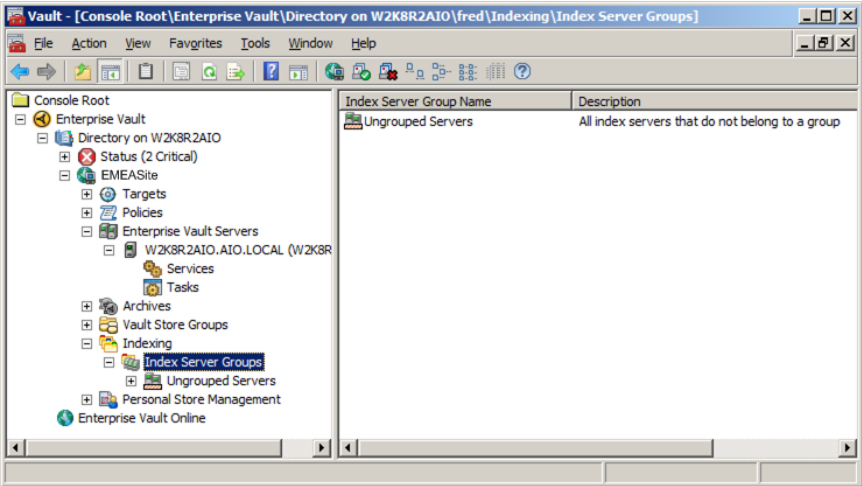
specified targets: for example, Microsoft Exchange Servers, Domino mail servers, Microsoft SharePoint Servers, and file servers.

A site also contains a collection of vault stores, index servers, archiving policies that define how and when items are to be archived, and Retention Categories that define how long items are to be stored before being deleted. A site may also include a list of target computers for the automatic importing of PST files.

An Enterprise Vault site is located in an Enterprise Vault Directory on an Enterprise Vault server computer. An Enterprise Vault Directory can contain one or more sites. The hierarchy of the sites, and Enterprise Vault servers belonging to those sites is shown in the Enterprise Vault Administration Console.

Figure 2-10 illustrates how the Enterprise Vault Administration Console shows the contents of an Enterprise Vault Directory.

Figure 2-10 Enterprise Vault Administration Console showing the contents of an Enterprise Vault Directory



When you configure an Enterprise Vault server for the first time you can either create a Directory and site on the computer you are configuring, or join a site in a Directory on another Enterprise Vault server computer.

The Enterprise Vault Directory is accessed by a Directory Service. The other Enterprise Vault services and tasks use this service to access the configuration information in the Enterprise Vault Directory database.

See [“Introduction to the Directory Service”](#) on page 47.

The Enterprise Vault Directory database holds configuration information for each site in the Directory. (In general, configuration information is not shared across

Enterprise Vault sites.) This SQL database can be located on a machine separate from the Enterprise Vault servers.

The Enterprise Vault Directory, sites, index server groups, targets, policies and Retention Categories are all configured using the Enterprise Vault Administration Console. You can use Microsoft SQL management tools to help with managing the SQL database.

## About Enterprise Vault tasks

Archiving and restoring activities are performed by Enterprise Vault tasks. Different tasks are used depending on the type of data that is being archived. Enterprise Vault tasks are managed by the Task Controller Service.

Tasks are also used to configure Exchange Server mailboxes or Domino mail files for archiving, and to locate and import PST files automatically.

### Introduction to provisioning and archiving tasks

The following kinds of tasks can be created and managed using the Enterprise Vault Administration Console:

- Exchange Provisioning task. This task configures user mailboxes for archiving.
- Exchange Mailbox Archiving task. This task archives items from user mailboxes. It updates mailbox configuration information with archiving policy changes, and synchronizes permissions on the mailbox with those on the associated archive. It also updates the location and the retention category of archived items whose shortcuts have been moved or copied to a different folder.
- Exchange Public Folder task. This task archives items from public folders.
- Exchange Journaling task. This task archives items from Exchange Server journal mailboxes.
- Domino Provisioning task. This task configures Domino mail files for archiving, updates mail file configuration information with archiving policy changes, and synchronizes permissions on the mail file with those on the associated archive.
- Domino Mailbox Archiving task. This task archives items from Domino mail files.
- Domino Journaling task. This task archives messages from Domino journal databases.
- SharePoint task. This task archives documents from document libraries on SharePoint servers.

- **File System Archiving task.** This task archives files from file systems, including NTFS file systems, NetApp® Filer devices, and EMC Celerra/VNX file servers.
- **Move Archive task.** This task manages Move Archive operations initiated in the Move Archive wizard.

When a task is configured, it is assigned a set of targets. Each target has an archiving policy assigned to it. The targets define the location of the items to be archived and the policy defines how and when the items are to be archived. A single task can archive several targets on different servers.

At the times that you schedule, the archiving task scans the configured target for items that are ready for archiving, that is, those items that satisfy the archiving policy. This is automatic or background archiving. With Exchange mailbox and public folder archiving and Domino mail file archiving, users can also store specific items in the archive using the Store in archive option in their mail client. This is manual archiving.

For each type of archiving, the archiving task collects the items that are to be archived and passes them on to the Storage Service. When the Storage Service has safely stored an item, the archiving task can delete the original, and create a shortcut to the archived item. You can configure whether the task deletes the original and also whether it creates a shortcut.

You can configure the archiving task to leave the original item as a safety copy until the vault store containing the archived copy is backed up.

When Enterprise Vault archives an item, the Enterprise Vault Directory database is accessed to find out where the required archive is. In addition, information is written to the Vault Store database.

Archiving tasks are also responsible for the automatic deletion of shortcuts.

The automatic deletion of shortcuts could be as follows:

- When an archived item is deleted automatically at the end of the retention period. This deletion is optional.
- When an archived item is deleted explicitly by users who have delete access to them.
- When the archive itself is deleted.

The item in the archive is deleted by the Storage Service, but shortcuts are deleted by the archiving task.

For some types of archiving you can configure automatic shortcut deletion separately from item deletion. For example, you could set all shortcuts to be deleted after a year. The archived items would remain in the archives, still available if required.

## Introduction to retrieval processes

Associated with each archiving task is a hidden retrieval process. This process is used when retrieving items from archives for viewing or restoring to a location specified by the user.

The retrieval process receives requests from the following sources:

- The Enterprise Vault Outlook Add-In and Enterprise Vault Client for Mac OS X, when a user views or restores an item from a shortcut in a mailbox.
- The Enterprise Vault extensions for Lotus Notes, when a user views or restores an item from a shortcut in a mail file.
- Archive Explorer, when a user views or restores an item in an archive.
- The Shopping Service, when a user uses the Enterprise Vault browser search to select items to be restored.
- FSA shortcuts, when a user double-clicks the shortcut to open the file.
- SharePoint shortcuts or archived version links, when a user clicks the shortcut or link to open the document.

The retrieval process responds to these requests by instructing the Storage Service to retrieve the items from the archives. If the requested item has been stored offline, there may be a delay in retrieving it.

## Introduction to provisioning tasks

In Exchange Server archiving, the Exchange Provisioning task is used to configure new Exchange Server user mailboxes for archiving.

In Domino archiving, the Domino Provisioning task is used to configure new Domino mail files for archiving.

The mailboxes or mail files are grouped in Provisioning Groups and the Provisioning task processes the Provisioning Groups.

Every Exchange mailbox or Domino mail file to be archived must be in a Provisioning Group. A Provisioning Group can contain a single user or a group of users. An Exchange Mailbox Policy or Domino Mailbox Policy assigned to each Provisioning Group determines how Enterprise Vault archives the users in the group. You can assign different archiving policies to different groups.

## Introduction to PST migration tasks

Enterprise Vault provides the following tools for migrating (importing) the contents of PST files to archives:

- **Locate and Migrate** – This locates PST files on users' computers, copies them to a central location, and then migrates them. Unless you have only a few PST files to migrate, Locate and Migrate is likely to require least effort on your part.
- **Client-driven Migration** – This is similar to Locate and Migrate, but finding PST files and sending them to a PST collection area is performed automatically by the user's computer, as opposed to by the Enterprise Vault Server Tasks.
- **Scripted migration using Policy Manager** – This is ideal for performing bulk migrations of PST files, but you need to collect the PST files in a central location.
- **PST Migrator wizard-assisted migration** – If you have a small number of PST files, this provides a quick and easy way of migrating them to Enterprise Vault.

Locate and Migrate partially automates the process of migrating the contents of PST files into Enterprise Vault. It can automatically search for PST files on users' computers and move them to a central holding area, from which they can be automatically migrated.

Locate and Migrate comprises the following Enterprise Vault task types:

- **A Locator task.** This searches your network for computers and PST files. There can be only one Locator task in your Enterprise Vault site.
- **A Collector task.** This moves PST files that the Locator task has found to a central holding folder, ready for them to be migrated. There can be many Collector tasks in your Enterprise Vault site.
- **A Migrator task.** This migrates the contents of PST files that are in the holding folder to Enterprise Vault archives. There can be many Migrator tasks in your Enterprise Vault site.

The tasks are configured and scheduled using the Enterprise Vault Administration Console.

It is possible to configure the Enterprise Vault Outlook Add-In so that users can perform their own PST migrations. The underlying mechanism that is used is still Locate and Migrate, but users are able to queue their own PST files for migration.

## About Enterprise Vault services

In addition to tasks, the Enterprise Vault Server has the following Windows services:

- **Directory Service**
- **Storage Service**
- **Indexing Service**

- Shopping Service
- Task Controller Service
- Admin Service

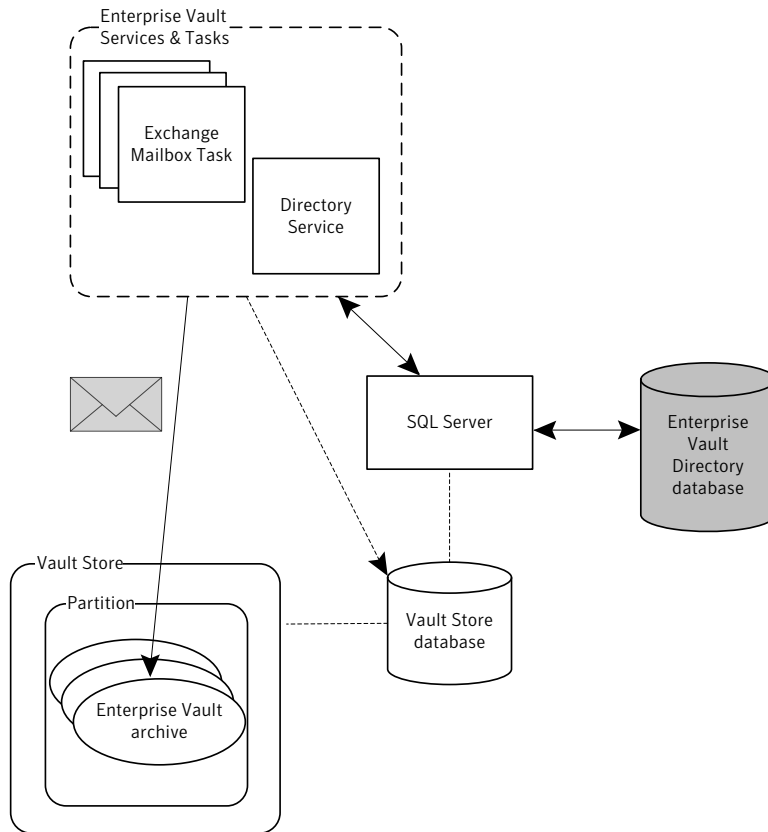
With the exception of the Directory Service and Admin Service, the services are listed and configured in the Enterprise Vault Administration Console. The Directory Service and Admin Service are managed using the Windows Services Management Console.

## Introduction to the Directory Service

The Enterprise Vault Directory has a Directory Service that the other Enterprise Vault services and tasks use to access the configuration information for their site. The Directory Service uses Microsoft SQL Server to access the configuration information in the Enterprise Vault Directory database.

[Figure 2-11](#) illustrates what happens when an Exchange Mailbox Archiving task archives an item.

**Figure 2-11** Accessing the Enterprise Vault Directory database



The Exchange Mailbox Archiving task requires information such as the location of the archive, permissions on the archive and the Indexing Service to contact, and instructs the Directory Service to retrieve this information from the Enterprise Vault Directory database. (The task also updates information in the Vault Store database.)

One Directory Service can provide access to configuration information for one or more Enterprise Vault sites. Because of this, the Directory Service is considered to be outside the Enterprise Vault site rather than a part of it.

The Directory Service is a Windows Service and is listed in the Windows Services Management Console. There is no requirement for the Directory Service to be on the same computer as its database.

A single computer can never run more than one Directory Service.



## Introduction to the Storage Service

The Storage Service manages the vault stores and archives on the computer where it is running.

The role of the Storage service can be summarized as follows:

- The Storage Service accepts items for archiving from the archiving tasks. If possible, it generates a text or HTML version of each item, which the Indexing Service uses to compile indexing data for the item. The Storage Service compresses and stores the items (and the text or HTML versions) in the appropriate archives.  
Some file types cannot be converted to text or HTML, for example, GIF and other binary file types. Also, in the default configuration, very large files (larger than 50 MB) are not converted.  
Information about each item that is archived is stored in the Vault Store database.
- The Storage Service responds to requests from the retrieval tasks to restore items.
- The Storage Service monitors open partitions to identify those that have met their partition rollover criteria.
- The Storage Service responds to requests to view archived items. It can also provide an HTML preview of the item (if a preview of the item is available).
- The Storage Service deletes archived items. This can be a manual deletion by a user or an automatic deletion when the retention period on an item expires. The archiving task deletes shortcuts.

Vault stores have been designed so that they are suitable for being managed by storage management software, such as Symantec NetBackup™. If it is available on the system, the storage management software manages the migration of files to secondary storage devices and retrieves files from secondary storage to the vault store on behalf of the Storage Service. The secondary storage devices are likely to be offline devices, such as optical disks or tapes.

## Introduction to the Indexing Service

The Indexing Service manages the indexes of archived data to enable users to search for archived items that they want to retrieve. There are two levels of indexing: brief, and full. With brief indexing, only information about the item such as the subject and author, can be searched. With full indexing you can also search the content of each item, including phrase searches.

When users search the archives to which they have access, the index files are searched. The more information that is indexed about an item, the easier it is for a user to find.

When you set up Enterprise Vault, you specify where indexes are to be stored. You also specify the default level of indexing that you want to apply across the site, although you can override this for groups or archives.

The role of the Indexing Service can be summarized as follows:

- On instruction from the Storage Service, the Indexing Service indexes items as they are archived.  
The locations of index files are specified in the Indexing Service properties, and also in the Index Server properties.
- If an index is out of date, the Indexing Service automatically updates the index.
- In response to requests from the Enterprise Vault web access components, the Indexing Service searches these indexes and returns information about the archived items that match the search criteria.

## Introduction to the Shopping Service

The Shopping Service is a Windows service that manages the selected items to be restored when using browser search or Archive Explorer.

With Exchange Server archives, the selected items are placed in containers called shopping baskets. The Shopping Service is responsible for managing these shopping baskets. It instructs the retrieval process to retrieve the contents of the shopping baskets from storage, if required.

When using browser search with Domino archives, the Shopping Service still manages the restoring of selected items, but there are no shopping baskets.

## Introduction to the Task Controller Service

Enterprise Vault archiving tasks are controlled by this service. If a task is configured as automatic, it will start when the Task Controller Service is started.

See [“About Enterprise Vault tasks”](#) on page 43.

## Introduction to the Admin Service

The Admin Service has two main functions: it installs new Enterprise Vault license keys, and it provides a general monitoring service that runs automatically whenever any other Enterprise Vault task or service starts. It is installed automatically when you install any of the other Enterprise Vault services.

The Enterprise Vault Admin Service monitors the following:

- Free space on local hard disks. By default, the Admin Service monitors all local hard disks, but you can restrict it to specific disks if required.
- The amount of available virtual memory.
- The number of items on system message queues.

The Admin Service has a warning threshold and a critical threshold for each type of check. When the warning threshold is reached, the Admin Service writes a warning message to the Windows Application Log. When the critical threshold is reached, the Admin Service shuts down all Enterprise Vault tasks and services running on the same computer.

By shutting down Enterprise Vault before problems arise, this behavior helps to maintain the stability of Enterprise Vault.

The online help for the Enterprise Vault Administration Console describes how to control the behavior of the Admin Service.

## About 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.

---

**Note:** In Enterprise Vault 10.0, the Discovery Search Service is available for use with the Clearwell eDiscovery platform only. The Identification & Collection Module that is part of this platform lets teams in corporations, government agencies, and law firms identify and collect data from a variety of data sources across the enterprise, including Enterprise Vault archives.

---

The Discovery Search Service provides methods through which client applications like Clearwell can do the following:

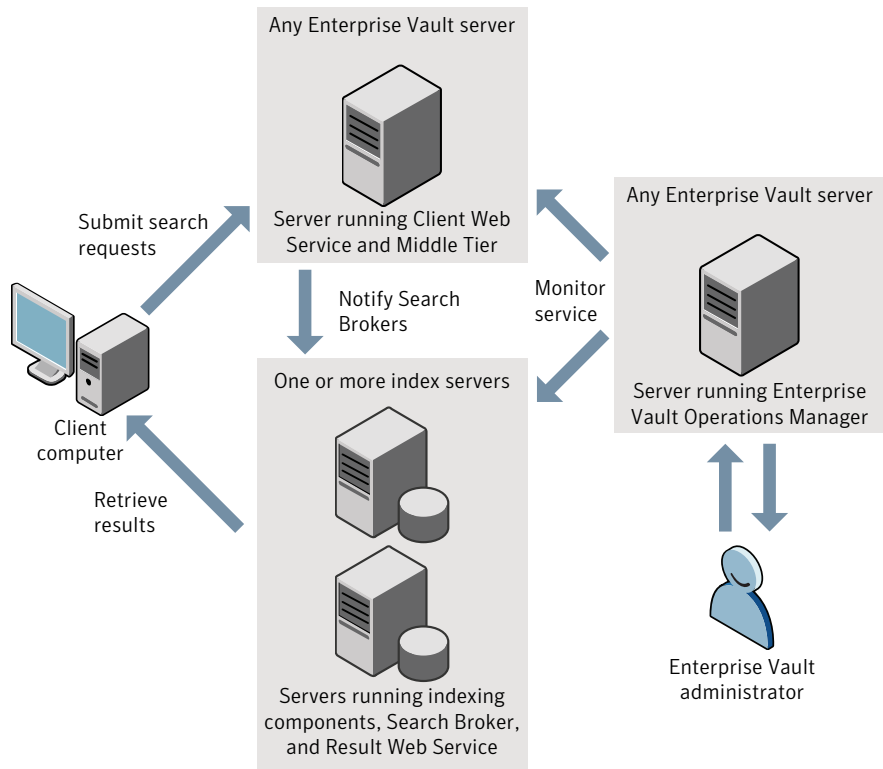
- Create and submit searches of Enterprise Vault archives.
- Check the status of searches.
- Retrieve the results of searches.
- Cancel and resubmit searches.
- Close searches to discard the search results and reclaim disk space.

You can install the Discovery Search Service on any Enterprise Vault server.

## About the Discovery Search Service components

Figure 2-12 shows the components in a typical Discovery Search Service environment.

**Figure 2-12** Components in a Discovery Search Service environment



A client application, such as the Clearwell Identification & Collection Module, submits its search requests to an Enterprise Vault server that hosts the *Client Web Service* of the Discovery Search Service. The Client Web Service is a web application that is hosted in Microsoft Internet Information Services (IIS), and it is the point of entry for the Discovery Search Service system.

The Client Web Service is a lightweight component that forwards all calls to the *Middle Tier*, which manages the searches and aggregates the results of them. The *Middle Tier* always runs on the same Enterprise Vault server as the Client Web Service. If you have multiple Enterprise Vault servers, you need install these components on just one of them.

One of the functions of the Middle Tier is to interact with a *Search Broker* that is running on an Enterprise Vault index server. In Discovery Search Service environments, each index server has a dedicated Search Broker. The Search Broker is responsible for retrieving the results of searches and storing them as XML files on disk. Each index server also hosts a *Result Web Service* from where the client application can retrieve the results of a search.

After you have installed the Enterprise Vault Operations Manager on any Enterprise Vault server, you can use it to monitor the Discovery Search Service. For Discovery Search Service purposes, you must install Operations Manager but you do not need to enable data collection with Operations Manager.

## About the Enterprise Vault Outlook Add-In

The Enterprise Vault Outlook Add-In provides Enterprise Vault functionality in Outlook clients so that users can access archives and manage items that have been archived from Exchange Servers. It also supports RPC over HTTP connections to Exchange Server mailboxes.

The Enterprise Vault Outlook Add-In is supplied as a Microsoft® Windows® Installer (MSI) kit on the Enterprise Vault release media.

For users who access their Exchange Server mailbox using IMAP or POP3 clients, you can configure customized shortcuts using the Enterprise Vault Administration Console.

### Introduction to the Outlook Add-In

The Outlook Add-In can be installed on users' computers to give access to Enterprise Vault mailbox archives. Enterprise Vault buttons and menu options are added to Outlook. The Outlook Add-In also adds Enterprise Vault online help to Outlook.

The Outlook Add-In includes the Virtual Vault feature. With Virtual Vault enabled, users can access their archives in the Outlook Navigation Pane, in a similar way to other mailbox folders and personal folders.

The Outlook Add-In can give users full management access to mailbox archives, as follows:

- Manually archive items. Users can select the destination archive and a Retention Category for the item.
- Delete items (if permitted).
- Use shortcuts to view items.
- Restore items.

- Search archive.
- Access the Archive Explorer application.

The administrator can control which functionality is available to users using policy settings in the Enterprise Vault Administration Console. In particular, the administrator can set the Outlook Add-In to work in full mode or light mode. In full mode, there are no functional restrictions on the behavior of the Outlook Add-In. In light mode, the following restrictions apply:

- Users have no access to the Enterprise Vault properties of folders.
- When users archive items manually, they cannot specify the destination archive and retention category.
- When users restore archived items, they cannot choose the destination folder. The Outlook Add-In only restores items to the folders where the shortcuts are.

Enterprise Vault can perform automatic archiving without the Outlook Add-In being installed, but, depending on shortcut configuration, users may not be able to use shortcuts or modify archiving settings. Archived items can still be accessed using the Enterprise Vault archive search or Archive Explorer applications in stand-alone browser sessions.

## Introduction to offline users

The Enterprise Vault Outlook Add-In can maintain a personal, offline Vault Cache for offline workers.

The Vault Cache has the following advantages:

- It provides instant access to archived items, even when the user is not connected to the corporate network.
- It operates in addition to the normal online archive, not instead of it.
- It is useful to laptop computer users who work offline. They are often used to synchronizing their offline folders and online folders.
- It may be useful in normal offices if you need to conserve bandwidth or improve performance. The retrieval of an archived item takes place on the local computer.

When an offline user starts Outlook, the Enterprise Vault client scans the user's synchronized folders, looking for the following:

- Items that will be archived from the mailbox fairly soon – These items are copied into the Vault Cache so that they will already be there when the items become shortcuts in the user's mailbox. These items have already been downloaded as part of the Outlook synchronize, so the copy takes place on the user's computer with no further download required

- Enterprise Vault shortcuts – If the corresponding items are not in the Vault Cache the client adds them to its download list.

Users can access and manage items in their Vault Cache using the Virtual Vault feature, shortcuts or Archive Explorer. They can also use Windows Desktop Search to search for items in their Vault Cache.

## About the Enterprise Vault Client for Mac OS X

The Enterprise Vault Client for Mac OS X provides Enterprise Vault functionality to Microsoft Entourage and Outlook 2011 for Mac users.

The installer kit for the Enterprise Vault Client for Mac OS X is available as a disk image (.dmg) file on the Enterprise Vault distribution media. After the user installs the client, a **Symantec Enterprise Vault Client** menu appears in the menu bar. By default, an Enterprise Vault toolbar also appears whenever the user starts the email client. This toolbar is optional, and users can choose to hide or show it by selecting a command on the **Symantec Enterprise Vault Client** menu.

The options on the menu and toolbar enable users to interact with their archives in the following ways:

- Download items from the archive and open them in their original form.
- Reply to and forward items in the archive.
- Manually archive items.
- Restore items from the archive.
- Delete items from the archive (if permitted).
- Search the archive.

The administrator can control which functionality is available to users by using configuration settings in the Exchange Desktop Policy in the Enterprise Vault Administration Console.

---

**Note:** This release of Enterprise Vault does not include migration tools with which you can import Entourage archive (.rge) files into Enterprise Vault archives.

---

## About Microsoft Exchange forms

For Exchange Server archiving, the Enterprise Vault Exchange forms extend the Microsoft Exchange Forms Library to include the forms needed by Enterprise Vault.

The forms are currently available in the following languages:

- |                        |             |           |
|------------------------|-------------|-----------|
| ■ Brazilian Portuguese | ■ French    | ■ Korean  |
| ■ Chinese, Simplified  | ■ German    | ■ Polish  |
| ■ Chinese, Traditional | ■ Hebrew    | ■ Russian |
| ■ Danish               | ■ Hungarian | ■ Spanish |
| ■ Dutch                | ■ Italian   | ■ Swedish |
| ■ English              | ■ Japanese  |           |

When the Microsoft Exchange forms are installed on Microsoft Exchange Server computers, users whose mailboxes are on those computers and who have the Enterprise Vault Outlook Add-In installed on their computers can use the features of Enterprise Vault.

The Microsoft Exchange forms are copied to the Enterprise Vault server computer when you install the Enterprise Vault Server component. You can either configure the Outlook Add-In to copy the forms automatically to the Outlook Personal Forms Library or you can install the forms in the Organization Forms Library on the Exchange Server (Exchange Server 2000 and 2003).

## About OWA Extensions

To enable users to access archives and manage archived items from within OWA clients, Enterprise Vault OWA Extensions must be installed on Exchange Server 2010 or 2007 CAS computers. On Exchange Server 2000 and 2003, the extensions must be installed and configured on front-end and back-end Exchange Servers.

In OWA 2003 and later clients, archives can be searched and items can be archived, viewed, restored and deleted, if permitted. Enterprise Vault buttons and menu items are added to the client. The administrator can configure in the Enterprise Vault Administration Console what functionality is available to OWA users. In OWA 2000 clients, users can only view archived items.

OWA users do not require the Enterprise Vault Outlook Add-In to be installed on their desktop computers.

