

Veritas Enterprise Vault™ Administrator's Guide

12.1

Veritas Enterprise Vault: Administrator's Guide

Last updated: 2017-07-28.

Legal Notice

Copyright © 2017 Veritas Technologies LLC. All rights reserved.

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

This product may contain third party software for which Veritas 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. Refer to the third party legal notices document accompanying this Veritas product or available at:

<https://www.veritas.com/about/legal/license-agreements>

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 Veritas Technologies LLC 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. VERITAS TECHNOLOGIES LLC 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, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Veritas as on-premises or hosted services. 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.

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

<http://www.veritas.com>

Technical Support

Technical Support maintains support centers globally. All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policies. For information about our support offerings and how to contact Technical Support, visit our website:

<https://www.veritas.com/support>

You can manage your Veritas account information at the following URL:

<https://my.veritas.com>

If you have questions regarding an existing support agreement, please email the support agreement administration team for your region as follows:

Worldwide (except Japan)

CustomerCare@veritas.com

Japan

CustomerCare_Japan@veritas.com

Before you contact Technical Support, run the Veritas Quick Assist (VQA) tool to make sure that you have satisfied the system requirements that are listed in your product documentation. You can download VQA from the following article on the Veritas Support website:

<http://www.veritas.com/docs/000095758>

Documentation

Make sure that you have the current version of the documentation. Each document displays the date of the last update on page 2. The latest documentation is available on the Veritas website:

<http://www.veritas.com/docs/000001907>

Documentation feedback

Your feedback is important to us. Suggest improvements or report errors or omissions to the documentation. Include the document title, document version, chapter title, and section title of the text on which you are reporting. Send feedback to:

evdocs@veritas.com

You can also see documentation information or ask a question on the Veritas community site:

<http://www.veritas.com/community>

Contents

Chapter 1	About this guide	15
	Required knowledge	15
	Where to get more information about Enterprise Vault	15
	Enterprise Vault training modules	18
Chapter 2	Managing administrator security	19
	About administrator security	19
	Roles-based administration	20
	About the predefined roles	21
	Roles and the Enterprise Vault Administration Console	24
	Roles-based administration (RBA) and the classification feature	30
	Roles and Enterprise Vault Operations Manager	30
	Roles and Enterprise Vault Reporting	31
	Working with predefined RBA roles	31
	Customizing RBA roles	34
	Determining your current role entitlements	36
	Resetting all roles and assignments	37
	Using permissions to control access	37
	Changing the vault service account	38
Chapter 3	Day-to-day administration	41
	Monitoring the system status	42
	Monitoring application logs	42
	About Exchange mailbox archiving reports	43
	Configuring Exchange mailbox archiving reports	43
	Using Exchange mailbox archiving reports	44
	Getting more information	46
	Monitoring MSMQ queues	46
	About starting or stopping tasks or services	46
	Starting or stopping tasks	47
	Starting or stopping services	48
	Checking logs with the Windows Event Viewer	49
	Monitoring journal mailboxes	49

Use the default ANSI codepage (ACP codepage)	51
About monitoring disks	52
Checking disk space for vault stores	52
Disk space and indexes	55
About maintaining the SQL databases	55
Vault store database maintenance	56
Directory database maintenance	56
Fingerprint database maintenance	57
Monitoring database maintenance	58
FSA Reporting database maintenance	58
Using SQL AlwaysOn availability groups	59
Enterprise Vault's PowerShell cmdlets	59
Implementing SQL AlwaysOn availability groups	59
About managing vault store groups and sharing	63
Viewing the status of the vault stores in a vault store group	64
Changing the sharing level of a vault store	65
Moving a vault store to a different vault store group	66
Deleting a vault store group	67
Monitoring the fingerprint databases	68
Monitoring the archive space reduction due to single instance storage	68
About managing safety copies	69
Configuring the removal of Enterprise Vault safety copies	69
Checking that partitions have been backed up	70
About managing partition rollover	71
Configuring partition rollover	71
Changing rollover order	73
Forcing partition rollover	74
Recovering deleted items	75
About expiry and deletion	75
Setting up storage expiry	76
Setting up shortcut deletion	77
Working with retention categories and retention plans	77
Creating a new retention category	78
About retention plans	79
Creating a retention plan	79
Applying retention plans to your Enterprise Vault archives	80
About the PowerShell cmdlets for working with retention plans	82
How retention plans affect storage expiry	83
About maintaining provisioning groups	84
Enabling archiving for new mailboxes	84
Checking for hidden mailboxes	87

About applying or removing legal holds on selected archives	87
Get-EVArchive	88
Set-EVArchive	92
About moving archives	94
How Move Archive works	95
About moving mailbox archives within a site	97
About moving mailbox archives between sites	99
About moving journal archives within a site	101
About configuring Move Archive	102
Running Move Archive	104
Monitoring Move Archive	110
Deleting archives after Move Archive	113
Managing Move Archive operations with Failed and Error statuses	114
Move Archive reporting and monitoring	115
Deleting an archive	116
Deleting a vault store	116
Setting a system message	118
About index volumes	118
Moving the directory database	119
Moving a vault store database	119
Moving a fingerprint database	120
Moving the Monitoring database	120
Moving the auditing database	120
Changing the Vault Service account password	121

Chapter 4 Using Enterprise Vault for records management

.....	122
Introducing records management	122
About records and non-records	123
How Enterprise Vault marks items as records	124
Setting up the required record types	125
Setting the default record type for users	126
Creating the required retention categories	127
Associating the retention categories with retention plans	128
Applying the retention plans to the target users	129
Allowing users to change the record types of individual items	130
Using the classification feature for records management	133
Potential conflicts between EVPM and the classification feature	134
Common configuration scenarios	135
Configuring users as Capstone officials and marking all their items as permanent records	135

	Configuring users as Capstone officials but using classification to exclude certain items from the permanent record set	136
	Configuring users as Capstone non-officials	138
	Searching archives for items marked as records	139
	Using the advanced search facilities in Enterprise Vault Search to find records	140
	Helping advanced search users to find records more easily	140
	Customizing Enterprise Vault Search to show record types and IDs in the results pane	141
	Viewing the records management settings for one or more archives	142
	Exporting items from archives	143
Chapter 5	Automatically filtering events	145
	About filtering events	145
	Events generated by event filtering	145
	Configuring event filtering	146
	Event filtering examples	148
Chapter 6	Managing indexes	149
	About the indexing wizards	149
	About indexing tasks and subtasks	150
	Configuring the deletion of indexing subtasks	151
	About the Upgrade wizard	151
	About the Verify wizard	152
	About the Synchronize wizard	153
	About the Rebuild wizard	153
	About the Change Location wizard	154
	Using the indexing wizards	155
	Managing indexing tasks	156
	Managing indexing exclusions	164
	How indexing exclusions work	164
	Managing indexing exclusions	164
	Viewing details of index volumes	165
	About the indexing PowerShell cmdlets	165
	Running the indexing PowerShell cmdlets	166
	Using Get-IndexServerForIndexLocation	166
	Using Set-IndexMetadataSyncLevel	166

Chapter 7	Advanced Domino mailbox and desktop policy settings	168
	About the advanced policy settings for Domino mailbox and desktop policy	168
	Editing the advanced settings for Domino mailbox and desktop policy	169
	How to apply the new settings for Domino mailbox and desktop policy	169
	Domino mailbox policy advanced settings	169
	Archiving General: Domino mailbox policy	169
	Domino desktop policy advanced settings	171
	Vault Cache: Domino desktop policy	171
Chapter 8	Advanced Exchange mailbox and desktop policy settings	173
	About the advanced Exchange mailbox and desktop settings	173
	Editing the advanced Exchange mailbox and desktop settings	174
	How to apply the new Exchange mailbox and desktop settings	174
	Exchange mailbox policy advanced settings	174
	Archiving General (Exchange mailbox policy advanced settings)	174
	Exchange desktop policy advanced settings	185
	Office Mail App (Exchange desktop policy advanced settings)	185
	Outlook (Exchange desktop policy advanced settings)	186
	OWA versions before 2013 (Exchange desktop policy advanced settings)	206
	Vault Cache (Exchange desktop policy advanced settings)	213
	Virtual Vault (Exchange desktop policy advanced settings)	218
Chapter 9	Advanced Exchange journal policy settings	229
	Editing the advanced Exchange journal policy settings	229
	Archiving General (Exchange journal policy advanced settings)	230
	ClearText copies of RMS Protected items (Exchange Archiving General setting)	230
	Expand distribution lists (Exchange Archiving General setting)	231
	Failed DL expansion behavior (Exchange Archiving General setting)	232
	Inherited permissions (Exchange Archiving General setting)	232

	Journal delay (Exchange Archiving General setting)	232
	Maximum message size to archive in MB (Exchange Archiving General setting)	233
	Pending shortcut timeout (Exchange Archiving General setting)	233
	Queue Journal items (Exchange Archiving General setting)	233
	Reset archive names (Exchange Archiving General setting)	233
	Return failed items to inbox (Exchange Archiving General setting)	234
Chapter 10	Advanced Exchange public folder policy settings	235
	Editing advanced Exchange public folder settings	235
	Archiving General (Exchange public folder policy advanced settings)	236
	Archive unexpired Calendar Events (Exchange Archiving General setting)	236
	Code pages for right-to-left custom shortcuts (Exchange Archiving General setting)	236
	Do not archive pending reminders (Exchange Archiving General setting)	237
	Inherited permissions (Exchange Archiving General setting)	237
	Maximum message size to archive in MB (Exchange Archiving General setting)	237
	Pending shortcut timeout (Exchange Archiving General setting)	237
	Set failed messages 'Do Not Archive' (Exchange Archiving General setting)	238
	Strip attachments to non-shortcut items (Exchange Archiving General setting)	238
Chapter 11	Advanced SMTP policy settings	239
	Editing advanced SMTP policy settings	239
	Journal Reports settings	240
	ClearText copies of RMS Protected items (Advanced SMTP policy setting)	240
	Journal report processing (Advanced SMTP policy setting)	241
Chapter 12	Site properties advanced settings	242
	About site properties advanced settings	242
	Editing site properties advanced settings	242

	How to apply new settings for site properties	243
	Site properties advanced settings	243
	Content Conversion (site properties advanced settings)	243
	File System Archiving (site properties advanced settings)	252
	IMAP (site properties advanced settings)	253
	Indexing (site properties advanced settings)	254
	SQL Server (site properties advanced settings)	259
	SMTP (site properties advanced settings)	259
	Storage (site properties advanced settings)	261
Chapter 13	Computer properties advanced settings	263
	About computer properties advanced settings	263
	Editing computer properties advanced settings	263
	How to apply new settings for computer properties	264
	Computer properties advanced settings	264
	Agents (computer properties advanced settings)	264
	IMAP (computer properties advanced settings)	265
	Indexing (computer properties advanced settings)	266
	Storage (computer properties advanced settings)	278
Chapter 14	Task properties advanced settings	281
	Editing task properties advanced settings	281
	Advanced SMTP Archiving task properties	281
	Checkpoint interval for the SMTP Archiving task	282
	Frequency to update SMTP Archiving task Summary Report	282
	Maximum occurrences of unchanged checkpoints	282
Chapter 15	Advanced Personal Store Management properties	283
	About the advanced Personal Store Management properties settings	283
	Editing the advanced Personal Store Management properties settings	283
	PST Message Sampling (Personal Store Management properties advanced settings)	284
	Change migration state percentage (Personal Store Management properties advanced settings)	284
	Message type exclude list (Personal Store Management properties advanced settings)	284

Chapter 16	Classification policy advanced settings	285
	Editing the classification policy advanced settings	285
	Classification Settings (Classification Policy advanced settings)	285
	Retention category selection (Classification Policy setting)	286
Chapter 17	Managing the Storage queue	287
	About the Storage queue	287
	How the Storage queue keeps safety copies	288
	Checking how many safety copies are on the Storage queue	288
	Viewing or changing Advanced settings	289
	Changing the Storage queue location	290
	Closing or opening a Storage queue location	291
Chapter 18	Automatic monitoring	292
	About automatic monitoring	292
	Monitoring in Site Properties	293
	About monitoring using Enterprise Vault Operations Manager	294
	Accessing Operations Manager	294
	About monitoring using MOM	295
	Installing MOM	296
	Configuring MOM	296
	About monitoring using SCOM	298
	Setting up SCOM monitoring for Enterprise Vault servers	299
	Using or removing an earlier SCOM management pack	302
	Optional SCOM configuration	303
	Points to note about SCOM monitoring	303
Chapter 19	Managing extension content providers	305
	About extension content providers	305
	Extension content provider properties	306
	Assigning the Extension Content Provider Administrator role	306
	Assigning the Extension Content Provider Application role	306
	Enabling an extension content provider	307
	Viewing the content provider reports	307
Chapter 20	Exporting archives	309
	About the Export Archive wizard	309
	Importing (migrating) exported files	310
	PST configuration files and exported archives	311
	Starting the export with the Export Archive wizard	312

Chapter 21	Enterprise Vault message queues	314
	Accessing Enterprise Vault message queues	314
	MSMQ queue summary	315
	Exchange Mailbox task queues	317
	Notes on the Exchange Mailbox task queues	319
	Exchange Journaling task queues	320
	Notes on the Exchange Journaling task queues	321
	Exchange Public Folder task queues	322
	Notes on the Exchange Public Folder task queues	323
	Retrieval queues	324
	Notes on the retrieval queues	325
	Storage service queues	326
	Notes on the Storage service queues	327
Chapter 22	Customizations and best practice	328
	Mailbox archiving strategies	328
	About mailbox archiving strategies	328
	Notes on archiving based on age	329
	Notes on archiving based on quota or age and quota	329
	Notes on archiving items from Exchange managed folders	334
	Archiving items only if they have attachments	339
	How to customize the Enterprise Vault settings for a journal mailbox	340
	Disabling archiving for mailboxes	341
	Public folder archiving best practice	342
	About performance tuning	343
	Moving the Windows Temp folder	344
	Improving performance on Storage service computers	344
Chapter 23	Auditing	347
	About auditing	347
	Recommended practice when configuring auditing	348
	Creating the auditing database	349
	Configuring audit categories	350
	Starting or stopping auditing	353
	Viewing the audit log	353
	Converting archive permissions to text	354
	Tuning auditing	355
	Modifying the connection pool sizes	355