The Enterprise Vault OWA 2003 Extensions are also required to support access to Enterprise Vault when using RPC over HTTP connections to Exchange Server 2003. (No server extensions are required to support RPC over HTTP (Outlook Anywhere) access in Exchange Server 2010 or 2007 environments.) RPC users must have the Enterprise Vault Outlook Add-In installed on their desktop computers.

## About Enterprise Vault Mobile Search

Enterprise Vault Mobile Search is a Web-based application. It lets you use a Web browser on a mobile device to search for and view Microsoft Exchange Server



emails that Enterprise Vault has archived. You cannot use Mobile Search to reply to or forward an archived email, or to save an attachment.

Mobile Search is deployed as a Web application using Microsoft Internet Information Services (IIS). It accesses the IIS Web server using HTTPS.

Mobile Search accepts valid connection requests from most common mobile devices without the need for any device-specific configuration.

## About Enterprise Vault extensions for Lotus Notes

These extensions provide users with Enterprise Vault functionality in Lotus Notes mail clients and Domino Web Access clients. The extensions consist of template and database files, which you install on target Domino mail servers. They are currently available in the following languages:

- |                        |             |           |
|------------------------|-------------|-----------|
| ■ Brazilian Portuguese | ■ French    | ■ Korean  |
| ■ Chinese, Simplified  | ■ German    | ■ Polish  |
| ■ Chinese, Traditional | ■ Hebrew    | ■ Russian |
| ■ Danish               | ■ Hungarian | ■ Spanish |
| ■ Dutch                | ■ Italian   | ■ Swedish |
| ■ English              | ■ Japanese  |           |

These extensions give users full management access to mail file archives. Users can:

- Manually archive items.
- Delete items (if permitted).
- Use shortcuts to view items.
- Restore items.
- Search archive.

Archive Explorer is not available with Domino archiving, as Domino mail files are not structured and the data can be presented in multiple views.

## About Enterprise Vault Web access components

The Enterprise Vault Web Access application is configured in the default Web site in IIS. This application manages client connections to Enterprise Vault archives. 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.

The Enterprise Vault Web access components are Active Server Page applications which give users access to archives with standard web browsers.

The following applications are available:

- **Browser search.** This application enables users to perform complex searches, using a wide range of search criteria, on one or more archives. Items returned by searches can be viewed as HTML or in their original format.

The methods for restoring items found in a browser search differ between Exchange and Domino:

- In Exchange browser search, the user adds items to shopping baskets, which are managed by the Shopping Service. The contents of the baskets are restored to the user's mailbox (or a PST file, if permitted).

Archived file system or SharePoint items cannot be restored to their original location or the user's local computer using this application.

- In Domino browser search, the user selects items from the search results. The items are restored to the user's mail database.

- **Integrated search.** This simple search is available in various places throughout the Enterprise Vault system, including Outlook and OWA when users click the Enterprise Vault search button. This means that searching for archived items is very similar to Outlook's own Find.

The integrated search is also available in custom shortcuts (configured in the Exchange Mailbox Policy in the Administration Console) and in Archive Explorer.

In Lotus Notes, the integrated search is available in the Mail window by selecting a command on the **Tools** menu.

- **Archive Explorer.** This web interface presents folders within archives in a tree structure that users can browse for required items. The Archive Explorer interface may be available from within Outlook or OWA, but can also be accessed using a stand-alone browser.

In addition to the browse feature, users can view, restore and manage archived items. There are links to both integrated and browser searches.

In a stand-alone browser Archive Explorer can be used to access and manage other archive types: mailbox, public folder, file system or SharePoint. If Archive Explorer is started from within Outlook, only mailbox archives are available. When folders are archived, access permissions set on them are copied to the associated folders in the archive. So users who have access to shared folders will also have access to the associated folders in the archive.

When a user requests a search, the web access component instructs the Indexing Service to search the index for items that match the search criteria. When users

request to view or restore an item, the application interacts with the Storage Service or retrieval task.

## About Enterprise Vault monitoring and reporting

Enterprise Vault Operations Manager and Enterprise Vault Reporting are two optionally installable features that provide remote browser-based monitoring and reporting of your Enterprise Vault servers.

Note that you must set up an Enterprise Vault Monitoring database even if you do not install these features.

See “Enterprise Vault Reporting” on page 66.

See “Enterprise Vault Operations Manager” on page 68.

## FIPS 140-2 compliance

Federal Information Processing Standards (FIPS) 140-2 is a standard for cryptographic modules in computer systems.

Enterprise Vault 10.0.1 uses a FIPS 140-2 validated cryptographic module to provide the required cryptographic functionality.

Note that at this release the Symantec Enterprise Vault Cryptographic Module is not used for indexing.

For more information about Enterprise Vault and compliance with the FIPS 140-2 standard, and about using Enterprise Vault in a FIPS 140-2-compliant environment, see the following article on the Symantec Support Web site:

<http://www.symantec.com/docs/DOC4820>



# Enterprise Vault administration

This chapter includes the following topics:

- [About Enterprise Vault administration](#)
- [Administration Console configuration of archiving](#)
- [Administration accounts and roles](#)
- [How to archive PST file contents](#)
- [How to archive NSF file contents](#)
- [How to export archived items](#)
- [Welcome message and other notifications](#)
- [About reporting and monitoring in Enterprise Vault](#)
- [How to script management tasks](#)
- [Checklist of day-to-day management tasks](#)

## About Enterprise Vault administration

This section gives an introduction to Enterprise Vault management.

For the majority of Enterprise Vault administration you use the Enterprise Vault Administration Console, which is a snap-in to Microsoft Management Console (MMC).

You can also use the standard Windows tools to perform general management tasks, such as granting permissions and viewing event logs. You use Microsoft SQL Enterprise Manager to maintain the SQL databases.

A number of tools are provided for monitoring and reporting, including the Operations Manager, and the Enterprise Vault Reporting feature.

## Administration Console configuration of archiving

Within the Administration Console, Enterprise Vault configuration of archiving is, broadly speaking, broken down into the following:

- **Tasks** – A task is a job of archiving work that Enterprise Vault is to perform. For example, archiving from mailboxes on a particular Exchange Server computer.
- **Policies** – A policy specifies how the task is to be carried out. For example, when archiving from a mailbox the policy specifies the age at which items are to be archived and whether to create shortcuts to items that are archived.
- **Targets** – A target is the object on which a task acts. For example, depending on the type of task the target could be a Domino mail file, a disk volume, or an Exchange Server public folder.

Additionally, there are settings that affect the general behavior of Enterprise Vault and all tasks. These settings are editable in the Enterprise Vault Directory and site properties.

## Administration accounts and roles

The most important Enterprise Vault account is the Vault Service account. You must set up the Vault Service account and give it suitable permissions before you install Enterprise Vault. This account must be used to run the Enterprise Vault configuration wizard when you are setting up Enterprise Vault.

Enterprise Vault services and tasks use the Vault Service account when accessing Enterprise Vault databases. In Exchange Server archiving, the Vault Service account is used by Enterprise Vault tasks when connecting to the Microsoft Exchange Server.

Enterprise Vault tasks can run under the Vault Service account or you can, if required, specify different accounts for individual tasks.

See the *Installing and Configuring* manual for more information on creating the Vault Service account.

Enterprise Vault also provides administration roles that can be assigned to other Enterprise Vault administrators. These roles provide limited privileges to allow the users to perform given management tasks using the Administration Console. A number of predefined roles are provided for specific management tasks.

## How to archive PST file contents

You can migrate (import) the contents of Outlook PST files (Personal Folder files) into Enterprise Vault. You also have the option of creating shortcuts in users' mailboxes, which they can open to go directly to the archived items.

Enterprise Vault provides administrators with the following ways to migrate the contents of PST files into Enterprise Vault:

- Wizard-assisted migration – If you have a small number of PST files, this provides a quick and easy way of migrating them to Enterprise Vault.
- Scripted migration – This scripted migration facility is provided by Enterprise Vault Policy Manager. It is ideal for performing bulk migrations of PST files. It offers more flexibility than is available when using the migration wizard.
- Locate and Migrate – This locates PST files on users' computers, copies them to a central location, and then migrates them. Locate and Migrate is designed to minimize the difficulties of collecting PST files from users' computers and is likely to require the least effort on your part.
- Client-driven migration – It is possible for you to configure the Enterprise Vault Outlook Add-In so that users can perform their own PST migrations. The underlying mechanism that is used is Locate and Migrate, but users are able to queue their own PST files for migration. This can be useful if, for example, there are users with laptop computers who are in the office only one or two days a week, thus making it difficult to obtain their PST files by other methods.

To aid PST migration you can configure desktop clients so that, when a user starts Outlook, the client writes a marker into each PST file that is listed in the mail profile. When a marked PST file is subsequently imported, the marker indicates the owning mailbox.

PST migration is described fully in the *Administrator's Guide*.

## How to archive NSF file contents

You can migrate (import) the contents of Lotus Domino and Notes NSF files into Enterprise Vault. You also have the option of creating shortcuts in users' mail files, which they can open to go directly to the archived items.

Enterprise Vault provides Administrators with the following ways to migrate the contents of NSF files into Enterprise Vault:

- Wizard-assisted migration – If you have a small number of NSF files, this provides a quick and easy way of migrating them to Enterprise Vault.
- Scripted migration – This scripted migration facility is provided by Enterprise Vault Policy Manager. It is ideal for performing bulk migrations of NSF files. It offers more flexibility than is available when using the migration wizard.

NSF migration is described fully in the *Administrator's Guide*.

## How to export archived items

Enterprise Vault provides Administrators with a wizard to export archived items.

You cannot use the wizard to export Enterprise Vault Domino archives.

The wizard enables you to export the following:

- Archives to PST files.
- Archives to their original Exchange Server mailboxes.
- A single archive to any Exchange Server mailbox.

You can export the following archive types:

- Exchange Server mailbox and journal archives.
- File system archives.
- SharePoint archives.
- Shared archives. (Shared archives are special archives that you can create and enable several users to access. These archives do not contain folders.)

You can filter the output by date and by Retention Category. So, for example, you could export items less than a year old that were archived with a Retention Category of "Business".

When you export archives to PST files you can then import them back into Enterprise Vault. This is useful if, for example, you are moving a mailbox to a different Enterprise Vault site and want to move its archived items too.

## Welcome message and other notifications

When you enable archiving for an Exchange Server mailbox or Domino mail file, Enterprise Vault automatically sends a Welcome message to the user. The message



contains instructions for the users, describing what they have to do to start using Enterprise Vault.

Just what the users have to do depends on how you have set up Enterprise Vault. Consequently, you must edit the supplied template message before it is sent out so that it gives users appropriate information about how you have set up Enterprise Vault.

There is a template Welcome message for each Enterprise Vault client language.

Similarly, Enterprise Vault automatically sends a Goodbye message when you disable archiving for an Exchange Server mailbox or Domino mail file. Once again there is a supplied template that you need to edit appropriately.

There are also notification messages sent when PST and NSF files are migrated, and when the size of users' Exchange Server mailbox archives are approaching their limit, if archive size limits are set. You may want to edit these.

## About reporting and monitoring in Enterprise Vault

Enterprise Vault provides a host of facilities with which you can report on and monitor its operation. These facilities include the following:

- An Enterprise Vault Reporting feature, 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. See [“Enterprise Vault Reporting”](#) on page 66.
- The option to run Enterprise Vault tasks in report mode. This mode lets you gauge the usage of Enterprise Vault when it runs with particular settings, but without archiving any items. See [“Report mode”](#) on page 67.
- The facility to view critical and informational Enterprise Vault events in three Windows event logs. See [“Event and diagnostic logging”](#) on page 67.
- A System Status feature with which you can monitor the health of your Enterprise Vault system from within the Administration Console. See [“System status in the Administration Console”](#) on page 68.
- A browser-based Enterprise Vault Operations Manager application, which lets you monitor Enterprise Vault remotely from any computer on which Internet Explorer is installed. See [“Enterprise Vault Operations Manager”](#) on page 68.

- Facilities to monitor Enterprise Vault events and performance automatically, including the option to use Microsoft Operations Manager to monitor critical Enterprise Vault events and alerts.  
See [“Automatic monitoring of events and performance”](#) on page 69.
- The facility to monitor the performance of the Microsoft Message Queue (MSMQ) queues, which Enterprise Vault uses to transfer information between components.  
See [“Message queue monitoring”](#) on page 70.
- Options to enable auditing for a number of different types of events for individual Enterprise Vault servers.  
See [“Enterprise Vault auditing”](#) on page 70.
- Support for Veritas Backup Reporter, a browser-based application that displays customizable, multi-level views of backup and archive resources and customizable reports for tracking service usage and expenditures.  
See [“Veritas Backup Reporter 6.6 support for Enterprise Vault”](#) on page 71.

## Enterprise Vault Reporting

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

The supplied reports cover a variety of topics, including the following:

- Enterprise Vault service and task status
- Volume of items archived per Enterprise Vault server
- Mailbox archiving status
- Archive quota usage per user
- Most frequently accessed archived items
- Exchange server journal mailbox archiving status and trends
- Domino server journal mailbox archiving status and trends
- Vault store usage by archive or billing account

Administrators can do the following:

- Customize report content using the parameters provided by the report
- Choose from a number of report export formats, including PDF, XLS, HTML, TIFF

- Schedule reports to be emailed to a configured email address, or saved to a shared folder

The Enterprise Vault Reporting feature generates some of its Enterprise Vault server reports using data obtained from the Enterprise Vault Monitoring database.

If you configure FSA Reporting for a file server, you can also generate FSA Reporting reports for that file server and its volumes.

See [“FSA Reporting”](#) on page 106.

## Report mode

To gauge the usage of Enterprise Vault when it runs with particular settings, you can run tasks in report mode. In this mode, Enterprise Vault does not archive items but produces a report about what would be archived on a normal run.

The reports are logged in a file in the `Reports` folder, which is a subfolder of the Enterprise Vault installation folder. The fields in the file are tab-separated, so you can easily import the file contents into a spreadsheet program such as Microsoft Excel.

The following are examples of the types of reports that are generated:

- Exchange mailbox preparation. When processing Provisioning Groups, the Provisioning task reports on mailboxes that have been prepared for archiving and the policies assigned.
- PST migration. In the case of Locate and Migrate there are separate reports for each phase of the migration: Location, Collection, and Migration.
- File System Archiving actions.
- SharePoint archiving actions.
- In the Administration Console, Vault Store Usage Reporter can generate different reports detailing vault store usage.

## Event and diagnostic logging

Enterprise Vault logs events to three Windows event logs. You can use the Windows Event Viewer to view these logs. Additionally, you may have your own or various third-party tools that you can use to monitor the Enterprise Vault log entries.

The logs that Enterprise Vault uses are as follows:

- Windows Application Event Log – This is used for events that are deemed to be critical. Service start-up and shutdown events are logged here and also events arising from the integrated monitoring that is on Site Properties. These include, for example, warnings if databases have not been backed up recently

or if there is a backlog of items in journal mailboxes with a status of archive pending.

When Enterprise Vault logs an event from the integrated monitoring it also shows the event in the Status pane of the Administration Console. The Status pane provides the quickest way for you to check the health of the Enterprise Vault system.

- **Enterprise Vault Log** – This is used for all events that are not deemed to be critical. For example, events relating to the progress of mailbox or public folder archiving. Additionally, events that are placed in the Windows Application Event Log are also placed in the Enterprise Vault Log, thus ensuring that the Enterprise Vault Log contains a complete record of all events.
- **Enterprise Vault Convertors Log** – This contains events arising from document conversions.

For each of the Enterprise Vault services, you can select the level of diagnostics that is reported. The diagnostic reports are logged in the Enterprise Vault Log.

## System status in the Administration Console

Enterprise Vault automatically runs checks to monitor the health of the Enterprise Vault system. If any check finds a problem Enterprise Vault displays an alert in the **Status** pane of the Administration Console.

You can also run the checks from the **Status** pane without waiting for the scheduled checks.

You can configure each of the checks on the **Monitoring** tab of **Site Properties**. For each check you can set the following:

- The threshold level. Enterprise Vault displays an alert when this threshold is exceeded.
- The frequency, which is how often you want the check to run.
- The start time. You can specify any required time. If you do not select a time, the statistics are collected when the monitoring process starts and then according to the frequency that you have defined for each check.

The **Status** pane provides the quickest way for you to check the health of the Enterprise Vault system.

## Enterprise Vault Operations Manager

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

Enterprise Vault Operations Manager lets the administrator monitor the following:

- The status of Enterprise Vault services.
- The status of Enterprise Vault archiving tasks.
- Performance counters for vault stores, disk, memory, and processors.
- Exchange Server journal mailbox target archiving parameters, including message counts for Inbox, Archive Pending, and failed operations such as Failed DL Expansion.
- Domino Server journaling target archiving parameters, including message counts for Inbox, Archive Pending and failed operations.
- The status of the Discovery Search Service components and of the searches that you have conducted with them.

A Monitoring agent on each Enterprise Vault server collects data at scheduled intervals, typically every few minutes. This data is then stored in the Monitoring database. The Enterprise Vault Operations Manager Web pages display the data from when the system was last monitored. Summary pages provide at-a-glance status assessment, while detailed data can help identify problems and bottlenecks.

## Automatic monitoring of events and performance

Enterprise Vault has the following further mechanisms that you can use for automatic monitoring:

- In the Administration Console, the Monitoring tab in Site Properties enables you to turn on performance monitoring of important aspects of Enterprise Vault. When a monitored item reaches its threshold settings, an alert is logged in the following places:
  - The Status pane in the Administration Console
  - The Enterprise Vault event log
  - The Windows Application event logIf you have other tools to monitor the log you can then, if necessary, be notified when such messages are logged.
- If you have Microsoft Operations Manager (MOM) then you can use the supplied Enterprise Vault Management Pack to monitor Enterprise Vault operations and performance and to take appropriate actions as required.

## Message queue monitoring

Enterprise Vault uses Microsoft Message Queue (MSMQ) Server to transfer information between Enterprise Vault components. It is important that you monitor MSMQ queues so that you can quickly spot any problems that may occur.

You can use the Windows Performance Monitor to monitor the performance of the queues. You may find it useful to have the Windows Performance Monitor running continuously, showing the number of messages on all the queues.

You will quickly become used to the normal behavior of the queues and will notice excessive backlogs. Investigate the cause of any such backlogs promptly.

More information on the queues used by Enterprise Vault processes is given in the *Administrator's Guide*.

## Enterprise Vault auditing

Enterprise Vault includes flexible auditing that you can enable for individual Enterprise Vault servers. The auditing events are written to a SQL Server database—you can have a single auditing database for all Enterprise Vault Servers in a site.

For example, the audit events record the following:

- The time an event occurred
- The account that initiated the event
- The archive in which an item was archived
- The category of the event, such as View, Archive, or Delete

You can enable auditing for a number of different types of event, showing for example, details of the following:

- Actions taken using the Administration Console
- Searches
- Viewing an item
- Deletions

For most types of event you can specify detail levels of Summary or Details, or both:

- Summary gives information about the event, such as the date and time, account used, vault used.
- Details lists more information, such as extracts from the content of a message, for example Subject, Mailbox Owner, and Folder.

Note that there will be a slight reduction in performance when you enable auditing.

By default, auditing is disabled.

For information on how to set up auditing, see "About auditing" in the *Administrator's Guide*.

## Veritas Backup Reporter 6.6 support for Enterprise Vault

Symantec Veritas Backup Reporter (VBR) is a Web-based software application that provides the following:

- Customizable, multi-level views of backup and archive resources.
- Customizable reports to track service usage and expenditure.
- Tools for defining cost metrics and chargeback formulas or for handling alerts.

Veritas Backup Reporter 6.6 extends the scope of VBR to provide comprehensive reporting on the Enterprise Vault archive data that relates to Microsoft Exchange Server:

- Reports can provide mailbox-level granularity for an Enterprise Vault site, provisioning group, Enterprise Vault server, or Exchange server.
- You can generate reports across your archiving targets and vault stores, including capacity reports down to the partition level.
- A full extension of the business views builder enables you to create management reports and facilitate chargeback.
- Historical trending and forecasting enable the analysis of archive policy objectives.

## How to script management tasks

Enterprise Vault Policy Manager provides a scripted method of modifying and controlling Exchange Server mailboxes and archives so that they conform to your Enterprise Vault archiving policies.

Additionally, you can use Policy Manager to migrate the contents of PST files and NSF files to Enterprise Vault.

Policy Manager enables you to apply settings to individual mailboxes in a much more specific manner than you can when using the Administration Console.

For example, you could write a script to do the following:

- Define a filter that archives all items older than 1 month.

- Create a folder called Personal Archive in all mailboxes and apply the new filter to the folder.
- Apply the Personal Retention Category to the new Personal Archive folder.

Policy Manager runs in Command Prompt window and uses an initialization file of settings to apply to mailboxes, archives, and to PST and NSF file migrations.

An additional Provisioning API is available. This can be used to provide the auto-enabling of mailboxes from a web page, for example. The API can also be used in conjunction with Enterprise Vault Policy Manager.

## Checklist of day-to-day management tasks

The following provides a checklist of the main day-to-day administration tasks required to maintain optimal performance of your Enterprise Vault system:

- Checking the system status in the Administration Console
- Checking logs
- Monitoring Enterprise Vault tasks and services
- Starting or stopping tasks or services
- Monitoring Exchange Server journal mailboxes and Domino journal databases
- Monitoring disk usage
- Monitoring MSMQ queues
- Maintaining SQL databases
- Backing up vault stores
- Enable archiving for new Microsoft Exchange Server mailboxes or Domino mail files
- Importing PST files (Personal Folder files)
- Importing NSF files
- Monitoring licenses
- Modifying the list of who has access to an archive that is being shared by a number of users

Full details of how to perform these tasks are given in the *Administrator's Guide*.

There are a number of utilities available for performing a variety of tasks, such as recreating FSA Placeholder shortcuts on a file server, moving archived data from an NTFS device to an EMC Centera device, and managing FSA archive points.



See the *Utilities Guide*.



# Exchange Server archiving

This chapter includes the following topics:

- [About Exchange Server archiving and user mailboxes](#)
- [Exchange Server and journal mailbox archiving](#)
- [Types of items to archive with Exchange Server archiving](#)

## About Exchange Server archiving and user mailboxes

User mailboxes hold many types of information, for example, messages, documents, spreadsheets, graphics, and voice mail. You can specify the types of items that Enterprise Vault archives (message classes) in the properties of the Enterprise Vault Directory or in the Exchange mailbox policy.

See [“Types of items to archive with Exchange Server archiving”](#) on page 81.

In Enterprise Vault, you create an Exchange Mailbox task to archive items from user mailboxes. The user mailboxes that the task is to archive are defined using Targets. Enterprise Vault automatically creates an archive for each user mailbox to be archived. How the mailboxes are to be archived is defined in Exchange Mailbox Policies.

A single Enterprise Vault site can serve more than one Exchange domain (Exchange Organization in Active Directory). Using policies, you can apply the same archiving strategy to all users in a domain or you can configure different archiving strategies for different groups of users within the domain.

If you use a database availability group (DAG) in your Exchange Server 2010 environment, you must set up archiving for all members of the DAG.

Mailbox archiving does not automatically archive information held in PST files stored on the user's computer. However, the administrator can use Enterprise Vault PST migration tools to copy items from PST files into user mailbox archives.

See [“How to archive PST file contents”](#) on page 63.

## Exchange Provisioning tasks

You use provisioning groups to group the user mailboxes that are to be archived using the same archiving policy.

You can select the mailboxes to be associated with a provisioning group using any of the following:

- Windows group
- Windows user
- Distribution Group (the Active Directory Group type, Distribution)
- Organizational Unit
- LDAP query
- Whole Exchange Server organization

The provisioning groups are then processed by the Exchange Provisioning task. This task assigns the correct policy settings to each mailbox.

The Provisioning task can also be used to relink mailboxes to the associated archives, if, for example, the mailboxes are moved to a different Exchange Server.

## Exchange Mailbox Archiving tasks

In the Administration Console, on the required Enterprise Vault server under Enterprise Vault Servers, you create an Exchange Mailbox Archiving task for each Exchange Server with user mailboxes to be archived. These tasks are controlled by the Task Controller Service.

The Exchange Mailbox Archiving task is responsible for the following:

- Enabling mailboxes that have been processed by the Exchange Provisioning task. The Exchange Mailbox Archiving task creates an archive for the mailbox and enables the mailbox for archiving.

When new mailboxes are created, these can be enabled manually or automatically, according to settings for the provisioning group.

- Accessing each mailbox and archiving items according to the policy set for the mailbox. The task works in cooperation with the Indexing Service, which converts and indexes items, and the Storage Service, which compresses and stores the items in the associated archive.

You can specify the Indexing Service and indexing level to use at various places in the Enterprise Vault Administration Console tree.

- The mailbox folders are replicated in the associated mailbox archive, as are the permissions set on the folders. The archiving task synchronizes folder permissions in Outlook with folder permissions in the archive. This means that if other users have been given access to an Outlook folder, they will also have access to that folder in the mailbox archive.

If required, you can set up shared archives that several users can access. For example, the mailboxes of legal staff could all be set up to have a folder for a case and, in each mailbox, the folder configured to be archived to a shared archive. Unlike mailbox archives, shared archives do not contain folders.

To obtain an estimate of the number of items that will be archived, without actually archiving anything, you can run the task in Report Mode.

Exchange Mailbox Archiving tasks run automatically according to the schedule defined for the Enterprise Vault site.

## Exchange archiving targets

The mailboxes to be archived are defined by targets that you create in the Administration Console under Targets > Exchange. A target can be a whole Exchange domain, defined in Active Directory as an Exchange Organization, or a group of users within the Exchange Organization, or an individual user. Within an Exchange Organization in Enterprise Vault, there may be several Exchange Servers. Exchange Server mailbox targets are defined using provisioning groups.

For a provisioning group, you can configure settings including the following:

- The Exchange mailbox policy and desktop policy to be used for the target group
- The default Retention Category to be used for items being archived
- The vault store to store archives in
- The Indexing Service to use
- Whether mailbox archives are to be enabled automatically
- A policy for importing PST file contents to archives

An Exchange mailbox policy and desktop policy are associated with each provisioning group. Together, these policies define how that group of user mailboxes is archived, and the user desktop experience in terms of the Enterprise Vault features and functions available. If you want to use different settings for different groups of users, you will need to create, in the Administration Console, a provisioning group for each group of users and a suitable Exchange mailbox policy and desktop policy for each group.

## Exchange mailbox policies

In Enterprise Vault Administration Console you create mailbox archiving policies under Policies > Exchange > Mailbox.

An Exchange mailbox policy supplies information for the archiving task to use when processing the target mailboxes, including the following:

- The indexing level to use.
- The archiving strategy. You can base the archiving strategy for an Exchange mailbox policy on one of the following:
  - Age: items are archived when they have not been modified for the time that you specify.
  - Quota: archiving keeps a percentage of each user's Exchange mailbox storage limit free.
  - Age and quota: Enterprise Vault performs age-based archiving first. If age-based archiving does not make the required percentage of mailbox storage limit free, quota-based archiving continues until the required percentage is reached.
- Archiving actions, such as deleting the original item or creating shortcuts after archiving an item.
- Whether shortcuts are created and what they contain.
- Whether items are archived from Exchange managed folders, and whether Enterprise Vault uses retention settings that are based on Exchange managed content settings.
- The types of items (Message Classes) that are archived. (You can set the default list of Message Classes in the Directory properties in the Administration Console.)

You can lock policy settings to prevent users from being able to change them in their Outlook client. This can be done from the Archiving Actions tab of the mailbox policy properties.

## Exchange desktop policies

An Exchange desktop policy defines the end users' experience when using the Enterprise Vault Exchange clients. It contains the settings that control the Enterprise Vault features and functionality available with these clients.

The desktop policy settings include the following options:

- Show or hide Enterprise Vault buttons and menu options, such as Archive Explorer, Search Vaults, Store in Vault, Restore from Vault, and Delete from Vault.
- Customize deletion behavior when the user deletes a shortcut.
- Show or hide the Browser Search link displayed to the user in Outlook integrated search.
- Add all servers to the users' Internet Explorer local intranet zone, so that users are not prompted for their logon details when they search their archives or view or restore archived items.
- Control the availability, the maximum size, and the available features of Vault Cache.
- Control the availability and the behavior of Virtual Vault.
- Change the method of deploying Exchange forms for Enterprise Vault.

In Enterprise Vault Administration Console you create Exchange desktop policies under Policies > Exchange > Desktop. When you create a provisioning group you assign a desktop policy to it. You can create multiple desktop policies if you want different provisioning groups to use different policy settings.

## Exchange archiving filters

An advanced filtering feature enables you to customize the way certain messages are processed by the archiving task. Messages can be filtered on a variety of attributes, such as sender, recipients, subject, message direction or custom MAPI properties added by a third party application. Using XML configuration files, you can define the required action for messages that meet the filter rules. For example, you may want messages from a certain domain to be given a different Retention Category and archived in a different archive.

The custom filtering feature is particularly useful if your enterprise adds custom MAPI properties to items and you want to be able to search archived items using these custom properties. Using the XML configuration files, you can specify custom properties that are to be indexed by Enterprise Vault when the message is archived.

To enable you to search on custom properties, the Enterprise Vault browser search supports the custom filtering feature. You define in the XML configuration files which properties are to be available in the user interface for searches, and how the search options for these are to be displayed.

An API is also available to enable you to add custom property searching to proprietary archive search applications.

Custom filtering can be configured for particular types of Exchange Server archiving (mailbox, public folder or journal archiving). If required, custom filtering can be restricted to particular mailboxes.

How to configure custom filters and properties is described in the *Setting up Exchange Server Archiving* manual.

If you want a customized filter written for this interface, contact your Symantec solutions provider.

## Exchange Server and journal mailbox archiving

You can set up an Exchange Server so that a copy of all messages sent and received by the Exchange Server is passed directly to a journal mailbox in addition to the recipient mailbox. This is particularly useful if you want to implement a company email monitoring policy and vital if there is a possibility that you may have to produce email as legal evidence at some later date.

When setting up Enterprise Vault Exchange Journal archiving in the Administration Console, you add Exchange journal targets, policies and tasks. You also create an archive for each target Exchange journal mailbox that Enterprise Vault will archive.

An Exchange Journaling task performs the archiving. One of these tasks can service multiple journaling mailboxes. Exchange Journaling tasks run under the control of the Task Controller Service.

Exchange Server journal mailbox archiving archives all types of messages sent to the journal mailbox; it does not take account of the message classes defined in the properties of the Enterprise Vault Directory.

Items in journal mailboxes are deleted from the mailbox as they are archived, or after the vault store is backed up, and no shortcuts are created. Administrators with access permissions to the journal archives can search for messages. As journaled items may be confidential, it is important to give such access to a few trusted users only.

See [“Types of items to archive with Exchange Server archiving”](#) on page 81.

The Enterprise Vault Exchange Journaling task automatically detects and processes correctly any messages from Exchange Servers with envelope journaling enabled.

See the *Setting up Exchange Server Archiving* manual for more information on how Enterprise Vault supports envelope journaling.

Enterprise Vault Accelerator products can be used on journaled data; Discovery Accelerator enables legal discovery, providing features such as searching, a



reviewing system and publishing; Compliance Accelerator provides message monitoring features, such as sampling, searching and a reviewing system.

As journaling generates a large amount of data, Enterprise Vault can be used to control the disk space used on the Exchange Server by continuously archiving the contents of the journal mailbox.

## Exchange Server and journal filtering

Selective and group journaling enable you to configure simple filtering of journal mailbox messages. You can set up special filters, called "external filters", to define how specific messages are processed. For example, you may not want to archive system messages or Out of Office messages or you may want to identify messages sent from one group of users to another.

Custom filtering provides more sophisticated journal filtering with a wide variety of filtering rules that you can apply when archiving journal mailboxes.

See [“Exchange archiving filters”](#) on page 79.

## Compliance Accelerator and Exchange journaling

Enterprise Vault Compliance Accelerator includes a special filter, called the Journaling Connector. This filter works with the Exchange Journaling task to take a random sample of messages being archived from the Exchange journal mailbox and add them automatically to the set of messages to be reviewed by compliance officers. The size of the sample required is configurable.

# Types of items to archive with Exchange Server archiving

In Exchange Server, items are categorized by message class. Enterprise Vault comes with a predefined set of message classes that identify different types of items. This list is defined on the Message Classes page of the Directory properties. You can add or remove message classes on this page. Note that this list of message classes applies across the Directory, not just to the site.

[Table 4-1](#) lists the predefined message classes and indicates which types of messages are archived by default.

**Table 4-1** Predefined message classes

Type of item	Message class	Archived by default
Calendar items	IPM.Appointment	No

Table 4-1            Predefined message classes (continued)

Type of item	Message class	Archived by default
Contact items	IPM.Contact	No
Documents	IPM.Document	Yes
Electronic sticky notes	IPM.Stickynote	No
Interpersonal messages	IPM.Note	Yes
Journal messages	IPM.Activity	No
Messages posted to a folder	IPM.Post	Yes
Tasks	IPM.Task	No

With the exception of Exchange Journal archiving, Enterprise Vault archives items whose message classes match the text listed. Exchange Journal archiving stores all items that are sent to the journal mailbox, irrespective of the message classes configured.

When adding message classes to the list in the Directory properties, you can use a trailing asterisk as a wildcard. For example, a message class of 'IPM\*' would include 'IPM.Appointment', 'IPM.Contact', 'IPM.Document', and so on.

If required, you can customize the message classes to archive in Exchange Public Folder Policies or Exchange Mailbox Policies.

# Exchange Public Folder archiving

This chapter includes the following topics:

- [Exchange Public Folder tasks, Targets, and Policies](#)
- [How an Exchange Public Folder task archives](#)
- [User access to Exchange Public Folder archives](#)

## Exchange Public Folder tasks, Targets, and Policies

You can add one or more Exchange Public Folder tasks to enable archiving from public folders. Exchange Public Folder tasks run under the Task Controller Service.

An Exchange Public Folder task archives a Public Folder target. Each Exchange Public Folder task can process multiple Public Folder targets. A Public Folder target is a single public folder hierarchy, starting from its root path and working down. You can add a Public Folder target with a root path that is higher up a public folder hierarchy than the root path of an existing Public Folder target. You cannot add one with a lower root path.

When you add a Public Folder target, you select the vault store and archive that is to be used for it. The archive must be a Public Folder archive but the vault store may be the same one used for other archive types, such as mailbox archives. If required you can also use the same archive for more than one Public Folder target. To be able to change the archiving settings for a Public Folder target you need owner access to the Public Folder.

An Exchange Public Folder Policy is assigned to each Exchange Public Folder target. This defines how the task will archive the items in the public folders that it services.

The Exchange Public Folder task processes all folders beneath each target's root path, except for folders that are processed by another Exchange Public Folder task and those that have archiving disabled (This can be set in Outlook using the Enterprise Vault Properties for the public folder or in the properties for the Public Folder target).

If required, custom filtering can be configured to select the items to be archived from Public Folders.

New Public Folders under a specified root can be automatically added as targets by setting the public folder target to be an Auto-Enabler. Whenever a new Public Folder is added under the target root, the folder is automatically enabled for archiving and a new archive is created for that folder and any subfolders.

This feature should be used with caution, as it could result in a very large number of archives being created. However, it can be useful in some organizations, such as legal departments, where folders are created for new cases.

Public Folder Auto-Enablers can generate targets for other tasks. On large systems, scanning for new public folders can take a long time, so passing new targets to other tasks means that processing of folder content is not held up by scanning.

## How an Exchange Public Folder task archives

When you add a new Exchange Public Folder task, the task runs at the scheduled times, archiving from each of its target folders.

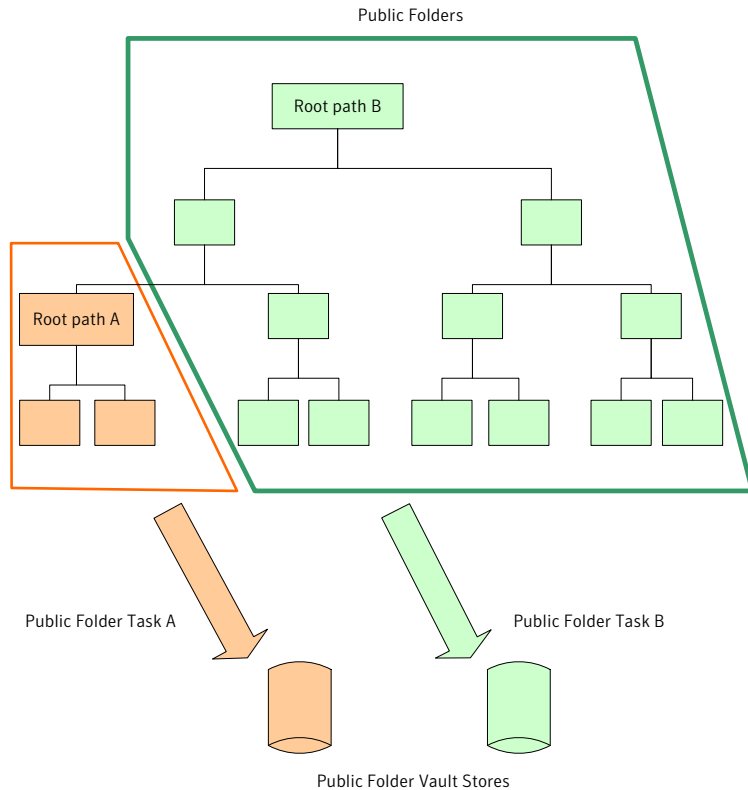
For each folder, the Exchange Public Folder task does the following:

- Matches the permissions on the folder's archive to those on the folder.
- If the folder has been given explicit Enterprise Vault archiving settings, then the Exchange Public Folder task archives according to those settings. Otherwise, the Exchange Public Folder task uses the default settings that you have defined in the Exchange Public Folder Policy.
- If the folder is the root path of a Public Folder target that is processed by a different Exchange Public Folder task, it does not archive the folder, nor any folders beneath it.
- If the folder is not accessible, then the Exchange Public Folder task does not archive the folder, nor any folders beneath it.

As with archiving other types of files, the Storage Service converts the Public Folder items to HTML, if possible, and stores them in the archives. The Indexing Service indexes the item details and content to enable searching. Note that the archive used for a Public Folder can be changed at any time by editing its properties in the Administration Console.

Figure 5-1 shows a Public Folder hierarchy that is archived by Exchange Public Folder tasks A and B.

**Figure 5-1** Archiving Public Folder hierarchies



When task B finds the root path folder for task A, it archives no further down that branch of the hierarchy.

Note that archiving on root path A was created before archiving on root path B, because you cannot add a Public Folder target with a root path that is already archived by an existing Exchange Public Folder task.

## User access to Exchange Public Folder archives

Users can access archived Public Folder items using shortcuts or using Archive Explorer to browse the required Public Folder archive.

All users with read access to the Public Folder's archive can do the following:

- View the contents of archived items. To view items, double-click shortcuts in the Public Folder or, in Archive Explorer, double-click the item in the archive.
- Restore from the Public Folder's archive to their own mailboxes. In Outlook, the users must first copy the shortcuts to their own mailboxes.

Users who have write access to a Public Folder can also:

- Modify the folder's Enterprise Vault settings.

Users with Owner access to a Public Folder can do the following:

- Manually archive from a folder
- Restore items to a folder

Use the Administration Console if you want to remove a Public Folder target, because this removes the marker that Enterprise Vault places on the root path folder.

# File System Archiving

This chapter includes the following topics:

- [About File System Archiving](#)
- [About File archiving policies](#)
- [About shortcut files with File System Archiving](#)
- [About setting up File System Archiving](#)
- [File System Archiving in a clustered environment](#)
- [The process of File System Archiving](#)
- [How File System Archiving handles older versions of archived files](#)
- [How File System Archiving synchronizes permissions](#)
- [File System Archiving reports](#)
- [How to restore files with File System Archiving](#)
- [About FSAUtility](#)
- [How to back up and scan shortcut files with File System Archiving](#)
- [Pass-through recall for placeholder shortcuts with File System Archiving](#)
- [File Blocking with File System Archiving](#)
- [Retention Folders and File System Archiving](#)
- [FSA Reporting](#)

## About File System Archiving

You can set up Enterprise Vault File System Archiving (FSA) to archive files from network shares. Users can then access the archived files using shortcuts in the original locations, Archive Explorer, or the browser search page.

The *Enterprise Vault Compatibility Charts* document provides a full list of the target platforms, operating systems and protocols that Enterprise Vault supports for FSA. The document also lists the operating systems supported for client access of archived items, including opening Internet and Placeholder shortcuts to archived items. The *Enterprise Vault Compatibility Charts* document is available at the following address on the Symantec Enterprise Support site:

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

By archiving from the file system, you can gain the following immediate benefits on the volumes that are being archived:

- It is easy to archive files. You may have files that you want to add to your archive system, perhaps because of legal requirements. You can create an archiving policy to archive them all immediately.
- Files that are archived are indexed, so they are searchable.
- Previous versions of archived files are retained. When a user creates a new version of a file that has been archived, that new version will be archived when it is matched by the rules you define. All the earlier archived versions of the file are retained and are searchable.
- There may be an immediate space usage reduction.

The Retention Folder feature enables you to create a hierarchy of folders automatically on file servers, to be managed by Enterprise Vault and archived according to assigned policies. For example, you could create a hierarchy of retention folders in every user's home folder.

The File Blocking feature enables you to prevent unwanted files from being saved on monitored server volumes.

FSA Reporting provides summary reports on the active data on your file servers, and on the data that has been archived from them.

## About File archiving policies

In the Enterprise Vault Administration Console you define File archiving policies to control which files are archived by FSA. You can apply policies to whole disks (volume policies), or to folders and subfolders (folder policies) as required.



A policy contains one or more archiving rules that you define to select the files you want Enterprise Vault to archive. You can apply the archiving rules in any order, as required. In combination with the other policy settings, the result is that you have a flexible mechanism to archive precisely what is required.

For example, you can create archiving policies that do the following:

- Start archiving when the volume is 80% full and continue until the volume is 60% full.
- Archive all files older than 30 days except Hidden and System files.
- Archive \*.zip and \*.avi files that are older than three days and larger than 20 MB.
- Delete \*.bak files that have not been accessed in the last week, without archiving them.
- Archive \*.doc files and do not create a shortcut for each file until one month after it was last modified.

A number of predefined file groups are available to enable you to quickly add the required file types to the policy.

File System Archiving can archive all file types. However, some file types such as executable files and .PST files are not suitable candidates for file archiving. The Default Volume Policy and Default Folder Policy include archiving rules that you can use to exclude unsuitable file types from archiving and shortcut creation. For more details, see *Setting up File System Archiving*.

## About shortcut files with File System Archiving

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

- An internet (URL) shortcut. This is a .url text file that contains a hypertext link to the archived file.
- A placeholder. This is a special file that appears exactly as the original file but, when opened, forces Enterprise Vault to fetch the archived file.

Internet shortcuts can be placed on any network share. When a user double-clicks an internet shortcut, the archived file is retrieved and is shown in the appropriate application.

If you open an internet shortcut from within an application, the application opens the contents of the shortcut, not the archived file.

Internet shortcuts have a suffix of .url. This suffix is appended to the file's existing suffix. For example, the shortcut for a Word document file named

`document1.docx` is named `document1.docx.url`. The inclusion of the original suffix enables you to determine the original file type that the internet shortcut references.

**Note:** If you choose the Windows Explorer option "Hide known file types", Windows still displays the original file type of an internet shortcut. For example, the internet shortcut `document1.docx.url` appears as `document1.docx`.

Internet shortcuts have the advantage that they can be used on both Windows and non-Windows devices.

Placeholder shortcuts behave exactly as the original files. A placeholder shortcut has the same file extension as the file to which it is a shortcut. When a user opens a placeholder shortcut, the original file is automatically retrieved.

[Table 6-1](#) shows the behavior of placeholder shortcuts when you open, copy, move, or delete them.

**Table 6-1** Characteristics of placeholder shortcuts

Action on placeholder	Effect
Open	<p>The file is recalled from the archive.</p> <p><b>Note:</b> If pass-through recall is in effect, Enterprise Vault recalls the file to disk only if the calling application requires a writeable version.</p> <p>See <a href="#">“Pass-through recall for placeholder shortcuts with File System Archiving”</a> on page 102.</p> <p>A file that is recalled to the file server replaces the placeholder shortcut.</p> <ul style="list-style-type: none"><li>■ If the recalled file remains unmodified, then Enterprise Vault converts the file back to a placeholder on the next archiving service run. The only exception is if the archiving policy's shortcut creation rules are based on the last access time. In that case, Enterprise Vault reverts the file only when the shortcut creation rules are met.</li><li>■ If the recalled file becomes modified, then Enterprise Vault converts the file back to a placeholder according to the archiving policy's shortcut creation rules.</li></ul>

**Table 6-1** Characteristics of placeholder shortcuts (*continued*)

Action on placeholder	Effect
Copy	<p>The source file is restored and then copied. The destination file is a copy of the restored original file.</p> <p><b>Note:</b> The copy operation does not restore the source file to disk if pass-through recall is in effect.</p> <p>See <a href="#">“Pass-through recall for placeholder shortcuts with File System Archiving”</a> on page 102.</p> <p>Enterprise Vault converts a restored original file back to a placeholder on the next archiving service run. The only exception is if the archiving policy's shortcut creation rules are based on the last access time. In that case, Enterprise Vault reverts the file only when the shortcut creation rules are met.</p>
Move	<p>If the destination is on the same volume, the placeholder is moved.</p> <p>If the destination is on a different volume, the archived file is restored and then moved to the destination.</p>
Delete	<p>You can configure Enterprise Vault to delete archived files when their placeholders are deleted, if you want. You must configure some settings for the file server, and apply an archiving policy with the appropriate settings.</p> <p>For more information, see the <i>Setting up File System Archiving</i> guide.</p>

Placeholder shortcuts are supported on NTFS devices, NetApp Filers, and EMC Celerra/VNX devices. For details of the exact requirements, see the Enterprise Vault *Compatibility Charts*.

In the archiving policy you can control the time at which Enterprise Vault creates shortcuts. For example, you can create a rule to archive Microsoft Office files. The rule can make Enterprise Vault leave the original files on the disk and create shortcuts to them later. Enterprise Vault can create a shortcut to a file according to any of the following:

- Archived time
- Last accessed time
- Last modified time
- Created time

By creating a rule like this one you can ensure that files are archived for safety but are still available for editing. When a file is no longer being changed frequently, Enterprise Vault creates a shortcut to the archived copy.

## About setting up File System Archiving

Very briefly, setting File System Archiving involves the following tasks:

- Preparing the file server as necessary, and then adding it as a target file server in the Administration Console. You must install the Enterprise Vault FSA Agent on a Windows file server on which you want to leave placeholder shortcuts, implement File Blocking, or collect 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>.

---

- Creating volume policies to define how and what to archive from target volumes. Optionally you can also create folder policies, to override the volume policies for specific target folders.
- Adding the target volumes to the Administration Console, and assigning the volume policies.
- Adding target folders, and assigning the parent volume policy or a folder policy. You can define an archive point for each folder that you want to associate with a separate archive. A folder with an archive point forms the top of an archive. Files from the folder and its subfolders are stored in the same archive.
- Configuring other features as required, such as File Blocking, retention folders, and FSA Reporting.
- Configuring the File System Archiving tasks to schedule archiving and associated activities, and to determine the mode in which the archiving is to run.

**Table 6-2** shows the properties of the Enterprise Vault Administration Console containers that you can use to control File System Archiving.

**Table 6-2** Controlling File System Archiving from the Administration Console

Item	Properties
Target file server (under Targets\File Servers)	<ul style="list-style-type: none"> <li>■ Whether to archive the file server.</li> <li>■ Configuration settings for pass-through recall for placeholder shortcuts.</li> <li>■ Configuration settings for File Blocking.</li> <li>■ Configuration settings for deletion of archived files on placeholder deletion.</li> <li>■ Configuration settings for FSA Reporting.</li> </ul>
Target Volume (under Targets\File Servers\<server>)	<ul style="list-style-type: none"> <li>■ Whether to archive the volume.</li> <li>■ The File System Archiving task that is to process the volume.</li> <li>■ The File System Archiving policy to apply when processing the volume.</li> <li>■ For NTFS volumes, whether to enable pass-through recall for placeholder shortcuts on this volume.</li> </ul> <p>A target volume is processed according to the File System Archiving task schedule, but can be processed manually by using the Run Now option.</p>
Target Folder (under Targets\File Servers\<server>\<volume>)	<ul style="list-style-type: none"> <li>■ Whether to archive the folder.</li> <li>■ Whether to archive the subfolders of the folder.</li> <li>■ The FSA policy to apply when processing the folder.</li> <li>■ The location of archive points, which mark a folder that forms the top of an archive.</li> </ul>

Table 6-2

Controlling File System Archiving from the Administration Console

(continued)

Item	Properties
Volume policy (under Policies\File)	<p>Each target volume is assigned a volume policy, which defines the following:</p> <ul style="list-style-type: none"><li>■ The File Blocking rules to apply to the volume, if File Blocking is configured.</li><li>■ For NTFS volumes, whether to use quotas.</li><li>■ The type of shortcut to leave, if the archiving rules specify that a shortcut is to be created.</li><li>■ For placeholder shortcuts:<ul style="list-style-type: none"><li>■ Whether to delete archived files on placeholder deletion.</li><li>■ Whether to delete placeholders for the items that are deleted from archives.</li></ul></li><li>■ The retention category to use for archived files.</li><li>■ The archiving rules to apply. These rules determine which files to archive, and when to create shortcuts.</li><li>■ Whether to archive files that have explicit permissions. When a file is archived, the version stored in the archive is given the same permissions as the folder that contained the original file. This could result in a change in permissions.</li></ul>
Folder policy (under Policies\File)	<p>Folder policies are optional. Use them when you want to override the volume policy for specific folders.</p> <p>A folder policy defines the following:</p> <ul style="list-style-type: none"><li>■ The type of shortcut to leave, if the archiving rules specify that a shortcut is to be created.</li><li>■ For placeholder shortcuts:<ul style="list-style-type: none"><li>■ Whether to delete archived files on placeholder deletion.</li><li>■ Whether to delete placeholders for the items that are deleted from archives.</li></ul></li><li>■ The retention category to use for archived files.</li><li>■ The archiving rules to apply. These rules determine which files to archive, and when to create shortcuts.</li><li>■ Whether to archive files that have explicit permissions.</li></ul>

**Table 6-2** Controlling File System Archiving from the Administration Console  
*(continued)*

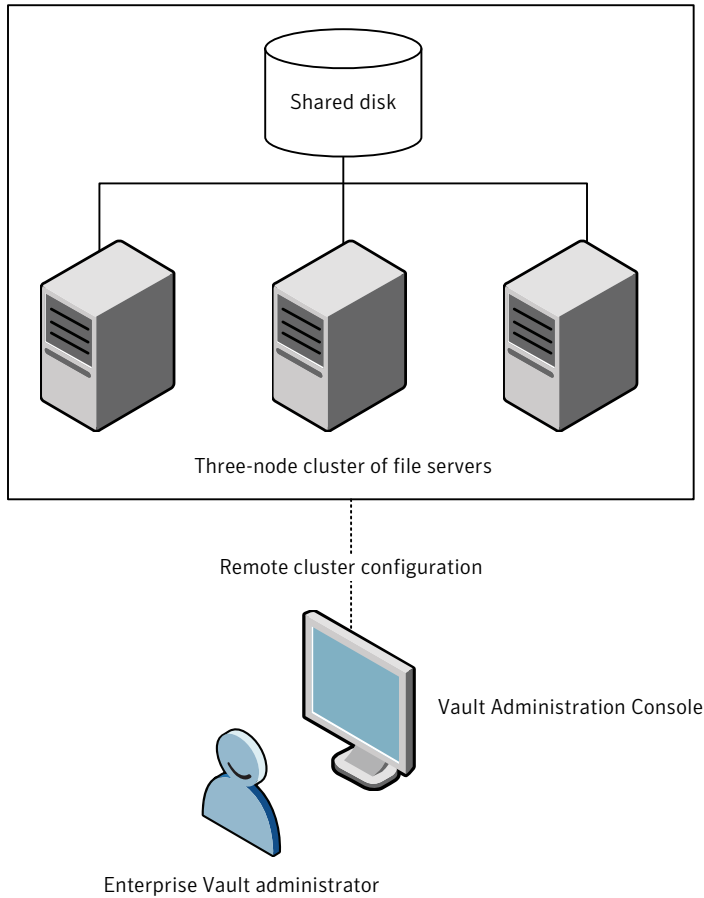
Item	Properties
File System Archiving Task  (under Enterprise Vault Servers\<server>\Tasks)	Processes target volumes and folders. The task properties define the following: <ul style="list-style-type: none"><li>■ Whether to run in report mode or normal mode.</li><li>■ Schedule settings, including the option for Run Now.</li><li>■ Settings to control generation of normal and pruning reports.</li><li>■ Synchronization schedule.</li><li>■ Pruning options and schedule.</li></ul>

## File System Archiving in a clustered environment

If your Windows file servers are grouped in a cluster, you can make the FSA services that run on them highly available. You must add an FSA resource to the cluster resource group or service group, and configure the FSA resource for high availability. The FSA resource monitors the state of the FSA services on the online node. If a problem occurs with the FSA services on the online node, then the cluster resource group or service group that contains the FSA resource fails over to the next available node.