Chapter 24	Failover in a building blocks configuration	357
	About Enterprise Vault services in building blocks configurations	357
	Extra requirements for building blocks	358
	Updating service locations after failover	359
	Additional actions after failover for SMTP Archiving	360
Appendix A	Ports used by Enterprise Vault	362
	About the ports used by Enterprise Vault	362
	Firewall settings for Enterprise Vault programs	362
Appendix B	Useful SQL queries	367
	About the SQL queries	367
Appendix C	Troubleshooting	368
	Installation problems	368
	Enterprise Vault servers: installation problems	368
	Desktop clients: installation problems	369
	Microsoft SQL Server problems	369
	Error: ODBC SQL Server Driver Connection is Busy	370
	Number of SQL Server licenses exceeded	370
	How to reset passwords after moving an Enterprise Vault database	371
	Server problems	371
	Fixing errors when opening MSMQ dead letter queue	372
	Client problems	372
	Problems logging on to the Enterprise Vault Web Access application	372
	MAPISVC.INF problems (client)	373
	Problems seen by Enterprise Vault users	374
	Problems enabling or processing mailboxes	375
	Checking the Enterprise Vault system mailbox	376
	Problems with Vault Cache synchronization	377
	Viewing the Vault Cache Diagnostics page	377
	About Vault Cache Diagnostics	377
	Advanced use of Vault Cache Diagnostics	379
	Exporting results	379
	Client synchronization status text	380
	Identifying and resolving Vault Cache issues on the Enterprise Vault server	383
	Identifying and resolving Vault Cache issues on an end-user computer	385

Examining IIS log files	388
Problems with Enterprise Vault components	390
Troubleshooting: All tasks and services	391
Troubleshooting: File System Archiving	393
Troubleshooting: Directory service	394
Troubleshooting: Exchange archiving or Journaling tasks	396
Troubleshooting: Restoring items	399
Troubleshooting: Indexing	399
Troubleshooting: Storage service	400
Troubleshooting: Shopping service	403
Troubleshooting: Web Access application	406
Troubleshooting: Enterprise Vault Operations Manager and the Monitoring database	407
Troubleshooting: Enterprise Vault Reporting and FSA Reporting	408
Specific problems	408
Restoring items for users	411
Techniques to aid troubleshooting	411
Veritas Quick Assist	412
Running on Demand: Run Now	412
Use the Exchange mailbox archiving reports	413
Moved Items report from the Exchange Mailbox task	413
Running DTrace from the Administration Console	414
Using the Deployment Scanner	415
Creating a mail message that contains the Outlook Add-In log	416
How to modify registry settings	417
About moving an Indexing service	420
Notes on the Indexing data structure of the Vault Directory database	421
Moving the Indexing service	421
Appendix D Enterprise Vault accounts and permissions	425
About accounts and permissions	425
Index	426

About this guide

This chapter includes the following topics:

- [Required knowledge](#)
- [Where to get more information about Enterprise Vault](#)

Required knowledge

To administer Enterprise Vault, you need a working knowledge of the following:

- Windows Server administrative tasks
- Microsoft SQL Server
- Microsoft Message Queue Server
- Internet Information Services (IIS)
- Your archive storage hardware and software

If you intend to use Enterprise Vault with Domino server, Microsoft Exchange, or Microsoft SharePoint, you also require 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
Veritas Enterprise Vault Documentation Library	<p>Includes all the following documents in Windows Help (.chm) format so that you can search across them all. It also includes links to the guides in Acrobat (.pdf) format.</p> <p>You can access the library in several ways, including the following:</p> <ul style="list-style-type: none"> ■ In Windows Explorer, browse to the <code>Documentation\language</code> subfolder of the Enterprise Vault installation folder, and then open the <code>EV_Help.chm</code> file. ■ On the Help menu in the Administration Console, click Help on Enterprise Vault.
<i>Introduction and Planning</i>	Provides an overview of Enterprise Vault functionality.
<i>Deployment Scanner</i>	Describes how to check the required 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 Domino Server Archiving</i>	Describes how to archive items from Domino mail files and journal databases.
<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 File System Archiving</i>	Describes how to archive the files that are held on network file servers.
<i>Setting up IMAP</i>	Describes how to configure IMAP client access to Exchange archives and Internet mail archives.
<i>Setting up SMTP Archiving</i>	Describes how to archive SMTP messages from other messaging servers.
<i>Setting up SharePoint Server Archiving</i>	Describes how to archive content from Microsoft SharePoint servers.
<i>Administrator's Guide</i>	Describes how to perform day-to-day administration procedures.

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

Document	Comments
<i>Backup and Recovery</i>	Describes how to implement an effective backup strategy to prevent data loss, and how to provide a means for recovery in the event of a system failure.
<i>Classification</i>	Describes how to assign classification values to the metadata properties of all new and existing archived items. Users of applications such as Enterprise Vault Search and Compliance Accelerator can then use the classification values to filter the items when they conduct searches or reviews.
<i>NSF Migration</i>	Describes how to migrate content from Domino and Notes NSF files into Enterprise Vault archives.
<i>PST Migration</i>	Describes how to migrate content from Outlook PST files into Enterprise Vault archives.
<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>PowerShell Cmdlets</i>	Describes how to perform various administrative tasks by running the Enterprise Vault PowerShell cmdlets.
<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.veritas.com/docs/000097605>

Enterprise Vault training modules

The Enterprise Vault and eDiscovery Tech Center (<http://www.veritas.com/elibrary>) is an eLibrary of self-paced learning modules developed around key features, best practices, and common technical support questions.

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

Managing administrator security

This chapter includes the following topics:

- [About administrator security](#)
- [Roles-based administration](#)
- [Using permissions to control access](#)
- [Changing the vault service account](#)

About administrator security

Enterprise Vault provides the following mechanisms to control the abilities of Enterprise Vault administrators:

Roles-based administration (RBA)

Many administrative tasks do not require all the permissions that are associated with the vault service account. Enterprise Vault's pre-defined RBA roles provide individual administrators with exactly the permissions that are required to perform their individual administrative tasks.

You can assign individuals or groups to roles that match their responsibilities, and they are then able to perform the tasks that are included in those roles. Because the permissions are associated with roles rather than individual administrators, you can control the role permissions without having to edit the permissions for each administrator.

The following role types exist:

- An administrator role typically limits your abilities by functional area, such as Messaging, Exchange, or Storage. Enterprise Vault provides several predefined administrator roles, which restrict your access within the Administration Console to the containers and commands that relate to a functional area. These roles also limit what you can see when you use Enterprise Vault Operations Manager and Enterprise Vault Reporting.
- An application role typically lets you perform the operations that are required to run a particular Enterprise Vault application. Application roles are not intended to control access to the Administration Console.
- The task role enables an account other than the vault service account to run Exchange Server tasks.

Admin permissions You can grant or deny access to the following containers in the Administration Console tree:

- File Servers
- Exchange
- Domino
- SharePoint
- Enterprise Vault Servers

You can control access to the Administration Console by assigning administrator roles, or by using admin permissions, or both.

Roles-based administration

Enterprise Vault's pre-defined RBA roles are associated with operations and tasks that assigned administrators are allowed to execute.

- An operation is a low-level permission that represents a privileged action or capability. When the Administration Console determines whether a role has

access to perform a task, it is the operations associated with the role that are checked.

Operations with names prefixed by "{STO}" or "{DIR}" are internal operations that do not affect the Administration Console display. Other, external operations control the view of the Administration Console that an administrator sees.

- A task is a group of operations that collectively provide sufficient permissions to do a particular job.

A role is a collection of tasks and, possibly, operations and other roles.

About the predefined roles

You can use the predefined roles as supplied, customize them, or create new roles, as required.

By assigning roles you can adjust the permissions of individual administrators to match their job responsibilities. The mechanism is flexible enough for you to be able to modify an individual's role to cope with any change in responsibility.

Table 2-1 Predefined administrator roles

Role	Description
Domino Administrator	Responsible for the day-to-day administration of Domino archiving, including NSF migration. In Enterprise Vault Operations Manager, can view Domino information and parameters. By default, users who are assigned to this role also acquire the permissions that are associated with the following roles: <ul style="list-style-type: none"> ■ IMAP Administrator ■ NSF Administrator ■ Search Administrator
Exchange Administrator	Responsible for the day-to-day administration of Exchange Server archiving. In Enterprise Vault Operations Manager, can view Exchange Server information and parameters. By default, users who are assigned to this role also acquire the permissions that are associated with the following roles: <ul style="list-style-type: none"> ■ IMAP Administrator ■ Search Administrator
Extension Content Provider Administrator	Has a view of the Administration Console interface that concentrates on those components that are required for the day-to-day administration of extension content providers.

Table 2-1 Predefined administrator roles (*continued*)

Role	Description
File Server Administrator	Responsible for the day-to-day administration of File System Archiving. By default, users who are assigned to this role also acquire the permissions that are associated with the following role: <ul style="list-style-type: none"> ■ Search Administrator
IMAP Administrator	Responsible for the day-to-day administration of IMAP. By default, users who are assigned to this role also acquire the permissions that are associated with the following role: <ul style="list-style-type: none"> ■ Search Administrator
Indexing Administrator	Has a view of the Administration Console interface that concentrates mainly on those components that are required to keep indexing running properly. This administrator does not have access to archiving policy settings for the various targets.
Messaging Administrator	Responsible for the day-to-day administration of Exchange Server and Domino archiving. This administrator does not have access to other parts of the product, such as File System Archiving or SharePoint archiving. By default, users who are assigned to this role also acquire the permissions that are associated with the following roles: <ul style="list-style-type: none"> ■ Domino Administrator ■ Exchange Administrator
NSF Administrator	Has a view of the Administration Console interface that concentrates on those components that are required to manage NSF files. In Enterprise Vault Operations Manager, can view Domino information and parameters.
Power Administrator	Can perform all the tasks in the other predefined administrator roles. Cannot perform reconfiguration tasks such as changing the vault service account or Directory SQL server. By default, users who are assigned to this role also acquire the permissions that are associated with the following roles: <ul style="list-style-type: none"> ■ Exchange Administrator ■ Extension Content Provider Administrator ■ Indexing Administrator ■ SMTP Administrator

Table 2-1 Predefined administrator roles (*continued*)

Role	Description
PST Administrator	Has a view of the Administration Console interface that concentrates on those components that are required to manage personal stores. In Enterprise Vault Operations Manager, can view and manage Exchange Server information and parameters.
Search Administrator	Responsible for the day-to-day administration of the Enterprise Vault Search application: defining search policies, setting up search provisioning groups, and creating and configuring Client Access Provisioning tasks.
SharePoint Administrator	Has a view of the Administration Console interface that concentrates on those components that are required to manage SharePoint archiving. By default, users who are assigned to this role also acquire the permissions that are associated with the following role: <ul style="list-style-type: none"> ■ Search Administrator
SMTP Administrator	Responsible for the day-to-day administration of SMTP archiving. By default, users who are assigned to this role also acquire the permissions that are associated with the following role: <ul style="list-style-type: none"> ■ Search Administrator
Storage Administrator	Has a view of the Administration Console interface that concentrates mainly on those components that are required to keep storage running properly. This administrator does not have access to archiving policy settings for the various targets. By default, users who are assigned to this role also acquire the permissions that are associated with the following role: <ul style="list-style-type: none"> ■ Indexing Administrator

Table 2-2 Predefined task role

Role	Description
Task Applications	This role provides access to archives to allow an account other than the vault service account to run Exchange Server tasks. Enterprise Vault grants this role automatically when you configure an Exchange Server task to run under an account other than the vault service account.

Table 2-3 Predefined application roles

Role	Description
Extension Content Provider Application	<p>This role allows a third-party application to act as an extension content provider. The role allows the application to create, delete, read, and update extension content provider entries and to store items into any archive.</p> <p>In Enterprise Vault Operations Manager, can view all information and parameters.</p> <p>This role does not enable full update access to all extension content provider properties. For example, an extension content provider application cannot enable or disable itself and cannot modify or override its own schedule.</p> <p>This role does not allow access to the Administration Console. The role is intended to be for an extension content provider application, not for an administrator.</p>
Monitoring Application	Able to query the state of Enterprise Vault tasks.
Placeholder Application	Able to run the FSAUndelete utility. This role enables the undeletion of items from archives.

Roles and the Enterprise Vault Administration Console

[Table 2-4](#) shows the Administration Console features and actions that are available to the supplied administrator roles.

Note: The predefined Placeholder Application role does not allow access to the Administration Console.