Figure 6-1 shows an environment in which three file servers are clustered together.

**Figure 6-1** Example FSA cluster configuration



Note that you can make the FSA Agent services highly available only when there is a shared disk resource.

The FSA clustering feature works with the following cluster software:

- Windows Server Failover Clustering (formerly known as *Microsoft Cluster Server*, or *MSCS*)
- Veritas Cluster Server (VCS)

Refer to the Enterprise Vault *Compatibility Charts* for details of the supported versions of this software, and the supported versions of Windows. The *Compatibility Charts* document is available on the Symantec Enterprise Support site at this address:



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

The following cluster types are supported:

- Active/passive cluster. To support high availability, the shared cluster resources are made available on one node of the cluster at a time. If a failure on the active cluster node occurs, the shared resources fail over to the passive node and users may continue to connect to the cluster without interruption.
- Active/active cluster. To support load balancing and high availability, the cluster resources are split among two or more nodes. Each node in the cluster is the preferred owner of different resources. In the event of a failure of either cluster node, the shared resources on that node fail over to the remaining cluster nodes.

Enterprise Vault supports multiple nodes in any combination of active/passive and active/active. We have validated configurations with up to four nodes.

For guidelines on how to make the FSA Agent services highly available in a clustered environment, see the *Setting up File System Archiving* manual.

## The process of File System Archiving

Once you have configured File System Archiving, Enterprise Vault archives files according to the schedule for each task. Enterprise Vault selects files that meet the criteria you have defined in the archiving rules.

For example, the rules cover the following:

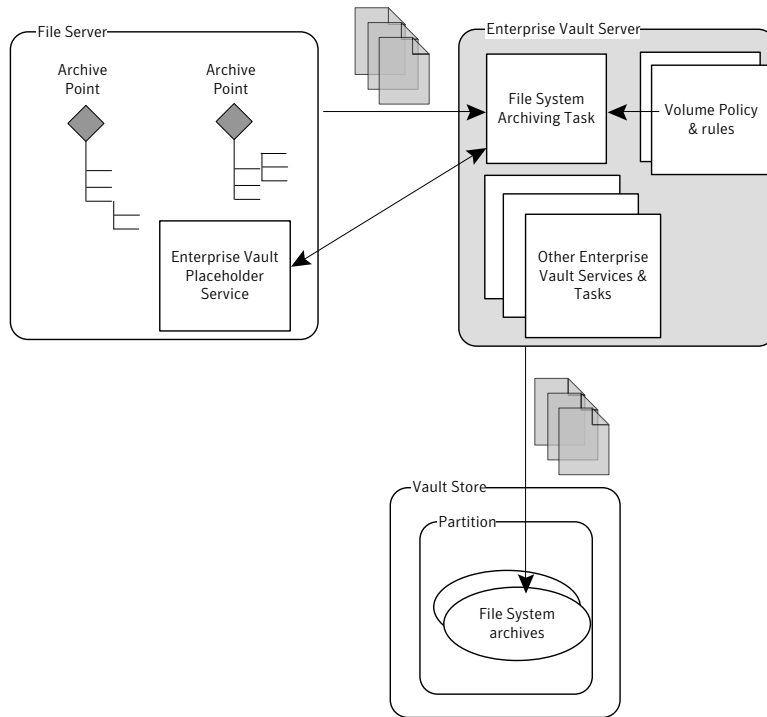
- File type
- File size
- Last access time or modification time
- Creation time
- File attributes

Enterprise Vault automatically creates an archive for each Archive Point and then selects and stores files according to the rules. The files are then replaced with shortcuts, or deleted, according to the policy setting.

Depending on the safety copy settings in the vault store properties, the original files may remain in place until the vault store has been backed up and then be replaced with shortcuts.

[Figure 6-2](#) shows the Enterprise Vault components involved when archiving files from a file server.

**Figure 6-2** File System Archiving process example



In this example, placeholder shortcuts are being used on an NTFS file system, so the Placeholder Service (part of the FSA Agent) is installed on the file server. Two Archive Points have been created on the file server to mark the top of the folder structures to be archived. Two archives will be created, one for each Archive Point.

On the Enterprise Vault server, a volume policy defines what files are to be archived. The File System Archiving Task runs under the control of the Task Controller Service according to the task schedule.

When a file is archived, the Enterprise Vault Storage Service converts the file to HTML, if possible, and stores the file in the archive. Using the HTML, the Indexing Service indexes the details and content of the file, so that users can later search for the file.

If many of items are being archived at once, you can speed up the archiving process by disabling indexing. Items can be indexed later, when the Enterprise Vault storage service computer is quiet, by rebuilding the archive indexes.

## How File System Archiving handles older versions of archived files

File System Archiving version pruning enables you to control the number of versions of files that are stored in Enterprise Vault archives.

When an archived file is recalled and modified, Enterprise Vault will archive the new version. This means that there are now two versions of the file in the archive. Each time a file is recalled and modified, subsequent archiving means that another version of the file is stored in the archive.

Pruning is the process of deleting the earlier versions of archived files. It is configured in the property settings for the File System Archiving task.

## How File System Archiving synchronizes permissions

Enterprise Vault automatically synchronizes archive permissions with folder permissions. When Enterprise Vault archives files, the version stored in the archive is given the same permissions as the folder that contained the original file.

This means the following:

- If there is a file with permissions that are different from those of the containing folder, the archived version has the folder permissions. A shortcut has the same permissions as the file.
- Someone who has access to the original folder can find and access the archived version of the file, even if the file permissions denied access. Such a person cannot use a shortcut to access the file, however.

Synchronization can be configured on the Synchronization tab in the properties of the File System Archiving task. Synchronization runs a maximum of twice each day and always runs until completion.

## File System Archiving reports

File System Archiving can create the following types of report:

- |                  |   |
|------------------|---|
| Archiving report | This report is generated for each normal mode archiving run. The report shows details of what was archived. You can use the following settings to control the level of detail in the report: <ul style="list-style-type: none"><li>■ Brief. Generate summary reports.</li><li>■ Full. Generate detailed reports that list each file that was matched by a rule.</li></ul> |
|------------------|---|

- Pruning report      This report is generated by each pruning run. You can use the following settings to control the level of detail in the report:
- Brief. Generate summary reports that show the number of items deleted from each archive.
  - Medium. Generate reports that list each deleted item.
  - Full. Generate reports that list all items, with a status for each, such as "Deleted" or "NeverExpires".

You can configure the reports on the Reports tab in the properties of the File System Archiving task.

If you have installed the Enterprise Vault component, you can configure the FSA Reporting feature to provide detailed reports on the status of your file servers..

See [“FSA Reporting”](#) on page 106.

## How to restore files with File System Archiving

Users can restore files in the following ways:

- Clicking a placeholder shortcut recalls the file from the archive.

---

**Note:** If pass-through recall is in effect, Enterprise Vault recalls the file to the file server only if the calling application requires a writeable version.

See [“Pass-through recall for placeholder shortcuts with File System Archiving”](#) on page 102.

---

A file that is recalled to the file server replaces the placeholder shortcut.

- If the recalled file remains unmodified, then Enterprise Vault converts the file back to a placeholder on the next archiving service run. The only exception is if the archiving policy's shortcut creation rules are based on the last access time. In that case, Enterprise Vault reverts the file only when the shortcut creation rules are met.
- If the recalled file becomes modified, then Enterprise Vault converts the file back to a placeholder according to the archiving policy's shortcut creation rules.
- Clicking an internet shortcut gives the user the option of opening or saving the file. Both of these options involve recalling the file from the archive.
- Using Archive Explorer, the user can select files and then use the right-click Copy to File System or Move to File System menu option. Copy places a copy

of the archived file in the selected location. Move places a copy of the archived file in the selected location and deletes the file from the archive.

---

**Note:** If you attempt to recall a file that is larger than 4 GB from an internet shortcut using Internet Explorer 7.0, the file is inaccessible. Enterprise Vault displays a message stating that files larger than 4 GB cannot be opened. This restriction is due to a limitation in Microsoft Internet Explorer. Note that placeholder shortcuts are not affected.

To work around this restriction you can restore the file by using the **Copy to File System** or **Move to File System** menu option in Archive Explorer.

---

## About FSAUtility

FSAUtility is a command-line utility with which you can do the following:

- Recreate archive points on the original path.
- Recreate the placeholders for archived files in their original location.
- Move placeholders from one location to another location and move the archived files to the corresponding destination archive, which is represented by the archive point on the path.
- Migrate placeholders from a source path to a destination path without any movement of the archived data.
- Delete orphaned placeholders for which no corresponding item exists in the archive.
- Restore all archived files, or archived files of the specified file types, to their original location or a new location.
- Recall the archived files that correspond to placeholders that are present in a folder.

The utility works with archive points and placeholders on Windows file servers, NetApp filers, and EMC Celerra/VNX devices.

For details of the utility, see the *Utilities* guide.

## How to back up and scan shortcut files with File System Archiving

Enterprise Vault placeholder shortcuts appear to the operating system as markers for offline files. Some backup and antivirus programs can be configured to ignore offline files, but others cannot.

Note the following:

- If you can configure your antivirus or backup program to ignore offline files, do so before running the application on disks with Enterprise Vault placeholder shortcuts.
- If you cannot configure your antivirus or backup program to ignore offline files, every placeholder that it checks will result in an offline file being recalled. In this case, you can use the Enterprise Vault backup mode program and settings to place the file server into backup mode before a scan or backup is run.

The Enterprise Vault backup mode program and settings enable you to specify the following:

- Programs that are prohibited from recalling archived items. This is most likely to be useful if you use an antivirus or backup program that does not honor the file system offline attribute.
- Specific user groups that backup mode is to be used for. When you restrict backup mode in this way, people who are not in those groups can still recall files as normal.

## Pass-through recall for placeholder shortcuts with File System Archiving

For Windows and NetApp file servers you can configure Enterprise Vault to perform pass-through recall for placeholder shortcuts. Enterprise Vault then passes the data directly through to the calling application on receipt of a read request for a placeholder. Enterprise Vault recalls the file to the file server, subject to permissions, only if the calling application makes a write request: for example if the application requires a writeable file, or if the user attempts to save changes to a file.

---

**Note:** Some applications such as Excel always recall to disk even when pass-through recall is enabled.

---

---

**Note:** For EMC Celerra/VNX file servers, Enterprise Vault supports the Celerra/VNX pass-through facility.

---

Pass-through recall can be useful in the following circumstances:

- With placeholders on read-only file systems, such as snapshots. A normal placeholder recall to a read-only file system fails because Enterprise Vault cannot write the recalled file to the file system.
- With Windows file servers where there is limited space on the file server, or when users have strict quotas for space usage. Recalled files normally occupy space on the target file system, and therefore count towards a user's space quota.

---

**Note:** For NetApp file servers the pass-through recall feature works only with read-only file systems. Pass-through recall is ignored for read-write file systems.

---

For Windows file servers you can enable or disable pass-through recall for each file server volume.

Pass-through recall uses a disk cache to reduce recall times for large files. For Windows file servers the disk cache is located on the file server. For NetApp file servers, the disk cache is located on the Enterprise Vault server.

Note the following:

- NetApp file servers must be running Data ONTAP 7.3 or later for pass-through recall.
- There is a setting "Delete archived file when placeholder is deleted" on the Shortcuts tab of volume policy properties and folder policy properties. That setting is ignored on Windows file server volumes if pass-through recall is enabled on the volume.

## File Blocking with File System Archiving

File Blocking monitors disk space in real time, according to the requirements that you define in a volume policy. File Blocking rules enable you to block files as follows:

- By file type. Inappropriate file types are blocked immediately.
- By scanning file content. This enables you to trap files that have been renamed to disguise their file types.
- Additionally, it is possible to scan the contents of compressed files, such as ZIP files.

---

**Note:** Files stored within .RAR and .CAB files cannot be blocked or quarantined. However, you can create rules to block .RAR and .CAB files.

---

You can also control monitoring as follows:

- The volume policy enables you to specify folders that must not be monitored and folders that must be monitored.
- You can edit the properties of a file server to define a list of users whose files are never blocked.
- You can enable, for each file server, a quarantine location for blocked files. Files that are blocked as a result of content-scanning are moved automatically to the quarantine location. Files that are blocked because of their file type are never moved to quarantine. Optionally, you can define a central quarantine location that is used by all file servers.

Within a policy you can have many different rules. Each rule enables you to configure notifications that are sent when that rule is broken.

The following notification types are available:

- Messenger Service messages (NET SEND)
- Event log entries
- Email
- SNMP traps

## File Blocking configuration with File System Archiving

File Blocking is carried out by the Enterprise Vault File Blocking service, which is a component of the FSA Agent.

File Blocking is available for the following:

- Windows computers. File Blocking is carried out by a File Blocking service that is installed on the Windows computer.

---

**Note:** File Blocking is 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>.

---

- NetApp filers with ONTAP 7.2 or later. File Blocking is carried out by a File Blocking service that is installed on a Windows file server. When you configure File Blocking for a NetApp filer you must select a target Windows file server



to perform the File Blocking. It is possible for a Windows file server to run File Blocking for more than one NetApp filer, but for best performance you are recommended to use a different Windows file server for each NetApp filer.

---

**Note:** A computer that runs a Server Core installation of Windows cannot run the File Blocking service for a NetApp filer.

---

You specify File Blocking rules within a volume policy and then apply that policy to disk volumes. You can have many rules within a single policy.

For example, you could configure rules to do the following:

- Allow graphics files to be created but for a warning message to be sent to the user and the event to be logged.
- Block video files and move them to quarantine.

You configure File Blocking at the volume level by applying a volume policy in which you have defined File Blocking rules. The rules control the file types that are allowed on the volume, which folders to monitor, and the actions to take when a policy violation occurs.

It is possible for the volumes also to be processed by a File System Archiving task, but there is no requirement to do this.

## Retention Folders and File System Archiving

The Retention Folder feature enables you to create a single folder or a hierarchy of folders automatically on file servers, to be managed by Enterprise Vault and archived according to assigned policies. The folder hierarchy can be added to a specified target folder or to its subfolders. For example, you could create a hierarchy of retention folders in every user's home folder. Items placed in the retention folders are archived by Enterprise Vault according to the particular policy assigned to each folder. You define the archives to use for the retention folders by specifying where archive points are to be created. If a user deletes any folders in the retention folder hierarchy, Enterprise Vault recreates the folders during the next run of the FSA archiving task in normal mode.

You configure retention folders using the Administration Console. The required steps are as follows:

- Create a suitable folder policy to use as the default folder policy for the retention folders.
- Create a Retention Folder policy, to define the hierarchy of folders to be created on the FSA target, and the folder policy to use on each folder

- Add the FSA target on which you want the retention folders created, assign the Retention Folder policy, and specify where archive points are to be created. You can specify that the retention folder hierarchy is added to the root of the FSA target, or to each subfolder.

The folders are created on the file server on the next normal mode archiving run. To test the effect of an assigned retention folder policy you can perform an archiving run in report mode. You can also assign policies to folders using a command line interface.

## FSA Reporting

FSA Reporting provides summary reports on the active data on your file servers, and on the data that has been archived from them. FSA Reporting's reports include data on a wide range of items including the following:

- The number of archived files for each file server, and the space used and saved as a result of archiving. You can also view the 10 largest files in a volume.
- Active and archived space usage by different file groups, per server and per archive point.
- Numbers of unaccessed or duplicated files, and the space they are occupying.
- Used and free space on the drives of each file server.

Many of the reports can provide either an overall view for all file servers with FSA Reporting configured, or a detailed view for a named file server.

In order to access FSA Reporting's reports, the Enterprise Vault Reporting component must be installed and configured on a machine with the required prerequisites, including Microsoft SQL Server Reporting Services. You use the SQL Server Reporting Services Report Manager Web application to view the reports.

You must also configure FSA Reporting for each file server target for which you want to obtain reports. The Administration Console provides wizards to help you do the following:

- The first time that you configure a file server target for FSA Reporting, a wizard helps you to set up an FSA Reporting database to hold the FSA Reporting scan data.

When you configure another file server target for FSA Reporting, you can assign the file server to an existing FSA Reporting database, or create another database. Multiple FSA Reporting databases can provide scalability if you obtain FSA Reporting data for many file servers.

- For a Windows file server, install the FSA Agent on the file server if the agent is not already present
- For a non-Windows file server, select another server to act as the FSA Reporting proxy server. The FSA Reporting proxy server gathers the FSA Reporting data for one or more non-Windows file servers.

Any of the following can act as an FSA Reporting proxy server, subject to some additional prerequisites:

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

For more information, see the *Reporting* guide.

---

**Note:** FSA Reporting is not supported on computers that run a Server Core installation of Windows. A computer that runs a Server Core installation of Windows cannot act as a proxy server for FSA Reporting.

---



# Archiving Microsoft SharePoint™ servers

This chapter includes the following topics:

- [About archiving Microsoft SharePoint servers](#)
- [How to configure SharePoint archiving](#)

## About archiving Microsoft SharePoint servers

You can use Enterprise Vault to archive documents from servers running any of the following:

- Microsoft SharePoint™ Foundation 2010
- Microsoft Windows SharePoint™ Services 3.0 (WSS 3.0)
- Microsoft SharePoint™ 2010
- Microsoft Office SharePoint™ Server 2007 (MOSS 2007)

At scheduled times, Enterprise Vault automatically copies content from the SharePoint server and stores them in Enterprise Vault SharePoint archives. Archived documents can be left on the SharePoint server or deleted, as required, and shortcuts to archived documents can be created on the SharePoint Server.

If versioning is enabled for a document library, you can configure the number of versions of a document that are to be left on the SharePoint server after archiving. An Enterprise Vault version history link enables users to view archived versions of a document from the SharePoint version history page.

An Archive Search web part and an Archive Explorer web part can be added to SharePoint site pages to enable users to search the SharePoint archives. Documents

can be viewed and saved. Users can also access SharePoint archives using Archive Explorer in a standalone browser.

The benefits of archiving SharePoint Servers can be summarized as follows:

- Control of SharePoint storage growth by moving older content to online archives. Archiving is automatic and policy driven.
- Enable the use of cost effective storage for long term retention of older information. Archives are storage independent, enabling the use of cost effective storage solutions such as disk, optical, tape, SAN, NAS, SSP.
- Retain the intellectual property represented by SharePoint stored content.
- Archive information to meet legal retention requirements.
- Central information retention for distributed departmental systems.
- Ease system consolidation.

SharePoint holds the newest, changing information, while Enterprise Vault provides managed, long term, high volume, online storage of older information.

SharePoint archiving requires a separate Enterprise Vault SharePoint license.

## How to configure SharePoint archiving

To enable SharePoint archiving, the Enterprise Vault Microsoft SharePoint component needs to be installed and configured on the SharePoint server computer. SharePoint must be installed and configured on the target server to be archived before Enterprise Vault components are installed. The Enterprise Vault Admin Service is installed automatically with the Enterprise Vault Microsoft SharePoint component.

Before configuring the Enterprise Vault Server for archiving, the SharePoint site collections for archiving must exist on the SharePoint server. In Enterprise Vault Administration Console, you can then create objects for SharePoint archiving tasks, Policies and Targets.

### SharePoint archiving tasks

The SharePoint task is the process that archives the SharePoint site collections. Task properties include the archiving schedule, the account the process is to use and the archiving reports to generate.

A single task can support several SharePoint targets, which may be Web applications or site collections. Alternatively, you can create multiple SharePoint tasks and assign targets to each task, as required. The SharePoint task runs under the control of the Task Controller Service.

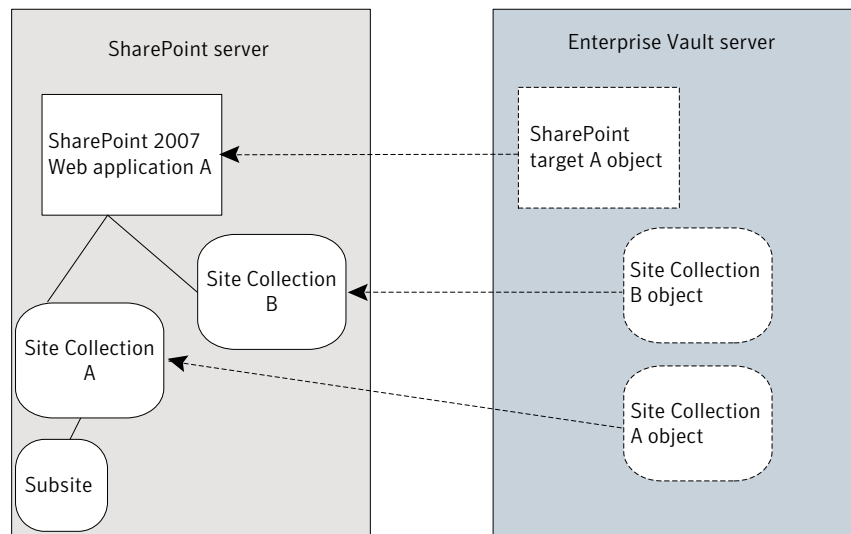
To archive regularly all the target sites associated with a task, you can use an Enterprise Vault site schedule or you can set a separate schedule for the SharePoint task. Alternatively, an immediate archive run can be started for all sites serviced by an archiving task, or for a particular site collection.

## SharePoint archiving targets

The SharePoint Servers and site collections to be archived by the archiving tasks are defined using Targets in the Administration Console. These reflect the SharePoint structure: site collection targets point to the top-level sites on the SharePoint server, and site targets point to subsites.

Before you can configure the archiving targets in Enterprise Vault, the site collections must exist in SharePoint and the Enterprise Vault components must have been installed and configured on the SharePoint server

**Figure 7-1** SharePoint archiving targets



When you add a SharePoint target URL, you can auto-enable site collection archiving and assign default values for the archiving task, vault store, policy and Retention Category to be used. Subsites will be archived automatically using the default settings for the target URL. If new subsites are created, these will be automatically included in the archiving. Content archived from a site collection are stored in the same archive.

If automatic site collection archiving is not enabled, or you want to override the default settings for a site collection, you can create site collection targets and

subsite targets manually under the target URL. For example, you may want to use a different archiving policy for a particular site collection.

For a site collection, you can limit the scope of archiving to the top level web site only, the subsites only, or both.

When the archiving task runs, a SharePoint archive is created automatically for each SharePoint site collection. In the Administration Console tree, you can see the archives under **Archives > SharePoint**. Content in the top level site and all subsites of that site collection are stored in the same archive.

Figure 7-1 illustrates the relationship between a SharePoint 3.0 Web application and site collections on the SharePoint server (on the left) and associated target objects in the Enterprise Vault Administration Console (on the right).

## SharePoint archiving reports

Reports can be generated for each run of the archiving task. You can select the amount of detail you want included in reports and the number of reports for a task that you want kept in the `Reports` folder (for example `C:\Program Files (x86)\Enterprise Vault\Reports`).

## SharePoint archiving policies

A policy defines which documents are to be archived and how they are to be archived.

In a SharePoint policy you can configure the following archiving actions:

- Leave the document in SharePoint. This means that the document will not be deleted from SharePoint once it is archived; users will be able to access all versions of the document both on the server and in the archive.
- Delete document from SharePoint once archived, and leave a shortcut to the archived document.
- Delete document from SharePoint once archived, without leaving a shortcut. This means that an archived document is deleted from SharePoint and is only available in the archive.
- Prune to a specified number of versions of the document. If versioning is enabled for the document library, you can set the number of versions of an archived document that you want left in SharePoint after archiving. Earlier versions will be available in the archive only.
- You can specify how to archive items with unique permissions and whether to archive drafts of items.



- You create rules to select the documents that you want to archive with the policy.

You can make Enterprise Vault delete shortcuts automatically, according to the age of the shortcuts. For example, you can choose to delete those shortcuts that are more than one year old.

## How to access archived SharePoint documents

By installing the optional Archive Search web part on the SharePoint Server, and adding the Archive Search web part (and optionally the Archive Explorer web part) to site pages, you can enable SharePoint users to search for documents stored in the Enterprise Vault SharePoint archive. The search is very similar to the SharePoint Portal Server search.

In Archive Explorer the archives are displayed in a tree structure with subsites and document libraries displayed as child objects of the site collection archive.

Using either Archive Search or Archive Explorer, documents can be viewed, saved, restored to the SharePoint Server and, if allowed, deleted.

When users view the version history of a document, the versions of the document on SharePoint are displayed on the versions history page. After the archiving task has run for the first time, a new link is displayed under the SharePoint versions that gives users access to archived versions of the document.

## About Enterprise Vault shortcuts in SharePoint

Shortcuts behave exactly like SharePoint documents. They use the same icons as the corresponding archived documents. Shortcuts are not created for social content.



# Domino mailbox archiving

This chapter includes the following topics:

- [About Domino mailbox archiving and Enterprise Vault](#)
- [Domino provisioning groups](#)
- [Domino mailbox archiving tasks](#)
- [Domino mailbox archiving policies](#)
- [Domino mailbox archiving retention folders](#)
- [Domino mailbox archiving desktop policies](#)

## About Domino mailbox archiving and Enterprise Vault

In the context of Enterprise Vault, the term "Domino mailbox archiving" refers to archiving items from user mail files on Domino mail servers.

Domino mail files hold many types of information, for example, messages, documents, spreadsheets, and graphics. You can specify the default types of items that Enterprise Vault archives (according to the Domino forms they use) in the properties of the Directory (Domino Forms tab). The list can be tailored in individual Domino Mailbox Policies.