Table 2-4 Administration Console features and actions

Role	Administration Console containers available	Administration Console actions available
Domino Administrator	<ul style="list-style-type: none"> ■ Targets: Domino ■ Policies: Domino; Retention and Classification ■ Services: Task Controller ■ Tasks: Domino Mailbox Archiving; Domino Journaling; Domino Provisioning ■ Archives: Domino Mailbox; Domino Journal 	<ul style="list-style-type: none"> ■ Enable Mailbox ■ Disable Mailbox ■ Site Property tabs: General; Archiving Settings; Site Schedule; Records ■ Advanced Features ■ Domino forms ■ Classification
<p>By default, this role also provides access to the Administration Console containers and actions that are available to the following roles:</p> <ul style="list-style-type: none"> ■ IMAP Administrator ■ NSF Administrator ■ Search Administrator 		
Exchange Administrator	<ul style="list-style-type: none"> ■ Targets: Exchange ■ Policies: Exchange; Retention and Classification ■ Services: Task Controller ■ Tasks: Mailbox Archiving; Public Folder; Exchange Journaling; Exchange Provisioning ■ Archives: Exchange Journal; Exchange Mailbox; Public Folder; Shared 	<ul style="list-style-type: none"> ■ Enable Mailbox ■ Disable Mailbox ■ Site Property tabs: General; Archiving Settings; Site Schedule; Records ■ Advanced Features ■ Exchange Message Classes ■ Classification
<p>By default, this role also provides access to the Administration Console containers and actions that are available to the following roles:</p> <ul style="list-style-type: none"> ■ IMAP Administrator ■ Search Administrator 		

Table 2-4 Administration Console features and actions (*continued*)

Role	Administration Console containers available	Administration Console actions available
Extension Content Provider Administrator	<ul style="list-style-type: none"> ■ Extensions: All extensions operations except for creation ■ Archives: Shared archives and custom archives ■ Policies: Retention and Classification 	<ul style="list-style-type: none"> ■ Site Property tabs: Site Schedule; Records ■ Manage Extension Content Providers ■ Manage Shared Archives ■ Classification
File Server Administrator	<ul style="list-style-type: none"> ■ Targets: File Server ■ Policies: File Archiving; Retention and Classification ■ Services: Task Controller ■ Tasks: File Server Archiving ■ Archives: File System; Shared 	<ul style="list-style-type: none"> ■ Site Property tabs: General; Archiving Settings; Site Schedule; Records ■ Advanced Features ■ Classification
<p>By default, this role also provides access to the Administration Console containers and actions that are available to the following role:</p> <ul style="list-style-type: none"> ■ Search Administrator 		
IMAP Administrator	<ul style="list-style-type: none"> ■ Client Access: IMAP; Search ■ Policies: IMAP; Search ■ Services: Task Controller ■ Tasks: Client Access Provisioning 	
<p>By default, this role also provides access to the Administration Console containers and actions that are available to the following role:</p> <ul style="list-style-type: none"> ■ Search Administrator 		

Table 2-4 Administration Console features and actions (*continued*)

Role	Administration Console containers available	Administration Console actions available
Indexing Administrator	<ul style="list-style-type: none"> ■ Services: Indexing; Task Controller; Storage ■ Tasks: Indexing ■ Archives: All types of archive ■ Indexing: All Index Servers 	<ul style="list-style-type: none"> ■ Site Property tabs: Indexing; Advanced ■ Advanced Features ■ Manage indexes
Messaging Administrator	<ul style="list-style-type: none"> ■ Targets: Exchange; Domino ■ Policies: Exchange; Domino Journaling; Retention and Classification ■ Services: Task Controller ■ Tasks: Mailbox Archiving; Public Folder; Exchange Journaling; Exchange Provisioning; Domino Mailbox Archiving; Domino Journaling; Domino Provisioning ■ Archives: Journal; Mailbox; Public Folder; Shared 	<ul style="list-style-type: none"> ■ Enable Mailbox ■ Disable Mailbox ■ Site Property tabs: General; Archiving Settings; Site Schedule ■ Import NSF ■ Advanced Features ■ Exchange Message Classes ■ Domino forms
<p>By default, this role also provides access to the Administration Console containers and actions that are available to the following roles:</p> <ul style="list-style-type: none"> ■ Domino Administrator ■ Exchange Administrator 		
NSF Administrator	<ul style="list-style-type: none"> ■ Policies: Domino Mailbox; Domino Desktop; Retention and Classification ■ Archives: Import NSF 	<ul style="list-style-type: none"> ■ Site Property tabs: Records ■ Import NSF ■ Domino forms ■ Classification

Table 2-4 Administration Console features and actions (*continued*)

Role	Administration Console containers available	Administration Console actions available
Power Administrator	<ul style="list-style-type: none"> ■ Targets: All targets ■ Policies: All policies ■ Services: All services ■ Tasks: All tasks ■ Archives: All types of archive ■ Vault stores: All vault stores ■ Indexing: All Index Servers and Index Server groups ■ Personal Store Management: All functions 	<ul style="list-style-type: none"> ■ Enable Mailbox ■ Disable Mailbox ■ Enable Workspace ■ Disable Workspace ■ Site Property tabs: All tabs ■ Manage Indexes ■ Import Archive ■ Export Archive ■ Import NSF ■ Advanced Features ■ Exchange Message Classes ■ Domino forms ■ Classification ■ Update Service Locations
<p>By default, this role also provides access to the Administration Console containers and actions that are available to the following roles:</p> <ul style="list-style-type: none"> ■ Exchange Administrator ■ Extension Content Provider Administrator ■ Indexing Administrator ■ SMTP Administrator 		
PST Administrator	<ul style="list-style-type: none"> ■ Policies: PST Migration; Retention and Classification ■ Services: Task Controller ■ Tasks: Mailbox Archiving; PST Locator; PST Collector; PST Migrator ■ Vault stores: All vault stores ■ Personal Store Management: All functions 	<ul style="list-style-type: none"> ■ Site Property tabs: General; Site Schedule; Records ■ Import Archive ■ Export Archive ■ Advanced Features ■ Classification

Table 2-4 Administration Console features and actions (*continued*)

Role	Administration Console containers available	Administration Console actions available
Search Administrator	<ul style="list-style-type: none"> ■ Client Access: Search ■ Policies: Search ■ Services: Task Controller ■ Tasks: Client Access Provisioning 	<ul style="list-style-type: none"> ■ Site Property tab: Search ■ Define Search Provisioning Group ■ Define Search Policy ■ Configure Client Access Provisioning Task
SharePoint Administrator	<ul style="list-style-type: none"> ■ Targets: SharePoint ■ Policies: SharePoint; Retention and Classification ■ Services: Task Controller ■ Tasks: SharePoint ■ Archives: SharePoint; Shared 	<ul style="list-style-type: none"> ■ Enable Workspace ■ Disable Workspace ■ Site Property tabs: General; Archiving Settings; Site Schedule; Records ■ Advanced Features ■ Classification
	<p>By default, this role also provides access to the Administration Console containers and actions that are available to the following role:</p> <ul style="list-style-type: none"> ■ Search Administrator 	
SMTP Administrator	<ul style="list-style-type: none"> ■ Targets: SMTP ■ Policies: SMTP; Retention and Classification ■ Tasks: SMTP Archiving ■ Services: Task Controller ■ Archives: All types of archive 	<ul style="list-style-type: none"> ■ Site Property tabs: General; Archiving Settings; Records ■ Classification
<p>By default, this role also provides access to the Administration Console containers and actions that are available to the following role:</p> <ul style="list-style-type: none"> ■ Search Administrator <p>Note: Accounts that have the SMTP Administrator role must be local administrators on Enterprise Vault servers and on computers on which they run the Administration Console.</p>		

Table 2-4 Administration Console features and actions (*continued*)

Role	Administration Console containers available	Administration Console actions available
Storage Administrator	<ul style="list-style-type: none"> ■ Tasks: Indexing ■ Services: Storage; Indexing; Task Controller ■ Archives: All types of archive ■ Vault stores: All vault stores ■ Indexing: All Index servers and Index Server groups 	<ul style="list-style-type: none"> ■ Site Property tabs: General; Archiving Settings; Site Schedule; Storage Expiry ■ Import Archive ■ Export Archive ■ Advanced Features
<p>By default, this role also provides access to the Administration Console containers and actions that are available to the following role:</p> <ul style="list-style-type: none"> ■ Indexing Administrator 		

Roles-based administration (RBA) and the classification feature

To administer the Enterprise Vault classification feature, you require one or more of the following RBA roles in the Vault Administration Console:

- Domino Administrator
- Exchange Administrator
- Extension Content Provider Administrator
- File Server Administrator
- NSF Administrator
- Power Administrator
- PST Administrator
- SharePoint Administrator
- SMTP Administrator

Roles and Enterprise Vault Operations Manager

Any user other than the Vault Service account must be assigned to a suitable administrator role to access the Enterprise Vault Operations Manager web application. Users can view only the tabs and tables in Operations Manager that are applicable to the role to which they are assigned. The tabs and tables that are available for a role are consistent with the containers that are available to that role in the Administration Console. The Power Administrator role is able to see all the tabs and tables in Operations Manager.

Roles and Enterprise Vault Reporting

Any user other than the Vault Service account must be assigned to a suitable administrator role to access Enterprise Vault Reporting's reports.

The default administrator roles have access to the Enterprise Vault Reporting reports that are appropriate to their role.

For more information on the reports that are available to each role, see the *Reporting* guide.

Note: If you have configured Enterprise Vault Reporting, you must enable the synchronization of Enterprise Vault Reporting roles-based security.

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

Working with predefined RBA roles

Enterprise Vault provides four PowerShell cmdlets that let you manage RBA roles and role membership. All these cmdlets are provided by

`Symantec.EnterpriseVault.PowerShell.AdminAPI.dll`, which is loaded automatically when you run the Enterprise Vault Management Shell.

You must log in using the Vault Service account to use all these cmdlets.

Table 2-5 Cmdlets for managing role membership

Cmdlet	Description
<code>Get-EVRBARole</code>	This cmdlet lists the RBA roles that exist in the Enterprise Vault Directory.
<code>Get-EVRBARoleMember</code>	This cmdlet lists the members of an RBA role.
<code>Add-EVRBARoleMember</code>	This cmdlet adds members to an RBA role.
<code>Remove-EVRBARoleMember</code>	This cmdlet removes members from an RBA role.

The following sections show you how to use the RBA cmdlets to manage Enterprise Vault RBA role membership:

- [Listing RBA roles](#)
- [Listing an RBA role's members](#)
- [Managing RBA role membership](#)

Listing RBA roles

Use `Get-EVRBARole` to list all the RBA roles in the Enterprise Vault Directory. You can list all roles, or specify a full or partial role name to list only matching roles.

For each RBA role, `Get-EVRBARole` lists the following role properties:

- Name. The name of the Enterprise Vault RBA role.
- RoleGuid. The GUID of the Enterprise Vault RBA role.
- TaskLinkDescription. The description of the associated TaskLink.
- TaskLinkGuid. The GUID of the associated TaskLink.

To list RBA roles

- 1 Log in to an Enterprise Vault server using the vault service account.
- 2 Launch the Enterprise Vault Management Shell.
- 3 Run `Get-EVRBARole` to list roles.

For example:

```
Get-EVRBARole -Name ex*
```

In this example, `Get-EVRBARole` lists all RBA roles that contain “ex”, such as “Exchange Administrator” and “Extension Content Provider Administrator”.

Note that the `-EVDirectoryServer` parameter is mandatory but `Get-EVRBARole` determines it automatically if it can.

`Get-EVRBARole` returns objects of type

`Symantec.EnterpriseVault.Admin.EVRbaRole`, which you can use as piped input to other cmdlets.

For more detailed information about running `Get-EVRBARole`, including more examples of its use, enter the following command at the Enterprise Vault Management Shell prompt:

```
Get-Help -full Get-EVRBARole
```

Listing an RBA role’s members

Use `Get-EVRBARoleMember` to list all the members of an RBA role.

For each RBA role member, `Get-EVRBARoleMember` lists the following role properties:

- Name. The member’s Windows account name. Note that RBA role members can be Active Directory users, groups, or security principals.
- SID. The member’s Windows security identifier.

To list RBA role members

- 1 Log in to an Enterprise Vault server using the vault service account.
- 2 Launch the Enterprise Vault Management Shell.
- 3 Run `Get-EVRBARoleMember` to list role members.

For example:

```
Get-EVRBARoleMember -Identity "File Server Administrator"
```

In this example, `Get-EVRBARoleMember` lists all the members of the “File Server Administrator” role. Note that the `-EVDirectoryServer` parameter is mandatory but `Get-EVRBARoleMember` determines it automatically if it can.

`Get-EVRBARoleMember` returns objects of type

`Symantec.EnterpriseVault.Admin.EVRbaRoleMember`, which you can use as piped input to other cmdlets.

For more detailed information about running `Get-EVRBARoleMember`, including more examples of its use, enter the following command at the Enterprise Vault Management Shell prompt:

```
Get-Help -full Get-EVRBARoleMember
```

Managing RBA role membership

Enterprise Vault provides the `Add-EVRBARoleMember` and `Remove-EVRBARoleMember` cmdlets with which you can manage the members of RBA roles.

You must log in using the vault service account to use these cmdlets.

To add members to an Enterprise Vault RBA role

- 1 Log in to an Enterprise Vault server using the vault service account.
- 2 Launch the Enterprise Vault Management Shell.
- 3 Run `Add-EVRBARoleMember` to add members.

For example:

```
Add-EVRBARoleMember -Identity "File Server Administrator" -Members  
"JohnDoe", "fsaAdmins",  
"S-1-5-21-1529523603-1500826627-74573220-1119"
```

In this example, `Add-EVRBARoleMember` assigns to the “File Server Administrator” role, the user `JohnDoe`, the `fsaAdmins` security group, and another account that is identified by its SID. Note that the `-EVDirectoryServer` parameter is mandatory but `Add-EVRBARoleMember` determines it automatically if it can.

`Add-EVRBARoleMember` either returns no output, or returns the newly modified objects of type `Symantec.EnterpriseVault.Admin.EVRbaRole`, which you can use as piped input to other cmdlets.

To remove members from an Enterprise Vault RBA role

- 1 Log in to an Enterprise Vault server using the vault service account.
- 2 Launch the Enterprise Vault Management Shell.
- 3 Run `Remove-EVRBARoleMember` to remove members.

For example:

```
Remove-EVRBARoleMember -Identity "File Server Administrator"  
-Members "JohnDoe", "fsaAdmins",  
"S-1-5-21-1529523603-1500826627-74573220-1119"
```

In this example, `Remove-EVRBARoleMember` removes from the “File Server Administrator” role, the user `JohnDoe`, the `fsaAdmins` security group, and another account that is identified by its SID. Note that the `-EVDirectoryServer` parameter is mandatory but `Remove-EVRBARoleMember` determines it automatically if it can.

`Remove-EVRBARoleMember` returns no output, or returns the newly modified objects of type `Symantec.EnterpriseVault.Admin.EVRbaRole`, which you can use as piped input to other cmdlets.

For more detailed information about running `Add-EVRBARoleMember` and `Remove-EVRBARoleMember`, including more examples of their use, enter the following commands at the Enterprise Vault Management Shell prompt:

```
Get-Help -full Add-EVRBARoleMember  
Get-Help -full Remove-EVRBARoleMember
```

Customizing RBA roles

If you want to create custom RBA roles, or change the low-level operations that particular roles are allowed to execute, you must first download the RBA store from the Enterprise Vault Directory, in the form of an XML file.

You can then edit the XML to customize the RBA store to suit the requirements of your environment.

When you have made the necessary changes to the RBA store, you can upload it back to the Enterprise Vault Directory.

Enterprise Vault provides two PowerShell cmdlets that let you download and upload the RBA store. These cmdlets are provided by

`Symantec.EnterpriseVault.PowerShell.AdminAPI.dll`, which is loaded automatically when you run the Enterprise Vault Management Shell.

You must log in using the vault service account to use these cmdlets.

Table 2-6 RBA store cmdlets

Cmdlet	Description
<code>Get-EVRBAAzStoreXml</code>	Downloads the RBA store from the Enterprise Vault Directory, to a file called <code>EvAzStore.xml</code> .
<code>Set-EVRBAAzStoreXml</code>	Uploads the RBA store from <code>EvAzStore.xml</code> to the Enterprise Vault Directory.

The following sections show you how to use these cmdlets to download and upload the RBA store:

- [Downloading the RBA store](#)
- [Uploading the RBA store](#)

Downloading the RBA store

Use `Get-EVRBAAzStoreXml` to download the RBA store from the Enterprise Vault Directory. `Get-EVRBAAzStoreXml` writes the RBA store to an XML file called `EvAzStore.xml`, in the location you specify.

To extract the RBA store from the Enterprise Vault Directory

- 1 Log in to an Enterprise Vault server using the vault service account.
- 2 Launch the Enterprise Vault Management Shell.
- 3 Run `Get-EVRBAAzStoreXml` to extract the RBA store.

For example:

```
Get-EVRBAAzStoreXml -FolderPath "C:\EvAzStoreXmlLocation"
-EVDirectoryServer "evserver.example.com"
```

This command uses the `-FolderPath` parameter to specify the location to which `Get-EVRBAAzStoreXml` downloads the RBA store. Note that the `-EVDirectoryServer` parameter is mandatory but `Get-EVRBAAzStoreXml` determines it automatically if it can.

For more detailed information about running `Get-EVRBAAzStoreXml`, including more examples of its use, enter the following command at the Enterprise Vault Management Shell prompt:

```
Get-Help -full Get-EVRBAAzStoreXml
```

Editing the RBA store

For more information about editing the RBA store, see the following article on the Veritas Support website:

<http://www.veritas.com/docs/000076648>

Uploading the RBA store

Use `Set-EVRBAAzStoreXml` to upload the RBA store from `EvAzStore.xml`, from the location you specify to the Enterprise Vault Directory.

To upload the RBA store to the Enterprise Vault Directory

- 1 Log in to an Enterprise Vault server using the vault service account.
- 2 Launch the Enterprise Vault Management Shell.
- 3 Run `Set-EVRBAAzStoreXml` to upload the RBA store.

For example:

```
Set-EVRBAAzStoreXml -FolderPath "C:\EvAzStoreXmlLocation"  
-EVDirectoryServer "evserver.example.com"
```

This command uses the `-FolderPath` parameter to specify the location where `Get-EVRBAAzStoreXml` can find the RBA store, which must be in a file called `EvAzStore.xml`. Note that the `-EVDirectoryServer` parameter is mandatory but `Get-EVRBAAzStoreXml` determines it automatically if it can.

For more detailed information about running `Set-EVRBAAzStoreXml`, including more examples of its use, enter the following command at the Enterprise Vault Management Shell prompt:

```
Get-Help -full Set-EVRBAAzStoreXml
```

Determining your current role entitlements

If you need to find out what your current role is, and which tasks you can perform, you can list the role entitlements.

To determine your current role entitlements

- 1 In the Administration Console, right-click the **Directory** container and, on the shortcut menu, click **Show Roles**.
- 2 If you want to keep a copy of the list, click **Copy to clipboard**. You can then paste the text into a document or mail message as required.
- 3 Click **OK**.

Resetting all roles and assignments

You can use a registry value to reset all the roles and role assignments so that they are the same as they were when installed.

See the description of the `ResetAuthorizationStore` value in the *Registry Values* guide.

Using permissions to control access

When you install or upgrade Enterprise Vault, only the Vault Service account has access to the Administration Console. You can then use the Vault Service account to assign administrative roles as required.

An administrator in any given role has access to all Administration Console containers that are relevant to that role. For example, a Messaging Administrator has access to every Exchange Server and Domino server in the Enterprise Vault Site.

You can assign administrator permissions to grant or deny access to individual containers in the Administration Console. For example, you can grant an administrator access to a single Exchange Server computer.

You can assign permissions to grant or deny access to any of the following Administration Console containers:

- A file server
- An Exchange Server
- A Domino Server
- A SharePoint web application
- An Enterprise Vault server

As soon as you modify a container's permissions, access to that container and its contents is controlled by the list you defined. The only exception to this is that the vault service account always has access.

For example, a Messaging Administrator who does not have access to a particular Exchange Server cannot enable mailboxes on that Exchange Server. This is because the Enable Mailbox wizard does not allow the administrator to list the mailboxes on that Exchange Server.

If you need to return to the state in which all administrators have access to a container, you must delete all entries in the administrator permissions list for that container.

To grant or deny permission to access a container

- 1 Using the Vault Service account, start the Administration Console.
- 2 In the Administration Console, right-click the file server, Exchange Server, SharePoint web application, or Enterprise Vault server to which you want to apply permissions and, on the shortcut menu, click **Properties**.
- 3 Click the **Admin Permissions** tab. The list shows the specific users or groups who have been granted or denied permission to administer this computer.
- 4 If you want to add an entry to the list, click **Add** and then proceed as follows:
 - If you are adding the first entry on the list, there is a warning that adding an entry to the list restricts access to those users with Grant access. Click **OK**.
 - In the Add Users and Groups window, add the users or groups to whom you want to grant or deny access to the container. Click **OK**.
The **Admin Permissions** list now shows the users and groups you have added, with a **Grant** and **Deny** option next to each.
- 5 If you want to remove an entry from the list, click the entry to select it and then click **Remove**.
- 6 For each user and group, select **Grant** to grant access to this container, or **Deny** to deny access to this container, as required.
- 7 If you need to delete an entry from the list
- 8 Click **OK** to close **Admin Properties**.

If you have removed all entries from the list there is a warning that all administrators in a role that allows access to this container now have access. Click **OK**.

Changing the vault service account

If you need to change the vault service account, this section describes how to proceed.

Note: You are recommended not to change the account name if possible, because of the amount of work involved, and the potential for introducing mistakes that take time to rectify.

Before you change the account, ensure that the following apply:

- The new vault service account is part of the Administrators group, with permission Full Control (All), on each Enterprise Vault computer in the Enterprise Vault Site.

- If Exchange Server archiving is implemented, the new account has full permissions on the Microsoft Exchange Server.
- The Microsoft Message Queue security has been set up to grant the Administrators group access to the Enterprise Vault queues.
- The new account has database creator access on the SQL server.
- If you use File System Archiving, you must ensure that the new account has the required permissions and privileges on the following:
 - All target Windows file servers.
 - Other Windows servers on which the FSA Agent is installed: any proxy servers for FSA Reporting and File Blocking agent servers for NetApp filers.

If you do not make the vault service account a member of the local Administrators group on the file server, you must grant the account a set of minimum permissions and privileges. See the appendix “Permissions and privileges required for the vault service account on Windows file servers” in *Setting up File System Archiving*.

For servers on which the FSA Agent is installed, you can use the EVFSASetRightsAndPermissions utility to help you set the required permissions and privileges. See “EVFSASetRightsAndPermissions” in the *Utilities* guide.

- If SharePoint Server archiving is implemented, add the new vault service account to the SharePoint sites, or to the group that contains the old vault service account. The new account must be a local administrator on the SharePoint Servers.

For instructions on how to set permissions for the vault service account, see Enterprise Vault required software and settings in *Installing and Configuring*.

Note the following:

- Always use the Administration Console to specify a new password for the vault service account or to change the vault service account itself. Do not use the Windows Services MMC snap-in to edit the logon credentials for an Enterprise Vault service unless you are instructed to do so.
- If you change only the password of the vault service account, and you have installed the FSA Agent on any computers, you must update the logon credentials that the FSA Agent services use.
 See “Updating the logon credentials of the FSA Agent services” in *Setting up File System Archiving*.

To change the vault service account

- 1 Start the Administration Console as the existing vault service account.
- 2 In the Administration Console, open Directory Properties and click the Service Account tab.

- 3** Change the vault service account details to reference the new account.
- 4** On SharePoint servers, run the Enterprise Vault SharePoint Configuration wizard and specify the new vault service account credentials.
- 5** If you have installed any Enterprise Vault add-ons, you may need to change the vault service account credentials in the add-on. See the documentation that accompanies the add-on for information on how to do this.
- 6** Restart all Enterprise Vault services on all Enterprise Vault servers in the Enterprise Vault Site.
- 7** Restart the Enterprise Vault services on any other computers that have Enterprise Vault services installed. This includes the FSA Agent services on any computers that have the FSA Agent installed.

See the following technical note for a summary of the various accounts and permissions that are required by Enterprise Vault:

<http://www.veritas.com/docs/000040861>

Day-to-day administration

This chapter includes the following topics:

- [Monitoring the system status](#)
- [Monitoring application logs](#)
- [About Exchange mailbox archiving reports](#)
- [Monitoring MSMQ queues](#)
- [About starting or stopping tasks or services](#)
- [Checking logs with the Windows Event Viewer](#)
- [Monitoring journal mailboxes](#)
- [About monitoring disks](#)
- [About maintaining the SQL databases](#)
- [Using SQL AlwaysOn availability groups](#)
- [About managing vault store groups and sharing](#)
- [About managing safety copies](#)
- [About managing partition rollover](#)
- [Recovering deleted items](#)
- [About expiry and deletion](#)
- [Working with retention categories and retention plans](#)
- [About maintaining provisioning groups](#)
- [Enabling archiving for new mailboxes](#)

- [About applying or removing legal holds on selected archives](#)
- [About moving archives](#)
- [Deleting an archive](#)
- [Deleting a vault store](#)
- [Setting a system message](#)
- [About index volumes](#)
- [Moving the directory database](#)
- [Moving a vault store database](#)
- [Moving a fingerprint database](#)
- [Moving the Monitoring database](#)
- [Moving the auditing database](#)
- [Changing the Vault Service account password](#)

Monitoring the system status

Enterprise Vault automatically runs checks to monitor the health of the Enterprise Vault system.

Enterprise Vault displays the results of the checks in the **Status** section of the Administration Console. Check the status results every day and fix any problems that are shown.

To customize the checks for your environment you can do the following:

- 1 Choose which checks to run.
- 2 Modify the levels at which the checks report errors.
- 3 Specify when to run each check.

See [“Monitoring in Site Properties”](#) on page 293.

Monitoring application logs

Messages from the various Enterprise Vault services and tasks go into the event logs on their respective computers. You need to check each of these logs for error messages and take appropriate action as necessary.

When using the Event Viewer, you can filter the messages using the options on the **View** menu.

Table 3-1 shows the event logs that Enterprise Vault uses.

Table 3-1 Enterprise Vault event logging

Event log	Contents
Application Log	The Application log includes Enterprise Vault events that show that components have started or stopped, or that require you to take some corrective action.
Veritas Enterprise Vault	All Enterprise Vault events, except for those from document conversion or from the Veritas Enterprise Vault CryptoModule. Events that are placed in the Application Log also appear in here.
Veritas Enterprise Vault Converters	Events resulting from document conversions.
Veritas Enterprise Vault CryptoModule	Events that the Veritas Enterprise Vault CryptoModule generates. For more information about Enterprise Vault and FIPS 140-2, see the following article on the Veritas Support website: http://www.veritas.com/docs/000002880

About Exchange mailbox archiving reports

Every time the Exchange mailbox archiving task runs, it automatically produces an Exchange mailbox archiving report. The Exchange mailbox archiving task produces the report when it completes its archiving run, or at the daily time you specify if it is configured to archive continuously.

Configuring Exchange mailbox archiving reports

You can configure the following Exchange mailbox archiving report settings:

- The number of reports that Enterprise Vault retains
- The time each day at which Enterprise Vault creates the reports, if the mailbox archiving task archives continuously

To configure Exchange mailbox archiving reports

- 1 Log in to the Enterprise Vault server that hosts the Exchange mailbox archiving task, using the Vault Service account.
- 2 In the Administration Console, open the **Exchange Mailbox Task Properties: Reporting** tab.

- 3 In **Number of reports to keep**, set the number of Exchange mailbox archiving reports that you want Enterprise Vault to retain.

Note: This determines both the number of reports kept for scheduled archiving runs, and the number kept for run-now archiving runs.

- 4 If you have configured the Exchange mailbox archiving task to archive continuously, in **Create report at the following time**, set the time at which you want the Exchange mailbox archiving task to create the report.

This setting has no effect if the Exchange mailbox archiving task does not archive continuously.

Using Exchange mailbox archiving reports

You can open Exchange mailbox archiving reports from the following locations:

- The Exchange mailbox archiving reports web page, which is accessible from the Administration Console, and directly in a web browser
- The `Exchange Mailbox Archiving` folder on the Enterprise Vault server

Using the Exchange mailbox archiving reports web page

To open the Exchange mailbox archiving reports web page, your user account must be assigned the Exchange Administrator role.

See “[Roles-based administration](#)” on page 20.

If you open the Exchange mailbox archiving reports web page locally on the Enterprise Vault server, User Access Control (UAC) might prevent you from seeing the page unless you run your browser with elevated privileges. For more information about UAC, see the following article on the Microsoft website:

<https://technet.microsoft.com/library/cc709691.aspx>

To open the Exchange mailbox archiving reports web page

- 1 Log in to the Enterprise Vault server that hosts the Exchange mailbox archiving task, using an account that is assigned the Exchange Administrator role.
- 2 In the Administration Console, open the **Exchange Mailbox Task Properties: Reporting** tab.
- 3 Click **View reports** to open the Exchange mailbox archiving reports web page.