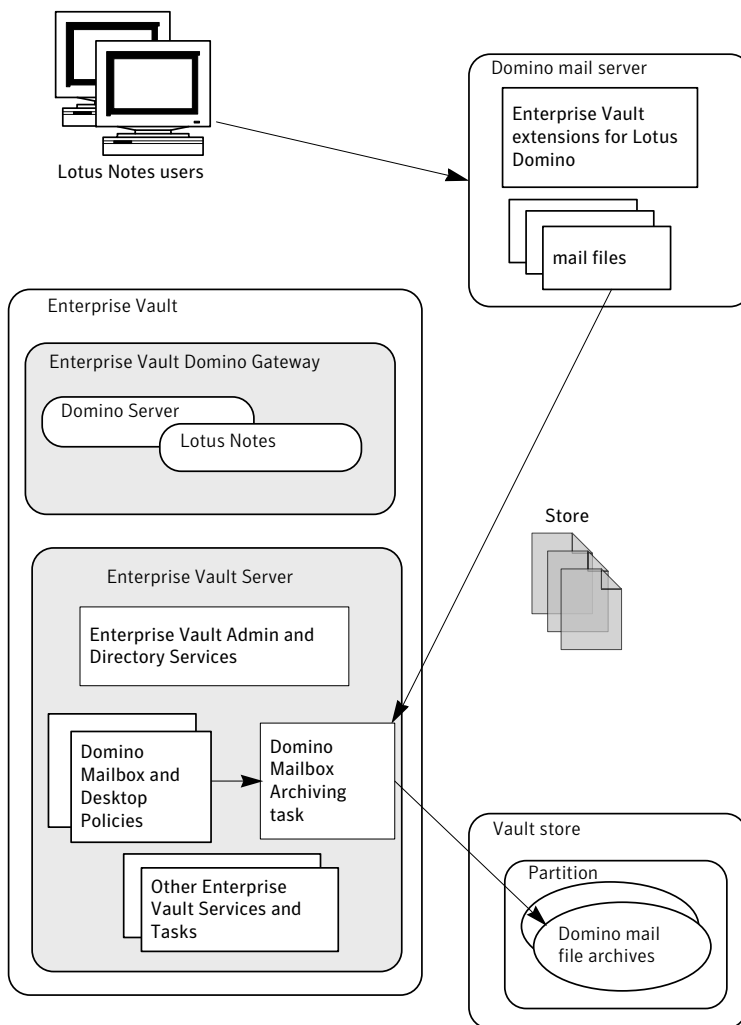
Domino mailbox archiving does not automatically archive content held in NSF files stored on users' computers. However, you can use NSF migrator to archive the content from NSF files.

See "[How to archive NSF file contents](#)" on page 63.

Enterprise Vault for Domino mailbox archiving comprises an Enterprise Vault Domino Gateway and an Enterprise Vault server. These can be on the same computer, but typically will be on separate computers to support larger Domino environments.

Figure 8-1 provides an overview of Domino mailbox archiving.

**Figure 8-1** Overview of Domino mailbox archiving



Domino mailbox archiving requires at least one Enterprise Vault Domino Gateway for each Domino domain. This is a computer with Domino Server, Lotus Notes and Enterprise Vault installed. If this is on a separate computer from the Enterprise Vault server, then only Enterprise Vault Admin Service and Directory Service are required. The Domino Server installed on the Enterprise Vault Domino Gateway computer is used by Enterprise Vault to access the Domino Directory and target Domino mail servers.

Enterprise Vault servers that are archiving Domino mail servers must have Lotus Notes installed.

On the Enterprise Vault server, using the Administration Console, you create a Domino Mailbox Archiving task to archive items from user mail files. You define as archiving targets the target Domino mail servers and user mail files that the task is to archive. Enterprise Vault automatically creates an archive for each user mail file to be archived.

Enterprise Vault can archive from mail-in databases. This feature enables you to archive mail items that several users share. Vault Cache is not available for the mail that is archived from mail-in databases.

Domino mailbox policies define how mail files are to be archived. Domino desktop policies define the features available in the Lotus Notes client, and control how the client functions.

If required, there can be several Enterprise Vault servers to one Enterprise Vault Domino Gateway. Each Enterprise Vault server can have a maximum of one Domino Mailbox Archiving task that archives to a local vault store.

If you use secondary Domino servers to keep replicas of users' mail files, it is possible to archive from those secondary servers instead of from the mail servers. When there are many mail servers and only a few secondary servers this approach can simplify the configuration.

## Domino provisioning groups

You use provisioning groups to group the user mail files that are to be archived using a particular mailbox policy and desktop policy. You then run the Domino Provisioning task to apply the settings in the provisioning group.

You can select any of the following target types to associate with a provisioning group:

- Directory Group
- Mailbox (mail file)
- Mail-in database

- Organizational Unit
- Corporate Hierarchy

A mail file must be part of a provisioning group before it can be enabled for archiving.

If a mail file appears in more than one provisioning group, it belongs to the first provisioning group in which it appears. You can change the order of provisioning groups by editing the properties of the "Provisioning Groups" container (under Targets > Domino > *domain*) in the Administration Console.

In the properties of a provisioning group you can choose to enable mail files for archiving and you can specify the indexing level to use when archiving. It is possible to override the indexing level for an individual archive by editing its properties.

## Domino mailbox archiving tasks

In the Administration Console, on the required Enterprise Vault server under Enterprise Vault Servers, you create a Domino Mailbox Archiving task. This Domino Mailbox Archiving task can process mail files on more than one Domino Server and more than one Domino domain.

If necessary, it is possible for multiple Enterprise Vault servers to process the same Domino server by provisioning different groups of users and archiving each group to a different vault store.

These tasks are controlled by the Task Controller Service.

The Domino Mailbox Archiving task is responsible for the following:

- Accessing each mail file and archiving items according to the policy set for the mail file. The task works in cooperation with the Indexing Service, which converts and indexes the items that are being archived.

To obtain an estimate of the number of items that will be archived, without actually archiving anything, you can run the task in Report Mode.

By default, Domino Mailbox Archiving tasks run automatically according to the schedule defined for the Enterprise Vault site. You can override this schedule for individual tasks.

Each mail file is processed by the Domino Mailbox Archiving task that runs on the same Enterprise Vault server as the Storage Service that hosts the associated vault store; in other words, the archive is created locally to the archiving task that processes the Domino mail file.

By default, the vault store that is used is the one defined in the Domino server properties, but you can override this setting as required by editing the properties of individual provisioning groups.

## Domino mailbox archiving policies

A Domino mailbox policy supplies information for the archiving task to use when processing the target mail files, including the following:

- The archiving strategy. This can be any of the following:
  - All items over a certain age are archived.
  - Archiving actions, such as deleting the original item or creating shortcuts after archiving an item.
  - Whether shortcuts to archived items are created and what the shortcuts contain.
- Which items to archive according to the Domino form types that they use.
- Whether to archive unread items.

The mailbox policy also defines whether Enterprise Vault deletes old shortcuts. You can configure the behavior as follows:

- Deletion based on shortcut age.
- Deletion of orphaned shortcuts. These are those shortcuts that no longer have corresponding archived items. Typically the archived items have been deleted by users or storage expiry.
- Deletion of shortcuts when the retention period has elapsed. The corresponding archived items may be removed by storage expiry. You can delete the shortcuts without deleting the archived items.

You create Domino mailbox archiving policies in the Enterprise Vault Administration Console under Policies > Domino > Mailbox.

## Domino mailbox archiving retention folders

The Retention Folder feature enables you to create a single folder or a hierarchy of folders automatically in users' mail files. Enterprise Vault archives these folders according to policies that you assign. If a user deletes any folders in the retention folder hierarchy, Enterprise Vault automatically recreates them.

You specify the retention folders and their retention categories in retention plans. You can create as many retention plans as you require.

You use Enterprise Vault provisioning groups to apply retention plans to mail files. Thus, different users can have different retention folders with the appropriate retention categories. You can also define a default retention plan that Enterprise Vault applies to all users for whom a specific plan is not defined.

If a user moves a retention folder, the folder does not retain the retention plan settings. Items that are archived in the future will be archived according to the policy that applies to the folder in its new location. Items that have already been archived from the folder are unaffected and retain the original retention category.

If a user creates a subfolder beneath a retention folder, that subfolder inherits the retention folder settings. For example, if you create a 'Projects' folder users could then create a subfolder for each project. The subfolders would automatically use the retention folder settings from the parent 'Projects' folder.

You create an XML file in which you define the retention plans. You then use the `EVDominoRetentionPlans.exe` command line tool to upload the XML file to Enterprise Vault.

See the section 'Domino Retention Plan Tool' in the *Utilities* manual for details of how to create Domino retention plans.

## Domino mailbox archiving desktop policies

A Domino desktop policy defines the end user's experience when using the Enterprise Vault Lotus Notes client. Its settings determine the Enterprise Vault features and functionality that the client provides.

The desktop policy settings include following options:

- Show or hide Enterprise Vault menu options, such as Search, Store, Restore, and Delete.
- Control the availability of Vault Cache and its maximum size.
- Control advanced settings for Vault Cache.

You create Domino desktop policies in the Enterprise Vault Administration Console under Policies > Domino > Desktop. When you create a provisioning group you assign a desktop policy to it. You can create multiple desktop policies if you want different provisioning groups to use different policy settings.



# Domino Journal archiving

This chapter includes the following topics:

- [About Domino Journal archiving](#)
- [Domino Journal archiving policies](#)
- [Domino journal archiving database considerations](#)
- [How to set up Domino Journal Archiving](#)
- [Support for clustered Domino Journal databases](#)

## About Domino Journal archiving

This section describes how Enterprise Vault archives the contents of Domino Journal databases.

You can set up Domino so that a copy of every message sent or received is saved in a Journal database. This is particularly useful if you want to implement a company email monitoring policy and vital if there is a possibility that you may have to produce email as legal evidence at some later date.

You can set up Enterprise Vault to archive all items from Domino Journal databases.

## Domino Journal archiving policies

In Enterprise Vault Administration Console you create archiving policies under Policies > Domino Journaling.

A Domino Journaling Policy supplies information for the archiving task to use when processing databases in the target location; currently the only option is whether or not to expand distribution lists when archiving.

## Domino journal archiving database considerations

Enterprise Vault archives from all databases in a specified folder in the server's data directory.

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 Journal 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** – Domino automatically places the old database in the server's data folder. In order to ensure that all items are archived from the old database, and to remove items when the archive has been backed up, you must move the old databases back to the Journal database folder.
- **None** – This method has the side-effect that the database will keep growing and will require manual maintenance.

You must configure your Domino Journal database appropriately so that it can be archived by Enterprise Vault.

## How to set up Domino Journal Archiving

To configure Domino Journal Archiving, you need to set up the following in the Enterprise Vault Administration Console:

- A Domino Journal archive for each Domino Journal database location that Enterprise Vault will archive.
- A Domino Journaling task to perform the archiving. If required, multiple Domino Journaling tasks can be created on one computer. Domino Journaling tasks run under the control of the Task Controller Service.
- A Domino Journaling Policy. You assign this to the target location and it enables you to tailor how the Domino Journaling task archives items from the database. For example, you may want to stop the Domino Journaling task from expanding distribution lists.

- The target location to archive. In order to do this you must add the Domino domain and server and then the location of the Domino Journal database. You configure these in the Targets > Domino section of the Administration Console.

Depending on the Enterprise Vault configuration, items in Journal databases are deleted either at the time they are archived or after the vault store is backed up.

Users with access permissions to a journal archive can search for messages within the archive. Because journaled items may be confidential, it is important to give such access to a few trusted users only.

## Support for 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.



# SMTP Archiving

This chapter includes the following topics:

- [Overview of SMTP Archiving](#)
- [Setting up SMTP Archiving](#)

## Overview of SMTP Archiving

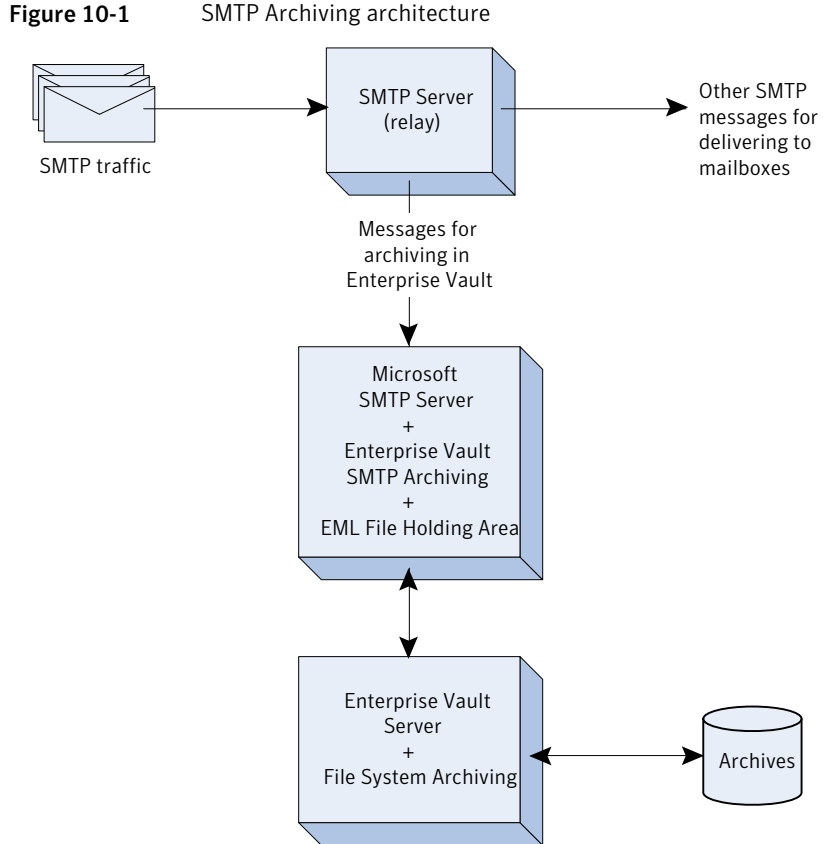
The SMTP Archiving feature allows third-party applications to enter data into an Enterprise Vault archive via SMTP messages. It enables Enterprise Vault to capture and archive these messages at the point of delivery to a Microsoft SMTP Server, and so operates independently of the messaging solution that you employ.

For example, you may have messaging or workflow applications in your organization that use SMTP to communicate with users or other applications. Increased compliance legislation may require you to archive such communication and make it available for auditing. Using SMTP Archiving, you can capture and store the messages centrally. Then you can search, view and, if necessary, restore the messages using Enterprise Vault Search or Archive Explorer clients.

You cannot use SMTP Archiving to archive MAPI messages.

## SMTP Archiving architecture

[Figure 10-1](#) shows how you can integrate SMTP Archiving into your messaging infrastructure.



Here, SMTP messages are sent to an SMTP server, which can be any third-party messaging server that supports SMTP. The server illustrated is performing a relay function and passing messages to other messaging servers, which deliver the messages to recipients.

Messages to specific domains are BCC'd to the Microsoft SMTP Server for archiving by Enterprise Vault. For example, you could configure an application to package data as SMTP messages and send all messages directly to the Microsoft SMTP Server for SMTP Archiving to process. You can configure SMTP Archiving to handle messages for multiple domains, if needed.

SMTP Archiving captures the messages from the Microsoft SMTP Server drop folder, processes them, and stores them in folders in a holding area according to the message recipient address and date. On the holding area, you create the root folder for each domain manually. SMTP Archiving then creates automatically the following sub-folder structure under each domain root folder:

<DomainRoot>\<MailboxName>\<Year>\<Month>\<Day>\<Hour>

A configuration file enables you to control SMTP Archiving. In this way you can specify information, such as the root folder to use for a specific domain, whether SMTP Archiving is to create Archive Points automatically, and the indexing level to apply to Archive Points.

You configure Enterprise Vault File System Archiving to retrieve the EML files from the holding area and store them in archives. The archives created depend on where the archive points are in the folder structure created in the holding area. You can configure SMTP Archiving to create archive points automatically, or you can create them manually. If they are created automatically, a separate archive is created for each mailbox.

Enterprise Vault recognizes the EML files as messages and indexes the appropriate data, such as sender, recipient, subject, date and time, and content. However, custom SMTP headers (X-headers) are not indexed (with the exception of x-KVS-MessageType, which is used by Compliance Accelerator to enable searches on Instant, Bloomberg and Exchange Server messages).

If required, users can quickly find and retrieve archived SMTP messages using Enterprise Vault Search or Archive Explorer, which they can run from a Web browser.

The Microsoft SMTP virtual server on the Enterprise Vault SMTP Archiving computer must not be configured as a relay.

All messages sent to SMTP Archiving are stored; it does not perform any filtering.

## Setting up SMTP Archiving

For detailed instructions on how to configure SMTP Archiving, see the *Setting up SMTP Archiving* guide.

### To set up SMTP Archiving

- 1 Install and configure the Microsoft SMTP Server.
- 2 Install Enterprise Vault SMTP Archiving components on the Microsoft SMTP Server computer.
- 3 On the Microsoft SMTP Server computer, create a suitable SMTP Archiving configuration file.
- 4 Create the holding area, including the required domain root folders. This is where SMTP Archiving puts the EML message files for File System Archiving to archive.

- 5 Run the SMTP Archiving configuration process to apply settings in the configuration file, and enable the SMTP Archiving feature.
- 6 On the Enterprise Vault server, configure File System Archiving to archive from the domain root folders.



## Enterprise Vault Accelerators

This chapter includes the following topics:

- [About the Enterprise Vault Accelerators](#)
- [Differences between the Enterprise Vault Accelerators](#)
- [About Compliance Accelerator](#)
- [About Discovery Accelerator](#)

### About the Enterprise Vault Accelerators

The Accelerator products are specialized add-on applications to Enterprise Vault.

Compliance Accelerator enables sampling and monitoring of an organization's electronic messages. Features include monitored employee management, message sampling and item reviewing and exporting.

Discovery Accelerator is designed for data-mining activities, such as finding messages and documents to present as evidence in legal cases or that relate to an internal inquiry. Features include case management, advanced, multi-archive searching and item reviewing and publishing.

Both Compliance Accelerator and Discovery Accelerator require separate licenses.

Running the Compliance Accelerator and Discovery Accelerator server software concurrently on the same computer is not currently supported.

## Differences between the Enterprise Vault Accelerators

It is important to understand that Compliance Accelerator and Discovery Accelerator were created for different purposes.

Discovery Accelerator is an electronic discovery and review system that integrates with Enterprise Vault services and archives. Discovery Accelerator lets authorized users search for, retrieve and preserve, analyze, review, mark, and export or produce emails, documents, and other electronic items for lead counsel examination or court-ready production—rapidly and in a cost-effective manner.

Using attorneys and external counsel to review large numbers of items is costly. With Discovery Accelerator, you can create a hierarchy of reviewers for a discovery action or case, with different levels of reviewers able to assign certain review marks. In this way, paralegal staff and non-legal staff can perform an initial review of search and collection results and leave only the privileged, relevant, or questionable items for counsel. Optionally, you can then produce the relevant items with an appropriate "Bates" number or else simply export them from Discovery Accelerator in various native formats and load file formats.

Compliance Accelerator enables companies to implement an ongoing electronic message monitoring policy, in order to meet requirements set by the company or by an industry regulatory body, such as SEC. As a company would set up monitoring for departments, work in Compliance Accelerator is set up in terms of departments and monitored employees within the departments. Compliance Accelerator deals exclusively with email, instant messages, Bloomberg messages, and faxes; you cannot search for or view documents held in file system archives.

Compliance Accelerator samples messages as they are archived and adds the messages automatically to the review set for the department. Although reviewers have a similar role to Discovery Accelerator reviewers, the marking scheme in Compliance Accelerator is simpler.

Both Accelerator products have an automatic search facility. In Compliance, this can be used for ongoing monitoring of company mail for particular behavior, such as unacceptable language or sending confidential information outside the company.

## About Compliance Accelerator

The use of Compliance Accelerator does not in itself make an organization compliant with regulatory requirements, such as NASD 3010 and 3110; it provides a tool that enables a company to implement its compliance strategy.

A company's compliance strategy may typically require the following:

- A certain percentage of employees' electronic messages to be captured and checked by compliance officers on a regular basis. Electronic messages may

include email, instant messages, faxes and, particularly in the financial sector, Bloomberg messages. Depending on the compliance strategy, monitoring may be required of internal messages (messages sent between employees in certain departments), or external messages (messages sent between employees in certain departments and people outside the company).

- Regular searches to be run on electronic messages to capture any instances of unacceptable language or illegal business practice, such as insider dealing.
- Messages to be stored securely for several years and retrieved quickly at any time.
- Detailed audit information showing the review history of a message.

Enterprise Vault Exchange and Domino Journaling Tasks can be used to provide secure archiving of all company messages.

Compliance Accelerator then builds on Enterprise Vault to provide the following additional features to assist an organization in implementing their compliance strategy:

- A journaling filter that works with the Journaling Tasks to capture automatically a random sample of messages sent to the journal archive.
- A system for defining the employees that are to be monitored and grouping them in an organizational structure that reflects the departments within the company. The messages of certain employees (called "exception employees"), such as senior managers, can be kept separate and reviewed by specially assigned reviewers.
- A client application that enables compliance administrators to configure Compliance Accelerator to fit the requirements of the company's compliance strategy. For example, departments of employees can be managed, granular access permissions can be assigned to designated compliance officers and administrators, automatic searches of messages can be scheduled, and sets of words for searches can be added and managed.
- The client application also enables designated compliance officers or reviewers to read and mark the messages that are captured.
- History information about all employees monitored, messages captured and the review process applied to each message is kept securely in a SQL database.

## Compliance Accelerator components

[Table 11-1](#) describes the Compliance Accelerator components.

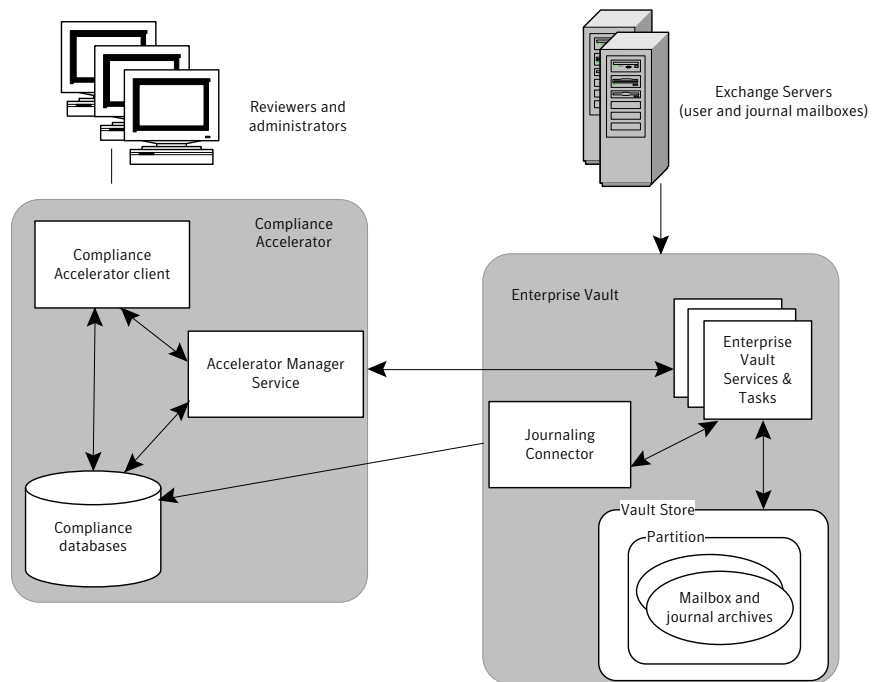
**Table 11-1** Compliance Accelerator components

Component	Notes
Compliance Accelerator client	The client is used by Compliance Accelerator administrators to set up and manage the system and by reviewers to access the items that they are to mark.
Accelerator Manager Web site	This Web site lets you set up and manage multiple Compliance Accelerator databases in which to store your data. For example, this facility lets you split your data by date range or organizational unit.
Enterprise Vault Accelerator Manager service	This service handles the requests from the Compliance Accelerator client and works with the Enterprise Vault components to access archives, perform searches, and so on.
Customer database	<p>The customer database is a SQL database in which Compliance Accelerator stores details of departments, user roles, search results, and more.</p> <p>You can set up multiple customer databases.</p>
Configuration database	The configuration database is a SQL database that specifies the location of the customer databases and stores details of the SQL Server, database files, and log files to use.
Support for Crystal Reports Web site (optional)	This Web site lets you view any legacy reports in Crystal Reports (. rpt) format that you created with Compliance Accelerator 2007 or earlier. In version 8.0 and later of Compliance Accelerator, the reporting facilities employ Microsoft SQL Server Reporting Services rather than Crystal Reports.
Journaling Connector (optional)	<p>The Journaling Connector collects a random sample of items that have been sent to the Enterprise Vault archive of a Microsoft Exchange or Lotus Domino journal mailbox. If you need to review a certain percentage of each employee's communications every day, the Journaling Connector is the best way to fulfil the requirement. At a set time, Compliance Accelerator adds the items during the previous 24 hours to the items to be reviewed for a department. You can specify the percentage of each employee's communications that you want to capture.</p> <p>Compliance Accelerator provides one Journaling Connector for Microsoft Exchange environments and another for Lotus Domino environments.</p>

Note that using the Journaling Connector to sample messages is different from searching messages for specific search criteria. The ability to run searches is provided in the Compliance Accelerator client application.

Figure 11-1 shows how Compliance Accelerator components work with Enterprise Vault to access archived data. In this diagram, data is archived from Exchange servers. Alternatively, data could be archived from Domino mail servers.

**Figure 11-1** How Compliance Accelerator works with Enterprise Vault



The Journaling Connector, which must be installed on the same computer as the Journaling Task, samples messages being archived from the journal mailbox and adds the sample automatically to the set of messages to review in the Compliance database.

The Accelerator Manager service finds out the location of archives and Enterprise Vault services and tasks from the Enterprise Vault Directory. It uses the Enterprise Vault Indexing service to run searches and the Enterprise Vault Storage service to view messages.

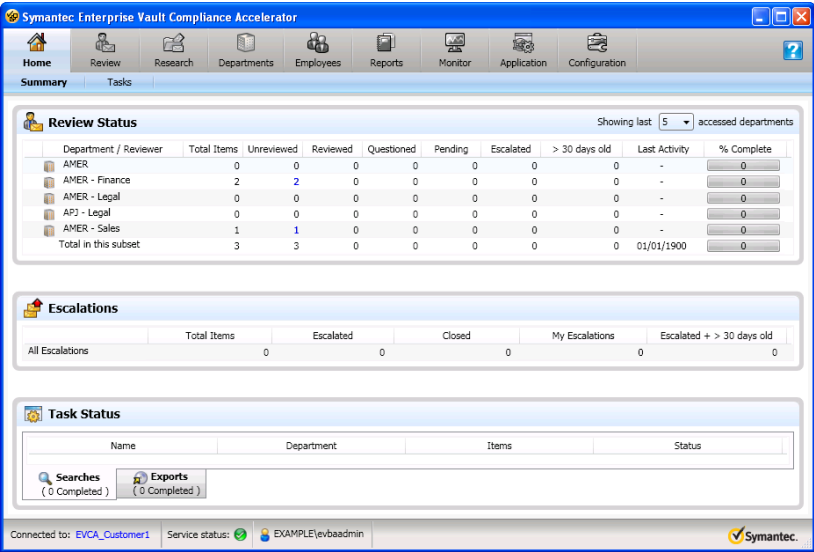
In small installations, the Compliance Accelerator components can all reside on the same computer as Enterprise Vault. In larger installations, a more distributed

setup is recommended, with Compliance Accelerator components on a separate computer from Enterprise Vault.

## The Compliance Accelerator client application

The client application provides administrators with application and department management facilities and reviewers with facilities for reviewing and marking messages. The role that is assigned to the logged-in user determines which facilities are available.

Figure 11-2      The Compliance Accelerator client



## Department administration with Compliance Accelerator

Within the Compliance Accelerator system, monitored employees are organized into departments, which would normally reflect the company organization. Tasks such as adding employees to departments and assigning reviewers can be done using drag and drop or right click options.

To perform any tasks within the Compliance Accelerator system, users must be assigned an appropriate role. Roles contain a configurable group of permissions. New roles to suit your organization can be created and the permissions assigned to most roles can be changed.

Administrators can be assigned system roles that allow them to perform application-level tasks. Other administrators can be assigned roles for managing a particular department only. Reviewer roles can enable a compliance officer to

mark messages and add comments or enable them only to view messages. The Compliance Supervisor role enables senior compliance officers to check (or appraise) the work of more junior officers, assign exception status to certain employees, and ensure that they are reviewed by an appropriate reviewer.

A reviewer can also be made a delegate for another reviewer.

## Compliance Accelerator searches

In addition to taking a random sample of messages, you may want to monitor employees' messages for unacceptable language or business conduct. For this requirement, you can use Compliance Accelerator to run searches on messages archived using Enterprise Vault services.

The Journaling Connector adds department information to journaled messages, which improves the performance and accuracy of searches run on messages to or from all members of a department.

Compliance Accelerator offers a wide range of search criteria: words and phrases to look for, date ranges, message size, type and direction, author and recipient details and attachment details.

Note that for phrase searching in the content of a message or attachment, the indexing on the Enterprise Vault archives must be set to full.

Searches can be run automatically, on a regular basis using a schedule for search runs, or manually for specific tasks. An application administrator can set up a search to run in several departments concurrently, while searches run by a department administrator are limited to the department that the administrator is responsible for. Messages returned by the searches can then be added to the review set for the department reviewers to read. Accepting search results can be automatic or manual.

By default, Compliance Accelerator identifies and remove duplicate items from the results of a search, and so prevents them from appearing in the review set. To determine whether one item is a duplicate of another, Compliance Accelerator compares the metadata properties of the items, such as their author display names, subjects, and number of attachments.

When a search is created in Compliance Accelerator, the Accelerator Manager service contacts the Enterprise Vault Indexing service to run the search. If the search results are accepted, details of the search and results are stored permanently in the customer database.

Schedules for searches use the SQL Server Agent service.

## Reviewing messages with Compliance Accelerator

Reviewers use the Compliance Accelerator client to read each message captured and allocate a review status mark to indicate whether the message is acceptable or requires further investigation. The status marks can be customized to suit your review system.

There is an audit trail of the review process. This makes it possible to see when a message was reviewed, who reviewed it, and what action they advocated.

## Compliance Accelerator reporting

A reporting system enables you to generate a variety of reports, such as the roles assigned to users, the percentage of messages captured for each employee in a department, and the progress of department message reviewing.

## Exporting messages with Compliance Accelerator

Messages can be exported from the Compliance Accelerator system together with any reviewing marks and comments that have been assigned. This allows users who do not have access to the Compliance Accelerator system to be able to view messages in a department review set.

## Compliance Accelerator configuration data

Configuration data for the Compliance Accelerator system, such as departments, employees, roles and monitoring policies, will typically be added using the Compliance Accelerator client. This lets you add employees to be monitored by synchronizing with Windows user accounts and groups.

Alternatively, you can bulkload the data using XML files.

## About Discovery Accelerator

A company can use Discovery Accelerator to search across their Enterprise Vault archives and quickly find documents and messages that meet criteria for inclusion in a particular inquiry or legal case. All types of archives can be searched: user and journal mailbox archives, file system archives, SharePoint archives, and public folder archives.

Although Discovery Accelerator uses the search facility available in Enterprise Vault, it adds the necessary security that is vital in legal discovery. To ensure that search criteria and results are secure, Discovery Accelerator stores details of all the searches performed, the criteria used and the items found. These details can be viewed but cannot be changed or deleted from the system.



Discovery Accelerator's online review system provides an orderly and efficient process for checking all the items found by searches. Using this system, permitted users view items found by the searches and assign review marks depending on the item's relevance to the case. As reviewers can see the marks applied by other reviewers, they can quickly select only the items that they need to work on, avoiding duplication of effort. The case administrator can track the progress of all reviewers for a case.

Using lawyers to review large numbers of items can be very costly. With Discovery Accelerator, a hierarchy of reviewers can be created for a case, with different levels of reviewers able to assign certain review marks. In this way, less expensive, non-legal staff can perform an initial review of search results, leaving only the relevant or questionable items for lawyers.

The relevant items can then be assigned an appropriate Bates number and published, typically in a PST file, for presentation as evidence in court. Once an item has been published as evidence in a particular case, it is secured, together with its review history, in the Discovery Accelerator system. No further marks can be added by reviewers, and the item cannot be re-published in that case. If required by the court, a report can be produced that shows the review process applied to a particular item.

By default, Discovery Accelerator automatically identifies and removes duplicate items from the review set and from the items in an export run. To determine whether one item is a duplicate of another, Discovery Accelerator compares the metadata properties of the items, such as their author display names, subjects, and number of attachments. In addition, for items in analytics-enabled cases only, Discovery Accelerator compares the content of the items.

To ensure that items in a case are not deleted, an administrator can assign legal hold status to the items associated with a case. This means that the items cannot be deleted manually or automatically (by Enterprise Vault expiry deletion).

## The analytics facility in Discovery Accelerator

Optionally, you can choose to enable *analytics* on a Discovery Accelerator case. This facility provides additional analyses of the metadata and content of items that are collected in the case. Among the extra benefits that analytics provides are the options to do the following:

- Set up rules by which Discovery Accelerator automatically marks or categorizes the items that it adds to the case.
- Classifying large numbers of items without much human intervention ultimately results in better and smaller review sets for manual review.
- Examine and review entire conversation threads in one view.

- Conduct quick or advanced searches within the items in a case.
- These facilities deliver a new review experience that is known as *Guided Review*.

## Discovery Accelerator components

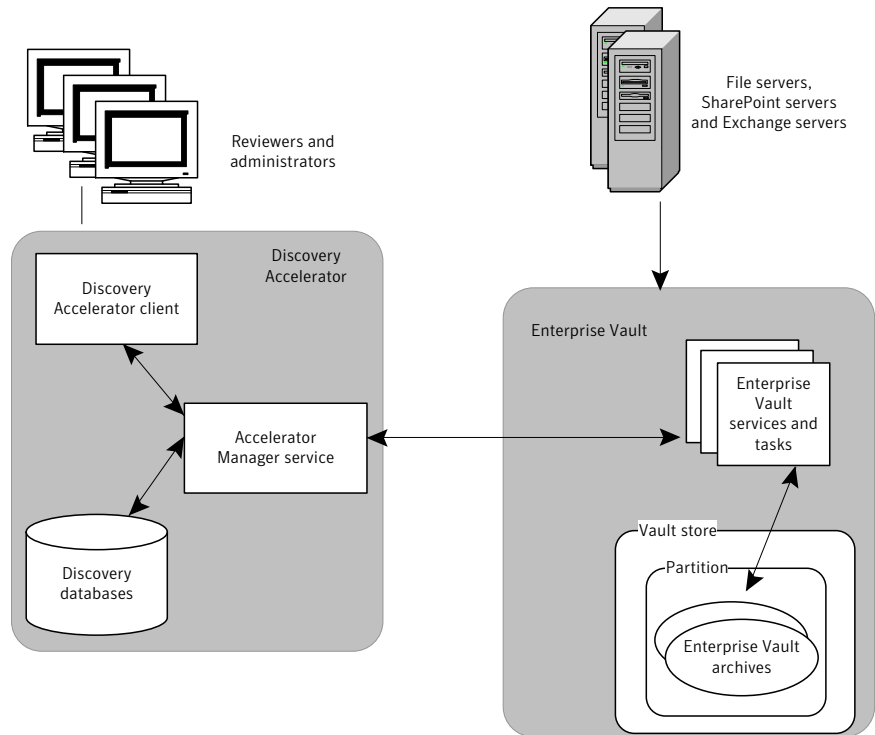
Table 11-2 describes the Discovery Accelerator components.

Table 11-2      Discovery Accelerator components

Component	Notes
Discovery Accelerator client	The client is used by Discovery Accelerator administrators to set up and manage the system and by reviewers to access the items that they are to mark.
Accelerator Manager Web site	This Web site lets you set up and manage multiple Discovery Accelerator databases in which to store your data. For example, this facility lets you split your data by date range or organizational unit.
Enterprise Vault Accelerator Manager service	This service handles the requests from the Discovery Accelerator client and works with the Enterprise Vault components to access archives, perform searches, and so on.
Customer database	The customer database is a SQL database in which Discovery Accelerator stores details of cases, user roles, search results, review marks and tags, and more.  You can set up multiple customer databases.
Configuration database	The configuration database is a SQL database that specifies the location of the customer databases and stores details of the SQL Server, database files, and log files to use.
Custodian Manager Web site (optional)	This Web site lets you store the details of the "custodians" (individual employees) and custodian groups for which you want to search with Discovery Accelerator. A custodian group is any collection of employees, such as Windows or Domino groups and distribution lists, Active Directory or Domino LDAP searches, and Active Directory containers.
Discovery Accelerator API Web site (optional)	This Web site lets you use the Discovery Accelerator API to integrate third-party tools with the software, and thereby retrieve data from or export it to a Discovery Accelerator customer database.  For more information on the Discovery Accelerator API, contact Symantec Support.

Figure 11-3 shows an overview of the Discovery Accelerator components and how the application integrates with Enterprise Vault.

**Figure 11-3** How Discovery Accelerator works with Enterprise Vault



Note the following:

- All communication between Discovery Accelerator and Enterprise Vault is through the Enterprise Vault Accelerator Manager service.
- The Enterprise Vault Accelerator Manager service uses the Enterprise Vault Directory service to find archives, databases and services. Enterprise Vault Storage services are used to preview items and fetch original items. Enterprise Vault Indexing services are used to search for items in the archives.

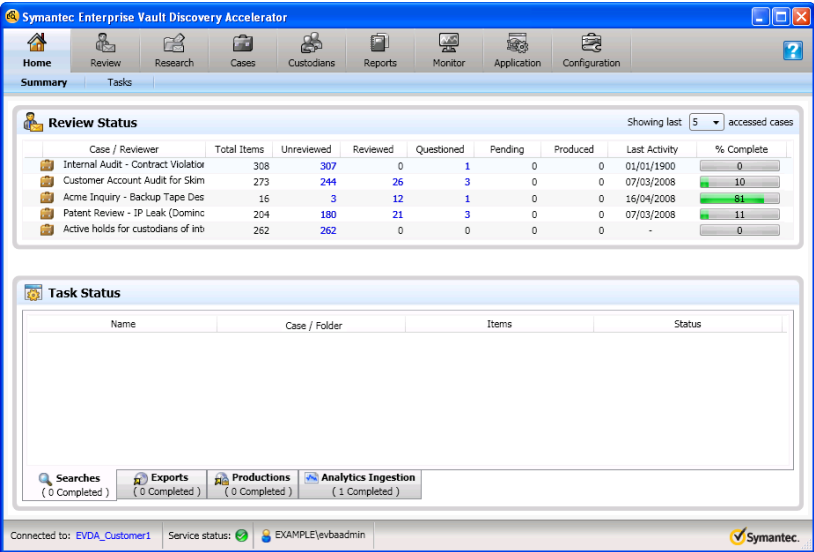
Before installing Discovery Accelerator, you need to consider your present Enterprise Vault and SQL server installation and plan how you want to integrate Discovery Accelerator. In small installations, Discovery Accelerator can be installed on the same computer as Enterprise Vault and the SQL Server, but it is often installed on a different computer.

Large companies may want to distribute the Enterprise Vault and Discovery Accelerator installation even more in order to spread the load over several servers.

## Discovery Accelerator client application

The client application provides administrators with application and case management facilities and reviewers with facilities for reviewing and marking the items in cases. The role that is assigned to the logged-in user determine which facilities are available.

Figure 11-4      The Discovery Accelerator client



## Case administration with Discovery Accelerator

Within the Discovery Accelerator system, information is organized in cases.

A case includes the following:

- Case administration and reviewer roles
- Case marking schemes to use when reviewing items
- Searches and search results
- Target addresses to use when searching messages
- Items that are "produced" (published) or exported from Discovery Accelerator

To perform any tasks within the Discovery Accelerator system, users must be assigned an appropriate role. Roles contain a configurable group of permissions. New roles to suit your organization can be created and the permissions assigned to most roles can be changed.

Administrators can be assigned system roles that allow them to perform application-level tasks, such as creating cases and running searches in multiple cases. Other administrators can be assigned roles for managing a particular case only. Reviewer roles can enable a user to review items and apply particular marks and add comments.

## Discovery Accelerator searches

The criteria for a Discovery Accelerator search can include items in a particular date range, messages to or from particular addresses or words or phrases in the file content (including attachments to messages). If an organization indexes custom attributes in Enterprise Vault, these custom attributes can also be used in Discovery Accelerator searches.

Note that for phrase searching in the content of an item, the indexing on the archives must be set to full.

Search results can be accepted or rejected. Accepted results are added to the review set for the case reviewers to read and can be assigned to particular reviewers. Accepting search results can be automatic or manual.

When a search is created in Discovery Accelerator, the Accelerator Manager service contacts the Enterprise Vault Indexing service to run the search. If the search results are accepted, details of the search and results are stored permanently in the customer database.

## Reviewing items with Discovery Accelerator

Reviewers use the Discovery Accelerator client to check each item and allocate a mark from the case marking scheme to indicate whether the item is relevant to the case or requires further investigation. The marks that a reviewer can use depends on the role that the user has been assigned.

The marking scheme can be customized to suit your cases. For example, you may want a hierarchy of reviewers, so that only the minimum number of items need to be reviewed by lawyers. A set of marks can be assigned to each level of reviewer.

There is an audit trail of the review process. This makes it possible to see when an item was reviewed, who reviewed it, and what action they advocated.

Although reviewers can view stored items and add marks, they cannot change the actual items in any way.

## Producing and exporting items with Discovery Accelerator

When all reviewers have finished checking the items in the case, they can be published (called "produced" in Discovery Accelerator) in a suitable format to present as evidence in court. When items have been produced, their status is changed to Produced and they are locked so that no further changes can be made to their status. Produced items are also assigned a formal Bates number that you define for documents associated with each case.

The export option is less formal than production. You can use this to allow another person, who does not have access to Discovery Accelerator, to view items in the review set. Exported items are not locked and their status is not changed; you can continue to work on them after they have been exported. Exported items are given an export ID but this is different from a Bates number.

Items can be produced or exported as MSG, HTML or PST files. With HTML, you can include item comments and review history information. With PST format, you have the option to set a password and size limit for each PST.

## Discovery Accelerator configuration data

Configuration data for the Discovery Accelerator system, such as cases, target addresses and roles, will typically be added using the Discovery Accelerator client.

Alternatively, you can bulkload the data using XML files.

# Building in resilience

This chapter includes the following topics:

- [About Enterprise Vault and VCS](#)
- [About Enterprise Vault and Windows Server Failover Clustering](#)
- [About Enterprise Vault building blocks](#)

## About Enterprise Vault and VCS

You can integrate Enterprise Vault with Veritas Cluster Server (VCS) to provide a highly-available solution for Enterprise Vault.

### 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.

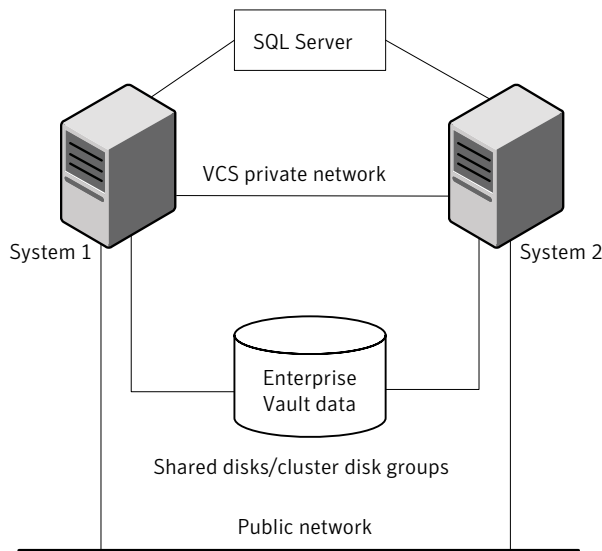
The GenericService agent detects an application failure if a configured service is not running. When this happens, the Enterprise Vault service group is failed over to the next available system in the service group's system list, and the services are started on the new system. This ensures continuous availability for the data that Enterprise Vault is managing and archiving.

## Typical Enterprise Vault configuration in a VCS cluster

[Figure 12-1](#) illustrates a typical configuration.



**Figure 12-1** 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.

## About Enterprise Vault and Windows Server Failover Clustering

You can cluster Enterprise Vault in a Windows Server 2008 R2 failover cluster to provide a high availability solution for Enterprise Vault.

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 server's resources to a different physical node in the cluster.

### Supported Windows Server Failover Clustering configurations

An Enterprise Vault cluster consists of:

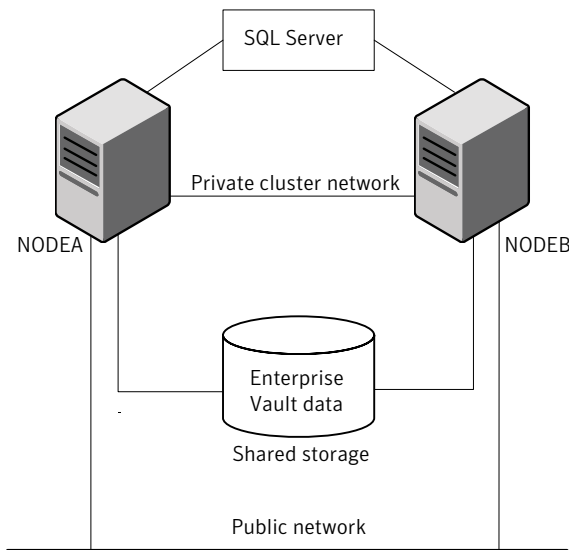
- One or more primary nodes, each normally hosting an Enterprise Vault cluster server.
- One or more failover nodes: standbys that can take over the job of hosting an Enterprise Vault cluster server if a primary node fails.

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.

## Typical Enterprise Vault configuration in a Windows Server failover cluster

[Figure 12-2](#) illustrates a typical configuration.

**Figure 12-2** 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.

## About Enterprise Vault building blocks

An alternative to clustering is to implement Enterprise Vault building blocks. This is part of a straightforward methodology for deploying Enterprise Vault in a way that is both scalable and reliable. You can easily extend a solution made from building blocks to increase capacity. In addition, you can configure building blocks for several different failover schemes such as active/passive and active/active.

Note the following:

- Using building blocks in a clustered configuration is not currently supported.
- The planning of configurations employing building blocks is beyond the scope of this manual. Contact your Symantec solution provider if you need a highly-available installation of Enterprise Vault.

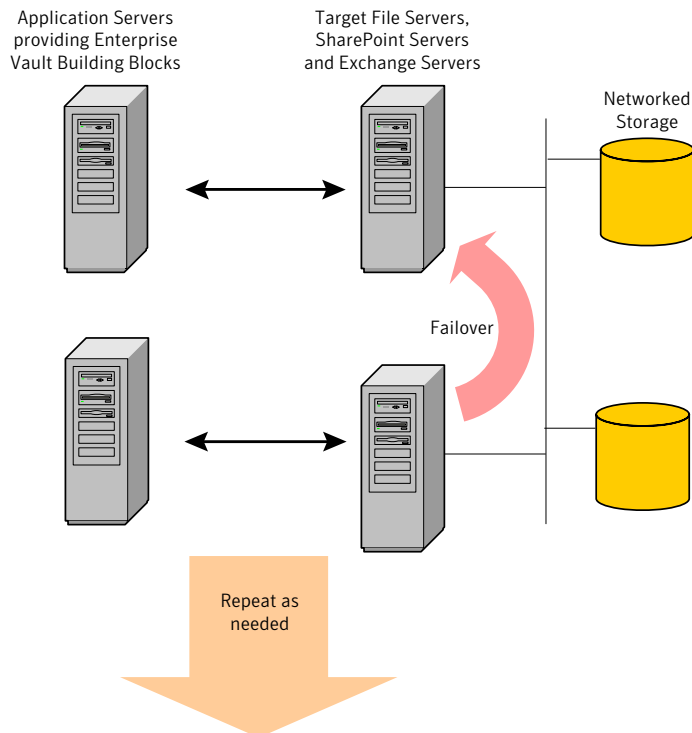
A building block is a repeatable unit of Enterprise Vault functionality hosted on an application server. By adding sufficient building blocks, Enterprise Vault can be extended to scale to the largest of workloads, as shown in [Figure 12-3](#).

Each building block comprises a set of Enterprise Vault services that deliver the same functionality.

The combined services form a unit known as a building block, which is identified by a building block name.

Each building block is hosted on a particular server, but in the event of a disaster on that server Enterprise Vault can failover a building block to another server (without the need for clustering technology). Failover does not require any reconfiguration on the desktop and users are unaffected.

**Figure 12-3** Enterprise Vault building blocks



## Building blocks and high availability

The building block approach can be used in an N+1 architecture in which an idle server stands by to replace any one of N servers that may fail. The "+1" server could also be used to run as an extra, hot standby server running IIS to take some of the workload from the other servers.

In an active/active architecture an existing server can take on the additional workload of a failed server. An active/active solution can be implemented if servers have spare capacity to handle extra work. After failover the net performance may drop, depending on the amount of spare capacity. Thought must be given to this during the design stage.



# Planning component installation

This chapter includes the following topics:

- [About planning component installation](#)
- [Prerequisites for Enterprise Vault components when planning installation](#)
- [Factors to consider when planning deployment of Enterprise Vault components](#)
- [Enterprise Vault Directory Service installation planning](#)
- [Where to set up the Enterprise Vault Services and Tasks](#)
- [Enterprise Vault databases and planning their installation](#)
- [Vault store groups and vault stores installation planning](#)
- [Administration Console installation](#)
- [Installation planning for client components](#)

## About planning component installation

This section helps you to plan which components of Enterprise Vault you need to install on the computers in your Enterprise Vault site.

## Prerequisites for Enterprise Vault components when planning installation

There is a standard list of required software and system settings that is needed for the majority of the Enterprise Vault components. When you install some of

the Enterprise Vault components, other components may also be installed automatically. For this reason you need to check that the prerequisites are correctly set up on each computer in your Enterprise Vault site. Details of all required software and settings are in the *Installing and Configuring* manual.

## Factors to consider when planning deployment of Enterprise Vault components

There are many different ways in which you can deploy the Enterprise Vault components.

Factors that influence how you deploy Enterprise Vault include the following:

- The amount of data you anticipate storing and how long you intend to retain the data.
- The amount of computing resources you have at your disposal, that is, disk space as well as memory.
- The network connections you have between computers.
- Whether you intend to use Enterprise Vault single instance storage.
- Whether you intend to use Index Server groups.
- Whether you are using offline storage, in which case the storage space you require for the vault stores will be reduced.

## Enterprise Vault Directory Service installation planning

The Enterprise Vault Directory Service must be able to connect to the Directory database, but there is no requirement for the Directory Service to be on the same computer as the database.

If necessary, Enterprise Vault sites can share a Directory Service and its associated Directory database. The Directory Service uses different DNS site aliases to distinguish between the different sites. With the exception of the types of files that can be archived (Exchange messages classes or Domino forms), there is no sharing of configuration information across sites.

The Directory Service, with its associated database, must be available at all times to all the computers in the Enterprise Vault sites that it serves, including any servers running Compliance Accelerator or Discovery Accelerator.

The Directory database is managed using SQL management tools.



See [“Enterprise Vault databases and planning their installation”](#) on page 161.

Enterprise Vault initially allocates the following amount of permanent disk space for the Directory database:

- 10 MB for the data files
- 25 MB for the transaction log files

After the database has been populated, the amount of data in the Directory database will not change very much over time.

## Where to set up the Enterprise Vault Services and Tasks

The core Enterprise Vault Server component includes the following main services:

- Directory Service
- Storage Service
- Indexing Service
- Task Controller Service
- Shopping Service
- Admin Service

Archiving and PST Migration tasks are created as required after Enterprise Vault is installed and configured. As they run under the Task Controller Service, this must be installed on any computer that is to host a task.

After you have installed the Enterprise Vault Server, the configuration wizard enables you to specify which particular services or items to run on that computer. The following sections give details of where to set up individual services.

You need to install the Enterprise Vault Server component on any computer on which you want to run any Enterprise Vault Service or Task. When you install the Enterprise Vault Server component, the Enterprise Vault Administration Console is also automatically installed.

If you want to install on the Exchange Server computer, perhaps as part of a pilot, then you can do so, but this is not recommended for production use.

[Table 13-1](#) provides summary information that will help you decide where to set up the Enterprise Vault Tasks and Services.