You can also open the Exchange mailbox archiving reports web page directly at the following URL:

<http://evsrv/EnterpriseVault/ExchangeArchivingReports.aspx?ExchSvr=exsrv>

where:

- *evsrv* is the Enterprise Vault server that hosts the Exchange mailbox archiving task.
- *exsrv* is the Exchange server that the Exchange mailbox archiving task targets.

The Exchange mailbox archiving reports web page contains links to the following reports:

- An HTML progress report for the Exchange mailbox archiving task, if the task is still archiving.
- A brief HTML report for each completed run of the Exchange mailbox archiving task. Note that each brief HTML report contains a link to a detailed HTML version of the report.
- A detailed CSV report for each completed run of the Exchange mailbox archiving task.

If the Enterprise Vault servers in your site target more than one Exchange server, you can use the Exchange mailbox archiving reports site summary page at the following URL:

<http://evsrv/EnterpriseVault/ExchangeArchivingReports.aspx>

In this case, *evsrv* can be any of the Enterprise Vault servers in your site.

This page lists all the Exchange servers targeted in your site, and provides a link to the individual Exchange mailbox archiving reports web page on the Enterprise Vault server that targets each Exchange server.

Using the Exchange mailbox archiving reports on the Enterprise Vault server

The Exchange mailbox archiving task saves reports on the Enterprise Vault server that hosts the task.

The task saves the reports in the `Reports\Exchange Mailbox Archiving` subfolder of the Enterprise Vault installation folder (for example `C:\Program Files (x86)\Enterprise Vault`).

`Reports\Exchange Mailbox Archiving` contains a subfolder for each targeted Exchange server, and each of these folders contains the following subfolders:

- `RunNow`, which contains reports from run-now runs of the mailbox archiving task.
- `Scheduled`, which contains reports from scheduled runs of the mailbox archiving task.

Each of these folders contains a subfolder for each report. The individual report folders are named using the following convention:

RunType_yyyyymmdd_hhmmss

where:

- *RunType* is “RunNow” or “Scheduled”.
- *yyyymmdd_hhmmss* is the date and time the report was created.

Each report folder contains brief reports and detailed reports in HTML format, and detailed reports in CSV format.

Note: The progress report for an Exchange mailbox archiving task that is still archiving, is generated when it is requested from the Exchange mailbox archiving reports web page. It is not stored on disk on the Enterprise Vault server.

Getting more information

For more information about Exchange mailbox archiving reports, see the following technical note on the Veritas Support website:

<http://www.veritas.com/docs/000068569>

Monitoring MSMQ queues

It is important that you monitor MSMQ queues so that you can quickly spot any problems that may occur.

To monitor the performance of the queues:

- ◆ Use the Windows Performance Monitor

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

See “[Accessing Enterprise Vault message queues](#)” on page 314.

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.

About starting or stopping tasks or services

You may want to stop an Enterprise Vault task or service for many possible reasons, such as when you do any of the following:

- Changing tasks, policies, or service settings. For many of the service settings you must stop and restart one or more services before the new settings come into effect. For details of which settings require a restart to take effect, see the help for the property pages of each service and task.
- Changing hardware configurations.
- Reconfiguring a service.
- Troubleshooting.

Starting or stopping tasks

You can start and stop tasks from the Administration Console.

To start a task

- 1 In the left pane of the Administration Console, expand **Enterprise Vault Servers**.
- 2 Expand the name of the computer that runs the task you want to start.
- 3 Click **Tasks**.
The right pane shows the tasks on that computer.
- 4 In the right pane, click the task you want to start.
- 5 Do one of the following:
 - Click **Start the Task** on the toolbar.
 - Right-click the name of the task and then, on the shortcut menu, click **Start**.

To stop a task

- 1 In the left pane of the Administration Console, expand **Enterprise Vault Servers**.
- 2 Expand the name of the computer that runs the task you want to stop.
- 3 Click **Tasks**.
The results pane shows the tasks on that computer.
- 4 In the right pane, click the task you want to stop.
- 5 Do one of the following:
 - Click **Stop the Task** on the toolbar.
 - Right-click the name of the task and, on the shortcut menu, click **Stop**.

Starting or stopping services

You can start and stop services from both the Administration Console and the Windows Service Control manager.

Note that there is a command-line utility, EVservice, with which you can start and stop local and remote Windows services. EVservice is useful if you have a backup procedure that you want to automate. The utility is in the Enterprise Vault program folder (for example `C:\Program Files (x86)\Enterprise Vault`). See the *Utilities* manual for guidelines on how to use it.

To start a service

- 1 In the left pane of the Administration Console, expand **Enterprise Vault Servers**.
- 2 Expand the name of the computer that is running the service that you want to start.
- 3 Click **Services**.
The right pane shows the services on that computer.
- 4 In the right pane, click the service you want to start.
- 5 Do one of the following:
 - Click **Start the Service** on the toolbar.
 - Right-click the name of the service and then, on the shortcut menu, click **Start**.

To stop a service

- 1 In the left pane of the Administration Console, expand **Enterprise Vault Servers**.
- 2 Expand the name of the computer that runs the service you want to stop.
- 3 Click **Services**.
The results pane shows the services on that computer.
- 4 In the right pane, click the service you want to stop.
- 5 Do one of the following:
 - Click the **Stop the Service** button on the toolbar.
 - Right-click the name of the service and then, on the shortcut menu, click **Stop**.

Checking logs with the Windows Event Viewer

Enterprise Vault services and tasks all write their diagnostic logging information to the standard Enterprise Vault Event Log. You can view the event log by using the standard Windows Event Viewer.

The amount of diagnostic logging information output depends on the diagnostic logging level you set for that service or task. Enterprise Vault generates many log entries. You must take some action to make sure that the log files do not grow too large.

The Event Viewer provides the following ways to ensure that the log files are the proper size:

- The default setting for the Event Viewer is for new events to replace old events. This ensures that all events are logged.
- You can specify a length of time to keep all log entries before they can be overwritten.
- You can set a maximum size for the log file, to make sure that the log file contains as much history as you are likely to need.
- You can keep all log entries and clear the log file manually, using the Event Viewer.

If you have purchased a suitable reporting tool, you can use information from the Application Log in your own, customized reports.

For more information on controlling log files, see the Event Viewer Help.

To check logs with the Windows Event Viewer

- 1 Start the Event Viewer (`eventvwr.exe`).
- 2 In the left pane of the Event Viewer, click the **Application** log or one of the Enterprise Vault logs:
 - **Veritas Enterprise Vault**
 - **Veritas Enterprise Vault Converters**
 - **Veritas Enterprise Vault CryptoModule**

The Event Viewer loads the log you selected.

Monitoring journal mailboxes

You can set up Enterprise Vault so that it archives all messages that the Microsoft Exchange Server system sends and receives, provided that the messages are passed to one or more specific Microsoft Exchange journal mailboxes.

The Exchange Journaling task runs continuously, checking for items in journal mailboxes and immediately archiving them. These items are deleted from the mailbox as they are archived and no shortcuts are created.

It is important that you monitor journal mailboxes to make sure that items are archived promptly. It is especially important that you do this if you have suffered some sort of system failure which required a system restart.

If you are running an Exchange Journaling task, messages in the journal mailbox should be archived soon after they arrive in the mailbox.

To check a journal mailbox

- 1 Run Microsoft Exchange Client or Microsoft Outlook.
- 2 Log on to a profile that has access to the journal mailbox.
- 3 Check that there are no messages in the Inbox folder that are older than one day. If there are any messages older than one day, then there is likely to be a problem.
- 4 Look in the following folders, which are under the Enterprise Vault Exchange Journaling Task folder:

Above maximum size Contains messages that exceed the maximum size that is set in the Exchange journaling policy.

Failed Codepage nnn To fix the problem, do one of the following:

- Install the missing codepage.
- Use the default ANSI codepage (ACP codepage).

These tasks are described below.

When you have set up codepages correctly, move the failed messages back to the Journal Inbox so that they are processed again.

Failed DL Expansion Contains the items that cannot be archived because Enterprise Vault is unable to expand their distribution lists.

Failed External Filter Contains the messages that cannot be processed by a custom filter.

Check the Enterprise Vault Event Log to determine the cause of the problem.

Also check that the rule set file references the correct XML schema.

Failed to copy	<p>Contains the messages that are probably corrupt. Try dragging them to your desktop and then, when they are on the desktop, double-clicking them.</p> <p>You may find that the messages are now not corrupt. If you drag them from your Desktop to the Inbox folder, the Exchange Journaling task tries to archive them again. Remember to delete the corrupt versions from the Failed to copy folder.</p>
Failed to store	<p>Contains the messages that cannot be archived. They probably failed because of a problem with the Storage service. You can move all these items back to the Inbox folder and the Exchange Journaling task tries again to archive them.</p>
Invalid Journal Report	<p>Contains messages whose journal report (P1 envelope message) does not conform to Microsoft's specification.</p>

To add the codepage

- 1 Install the required codepage on the Exchange Journaling task computer.
- 2 To prevent a similar problem from happening on Exchange Mailbox task computers, install the codepage on each Exchange Mailbox task computer.
- 3 If you use a building blocks configuration, repeat the changes on every Enterprise Vault server in your site.

Use the default ANSI codepage (ACP codepage)

Enterprise Vault has a list of codepages in the file `CodePages.txt`, which is installed in the Enterprise Vault program folder (for example `C:\Program Files (x86)\Enterprise Vault`).

You can force Enterprise Vault to use the default ANSI codepage (ACP codepage) by deleting the appropriate codepage entry from the file. If you find that the ACP codepage does not give you good conversions, replace the entry in `Codepages.txt` and install the missing codepage.

To delete a codepage entry

- 1 Edit `CodePages.txt` on the Exchange Journaling task computer to remove the entry for the codepage that caused the problem.
- 2 To prevent a similar problem happening on Exchange Mailbox task computers, make the same change to `CodePages.txt` on each Exchange Mailbox task computer.
- 3 If you use a building blocks configuration, repeat the change on every Enterprise Vault server in your site.

About monitoring disks

You need to check that there is enough free space on the disks that contain the vault stores and indexes. Just how much space you need depends on your use of Enterprise Vault. However, during the course of monitoring, you will quickly get used to the rate at which the various Enterprise Vault databases consume disk space.

Checking disk space for vault stores

You must ensure that there is enough disk space for the vault store databases. When your Enterprise Vault installation has reached its normal running state, you can estimate the rate at which disk space is consumed and so be able to plan accordingly.

If a disk is running out of space, you can use SQL Enterprise Manager to create a new SQL device on another disk and then expand the database on to the new device.

How the Admin service monitors disk space

The Admin service runs automatically when any other Enterprise Vault service starts.

The main task of the Admin service is to monitor 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 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 stops all Enterprise Vault services.

Stopping Enterprise Vault before problems arise helps to maintain its stability. However, it is important to watch the Application Log for Enterprise Vault messages so that you can take corrective action as necessary.

[Table 3-2](#) describes the thresholds that the Admin service uses.

Table 3-2 Admin service thresholds

Check	Warning threshold	Critical threshold	Example of message
Free space on local hard disks	95% full	99% full	<ul style="list-style-type: none"> ■ Warning message: The system is running out of disk space on drives C: and D: - delete any unwanted files. Enterprise Vault will be shut down when 99% of the disk space is used. ■ Critical message: Insufficient disk space is available on drive C: for Enterprise Vault to run. Enterprise Vault will now be shut down; to correct this problem, delete any unwanted files and restart Enterprise Vault.
Virtual memory	90% of limit	95% of limit	<ul style="list-style-type: none"> ■ Warning message: The system is running out of Virtual Memory - free memory by closing any unwanted applications. Enterprise Vault will be shut down when 95% of Virtual Memory is used.

Modifying the Admin service

You do not normally need to make any changes to the Admin service. However, there may be occasions when you want to turn off or modify the monitoring. For example, you may have a disk on the system that is nearly full but that Enterprise Vault does not use. The Admin service monitors all local disks, so it may stop Enterprise Vault even though Enterprise Vault has enough space. In such circumstances you probably want to stop monitoring the disk.

Note: Do not stop the Admin service unnecessarily. Enterprise Vault requires the Admin service to be present at all times. If you do stop the Admin service, all the other Enterprise Vault services on the same computer stop as well. Also, if you start one of the other services and the Admin service is not running, the Admin service automatically starts.

To pause monitoring by the Admin service

- 1 In the Windows Control Panel, double-click **Services**.
- 2 In the list of services, click **Enterprise Vault Admin Service**.
- 3 On the **Action** menu, click **Pause**.

To resume monitoring, click **Resume** on the **Action** menu.

To modify the behavior of future instances of the Admin service

- 1 In the Windows Control Panel, double-click **Services**.
- 2 In the list of services, double-click **Enterprise Vault Admin Service**.
- 3 If the Admin service is running, click **Stop**, and then click **Yes** when prompted to stop other Enterprise Vault services.
- 4 In the **Start Parameters** box, type the parameters to use.

To specify the disks that the Admin service should monitor. By default, the service monitors all local hard disks.

Type the following start parameter:

/DISKS[=list]

where list specifies one or more disks to monitor. Do not include any spaces or tabs in the list. The colon (:) in the disk name is optional.

For example, to monitor disks C, E, and F only, type either of the following:

/DISKS=C:E:F:

/DISKS=CEF

To make this apply every time the Admin service starts, add the **/SAVE** parameter as follows:

/DISKS=C:E:F: /SAVE

/DISKS=CEF /SAVE

To monitor all disks (this restores the default behavior), type the following:

/DISKS

To turn off monitoring for the instance of the Admin service that will start when you click **Start** in the Services control panel.

Type the following start parameter:

/NOMONITOR

To turn off monitoring every time the Admin service starts.

Type the following start parameter:
/NOMONITOR /SAVE

To turn on monitoring for the instance of the Admin service that will start when you click **Start** in the Services control panel.

Type the following start parameter:
/MONITOR

To turn on monitoring every time the Admin service starts.

Type the following start parameter:
/MONITOR /SAVE

To apply the changes every time the Admin service starts.

Type the following start parameter:
/SAVE

For example, to monitor disks E and F every time the Admin service starts, type the following:

/DISKS=EF /SAVE

- 5 Click **Start** to start the Admin service.
- 6 Start other Enterprise Vault services as necessary.