**Table 13-1** Where to set up the Enterprise Vault Tasks and Services

Task or Service	Number in Enterprise Vault site	Notes
Exchange Provisioning Task	One per Exchange domain.	You can install more than one Exchange Provisioning Task on an Enterprise Vault server. One Provisioning Task will typically process multiple Provisioning Groups.
Exchange Mailbox Archiving Task	As many as the number of Exchange Servers to be archived; one per Microsoft Exchange Server.	<p>You can install more than one Exchange Mailbox Task on an Enterprise Vault computer. Exchange Mailbox Tasks in a single site can archive multiple Exchange Servers in more than one Exchange domain.</p> <p>The Vault Service account must have access in Active Directory to the domains associated with the Exchange Servers being archived.</p>
Exchange Journaling Task	As many as resources permit.	<p>With Exchange 2000 or later, an Exchange Journaling Task can process multiple journal mailboxes.</p> <p>You can install more than one Exchange Journaling Task on an Enterprise Vault computer.</p> <p>The Vault Service Account must have access in Active Directory to the Exchange domains associated with the Exchange Servers being archived.</p>
Exchange Public Folder Task	As many as required to process your public folder hierarchy.	<p>A single Exchange Public Folder Task can process one or more branches of the hierarchy.</p> <p>The Vault Service Account must have access in Active Directory to the domains associated with the Exchange Servers being archived.</p>

**Table 13-1** Where to set up the Enterprise Vault Tasks and Services *(continued)*

Task or Service	Number in Enterprise Vault site	Notes
SharePoint Task	As many as required to archive your SharePoint Archiving Targets.	<p>The SharePoint Task will run on the same computer as the Storage Service that you select when creating the SharePoint Task.</p> <p>You can install more than one SharePoint Task on an Enterprise Vault computer.</p>
Domino Journaling Task	As many as required to archive your archiving target Domino journal location.	<p>You will need to ensure that Enterprise Vault has the correct access to the Domino server, domain and journaling location.</p> <p>Domino Journaling database must have its Database Management method set to Periodic Rollover, Size Rollover or None.</p>
Domino Provisioning Task	One per Domino domain.	You can install only one Domino Provisioning Task on an Enterprise Vault server. One Provisioning Task will typically process multiple Provisioning Groups.
Domino Mailbox Archiving Task	One per Enterprise Vault server.	You cannot install more than one Domino Mailbox Archiving Task on an Enterprise Vault computer. Each task in a single site can archive multiple Domino mail servers in more than one Domino domain. Multiple Domino Mailbox Archiving Tasks can archive the same Domino mail server.
File System Archiving Task	As many as required to process the Archive Points defined.	<p>The Task should run on the same computer as the Storage Service that you select when you create a File Server Archiving Target.</p> <p>Vault Service account must have access to the file system being archived.</p>

**Table 13-1**      Where to set up the Enterprise Vault Tasks and Services *(continued)*

Task or Service	Number in Enterprise Vault site	Notes
Move Archive Task	One per Enterprise Vault storage server.	Enterprise Vault creates this task automatically when you run the Move Archive wizard.  See <a href="#">“How to plan installing the Move Archive task”</a> on page 158.
Storage Service	At least one.	You cannot install more than one Storage Service on an Enterprise Vault computer.  There must be sufficient storage space to hold the vault stores.
Indexing Service	At least one.	You cannot install more than one Indexing Service on an Enterprise Vault computer but you can have more than one Indexing Service in a site.  There must be sufficient storage space to hold the indexes.
Admin Service	One per computer with other Enterprise Vault Services.	Mandatory. The Admin Service is installed automatically when you install the Enterprise Vault Server component.
Shopping Service	One per Enterprise Vault server.	Requires IIS.  There must be sufficient disk space on the computer to hold the shopping baskets until users delete them.
Accelerator Service	One.	Compliance Accelerator and Discovery Accelerator should not be run on same computer.

## How to plan installing Exchange Mailbox Archiving Tasks

To archive user mailboxes, there must be one Exchange Mailbox Archiving Task for each Microsoft Exchange Server computer that is being served in the Enterprise Vault site. A Microsoft Exchange Server can be served by only one Exchange Mailbox Archiving Task. However, there can be more than one Exchange Mailbox

Archiving Task running on the same computer in an Enterprise Vault site, servicing different Microsoft Exchange Servers.

The Exchange Mailbox Archiving Task interfaces most directly with Microsoft Exchange Server (using MAPI), the Storage Service and the Indexing Service. Therefore, it makes most sense to install the task on the same computer as the Storage Service and Indexing Service with which it interfaces. This reduces the amount of data that has to cross network links.

## How to plan installing Exchange Journaling Tasks

An Exchange Journaling Task can archive from multiple Microsoft Exchange Server journal mailboxes. However, a journal mailbox can be served by only one Exchange Journaling Task. There can be more than one Exchange Journaling Task running on the same computer in an Enterprise Vault site, processing one or more journal mailboxes on one or more Exchange Servers.

Like the Exchange Mailbox Archiving Task and Exchange Public Folder Tasks, the Exchange Journaling Task interfaces most directly with Microsoft Exchange Server, the Storage Service and the Indexing Service. For this reason, you are recommended to install the Exchange Journaling Task on the Enterprise Vault computer that hosts the associated Storage and Indexing Services.

## How to plan installing Exchange Public Folder Tasks

There can be many Exchange Public Folder Tasks. Each Exchange Public Folder Task process can archive one or more branches of the Microsoft Exchange Server public folder hierarchy.

When an Exchange Public Folder Task archives from a public folder it uses the archiving settings you specify in the associated Exchange Public Folder Policy in the Administration Console. You can, however, modify the archiving settings for individual public folders, by changing their properties from within Outlook, in the mailbox that owns the public folder. The Enterprise Vault Outlook Add-In must be installed.

The Exchange Public Folder Task requirements are similar to those for the Exchange Mailbox Task; as it interfaces most directly with Microsoft Exchange Server and the Storage and Indexing Services, it makes most sense to install the task on the same computer as the associated Storage and Indexing Services. This reduces the amount of data that has to cross network links.

## How to plan installing Domino Journaling and Mailbox Archiving Tasks

As the planning requirements for these tasks are complex, it is important that you read the information in the *Installing and Configuring* manual during the planning stage of your Enterprise Vault environment.

## How to plan installing the Move Archive task

The Move Archive task is installed automatically on storage servers when you run the Move Archive wizard. The first time you move an archive associated with a particular storage server, Enterprise Vault creates a Move Archive task on that server. The task is configured to start automatically each time the task controller service starts.

## How to plan installing the Storage Service

There must be at least one Storage Service in an Enterprise Vault site. There can be only one Storage Service on a computer. If you want more than one Storage Service in an Enterprise Vault site, they must run on separate computers. It is usually best to put the Storage Service on the same computer as the Indexing Service.

When associated Storage and Indexing Services are on different computers, the computers must be able to communicate over a fast connection.

If you anticipate that your archiving needs are great and require much storage, consider having more than one Storage Service in the site. This would require more than one computer running Enterprise Vault in the site.

## How to plan installing the Indexing Service

There must be at least one Indexing Service in an Enterprise Vault site. However, there can be only one Indexing Service on a computer. If you have more than one Indexing Service in an Enterprise Vault site they must run on separate computers. It is usually best to install the Indexing Service on the same computer as the Storage Service.

In larger or distributed deployments, consider using Index Server groups to spread the indexing load. Ensure that associated Storage and Indexing Services are either collocated, or can communicate over fast connections.

An Indexing Service can manage simultaneously the indexes for many archives, which may be stored in different vault stores on different Storage Service computers. The index locations assigned to the Indexing Service must have sufficient disk space to store the indexing data.

The indexes are organized as follows:

- There is a separate index for each archive.
- Each index consists of a set of related files.
  - Always back up and restore these files as a complete set; never restore only some of the files.
  - The number of files will both increase and decrease over time.
- Files are held in folders; for most archives, there is one folder (index volume) for the index files. When an index volume becomes full, Enterprise Vault automatically creates a new one. This may occur for FSA archives, Exchange or Domino Journal archives, and Exchange Public Folder archives, but is unlikely to occur for normal user mailbox archives.

You specify during configuration the index locations where index volumes are to be created. If you want multiple index locations, you are recommended to spread them over different physical devices. (These locations are sometimes referred to as "index root paths" in error and diagnostic messages.)

If you specify more than one index location, indexes for new archives and new index volumes are spread over the locations. If you create Index Server groups, then indexing the associated vault stores is shared by all the Index Servers in the group. The index volumes are spread over the locations assigned to the Index Servers in the group.

You can choose how much information is indexed for items in an archive using the indexing level; this can be brief, or full indexing. If you want to be able to search item content for phrases, for example using Compliance Accelerator or Discovery Accelerator, then you need to use full indexing.

The more information that is indexed about an item, the easier it is to search for it. However, the more information that is indexed about an item, the more disk space is required for the index. The size of index data for an item varies with the indexing level.

[Table 13-2](#) shows the estimated size of an index as a percentage of the unarchived size of the item for the different indexing levels.

**Table 13-2** Estimated size of indexing data

Indexing level	Estimated size
Brief	4%
Full	12%

So, if you have allowed in the region of hundreds of gigabytes (or terabytes) of space for your vault stores, you are likely to require in the region of gigabytes (or tens of gigabytes) for your indexes.

## How to plan installing the Shopping Service

There is one Shopping Service on each Enterprise Vault server.

When users select items to restore, the items are held in shopping baskets, which are held in Shopping storage locations on the Shopping Service computer.

Make sure you have sufficient disk space on the computer to store the shopping data. In the web browser search, the shopping data remains in the storage location until users delete the associated basket.

## How to plan installing File System Archiving

For Windows file servers you need to install the Enterprise Vault FSA Agent on each file server on which you want to leave placeholder shortcuts, implement File Blocking, or obtain data for FSA Reporting. The FSA Agent provides the services required by these features.

File System Archiving from NetApp Filers (running Data ONTAP 7.2 or later) and EMC Celerra/VNX devices is configured differently: The FSA Agent services or their equivalent do not run on the file server; but on the Enterprise Vault server or another Windows server.

## How to plan installing SharePoint Archiving

A single SharePoint Task in the Enterprise Vault site can archive several virtual SharePoint Servers or SharePoint site collections, but if required you can configure multiple SharePoint Tasks on an Enterprise Vault Server. In addition to the SharePoint Task on the Enterprise Vault Server, you need to install Enterprise Vault SharePoint components on each SharePoint Server computer that is to be archived.

For users to be able to use the Archive Search Web Part, this also needs to be installed on each SharePoint Server computer.

## How to plan installing SMTP Archiving

For this archiving, you will need a server that is configured with a Windows SMTP service and the Enterprise Vault SMTP archiving components. Typically, this server will be a separate computer from the Enterprise Vault server computer. The messages to be archived need to be directed to this server.



You will need to configure File System Archiving to archive the messages from the holding area that SMTP Archiving uses.

## How to plan installing Accelerator Services

The Accelerator Manager Service can be installed on the Enterprise Vault computer, but would typically be installed on a separate computer. You can only have one Accelerator Manager Service in a site.

Currently, running Compliance Accelerator and Discovery Accelerator at the same time on one computer is not supported.

The Accelerator Web Application requires IIS and is typically installed on the Accelerator Manager Service computer, but it can be installed on a different IIS computer, if required.

If required, the Compliance Accelerator Journaling Connector must be installed on each computer with an Enterprise Vault Exchange Journaling Task that Compliance Accelerator is to monitor. One Journaling Connector can serve multiple Exchange Journaling Tasks on one computer.

In large installations, where frequent large searches are performed using Compliance Accelerator or Discovery Accelerator, the Indexing and Storage Services are likely to be heavily used. Performance may be improved by using computers with more memory and CPU for the Indexing and Storage Services.

## Enterprise Vault databases and planning their installation

Enterprise Vault has the following core databases:

- The Enterprise Vault Directory database. There is just one of these and it may be shared by more than one Enterprise Vault site.
- The vault store databases. There is one of these for each vault store in a site.
- The fingerprint databases. There is one of these for each vault store group. One possible exception is the Default Upgrade Group, which Enterprise Vault creates if you previously upgraded to Enterprise Vault 8.0. Enterprise Vault does not create a fingerprint database for the Default Upgrade Group until you configure sharing for it.
- The Enterprise Vault Monitoring database. There is one of these for each Enterprise Vault Directory database. If multiple Enterprise Vault sites share a Directory database, then they must also share a Monitoring database. The

Monitoring database holds the status information that the Monitoring agents gather about the Enterprise Vault servers.

If you configure FSA Reporting, Enterprise Vault also uses one or more FSA Reporting databases to hold the FSA Reporting data that it gathers from the file servers.

SQL Server must be installed and set up before configuring Enterprise Vault. Note that the sort order/collation setting for the SQL Server installation must be case-insensitive; case-sensitive installations are not supported.

Microsoft SQL Server does not need to be on the same computer as the Directory Service computer, nor does it have to be on the vault store computers. On each computer, run Microsoft SQL Enterprise Manager to register the SQL Servers you have installed.

It is possible, perhaps as part of network reconfiguration, to change the instance of SQL Server that manages the Directory database. The process is described in the Administration Console help.

When configuring Enterprise Vault, you are asked to supply the following:

- The Vault Service account details. This enables Enterprise Vault to create the Directory database and vault store databases
- The SQL server location and the data and log file locations for the Enterprise Vault Directory database
- The SQL server location and the data and log file locations for the Enterprise Vault Monitoring database

Enterprise Vault creates databases with the following names:

- EnterpriseVaultDirectory – for the Directory database
- EVvaultstore – for the vault store databases
- EnterpriseVaultMonitoring – for the Monitoring database

Enterprise Vault also creates the following database locations:

- VaultDev – for the Directory database data
- VaultLog – for the Directory database transaction log
- EVvaultstore – for the vault store database data
- EVvaultstore – for the vault store database transaction logs
- A location for the Monitoring database data
- A location for the Monitoring database transaction log

Each vault store database contains an entry for each item that is archived in the associated vault store, so the vault store databases will grow over time. Only when

an item is deleted from the archive will references to it be deleted from the relevant vault store database.

When you create a vault store group, Enterprise Vault creates a fingerprint database for the group. The New Vault Store Group wizard provides the following options for configuring the database filegroups:

- A basic configuration, in which 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.

On the first occasion that you configure a file server for FSA Reporting, a wizard helps you to create an FSA Reporting database. When you configure additional file servers for FSA Reporting, you can choose to use the existing FSA Reporting database or to configure an additional one.

For database storage requirements, see "Storage requirements" in *Installing and Configuring*.

If Compliance Accelerator or Discovery Accelerator is installed, there will also be separate databases created for each of these. The Accelerator databases can be managed by the same SQL Server as the Enterprise Vault databases or a different one, as required.

In Compliance Accelerator, data about all departments, captured items, searches and items reviewed is kept permanently in the databases. Similarly, in Discovery Accelerator, data about cases, searches, search results and items reviewed is kept permanently in the databases. Ensure that there is enough storage space for the growing database files. The databases can be managed using standard SQL administration tools.

## Vault store groups and vault stores installation planning

Vault stores are contained in vault store groups. A vault store group defines the outer boundary for sharing items in Enterprise Vault single instance storage.

See [“About single instance storage”](#) on page 32.

A vault store can comprise one or more partitions. A vault store partition resides on a storage device. When you set up Enterprise Vault, you specify on which device each partition is created.

If a partition is created on an NTFS volume set, it must be contained within a single NTFS volume set, and cannot span volume sets. Bear in mind that a volume set can contain multiple physical disks, so your partition can be spread over more than one disk. There can be more than one partition on an NTFS volume set. If you need to create or extend NTFS volume sets to accommodate the partition, use the Windows Administrative Tools.

The amount of space you will require for your vault stores depends on the following:

- The average size of items that you anticipate archiving.
- The number of items you anticipate archiving in a day to that vault store.
- The reduction in archive storage space due to single instance storage.
- The reduction in storage space due to compression of files.
- How often you anticipate archiving items from the Archiving Target.
- How long you anticipate archived items remaining in the vault store.

---

**Note:** For assistance with storage sizing, contact your Symantec supplier.

---

The first two items in this list give you some idea of the amount of space that you would need in the vault store for one day, before any savings due to single instance storage or compression.

Single instance storage and compression can provide significant savings in storage space.

If you use expiry to delete archived items automatically at the end of their retention period, then the amount of space required will not increase as much over longer periods.

If you set up an aggressive archiving policy that archives items from the archiving targets after about two weeks, users are likely to want to access those items frequently. Keep the archived items online in the vault store for a period of time so users can easily restore them. You will need adequate online space to accommodate the data in the vault stores.

If, on the other hand, you set up archiving so that items are not archived from the archiving targets for about six months or a year, users are much less likely to want to access the archived items. You could then almost immediately move the archived items from the vault stores offline to secondary storage.

You can select a default vault store for archives when creating archiving targets.

For Exchange mailbox archiving, you can select a different vault store at provisioning group, Exchange Server or Enterprise Vault server level. For public

folder archiving, you can select a different vault store at Exchange Server or Enterprise Vault server level. For Domino mailbox archiving, you can select a different vault store at provisioning group or Domino Server level.

The vault store selected will be used for automatically-enabled archives associated with the target. Similarly, for SharePoint archiving, the vault store selected for a target will be used for any auto-enabled site collection archives associated with the target.

The vault store databases do not need to be on the same computer as the vault stores. The databases are managed using SQL Enterprise Manager.

See [“Enterprise Vault databases and planning their installation”](#) on page 161.

## Administration Console installation

When you install the Enterprise Vault Server component, the Administration Console is also automatically installed.

You can install more than one Administration Console in an Enterprise Vault site.

The following are installed with the Administration Console:

- PST Migrator
- NSF Migrator
- Export archive
- Microsoft Exchange Forms
- Enterprise Vault documentation

## Installation planning for client components

Archived items can be accessed from a stand-alone browser using the Web access components, which include the Enterprise Vault Integrated Search, Browser Search and Archive Explorer.

See [“How to access items in archives”](#) on page 19.

In addition, Exchange Server mailbox and public folder archives can be accessed from within Outlook if the Enterprise Vault Outlook Add-In is installed.

Only Domino mailbox and Exchange mailbox and public folder items can be manually archived by users.

## Installation planning for Outlook Web Access (OWA) and RPC over HTTP components

As the planning requirements for these components are complex, it is important that you read the information in the *Installing and Configuring* manual during the planning stage of your Enterprise Vault environment.

# Planning your archiving strategy

This chapter includes the following topics:

- [About archiving strategies](#)
- [Where to define default settings for the Enterprise Vault Site](#)
- [How to allow users flexibility](#)
- [How to plan the types of items to archive](#)
- [How to define your archiving policy for user mailboxes](#)
- [How to plan the archiving policy for journal mailboxes](#)
- [How to plan the archiving strategy for Exchange public folders](#)
- [How to plan an archiving strategy for FSA](#)
- [How to plan a strategy for SharePoint archiving](#)
- [How to plan settings for Retention Categories](#)
- [How to plan the automatic deletion of archived items](#)
- [How to plan PST migration](#)
- [How to plan NSF migration](#)
- [How to plan shared archives](#)
- [How to plan vault stores and partitions](#)
- [How to plan single instance storage](#)

- [About Enterprise Vault reports](#)

## About archiving strategies

This section considers the main points that you need to consider when defining how archiving is to be implemented in your organization and describes configurations settings that will enable you to implement your strategy. Your archiving strategy will determine how you set up Enterprise Vault.

The considerations that you must weigh include the following:

- What types of data you want to archive – user mailbox items, journaled items, public folders, files on file servers or SharePoint servers
- Which mailboxes, journal mailboxes, public folders, file servers and SharePoint servers to target for archiving
- How often to archive the archiving targets
- The vault stores to use for particular archives
- Required indexing levels
- The policies needed for each archiving target
- The Retention Categories to define
- How and when shortcuts and items are to be deleted
- The type of shortcuts to use in mailboxes and on file servers
- Whether to enable archives automatically for mailboxes, public folders and SharePoint site collections
- Whether to keep safety copies
- Which settings to apply across the site
- How to configure single instance storage for your archives.
- Location of PST and NSF files and how they are to be archived
- How much flexibility you give users
- How much Enterprise Vault functionality to show on the users' desktops

These options, and others, are considered in the following sections.



# Where to define default settings for the Enterprise Vault Site

Table 14-1 lists default settings that are to apply across the Enterprise Vault Site.

Table 14-1      Site properties

Tab	Settings
General	<ul style="list-style-type: none"><li>■ The Site alias and description.</li><li>■ The protocol and port to use for the Web Access application.</li><li>■ PST holding area details.</li><li>■ A system message for users, if required.</li><li>■ A system message 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.</li><li>■ Whether users can delete items from their archive, and recover deleted items.</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><li>■ What expiry is to be based on.</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>

Some of these can be overridden for individual archiving targets. For example, when archiving Exchange Servers, some of the defaults shown in Archive Settings can also be defined at provisioning group, Exchange Server and Enterprise Vault server levels. Consider the planned structure of your Site and decide where these defaults need to be defined.

Site properties enable you to have overall control of some aspects of archiving in the site, such as the schedule for archiving runs and whether users can delete items in archives. Archiving target and policy settings enable you tailor archiving for particular archiving targets or groups of users.

Site properties settings are described in the Administration Console help. Refer to this for more details about these settings.

## How to allow users flexibility

For Exchange Server mailbox and public folder archiving, you can allow users the ability to change some of the archiving settings for their own profile. You do this by clearing the appropriate Lock check boxes in policy properties. If you select the check box, users are not allowed to change the setting.

Decide which settings you want users to be allowed to change and leave these unlocked.

## How to plan the types of items to archive

In Exchange Server archiving, the types of message files to be archived are defined by message classes. In Domino Mailbox Archiving, the types of files to be archived are defined by Domino Forms. The default list of Message Classes or Domino Forms to be archived by Enterprise Vault are defined in Directory properties. These apply across all sites using the Directory.

In archiving policies you can select the types of messages to be archived from the targets.

In your email system there may be other types of messages that you want to archive. These messages may come from a third party, or may be ones that you define yourself. Decide which types of message files that you want Enterprise Vault to archive.

## How to define your archiving policy for user mailboxes

You must decide on the different groups of users that you want to archive (Provisioning Groups) and the policies to use for each group for automatic mailbox archiving.

Archiving from mailboxes can be based on one of the following strategies:

- Age: Enterprise Vault archives items automatically as soon as they reach the specified age.
- Quota: archiving keeps a percentage of each user's Exchange mailbox storage limit free. (Archiving based on quota does not apply to Exchange public folders.)
- Age and quota: Enterprise Vault performs age-based archiving first. If age-based archiving does not make the required percentage of mailbox storage limit free, quota-based archiving continues until the required percentage is reached.

Consider archiving based on age and quota when archiving by age only or quota only do not give the results you want. When archiving is based only on age, it may not archive enough items to keep some mailboxes within their quota. When

archiving is based only on quota, some mailboxes may not come close to the Exchange mailbox storage limit. In this case, Enterprise Vault does not even archive older items.

You can set a minimum age limit so that recent items are not archived to meet the archiving criteria.

Additionally, it is possible to archive the largest items first, so you get the greatest benefit from archiving relatively few items. This option is particularly helpful if you use archiving based on quota, or on age and quota.

For example, you can use the following settings. With these settings, Enterprise Vault first archives items that are larger than 3 MB and older than 30 days. It then archives all items older than 60 days:

- Never archive items younger than 30 days
- Start with items larger than 3 MB
- Archive items when they are older than 60 days

As another example, you can use the following settings. With these settings, Enterprise Vault first archives items larger than 1 MB. It then archives items until each mailbox has 10% of its storage limit free:

- Never archive items younger than 30 days
- Start with items larger than 1 MB
- Archive items until mailbox available storage reaches 10%

Enterprise Vault obeys the minimum age limit even if the result is that the available storage percentage is not achieved.

For more detailed information about archiving based on quota or age and quota, see the *Administrator's Guide*.

## How to plan enabling mailboxes

You have the option of automatically enabling new mailboxes for archiving. If you choose this option, all mailboxes that are new to Enterprise Vault are treated in the same way, using the defaults set for the provisioning group. The archives that are automatically created for the newly enabled mailboxes are stored in the default vault store and items in the mailboxes are assigned the default Retention Category. Items in the mailboxes are indexed according to the default Indexing settings.

If you think that some users will want to change the archiving defaults, you can initially suspend archiving for the new mailboxes that have been automatically

enabled. Archiving does not start until the user of the new mailbox enables archiving. This gives users the opportunity to change the archiving defaults.

When you first start using Enterprise Vault, you should gradually introduce users to Enterprise Vault. You are recommended to initially choose not to automatically enable new mailboxes. This way you can control the number of users who use Enterprise Vault and can assess your requirements and the performance of Enterprise Vault. Use the Enable Mailbox wizard in the Administration Console to enable mailboxes manually.

As you get more familiar with your usage of Enterprise Vault and can predict the resources that are required, then you can choose to automatically enable new mailboxes for archiving.

## How to plan controlling the appearance of the desktop

You can use settings in the desktop policy to hide Enterprise Vault menu options, buttons, and property sheets in the client interface for the following users:

- Outlook users with the Outlook Add-In installed
- OWA users
- Lotus Notes users
- Mac OS X users with the Enterprise Vault Client for Mac OS X installed

Additionally, you can control the appearance of the client for those Outlook users who work with Vault Cache and Virtual Vault.

For users who use other email clients, you can configure customized shortcuts on the mailbox policy to enable users to access archived items from shortcuts.

## How to plan the archiving policy for journal mailboxes

Implementing journal archiving is important if your archiving strategy is to satisfy regulatory compliance requirements. If you are installing Compliance Accelerator or Discovery Accelerator in your site, you are strongly recommended to use journal archiving with full indexing.

Enterprise Vault supports Domino Server journal archiving and Exchange Server journal archiving.

In the Journaling Policy you can specify a number of settings, including whether the Journaling Task is to expand distribution lists.

If you want to process certain messages in a particular way, you may want to consider using custom filters. This is described in detail in the *Setting up Exchange Server Archiving* and *Setting up Domino Server Archiving*.

As journal archives contain sensitive information, consider carefully which users should have search access on journal archives.

## How to plan the archiving strategy for Exchange public folders

Since items in public folders are usually there for many people to read, some of the options that are acceptable for individual users are not appropriate.

The main control you have for public folders is the age at which you archive items. For example, you could decide to archive items that have been unmodified for 60 days, rather than 90 days. If the items are likely to be in frequent use, though, archiving them too soon means that users will frequently be retrieving them.

You can also control archiving by size and there is also a minimum age limit, below which items are not archived.

For example, you could use the following combination of settings, which would have the effect of archiving all items larger than 10 MB:

- Never archive items younger than 0 days
- Start with items larger than 10 MB
- Archive remaining items, taking oldest items first and stopping when all items older than 99 years are archived

As an alternative, you could use the following settings, which would have the effect of archiving all items older than 90 days, but would first remove items larger than 5 MB and older than 60 days:

- Never archive items younger than 60 days
- Start with items larger than 5 MB
- Archive remaining items, taking oldest items first and stopping when all items older than 90 days are archived

You can also, however, choose to archive larger items sooner than smaller items. The setting is in the Exchange Public Folder Policy.

Also, if storage space is really important to you, you could decide not to keep safety copies of archived items.

The types of items to archive are defined in the Directory.

See [“How to plan the types of items to archive”](#) on page 170.

## How to plan enabling public folders

When you set up archiving for public folders, you add an Exchange Public Folder Task and assign to it one or more public folder root paths in the public folder hierarchy. You also specify a vault store for the task to use.

New public folders can be auto-enabled for archiving, with a new archive created automatically for each new public folder created under the specified root path.

This feature should be used with caution and only where the creation of public folders is strictly controlled.

## How to plan an archiving strategy for FSA

Why you are implementing file system archiving will to a great extent determine your archiving strategy. For example, you may need to store legal and financial documents for a set period of time in order to comply with industry regulations. You need to consider which files need to be stored and where they are in your file system. Obviously, the more organized your file system is, the easier it will be to define the files to archive.

When you have decided which file servers need to be included in archiving, you need to decide where the Archive Points should be created. These mark the top of each folder structure that is to be stored in a single archive. To ensure that the archive does not fill up too quickly, you need to consider the size of the folder structure below each Archive Point.

How files below an Archive Point are archived is determined by assigning an archiving policy to the target Archive Point. Archiving policies include rules to filter what files are archived and settings such as the Retention Category to be assigned, how permissions on files are to be treated and the type of shortcuts to be created. You can use Volume Policies for the whole folder structure and override settings for certain folders using Folder Policies. For example, in most folders under a particular Archive Point you may want to archive documents and leave shortcuts. However, in one folder you just want a copy of the files archived and the original files left in the folder. You can see that archiving policies could potentially become very complicated if your file system is not organized. By keeping policies simple, it is easier to manage your file system archiving.

If files are going to be removed from the file server when they are archived, you need to consider whether to leave shortcuts or just let users search the archives for stored data. Your choice will to some extent depend on the experience that you want users to have when accessing archived files; how transparent do you want the operation to be.

If you want to use shortcuts, you need to decide what kind to use—placeholder or internet shortcuts. Placeholder shortcuts are more transparent than internet shortcuts. However, your choice will also depend on the type of storage devices you are using.

Check that your backup and virus scanning applications honor the file system offline attribute if you use placeholder shortcuts. If they do not, they may try to recall each file during a run or scan. A backup mode program is included with Enterprise Vault to enable you to switch the file server into backup mode before running your application. This prevents files from being recalled.

Using shortcuts on frequently modified files may mean that a large number of versions of the file are stored. You may want to consider running the Enterprise Vault pruning process at intervals, to delete earlier version of files in the file system archives.

If you want to set up special folders on target file systems that are created and managed by Enterprise Vault, you can use the Managed Folders feature.

Enterprise Vault File Blocking enables you to restrict the files that users store on target file systems.

## How to plan a strategy for SharePoint archiving

As with file system archiving, why you are implementing SharePoint archiving will determine the archiving policies that you implement. This may be to meet compliance regulations or to control disk space usage on the server, or both. If compliance is a requirement, then this will obviously take priority.

When you have decided which SharePoint servers are to be archived, you also need to work out which site collections to include as archiving targets and the archiving policy that you want applied to each one.

Auto-enabling site collections means that new sites created under the target top level site are automatically enabled for archiving and the policy for the site collection applied. This reduces the need for manual administration intervention but requires that your sites are well defined and organized. If, for example, on a SharePoint Server you create a site collection but decide that some of the subsites are not to be archived, you should not set auto-enable on and must manually create site collection objects for each new subsite created.

To enable users to search for archived items from SharePoint site pages, you will need to install the Archive Search Web part on each SharePoint server being archived. You can then place the Archive Search Web part on site pages, as required. Alternatively, users can access SharePoint archives using Archive Explorer Web part or in a browser. The access method you choose will depend on the experience that you want users to have. The Archive Search Web part behaves

in a very similar way to the SharePoint Portal Server search, which users may already be familiar with. Archive Explorer may offer additional facilities, such as copy and move, but may require some end user training, depending on users' level of IT understanding.

If versioning is enabled, the version history link also needs to be added to allow users to see earlier versions of a document that have been archived.

If you are archiving drafts (from SharePoint 3.0 targets), and some users have access to approved documents but not drafts, then you need to consider carefully the SharePoint draft options that you select in the SharePoint archiving policy.

## How to plan settings for Retention Categories

You can categorize archived items using Retention Categories. Settings for Retention Categories define how long the item is to be stored and whether the item can be deleted automatically at the expiry of the retention period.

Enterprise Vault comes with a single, predefined Retention Category called Default Retention Category. The Retention Period is forever.

You can create other Retention Categories as required. For example:

- If you have documents that you must retain for ten years for legal requirements, you could create a new Retention Category, named Legal, with a retention period of ten years.
- You might want to keep the minutes of your regular meetings for three years. In this case, create another new Retention Category, named Minutes, and give it a retention period of three years.

You select one of the Retention Categories, predefined or otherwise, to be the default for all archiving in the Site.

If permitted, Outlook users can change the Retention Category for their Exchange Server mailbox, selected folders or selected items. Because you may want to prevent Outlook users from archiving with particular Retention Categories, you can hide a Retention Category from the list of available Retention Categories. Users are still able to search for items that have been archived with Retention Categories that are now hidden.

Retention Categories cannot be deleted, because they may still be assigned to items in archives.



## How to plan the automatic deletion of archived items

Enterprise Vault can automatically delete items from archives when the retention period expires. Settings for storage expiry are in site properties.

The deletion is based on the retention period that is defined in an archived item's Retention Category.

The start of the retention period is one of the following:

- **Modified date.** For mail messages, this is the time since the message was received. For files and documents, it is the time since the document was last modified.
- **Archived date.** This is the date that the item was archived. This setting is useful if you import old items from other mail systems and want to prevent the items from being expired according to their original received date.

You need to decide the following:

- Whether to make Enterprise Vault delete items automatically.
- Whether to use modified date or archived date as the basis for calculating the start of the retention period.

## How to plan PST migration

How you implement the archiving of PST files will depend on the number of files to be archived, your company policy on the use of PST files and whether users have infrequent access to a fast network connection.

There are several ways to import PST files into Enterprise Vault:

- Wizard-assisted migration can be used for a small number of PST files.
- Scripted migration using Enterprise Vault Policy Manager is ideal for performing bulk migrations of PST files.
- **Locate and Migrate** uses Enterprise Vault Tasks to locate PST files on users' computers, copy them to a central location, and then import them. Locate and Migrate is designed to minimize the difficulties of collecting PST file from users' computers and is likely to require least effort on your part.
- **Client-driven Migration** is similar to Locate and Migrate but the locating of PST files and sending them to a collection location is done automatically by the user's computer and not by Enterprise Vault Server Tasks. This can be useful if, for example, there are users with laptop computers who are in the office only one or two days a week, thus making it difficult to obtain their PST

files by other methods. Client-driven migration needs to be enabled in the Administration Console.

To aid PST migration you can configure desktop clients so that, when a user starts Outlook, the client writes a marker into each PST file that is listed in the mail profile. When a marked PST file is subsequently imported, the marker indicates the owning mailbox.

PST migration is described in the *Administrator's Guide*.

When planning PST migration, take the following points into consideration:

- Do not enable PST migration for all users at the same time. Migrate the PST files for a small group of users and then move onto the next group.
- A typical rate of PST migration is 2 GB/hour.
- An administrator has to allow each PST file before it can be imported.
- It is important that the language setting in the properties for each PST is correct before the PST is imported.

## How to plan NSF migration

Enterprise Vault provides two tools that let you migrate items from NSF files:

- The NSF migration wizard lets you migrate items from NSF files into users' archives. The NSF migration wizard is described in the *Administrator's Guide*.
- Enterprise Vault Policy Manager lets you script the migration of items from NSF files. This approach is suitable for large-scale migrations. Policy Manager is described in the *Utilities* guide.

## How to plan shared archives

When a user mailbox or folders on a file server are archived, the access permissions set on the original folders are also set on the associated folders in the archive. So users that had access to the original folders will also have access to the folders in the archive. This includes delegate access permissions in Outlook. For folder permissions to be set up on new archives, you need to synchronize folders and permissions.

Alternatively, you can share access to an archive either by modifying the archive's properties in the Administration Console, or using the New Archive wizard in the Administration Console to create an archive specifically for sharing. Archives created using the New Archive wizard do not contain a folder structure.

## How to plan vault stores and partitions

Consider where to create vault stores and partitions and the most appropriate type of storage devices to use. For example, some devices provide a large amount of secure storage (WORM) at reasonable cost, which may suit a compliance archiving strategy.

Enterprise Vault's partition rollover feature provides automatic rollover from one partition to another to support continuous archiving. For example, when the physical disk that hosts your open partition reaches capacity, Enterprise Vault can automatically close this partition and open another.

Where vault store partitions are held on non-WORM devices other than EMC Centera, the speed and efficiency of vault store backups can be improved by using the Enterprise Vault "collection" feature. This feature collects multiple small files into CAB files. Collection is not recommended on devices that perform deduplication, as it causes loss of deduplication.

Collections are handled differently on EMC Centera devices, as follows:

- Centera collection files are used instead of CAB files.
- Files are collected as soon as they are archived (not according to a schedule).

## How to plan handling safety copies

Safety copies are copies of the archived items. In a mailbox, they are identified by the pending archive icon. When you set up a vault store, you must specify when Enterprise Vault deletes safety copies.

The options on vault store properties are as follows:

- Never
- After vault store backup
- Immediately after archive

The type of environment in which you are running Enterprise Vault influences how you configure the process for safety copies.

If you are setting up a pilot system in a test environment, where there is no need to keep users' data, set up the vault store so that Enterprise Vault deletes the safety copies immediately after archiving.

If you are setting up a pilot system in a production environment, it may be necessary for users to get their data back again after testing Enterprise Vault. In this situation, set up the vault store so that Enterprise Vault never deletes the safety copies. All the safety copies will remain in the original locations.

In mailbox archiving, if you have set up Enterprise Vault so that it creates shortcuts for archived items and safety copies are not deleted, the icons in the mailbox for the archived items remain as pending archive and do not revert to the shortcut icon.

When you have completed your testing, you can set Enterprise Vault to delete the safety copies at the selected time.

## How to plan single instance storage

Enterprise Vault can use single instance storage to optimize archive storage space. Enterprise Vault's single instance storage mechanism archives a single instance of parts of an item that are suitable for sharing, such as large message attachments. Enterprise Vault can share the single instance storage parts (SIS parts) within a vault store, or across two or more vault stores within a vault store group. A vault store group forms an outer boundary for sharing.

Enterprise Vault single instance storage is not performed when items are stored to partitions that are hosted on EMC Centera devices. You can configure a partition for an EMC Centera device to use the Centera's device-level sharing mechanism, 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.

If you use Enterprise Vault's single instance storage mechanism, 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. Enterprise Vault cannot share items retrospectively. Also there are limits to what you can change after Enterprise Vault has started sharing items.

For more information about setting up single instance storage, see "Setting up Storage" in *Installing and Configuring*.

## About Enterprise Vault reports

You can run an Enterprise Vault task in Report Mode. When you do this, nothing is processed, but you get a report for each archiving target that shows what would be processed if you ran the task normally.

Reports created by mailbox and Exchange Public Folder Tasks include details about the number and total size of items that would be archived when the task is run in Normal Mode and the number of expired shortcuts ready to be deleted.

In mailbox archiving, reports are generated for enabled, disabled or new mailbox archives, so that you can determine how much space you would save by enabling more mailboxes for archiving.

The Provisioning tasks can be configured to generate brief or full reports. Full reports list the mailboxes that will be processed, the Provisioning Group assigned, and the policies that will be used. Reports are also produced by this task on a normal run.

File system and SharePoint archiving tasks can be run in Report Mode but can also be configured to generate reports for normal archiving runs. You can also specify the level of reporting required.

There are several levels of reporting for file system archiving reports:

- Brief reporting includes a summary for each Volume and Archive Point of the number and total size of items that will be archived. Each policy and rule is listed together with the number and total size of items that meet the criteria.
- Full reporting includes details of the items that satisfy each rule.

Similarly, in SharePoint archiving, there are several levels of reporting:

- Brief reporting includes a summary for each site collection of the number and total size of documents that will be archived. Each policy and rule is listed together with the number and total size of documents that meet the criteria. The summary also contains information about version pruning and the space saved as a result of pruning.
- Full reporting includes details of the documents that satisfy each rule and document versions pruned.

For all types of archiving, reports go into a text file in the `Reports` subfolder of the Enterprise Vault installation folder. The text file has tab-separated fields, so you can easily import it into a spreadsheet program such as Microsoft Excel. You can use these reports to gauge the usage of the archiving task under different setup conditions.

## Enterprise Vault Reporting feature

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

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



# Index

## A

- Accelerator Services 161
- Accelerator Web Application 161
- Accessing archives 53
- Accessing items without Outlook 54
- Active/passive failover configuration 144
- Adapter for Secure Messaging and Rights Management 24
- Add-on applications 23
- Admin Service
  - description 50
- Administration Console 165
  - description 62
  - File System Archiving containers 92
  - overview 41
- Administration tasks
  - overview 72
- Age-based archiving 170
- Application Log 68
- Applications 23
- Archive
  - sharing 178
- Archive Explorer 20, 58
- Archiving
  - accessing items 19
  - benefits 19
  - Domino Journal 121
  - Domino mailbox archiving 115
  - overview 18
- Archiving filters 79
- Archiving process
  - overview 31
- Archiving strategy
  - defining default settings 169
  - deletion of archived items 177
  - desktop appearance 172
  - enabling mailboxes 171
  - enabling public folders 174
  - Exchange public folders 173
  - FSA 174
  - journal mailboxes 172

- Archiving strategy *(continued)*
  - NSF migration 178
  - planning 168
  - planning what to archive 170
  - PST migration 177
  - Reporting feature 181
  - reports 180
  - retention categories 176
  - safety copies 179
  - shared archives 178
  - SharePoint 175
  - single instance storage 180
  - user flexibility 170
  - user mailboxes 170
  - vault stores and partitions 179
- Archiving Targets
  - user mailbox 77
- Archiving task
  - installation planning 157
  - overview 43
- ASP components 31
- Automatic archiving 44
- Automatic Classification Engine 27

## B

- Backup solutions 31, 49
- Browser search 20, 58
- Building Blocks
  - high availability 149
- Building blocks
  - overview 147
- Business Accelerator products 23

## C

- Client components
  - installation planning 165
- Client for Mac OS X 55
- Client-driven migration 46
- Client-driven PST migration 63
- Clients
  - languages 21

Clients (*continued*)

overview 20

## Clustering

Microsoft server clusters 145

VCS 143

Veritas Cluster Server 143

## Collector Task 46

## Compliance 81

## Compliance Accelerator 27, 129

client application 134

components 131

configuration data 136

department administration 134

exporting messages 136

journaling 81

overview 130

purpose of 23

reporting 136

reviewing messages 136

searches 135

## Compliance Accelerator Journaling Connector 161

## Compressing items 49

## Configuration

typical setup 144

## Configuration options

overview 18

## Configurations

active/passive failover 144

## Converting items 49

## Convertors Log 68

**D**

## Data Classification Services 27

## Data Loss Prevention 27

## Database availability group 75

## Databases

overview of planning installation 161

## Deleting items 44, 49

## Deleting shortcuts 44

## Desktop policies

Domino mailbox archiving 120

Exchange Server archiving 78

## Diagnostics

selecting the level of 68

## Directory

overview 42

## Directory Database

data device 162

disk space requirements 152

Directory Database (*continued*)

installation requirements 162

name 162

overview 31, 43

transaction log device 162

## Directory Service

function 47

installation planning 152

overview 42

SQL requirements 162

## Discovery Accelerator 27, 129

analytics facility 137

case administration 140

client application 140

components 138

configuration data 142

overview 136

producing and exporting 142

purpose of 23

reviewing items 141

searches 141

## Discovery Collector 25

## Discovery Search Service

description 51

## Domino Journal Archiving 121

## Domino Journal archiving 121

archive 122

archiving policies 121

clustered databases support 123

database considerations 122

database management 122

Journaling policy 122

setting up 122

target location 123

task 122

## Domino Journaling Tasks 158

## Domino mailbox archiving 115

desktop policies 120

Domino Mailbox Archiving task 118

Domino provisioning groups 117

mailbox policies 119

## Domino Mailbox Archiving task 118

## Domino provisioning groups 117

## Domino retention folders 119

## Domino retention plan 119

XML file 120

**E**

## eDiscovery 25



- Enabling mailbox archives 76
- EnCase Ingest Connector 24
- Enforce Server 27
- Enterprise Vault
  - Admin Service 50
  - Administration Console 28
  - Client for Mac OS X 28, 55
  - Directory Service 47
  - Discovery Search Service 51
  - extensions for Lotus Notes 57
  - FSA Agent 29
  - how it works 28
  - Indexing Service 49
  - Lotus Notes and DWA clients 28
  - Microsoft Exchange forms 55
  - Mobile Search 28, 56
  - monitoring and reporting 59
  - Offline users 54
  - Outlook Add-In 28, 53
  - overview 17
  - OWA Extensions 56
  - OWA Extensions 28
  - provisioning and archiving tasks 43
  - provisioning task 45
  - PST migration task 45
  - Retrieval process 45
  - Server component 28
  - Services 46
  - SharePoint archiving 29
  - Shopping Service 50
  - Sites, Directory and Directory database 42
  - SMTP 29
  - Storage Service 49
  - Task Controller Service 50
  - tasks 43
  - Web access components 57
  - web access components 28
- Enterprise Vault Accelerators 129
  - differences 130
- Enterprise Vault administration
  - accounts and roles 62
  - Administration Console 62
  - archiving NSF file contents 63
  - archiving PST file contents 63
  - auditing 70
  - automatic monitoring 69
  - exporting archived items 64
  - logging 67
  - management tasks 72
  - Enterprise Vault administration (*continued*)
    - message queue monitoring 70
    - overview 61–62
    - reporting 66
    - reporting and monitoring 65
    - scripted management tasks 71
    - system status 68
    - Veritas Backup Reporter 6.6 support 71
    - Welcome message 65
  - Enterprise Vault Client for Mac OS X 55
  - Enterprise Vault client for Mac OS X 20
  - Enterprise Vault Discovery Collector 25
  - Enterprise Vault Operations Manager
    - component 29
    - overview 68
  - Enterprise Vault Reporting
    - component 29
  - Enterprise Vault Services and Tasks
    - planning 153
  - EnterpriseVaultDirectory 162
  - EnterpriseVaultMonitoring 162
  - Entourage 20, 55
  - Envelope journaling 80
  - EVDominoRetentionPlans.exe 120
  - EVPM 46, 71
  - Exchange agent
    - about 144
    - supported services 144
    - typical setup 144
  - Exchange cluster
    - active/passive setup 144
  - Exchange cluster configuration
    - Active/Passive failover 144
  - Exchange desktop policies 78
  - Exchange Journaling Tasks 157
  - Exchange Mailbox Archiving Tasks 157
  - Exchange Mailbox Archiving tasks 76
  - Exchange mailbox policies 78
  - Exchange Provisioning tasks 76
  - Exchange Public Folder archives
    - user access 85
  - Exchange Public Folder Policies 83
  - Exchange Public Folder Targets 83
  - Exchange Public Folder Tasks 157
  - Exchange Public Folder tasks 83–84
  - Exchange Server archiving 75
    - desktop policies 78
    - mailbox policies 78
    - managed folders 78

- Exchange Server Forms 55
- Exchange Service agent 144
- Export archive
  - installation 165

## F

- FAT volumes 32
- File Blocking 103
  - NetApp devices 104
  - notifications 104
  - NTFS devices 104
  - quarantine location 104
- File System Archiving 87
  - archiving process 97
  - configuring 92
  - containers in Administration Console 92
  - File Blocking 103
  - file blocking 104
  - FSA Agent 160
  - FSA Reporting 106
  - FSAUtility 101
  - overview 88
  - placeholder shortcuts 102
  - policies 88
  - pruning files 99
  - reports 99
  - restoring files 100
  - retention folders 105
  - shortcut files 89
  - shortcut files backup and scan 102
  - synchronizing permissions 99
- File System Archiving tasks 44
- Filters for mailbox archiving 79
- FIPS compliance 59
- FSA Agent 29, 160
- FSA Reporting 106
- FSA Reporting database
  - overview 31
- FSAUtility 101

## I

- Icon
  - pending archive 179
- IM Manager 25
- Importing
  - previously-exported items 64
- Index Server
  - standalone 38

- Index Server (*continued*)
  - ungrouped 38
- Index Server group 39
  - distribution of index volumes 37
  - introduction 38
- Index size 35
- Index storage location 50
- Index volumes 36
  - location of rollover volumes 36
- Indexes
  - 32-bit and 64-bit 35
  - disk space requirements 159
  - updating 50
- Indexing
  - estimated size of data 159
  - in distributed environment 39
  - load balancing 39
  - overview 35
  - tools 37
- Indexing items 49
- Indexing level 159
- Indexing levels 35, 49
- Indexing Service
  - description 49
  - planning installation 158
  - specifying 76
- Indexing service 36
- Ingest Connector 24
- Installation
  - Export archive 165
  - NSF Migrator 165
  - PST Migrator 165
- Instant Messages 17
- Integrated search 58
- IPM classes 81
- Items
  - previewing 59
  - restoring 50

## J

- Journal archives
  - access permissions 80
- Journal Filtering 81
- Journal mailbox archiving 80
- Journaling and Business Accelerators 81
- Journaling Connector
  - Exceptions 135
  - overview 132

Journaling Task  
     planning installation 157

## L

Languages  
     clients 21  
     extensions for Lotus Notes 57  
     Microsoft Exchange forms 55  
 Legal discovery 81  
 Liquid Machines Document Control 24  
 Loading data 136, 142  
 Locate and Migrate 46, 63  
 Locator Task 46  
 Lock feature  
     planning how to use 170  
 Locking settings 78  
 Logging 67  
 Lotus Notes extensions 57

## M

Mac OS X client 55  
 Mailbox archiving policy 170  
 Mailbox Archiving task  
     overview 76  
 Mailbox Archiving Tasks 158  
 Mailbox folder permissions 77  
 Mailbox policies  
     Domino mailbox archiving 119  
     Exchange Server archiving 78  
 Mailboxes  
     enabling 171  
 Managed folders 78  
 Manual archiving 44  
 Message classes 81  
 Message Queues 70  
 Microsoft Entourage 55  
 Microsoft Exchange Forms  
     description 55  
     Installation  
         Microsoft Exchange Forms 165  
 Microsoft Exchange Organization Forms Library 55  
 Microsoft Exchange Server  
     journal mailbox 80  
 Microsoft Operations Manager 69  
 Microsoft Outlook for Mac 55  
 Microsoft server clusters 145  
 Microsoft SharePoint 109  
 Microsoft SQL Server 162

Migrator Task 46  
 MMC 41  
 Mobile Search 20, 28, 57  
 MOM 69  
 Monitoring 69  
 Monitoring agents  
     overview 31  
 Monitoring and reporting 59  
 Monitoring database  
     installation requirements 162  
     name 162  
     overview 31  
     purpose 162  
 Move Archive task 158  
 MSMQ 70

## N

NSF files 63  
     introduction 19  
 NSF migration 178  
 NSF Migrator  
     installation 165  
 NSF migrator 64

## O

Offline users 54  
 Offline vault overview 54  
 Operations Manager  
     component 29  
     overview 68  
 Organization 75  
 OST files 54  
 Outlook Add-In 20, 53  
 Outlook settings 54  
 Outlook Web Access Extensions  
     installation planning 166  
 OWA 20  
 OWA components 56  
 OWA Extensions 20, 56

## P

Partition  
     definition 32  
 Pass-through recall  
     about 102  
 Perfmon 70  
 PGP 24

- Pilot system 31
  - deleting safety copies 179
- Placeholder shortcuts
  - pass-through reall 102
- Planning
  - component installation 151
  - Directory Service 152
  - Enterprise Vault Services and Tasks 153
  - factors for deployment of components 152
- Policies 62
- Prerequisites
  - planning installation of components 152
- Previewing items 49, 59
- Provisioning API 72
- PST file 63
- PST files
  - archiving contents 75
  - importing 45
  - introduction 19
  - marking by client 63, 178
- PST migration 64
- PST migration tools 45
- PST Migrator
  - installation 165
- PST Migrator wizard 46
- PST Wizard 63
- Public folders
  - enabling 174

## Q

- Quota-based archiving 170

## R

- Report Mode 67, 180
- Reporting
  - component 29
  - overview 66
- Reports 67
- Restoring items 49–50
- Retention Category
  - definition 18
  - planning 176
- Retention folders 105
- Retention folders, Domino 119
- Retention plan, Domino 119
- Retrieving
  - description 45
- Review audit trail 136, 141

- .rge files 55
- RPC over HTTP components
  - installation planning 166
- RPC over HTTP connections 20

## S

- Safety copy 44
  - how to identify 179
  - planning considerations 179
- Scripted NSF migration 64
- Scripted PST migration 46, 63
- Scripting management tasks 71
- Searching
  - phrases in content 49
- Services 46
  - diagnostics reporting 68
  - in Services Console 47
- SharePoint archiving 29, 109, 160
  - access to archived documents 113
  - configuration 110
  - policies 112
  - reports 112
  - tasks 110
- Shopping baskets 50
  - requirements 160
- Shopping Service
  - description 50
  - installation 160
- Shortcuts
  - defining for mailboxes 78
  - definition 18
- Single instance storage
  - mechanisms 180
  - overview 32
- Site
  - definition 42
  - multiple Sites sharing a Directory 48
- Site Properties 170
- SMTP 29
- SMTP Archiving 125, 160
  - architecture 125
  - MAPI messages 125
  - overview 125
  - setting up 127
  - x-headers 127
- SMTP archiving
  - relaying messages 127
- SMTP holding area folders 126
- SQL Administrator 162

- Status pane
  - in Administration Console 68
- Storage
  - types of devices 31
- Storage Service
  - description 49
  - planning installation 158
- Supported services 144
- Supported versions 143
- Synchronizing folders 77
- System status 68

## T

- Targets 62
- Task Controller Service 50
  - overview 43
- Tasks 43, 62
- Testing
  - usage 180
- Types of data supported 17

## U

- Ungrouped Index Server 38
- User mailbox archiving
  - overview 75

## V

- Vault Service account 62
- Vault store
  - definition 32
  - deleting safety copy 179
  - installation planning 163
  - requirements 163
- Vault Store database
  - data device 162
  - installation requirements 162
  - name 162
  - overview 31, 49
  - transaction log device 162
- Vault store groups
  - installation planning 163
- VaultDev 162
- VaultLog 162
- VBR support for Enterprise Vault 71
- VCS 143
- Veritas Backup Reporter 71
- Veritas Cluster Server 143
- Veritas Cluster Server (VCS) 143

- Virtual Vault 20, 53

## W

- Warning threshold 51
- Web access components 57
- Welcome Message 65
- Wizards
  - New Archive 178
- WORM storage 31

## X

- XML file
  - for Domino retention plan 120
- XML files for loading data 136, 142