Disk space and indexes

If you are running out of disk space for indexes, you can create new index locations for the Indexing service to use to store its indexes. You can add more locations if needed. When you add a new location, the Indexing service may choose to use it when creating indexes for a new archive. If you want to force the Indexing service to use a particular location, use Close Location to close all the other locations, thus leaving just one location open.

Enterprise Vault does not create new indexes in a closed location or update existing indexes that are in a closed location. Enterprise Vault automatically creates new indexes in an open location, as required.

About maintaining the SQL databases

You can use Microsoft SQL Enterprise Manager to maintain all the Enterprise Vault databases, but if you have other tools that you prefer to use, you can use those instead. For more information on using Microsoft SQL Enterprise Manager, see the Microsoft SQL Server documentation.

Back up all the databases as part of a planned backup procedure. Depending on your procedures, you may decide to truncate the transaction logs after each database has been backed up.

For more information, see the *Backup and Recovery* guide.

You may find that the transaction logs do not need all the disk space that has been allocated to them. If so, you can shrink them to some suitable size. Do not do this until you are sure that you have understood the disk space requirements for the transaction logs.

Vault store database maintenance

Monitor the amount of allocated space that the vault store databases and transaction logs have used, and take appropriate action as necessary.

The initial size of each vault store database is as follows:

Data device	100 MB
Transaction log	80 MB
Total	180 MB

The vault store database components are named as follows:

Database name	EVVSwaultstore_ <i>n</i>
Data device name	EVVSwaultstore_ <i>n</i>
Log device name	EVVSwaultstore_ <i>n</i> LOG

The variables in the names are as follows:

- *vaultstore* is the name of the vault store, with any spaces removed.
- *n* is an internally generated integer, which ensures that the database name is unique across an Enterprise Vault site.

Directory database maintenance

The directory database contains the configuration information for Enterprise Vault. The initial size for the data device of 10 megabytes was chosen to support 10,000 archives. This database is not likely to increase much in size.

The initial size of the directory database is as follows:

Data device	10 MB
-------------	-------

Transaction log	25 MB
Total	35 MB

The directory database components are named as follows:

Database name	EnterpriseVaultDirectory
Data device name	VaultDev
Log device name	VaultLog

Fingerprint database maintenance

Each vault store group has a fingerprint database. One possible exception is the Default Upgrade Group, which Enterprise Vault creates if you previously upgraded to Enterprise Vault 8.0. The Default Upgrade Group does not have a fingerprint database until you configure sharing for it.

The total initial disk space requirement is 212 MB.

The fingerprint database holds information about each Enterprise Vault single instance storage part (SIS part) that is stored in the group's vault stores. In addition to the primary filegroup, a fingerprint database has 32 non-primary filegroups, which hold the information about the SIS parts.

If you share items using Enterprise Vault single instance storage, Enterprise Vault generates a large amount of SIS part data. The non-primary filegroups may therefore grow very rapidly in size. To ensure acceptable archiving and retrieval performance, you must locate the non-primary filegroups appropriately for the amount of sharing in the vault store group. You can configure the filegroup locations when you create the vault store group, or when you configure sharing for the Default Upgrade Group.

See "Creating vault store groups" and "Configuring sharing for a vault store group" in *Installing and Configuring*.

To add or change the filegroup locations after the fingerprint database is configured is a SQL Server administration task. See your Microsoft SQL Server documentation for details.

The initial size of the fingerprint database is as follows:

Primary filegroup	100 MB
Non-primary filegroups	32 MB (1 MB for each of the 32 non-primary filegroups)
Transaction log	80 MB

Total 212 MB

The fingerprint database components are named as follows:

Database name	EVVSGvaultstoregroup_ <i>n</i> _ <i>m</i>
Data device name	EVVSGvaultstoregroup_ <i>n</i> _ <i>m</i>
Log device name	EVVSGvaultstoregroup_ <i>n</i> _ <i>m</i> LOG

The variables in the names are as follows:

- *vaultstoregroup* is the name of the vault store group, with any spaces removed.
- *n* and *m* are internally generated integers.

Monitoring database maintenance

The Monitoring database contains the data that is gathered by the Enterprise Vault Monitoring agents. The data is used by Enterprise Vault Operations Manager, and in some of the reports generated by Enterprise Vault Reporting.

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

The initial size of the Monitoring database is as follows:

Data device	100 MB
Transaction log	80 MB
Total	180 MB

The Monitoring database components are named as follows:

Database name	EnterpriseVaultMonitoring
Data device name	EnterpriseVaultMonitoring_Data
Log device name	EnterpriseVaultMonitoring_Log

FSA Reporting database maintenance

Enterprise Vault creates at least one FSA Reporting database if you configure FSA Reporting. The data is used in the Data Analysis reports that FSA Reporting generates.

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

Using SQL AlwaysOn availability groups

Enterprise Vault supports SQL AlwaysOn availability groups. You can use the procedures described in this chapter to implement availability groups in your Enterprise Vault environment.

Enterprise Vault's PowerShell cmdlets

Enterprise Vault provides the following PowerShell cmdlets, which you can use during the implementation of AlwaysOn availability groups in your Enterprise Vault environment:

- `Get-EVDatabaseDetail`: gets information about the configuration of Enterprise Vault databases.
- `Set-EVDatabaseDetail`: lets you reconfigure Enterprise Vault to connect to its databases after you have added them to an availability group.

Both these cmdlets are used in the procedures described in this chapter.

To run these cmdlets, first run the Enterprise Vault Management Shell, then load `EnterpriseVault.PowerShell.Core.dll` which makes the cmdlets available in the shell.

To load EnterpriseVault.PowerShell.Core.dll

- 1 Run the Enterprise Vault Management Shell.
- 2 In the Enterprise Vault Management Shell, run the following command:

```
Import-Module .\Symantec.EnterpriseVault.PowerShell.Core.dll
```

When you have loaded the module, help is available for the cmdlets. For example, the following command shows the detailed help for `Get-EVDatabaseDetail`:

```
Get-Help Get-EVDatabaseDetail -detailed
```

Implementing SQL AlwaysOn availability groups

[Table 3-3](#) introduces the procedures you must complete to use availability groups in your Enterprise Vault environment. You must complete these procedures in the order shown.

Table 3-3 Implementing SQL AlwaysOn availability groups

Step	Task	See this section for more details
Step 1	Upgrade to Enterprise Vault 12, which is the first version to support SQL AlwaysOn availability groups. You can use the procedures in this section only after you have upgraded.	See “Upgrading to Enterprise Vault 12” on page 60.
Step 2	Stop all Enterprise Vault services, to ensure that Enterprise Vault does not write changes to the databases while you set up your availability group.	See “Stopping Enterprise Vault services” on page 60.
Step 3	Deploy an availability group to support your Enterprise Vault environment.	See “Deploying a SQL AlwaysOn availability group” on page 60.
Step 4	Find the configuration of your existing Enterprise Vault databases.	See “Finding existing database configuration using Get-EVDatabaseDetail” on page 61.
Step 5	Reconfigure Enterprise Vault to connect to its databases, using the availability group’s listeners.	See “Reconfiguring Enterprise Vault using Set-EVDatabaseDetail” on page 62.
Step 6	Restart all Enterprise Vault services.	See “Starting Enterprise Vault services” on page 63.

Upgrading to Enterprise Vault 12

Enterprise Vault 12 introduces support for SQL AlwaysOn availability groups. To implement AlwaysOn availability groups in your Enterprise Vault environment, you must first upgrade Enterprise Vault 12.

To upgrade to Enterprise Vault 12, follow the instructions in *Upgrading to Enterprise Vault 12*.

Stopping Enterprise Vault services

Before you implement AlwaysOn availability groups in your Enterprise Vault environment, stop all Enterprise Vault services on all your Enterprise Vault servers to ensure that no database changes are made during the implementation.

Deploying a SQL AlwaysOn availability group

When you have stopped all Enterprise Vault services in your environment, you can deploy a SQL AlwaysOn availability group.

You can retain the SQL server that hosts the Enterprise Vault databases, and it can become primary server in an availability group.

Deploy one or more additional SQL servers and, using SQL's management tools, create a new availability group containing the primary server and any additional servers.

Back up all your Enterprise Vault databases, then add to the new availability group all the databases that you want to belong to it.

Finding existing database configuration using `Get-EVDatabaseDetail`

`Get-EVDatabaseDetail` provides details of Enterprise Vault databases, which can be useful when you implement an AlwaysOn availability group to support your Enterprise Vault environment.

Initially, you can use `Get-EVDatabaseDetail` to list details of all your Enterprise Vault databases, including which SQL instance each uses, before you add them to the new availability group.

For example, use the following procedure to list details of all Enterprise Vault databases.

To list details of all Enterprise Vault databases

- 1 In the Enterprise Vault Management Shell, run the following command:

```
Import-Module .\Symantec.EnterpriseVault.PowerShell.Core.dll
```

- 2 Run the following command:

```
Get-EVDatabaseDetail
```

For each database, this produces output like the following:

```
IsCollationOK      : True
IsInAG              : False
IsAccessible       : True
DBName              : EnterpriseVaultAudit
SQLInstanceName    : evsql
SQLServerVersion   : 11.0.3128.0
Type                : Audit
SQLServerName      : EVSQL
IsClustered        : False
```

This example shows that the Directory database has not yet been added to an availability group, and that it currently uses SQL instance "EVSQL\evsql".

When you have added the databases to the availability group, you can use `Get-EVDatabaseDetail` again to check that you have achieved the correct result.

You can just run `Get-EVDatabaseDetail` again, to show details of all databases, or you could use the following example procedure to identify only Enterprise Vault databases that have not been added to your new availability group.

To list details of Enterprise Vault databases that have not been added to an availability group

- 1 In the Enterprise Vault Management Shell, run the following command:

```
Import-Module .\Symantec.EnterpriseVault.PowerShell.Core.dll
```

- 2 Run the following command:

```
Get-EVDatabaseDetail | where {$_.IsInAG -eq $FALSE}
```

This following example output show that the Enterprise Vault Directory database has not yet been added to an availability group:

```
IsCollationOK      : True
IsInAG              : False
IsAccessible       : True
DBName              : EnterpriseVaultDirectory
SQLInstanceName    : evsql
SQLServerVersion   : 11.0.3128.0
Type                : Directory
SQLServerName      : EVSQL
IsClustered        : False
```

Reconfiguring Enterprise Vault using `Set-EVDatabaseDetail`

`Set-EVDatabaseDetail` updates SQL server connection details for Enterprise Vault databases.

For any Enterprise Vault databases that you have added to an availability group, you must run `Set-EVDatabaseDetail` to replace the SQL instances they used before you added them to the availability group, with a listener name. You can do this for all Enterprise Vault databases in a single operation, or do it selectively.

For example, you can use the following procedure to reconfigure all Enterprise Vault's databases to use the availability group listener, "evaglistener".

To reconfigure all Enterprise Vault's databases

- 1 In the Enterprise Vault Management Shell, run the following command:

```
Import-Module .\Symantec.EnterpriseVault.PowerShell.Core.dll
```

- 2 Run the following command.

```
Get-EVDatabaseDetail | Set-EVDatabaseDetail -ServerName  
evaglistener
```

This uses the `Get-EVDatabaseDetail` to get all the Enterprise Vault databases, and pipe them into `Set-EVDatabaseDetail`, which reconfigures each to use the listener, “evaglistener”.

Note that `Set-EVDatabaseDetail` produces no output when it is successful.

You can also use `Get-EVDatabaseDetail` and `Set-EVDatabaseDetail` to reconfigure Enterprise Vault selectively. For example, you could use the following procedure in a more complex environment, to reconfigure just the databases that currently use a specified SQL instance.

To reconfigure Enterprise Vault databases that use a specified listener

- 1 In the Enterprise Vault Management Shell, run the following command:

```
Import-Module .\Symantec.EnterpriseVault.PowerShell.Core.dll
```

- 2 Run the following command.

```
Get-EVDatabaseDetail | where {$_.SQLInstanceName -eq 'evsql'} |  
Set-EVDatabaseDetail -ServerName evaglistener
```

This uses the `Get-EVDatabaseDetail` to get all the Enterprise Vault databases that currently use SQL instance “evsql”, and pipe them into `Set-EVDatabaseDetail`, which reconfigures each to use the listener, “evaglistener”.

Starting Enterprise Vault services

When you have implemented an AlwaysOn availability group in your Enterprise Vault environment, you can start all Enterprise Vault services, on all your Enterprise Vault servers.

About managing vault store groups and sharing

This section describes how to do the following:

- View the status of the vault stores in a vault store group.
- Change the sharing level of a vault store.

- Move a vault store to a different vault store group.
- Delete a vault store group.
- Monitor the fingerprint databases.
- Monitor the archive space reduction due to single instance storage.

You must back up each vault store group's fingerprint database as part of your backup regime.

For more information, see the *Backup and Recovery* guide.

Note: For information on how to create vault store groups and vault stores, and how to set up a sharing regime that is suitable for your organization, see "Setting up Storage" in *Installing and Configuring*.

Viewing the status of the vault stores in a vault store group

The Administration Console shows a summary of the status of each vault store in a vault store group.

To view a status summary for the vault stores in a vault store group

- 1 In the Administration Console, expand the Site and then expand **Vault Store Groups**.
- 2 In the left pane, click the Vault Store Group for which you want to see details.

The right pane of the Administration Console lists the details of each vault store in the group. To refresh this view at any time, click F5.

Enterprise Vault displays the following information for each vault store in the group:

- **Name:** The name of the vault store.
- **Status:** The status of the vault store. The status is either Available or Marked for deletion.
- **Backup Mode:** If the vault store is in backup mode, "Yes" appears in this column. To place a vault store in backup mode, or to clear it from backup mode, right-click the vault store and select **Set backup mode** or **Clear backup mode**.
- **Sharing Type:** Indicates the vault store's sharing level. You can change a vault store's sharing level from the **Sharing** tab of its parent Vault Store GroupVeritass properties.

See "[Changing the sharing level of a vault store](#)" on page 65.

- **Computer:** The computer whose Enterprise Vault Storage service the vault store uses.
- **Safety Copy:** The safety copy setting. This setting determines when Enterprise Vault deletes safety copies. You can change the safety copy setting from the **Safety Copies** tab of the vault store's properties.
- **Journal Safety Copy:** The journal safety copy setting. This setting determines when Enterprise Vault deletes journal safety copies. You can change the safety copy setting from the **Safety Copies** tab of the vault store's properties.

To see more details for a particular vault store, right-click the vault store and select **Properties**.

Changing the sharing level of a vault store

You can change the sharing level of any vault store within a vault store group. You can also configure all vault stores to use a specific sharing level, including any new vault stores that you add to the group.

The sharing level of a vault store must be one of the following:

- **No sharing.** The vault store does not participate in Enterprise Vault single instance storage.
- **Share within Vault Store.** The vault store shares SIS parts only within itself.
- **Share within group.** The vault store shares SIS parts with other vault stores in the group that also have the **Share within group** sharing level.

To change the sharing levels you must run the Configure Sharing wizard on the vault store group. The vault store group must contain at least one vault store.

Note: You can rerun the Configure Sharing wizard at any time, but changes you make to the vault store sharing levels do not act retrospectively.

To configure sharing for a vault store group

- 1 In the left pane of the Administration Console, expand the Enterprise Vault site hierarchy until **Vault Store Groups** is visible.
- 2 Expand the **Vault Store Groups** container to show the existing vault store groups.
- 3 Right-click the vault store group for which you want to configure sharing, and on the shortcut menu click **Properties**.

4 Click the **Sharing** tab.

The Sharing tab lists the vault stores in the vault store group, and their current sharing levels.

5 Click **Configure Sharing**.

The Configure Sharing wizard starts.

6 In the special case of the Default Upgrade Group, Enterprise Vault helps you to configure a fingerprint database for the group, if one does not exist already.**7** The Configure Sharing wizard takes you through the steps to configure sharing levels for the vault stores in the vault store group. You can set the vault store sharing levels individually, or apply a sharing level to all the current vault stores.

If you change one or more vault store sharing levels to **Share within vault store** or **Share within group**, the wizard prompts you to run a connectivity test before the wizard makes any changes. The connectivity test helps to determine whether the network connectivity is sufficient to support the sharing configuration you have selected.

The wizard makes no changes until you click **Finish** on the final page of the wizard.

If the connectivity test shows poor results you may want to do one of the following:

- Click **Back**, modify the vault store sharing levels and rerun the connectivity test.
- Click **Cancel** to discard your changes.

For more information on the connectivity test, see the Administration Console help for the Configure Sharing wizard.

Moving a vault store to a different vault store group

In most cases you cannot move a vault store to a different vault store group.

You can move a vault store to a different vault store group only if all of the following circumstances apply:

- You previously upgraded to Enterprise Vault 8.0.
- The vault store is one that Enterprise Vault upgraded to Enterprise Vault 8.0, or one that you created in the Default Upgrade Group.
- The vault store's sharing level is "No sharing" and has never been changed.

Note that when you move a vault store, it retains the sharing level "No sharing".

To move a vault store to another vault store group

- 1 Right-click the vault store and select **Change Vault Store Group** from the shortcut menu.

The **Change Vault Store Group** wizard starts.

- 2 Work through the **Change Vault Store Group** wizard.

For more information, see the help that is provided with the wizard.

Deleting a vault store group

You can delete a vault store group if you no longer want to use its vault stores and their associated archives. Deletion permanently removes all the partitions and archives that the vault stores contain, and all the items that are stored in these partitions and archives.

You can delete a vault store group only if its vault store group database is not in a SQL AlwaysOn availability group, and if all of the following conditions apply to every vault store in the group:

- It is not a default vault store for automatically-enabled archives.
- It does not contain any archives that are associated with archiving targets.
- Its status is Available.
- It is not in backup mode.
- Its vault store database is not in a SQL AlwaysOn availability group. If it is, you must first remove it from the availability group.

When you delete a vault store group, the status of each vault store changes to Marked for deletion. Shortcuts to items within the vault stores' archives no longer work.

Enterprise Vault may take a long time to complete the deletion operation. If a vault store contains any items that are on legal hold, or any SIS parts that are referenced by other vault stores, Enterprise Vault marks the vault store for deletion but it does not delete the vault store or the group until these conditions no longer apply.

Note: If you delete a vault store group, you cannot stop or undo the process. The action overrides any form of deletion protection that is applied to items or Retention Categories, other than legal hold.

To delete a vault store group

- 1 In the Administration Console, select the vault store group that you want to delete.
- 2 The right pane of the Administration Console displays the status of the group's vault stores. Click F5 to refresh the view. The right pane displays each vault store's current status, and indicates whether backup mode is set. You can only delete a vault store if the status is Available and backup mode is not set.
- 3 Right-click the vault store group and select **Delete** from the shortcut menu.
- 4 On the warning dialog, click **Delete**.

The status of each vault store in the group changes to Marked for Deletion. The icon for the Vault Store Group also changes to indicate that it is marked for deletion.

When Enterprise Vault eventually completes the deletion, it removes the vault stores and the vault store group from the Administration Console.

Monitoring the fingerprint databases

If you enable monitoring on the **Monitoring** tab of the Site Properties, a number of alerts are available for the vault store group fingerprint databases. These alerts are as follows:

- **Vault Store fingerprint database backup.** The number of days before Enterprise Vault issues a warning about a fingerprint database that is not backed up. The default value is 3.
- **Vault Store fingerprint database log backup.** The number of days before Enterprise Vault issues a warning about a fingerprint database transaction log that is not backed up. The default value is 1.
- **Vault Store fingerprint database log size.** The percentage of available space that a fingerprint database transaction log can occupy before Enterprise Vault issues a warning about space usage. The default value is 85 percent.

See [“Monitoring in Site Properties”](#) on page 293.

The fingerprint databases must be backed up as part of your backup regime.

For more information, see the *Backup and Recovery* guide.

Monitoring the archive space reduction due to single instance storage

If you have installed and configured Enterprise Vault Reporting, you can access the reports that provide information on the archive storage savings that are due to Enterprise Vault single instance storage.

The reports that relate to single instance storage are as follows:

- **Single Instance Storage Reduction Summary.** This report shows the storage reduction that has resulted from Enterprise Vault single instance storage for each vault store group in an Enterprise Vault Site.
- **Single Instance Storage Reduction per Vault Store Group.** This report shows the storage reduction that has resulted from Enterprise Vault single instance storage for each vault store in a vault store group.
- **Single Instance Storage Reduction by File Type.** This report shows the storage reduction that has resulted from Enterprise Vault single instance storage for each file type within a vault store group.

You can access the single instance storage reports from the Microsoft SQL Server Reporting Services Report Manager web application, or from within the Administration Console. See the *Reporting* manual for more information.

About managing safety copies

Enterprise Vault can be configured to retain archived items until the vault store partition in which they are archived has been backed up. During the time between archiving and removal, Enterprise Vault treats the original items as safety copies. For each vault store you can choose to keep the safety copies on the Enterprise Vault storage queue rather than in the original locations. This option has the advantage that the original items are removed immediately after archiving so users benefit from an immediate space gain.

When the vault store partition has been backed up, Enterprise Vault can remove the safety copies. Enterprise Vault also creates shortcuts and placeholders at this time if it is configured to do so.

Note: Enterprise Vault removes safety copies when the Storage service is started or when backup mode is cleared from the vault store.

For more information about the configuration of safety copies, see “About Enterprise Vault safety copies” in *Installing and Configuring*.

Configuring the removal of Enterprise Vault safety copies

To configure the removal of safety copies for an existing vault store

- 1 In the left pane of the administration console, expand the **Vault Store Groups** container and find the vault store.
- 2 Right-click the vault store and click **Properties**.

- 3 On the **Safety Copies** tab of the **Vault Store Properties** choose an option from the **Default behavior** list.
- 4 If you want the behavior to be different for journal archives, select an option from **For journal archives** list.

Note: This option is available only if **Default behavior** is set to **Yes, in the original location**. If you require different settings for journaling you can use a separate vault store.

Checking that partitions have been backed up

If you choose to keep safety copies Enterprise Vault must check that the partition has been backed up before it removes those safety copies.

During the creation of each vault store, you chose from the following options:

- **Use the archive attribute.** Files on the partition whose archive attributes are cleared are considered backed up and Enterprise Vault removes the corresponding safety copies. This option is appropriate only if your backup software clears archive attributes after backup.
- **Check for a trigger file.** A partition is considered backed up when Enterprise Vault finds a trigger file on the partition. Typically, this trigger file is placed on the partition by your backup software. When you choose this option, you can also configure how often the partition is checked for the presence of a trigger file

You can change this setting subsequently in the Administration console.

To configure which method Enterprise Vault uses to ensure a partition's data is backed up

- 1 In the left pane of the administration console, expand the **Vault Store Groups** container and select the vault store contains the partition.
- 2 In the right pane, right-click the partition and click **Properties**.
- 3 Click the **Backup** tab.
- 4 Select one of the following options:
 - **Use the archive attribute**
 - **Check for a trigger file**

- 5 If you selected the **Check for a trigger file** option, you can also set a partition scan interval, which determines how often Enterprise Vault checks the partition for a trigger file. Select the **Scan partition every** option and set a scan interval in minutes.
- 6 Click **OK**.

About managing partition rollover

Each vault store must contain at least one partition, which is the physical location where Enterprise Vault stores archived data. As the data in a vault store grows, you can create more partitions to provide additional capacity.

You can manually change the open partition in a vault store. For example, when the disk that hosts the open partition reaches capacity, close the partition and open a partition on a different disk.

Enterprise Vault also provides an automatic partition rollover feature. This feature lets you configure partitions so that archiving rolls over from one partition to another when certain criteria are met. For example, you can configure a partition to roll over to the next available partition when the host disk has only 5% free space. You can also configure a partition to roll over on a specific date.

In support of both these features, each partition can exist in one of three states:

- **Closed.** A partition that is closed, is not available for archiving until you manually open it, or make it ready for partition rollover.
- **Open.** Each vault store can have only one open partition. Enterprise Vault archives data into the open partition. Without partition rollover, Enterprise Vault automatically closes a partition when the disk that hosts it becomes full, but does not open another.
However, if the open partition is rollover enabled, and a ready partition exists, Enterprise Vault automatically opens the ready partition when the open partition meets its rollover criteria.
- **Ready.** Each vault store can have any number of ready partitions that are available to Enterprise Vault when partition rollover occurs.

Configuring partition rollover

In each vault store where you use partition rollover, the open partition must be rollover enabled, and there must be at least one ready partition. For partition rollover to work for an extended period without intervention, each ready partition in a vault store must also be partition rollover enabled. If not, partition rollover stops at the first partition that is not rollover enabled. In summary, for Enterprise Vault to roll

over through a series of partitions, each must be both ready for partition rollover, and partition rollover enabled.

Note: Centera partitions cannot be rollover enabled, which means Enterprise Vault cannot roll over from a Centera partition. However, Centera partitions can be rollover ready.

You can enable and configure partition rollover for each partition when you create it using the **New Partition** wizard. For more information on creating a new vault store partition, see the *Setting up storage* chapter of the *Installing and Configuring* manual. You can also configure partition rollover for existing vault store partitions, using the **Vault Store Partition Properties** page.

Each partition can be configured to roll over using any of the following options:

- **Enabled based on volume.** Partition rollover is enabled for this partition, and occurs according to the amount of free space on the volume that hosts the partition.
- **Enabled based on time.** Partition rollover is enabled for this partition, and occurs according to the time criteria you specify.
- **Enabled based on time or volume.** Partition rollover is enabled and occurs according to whichever of the volume criteria or time criteria are met first. For example, you can configure the partition to roll over when its host volume falls below 5% free space, or on a specific date, whichever comes first.

Depending on the choice you make, you can then set appropriate rollover criteria. If you choose either **Enabled based on volume** or **Enabled based on time or volume**, you can make appropriate settings to trigger partition rollover according to the remaining free space on partition's host volume. Set one of the following criteria to trigger rollover:

- A percentage of free space.
- A specific amount of free space in MB, GB, or TB.

If you chose either **Enabled based on time** or **Enabled based on time or volume**, you can make appropriate settings to trigger partition rollover. Set one of the following criteria to trigger rollover:

- An elapsed period of time, in days, weeks, months, or years.
- A specific date and time for rollover to occur.

This flexibility enables a number of approaches to the management of partition rollover. You can take a purely volume-based approach, in which you configure a series of partitions that roll over when their host disks approach capacity. Normally, this approach would require you to create the partitions on separate physical disks.

However, it is still possible to host partitions on a single disk when you mount multiple physical volumes in one file system. In this case, Enterprise Vault rolls over based on the free space on the physical volume, rather than on the host file system.

The time-based approach to partition rollover lets you roll over according to any time criteria that suit your environment. For example, you can configure partitions to roll over at the end of each week, or on a specific date each month.

Note: When you use date-based partition rollover, you must ensure that each partition has sufficient storage capacity for period it is open.

Enterprise Vault also lets you use a mixture of volume and time criteria.

To enable and configure partition rollover on an existing partition

- 1 In the left pane of the administration console, expand the **Vault Store Groups** container and select the vault store in which you want to configure partition rollover.
- 2 In the right pane, right-click a partition and click **Properties**.
- 3 Click the **Rollover** tab.
- 4 From the **Partition Rollover** list, select one of the following options:
 - **Enabled based on volume**
 - **Enabled based on time**
 - **Enabled based on time or volume**
- 5 Use the options that are available to you to set appropriate rollover criteria for this partition.

Changing rollover order

As you create and configure rollover ready partitions, the order in which they are used depends on the rollover criteria you set. By default, partitions configured with volume-based criteria are used in the same order they are made ready for rollover. Partitions configured with time-based criteria are used in the order the rollover dates determine.

You can change partition rollover order using the **Partition Rollover** tab on the **Vault Store Properties** page.

Note: You can place the partitions that are configured for volume-based rollover in any order. However, you cannot break the rollover order for any partitions that are configured for time-based rollover. For example, you cannot move a partition that is configured to roll over on 10 October before one that is configured to roll over on 3 October.

To change rollover order

- 1 In the administration console, right-click a vault store and click **Properties**.
- 2 Click the **Partition Rollover** tab.
- 3 From the list of ready partitions, select the one whose position you want to change.
- 4 Click **Move Up** or **Move down** until the partition is in the correct position.
- 5 Repeat the previous two steps until the ready partitions are in the correct order.

Forcing partition rollover

You can force partition rollover using the PowerShell cmdlet `Start-PartitionRollover`. This cmdlet forcibly closes the open partition in the vault store you specify and, if one is available, opens the first ready partition.

Note: `Start-PartitionRollover` forces partition rollover irrespective of the rollover criteria on the current open partition.

To force partition rollover

- 1 Open the Enterprise Vault management shell.
- 2 Run `Start-PartitionRollover`.

The syntax for this cmdlet is:

```
Start-PartitionRollover -EVServerName server -VaultStore  
vault_store
```

where:

server is the Enterprise Vault server that runs the storage service for the vault store in which you want to force partition rollover.

vault_store is the name or ID of the vault store in which you want to force partition rollover.

For example:

```
Start-PartitionRollover EV1 VS1
```

This connects to the Enterprise Vault server EV1 and verifies that vault store VS1 uses the storage service on this server. If it does, `Start-PartitionRollover` forces partition rollover in vault store VS1.

Recovering deleted items

Enterprise Vault can retain items that users have deleted so that you have some time in which to recover items that users have deleted accidentally. You can configure this recovery feature on the Archive Settings tab of Site Properties.

If recovery is enabled, Enterprise Vault retains deleted items for the period of time that is specified on the Archive Settings tab of Site Properties. At the end of that time the item is permanently deleted.

When a user deletes an archived item, it is removed from the index so that the item can no longer be found by browsing or searching the archive. However, direct links to the item, such as mailbox shortcuts, still work. The deleted item no longer contributes to the archive quota usage.

Note that a user can retrieve a copy of a deleted item by using a shortcut. If the user then rearchives this item without modifying it, the item is still in a deleted state and therefore is not searchable.

Recovery is available only for those items that users have deleted. You cannot recover items that Storage Expiry has deleted. Also, if Storage Expiry deletes an item that has already been deleted by a user, you cannot then recover that item.

To recover items that have been deleted from an archive

- 1 In the Administration Console, expand the tree view until the **Archives** container is visible.
- 2 Expand the **Archives** container and then click the container that has the archive with the deleted items.
- 3 Right-click the archive with the deleted items and, on the shortcut menu, click **Properties**.
- 4 Click the **Deleted Items** tab. The tab shows the number of items that can be recovered.
- 5 Click **Recover Items**. This recovers all available items in the archive. You cannot select specific items.

About expiry and deletion

Enterprise Vault can automatically perform the following:

Storage expiry	Delete items from archives when the items' retention periods have expired.
Shortcut deletion	Delete shortcuts from users' Exchange mailbox folders and Exchange public folders. You can configure Enterprise Vault to delete shortcuts over a certain age, or shortcuts to items that have been deleted from an archive.

Setting up storage expiry

If you configure storage expiry, the Enterprise Vault Storage service automatically deletes items from archives when their retention periods expire. When the Exchange or Domino Mailbox task next runs, it automatically deletes the associated shortcuts from the mailboxes if the **Delete orphaned shortcuts** option is selected in the policy. Similarly, the Exchange Public Folder task deletes the shortcuts that are associated with expired items in public folders.

When certain items such as calendar, task, and meeting items are archived, the original item in the mailbox is not replaced with a shortcut. By default, the archiving task does not delete the original items when it performs shortcut deletion. To include such items in shortcut deletion, configure the registry setting, `DeleteNonShortcutItems`. The setting is described in the *Registry Values* manual.

If storage expiry for Exchange Server Archiving is based on archived date, and you have configured Enterprise Vault to archive unexpired calendar, meeting, and task items (that is, items with an end date in the future), then we recommend that you use the advanced Exchange Mailbox policy setting, **Future item retention category**. This ensures that storage expiry does not delete any archived calendar, meeting, or task items before their end date.

See [“Future item retention category \(Exchange Archiving General setting\)”](#) on page 180.

To set up storage expiry

- 1 In the left pane of the Administration Console expand the hierarchy until the appropriate vault site is visible.
- 2 Right-click the vault site and then, on the shortcut menu, click **Properties**.
- 3 In the **Site Properties** dialog box, click the **Storage Expiry** tab.
- 4 Select the settings to use, and then click **OK**.
- 5 You also need to configure shortcut deletion in the Exchange or Domino Mailbox policy or Exchange Public Folder policy. The Exchange or Domino Mailbox task and Exchange Public Folder task automatically delete expired item shortcuts when they next run.

Setting up shortcut deletion

The Exchange Mailbox task and Exchange Public Folder task perform shortcut deletion. The tasks delete the shortcuts for expired items automatically. The following additional shortcut deletion options are available on the **Shortcut Deletion** tab of the Exchange Mailbox policy and the Exchange Public Folder policy:

- Delete shortcuts that exceed the specified age. Enterprise Vault uses the modified date or archived date to determine the age of a shortcut. You can specify which date to use on the **Storage Expiry** tab of **Site Properties**.
- Delete orphaned shortcuts. Orphaned shortcuts are shortcuts for items that have previously been deleted from the archive.

When certain items such as calendar, task, and meeting items are archived, the original item is not replaced with a shortcut. By default, the archiving task does not delete the original items when it performs shortcut deletion. To include such items in shortcut deletion, configure the registry setting, `DeleteNonShortcutItems`. The setting is described in the *Registry Values* manual.

If you have configured Enterprise Vault to archive unexpired calendar, meeting, and task items, any items with an end date in the future will not be deleted from users' mailboxes.

To set up shortcut deletion options

- 1 In the Administration Console, expand the hierarchy until the appropriate Exchange Mailbox or Public Folder policy is visible.
- 2 Right-click the policy. On the shortcut menu, click **Properties**.
- 3 In the policy dialog box, click the **Shortcut Deletion** tab.
- 4 Select the required options, and then click **OK**.

Working with retention categories and retention plans

When Enterprise Vault archives an item, it automatically assigns a retention category to the item to specify how long to keep it. You can define different retention categories for different types of data. As Enterprise Vault monitors the archives, it can then delete the items when their retention periods expire.

Retention plans extend the functionality of retention categories. As well as specifying the retention category to assign to the items in one more archives, a retention plan also lets choose additional options: whether to use the Enterprise Vault classification feature to classify the items, for example, or whether the retention category that

you have set with the retention plan overrides any retention categories with which Enterprise Vault may previously have stamped the items.

Creating a new retention category

By assigning a retention category to items at the time they are archived, it is possible to categorize stored items. This categorization makes it easier to retrieve items because it is possible to search by retention category.

Users can select retention categories from the list and assign them to items in their mailboxes. When Enterprise Vault archives an item, it is stored with the appropriate retention category.

A retention category specifies a retention period, which is the minimum amount of time for which an item must be retained after its last modification date. For mail messages, the retention period is the time since the message was received. For documents, it is the time since the document was last modified. When the retention period has elapsed, Enterprise Vault can automatically delete the items. See the Storage Expiry tab in Site Properties to set up expiry.

If you later modify a retention category, the changes are retrospective. For example, if you have a retention category called "Customer Accounts" with a retention period of 5 years and you change it to 10 years, then items that have been already archived with the "Customer Accounts" retention category are retained for a minimum of 10 years.

You can create as many retention categories as you require. You can also modify the standard retention categories to suit your own needs.

A retention category also includes settings that let you do the following:

- Prevent automatic deletion of expired items.
- Prevent user deletion of items.
- Hide the retention category from users.
- Lock the retention category.

To change these settings, open the properties of the retention category in the Vault Administration console. The settings are not options in the New Retention Category wizard.

Note: If you plan to store items indefinitely on a WORM storage device, then ensure that the retention settings on the device are correctly configured. For details, refer to *Enterprise Vault hardware requirements* in the manual, *Installing and Configuring*.

To create a new retention category

- 1 In the left pane of the Administration Console, expand the vault site hierarchy until **Policies** is visible.
- 2 Expand **Policies** and then expand **Retention & Classification**.
- 3 Right-click **Categories** and then, on the shortcut menu, click **New > Retention Category**.

The New Retention Category wizard starts.

- 4 Work through the wizard.

About retention plans

With a retention plan, you can associate a retention category with a number of other settings, such as a classification policy and the criteria for discarding expired items, and apply them all to one or more archives. If you choose to set a classification policy with a retention plan then, for the archives to which you assign the retention plan, the classification policy determines the following:

- Whether to classify items at the same time that Enterprise Vault indexes and archives them. After Enterprise Vault has applied the classification tags, users of applications like Compliance Accelerator and Discovery Accelerator can use them to filter items when they conduct searches and reviews.
- Whether to classify items when users manually delete them or Enterprise Vault automatically expires them.

For more information on the classification feature, see the *Classification* guide.

Applying a retention plan to an archive gives you greater control over the retention periods of the items in the archive. In particular, a retention plan lets you dispose of already-archived items by giving them a different retention period than the one that Enterprise Vault first gave them when it archived the items. For example, you can configure a retention plan so Enterprise Vault expires the affected items according to the retention category that you have associated with the retention plan, and not the retention categories with which Enterprise Vault originally stamped them.

Creating a retention plan

We recommend that you only create retention plans after you have defined the retention categories and classification policies that you want to assign with those plans.

You can modify a retention plan after you have created it and applied it to one or more archives. You can also dissociate the plan from those archives and assign a different plan to them.

To create a retention plan

- 1 In the left pane of the Enterprise Vault Administration Console, expand the tree view until the **Policies** container is visible.
- 2 Expand the **Policies** container and then expand the **Retention & Classification** container.
- 3 Right-click **Plans** and then point to **New** and click **Retention Plan**.
The New Retention Plan wizard appears.
- 4 Work through the pages of the wizard, which prompt you to enter the following:
 - A name for the new retention plan. The name must be unique, and it can contain up to 40 alphanumeric or space characters.
 - A description of the plan. The description can contain up to 127 alphanumeric, space, or special characters.
 - A retention category to associate with the retention plan. If no suitable retention category exists, the wizard provides the option to create one.
 - Optionally, whether to allow the Enterprise Vault classification feature to classify the items that the retention plan handles. If you choose to classify the items, you must also select the required classification policy.
 - The expiry settings to assign to the affected items.

Applying retention plans to your Enterprise Vault archives

After you have created a retention plan, you can apply it to one or more archives. The Administration Console provides many different ways to do this, as you can associate a retention plan with any of the following features:

- An Exchange, Domino, or IMAP provisioning group
- An Exchange journal archive, Domino journal archive, or SMTP archive
- An FSA volume or folder policy
- A public folder target
- A SharePoint target or site collection
- Mailboxes that you manually enable for archiving by running the Enable Mailbox wizard

The documentation for each of these features describes how to associate a retention plan with it. You can also apply a retention plan to a selected archive with the PowerShell command `Set-EVArchive`. See the *PowerShell Cmdlets* guide for more information.

After you have associated the retention plan with the required feature, you must run the appropriate provisioning task or archiving task to apply it to the target archives. For instance, you must run the Client Access Provisioning task in the case of an IMAP provisioning group and the Sharepoint Archiving task in the case of a SharePoint site collection.

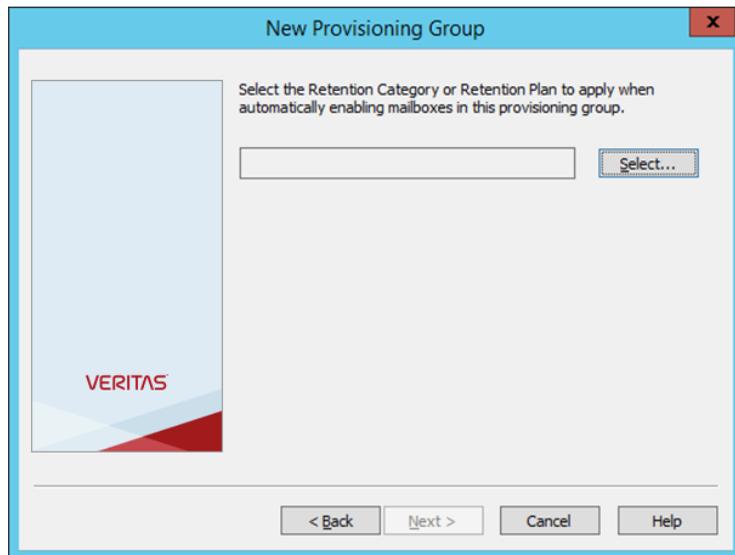
As an example, the following procedure describes how to choose a retention plan when you set up a new Exchange provisioning group.

To associate a retention plan with an Exchange provisioning group

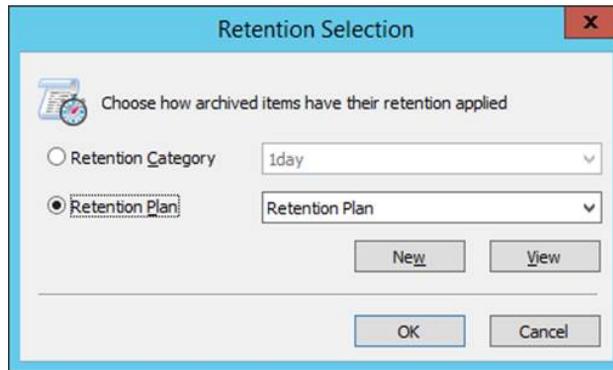
- 1 In the left pane of the Administration Console, expand the hierarchy until the **Targets** container is visible.
- 2 Expand the Exchange domain.
- 3 Right-click the **Provisioning Groups** container, and then point to **New** and click **Provisioning Group**.

The **New Provisioning Group** wizard appears.

- 4 Work through the wizard until you reach the page that prompts you for the required retention category or retention plan.



- 5 Click **Select** to open the **Retention Selection** dialog box.



- 6 Select the required retention plan, or click **New** to create a new one.
- 7 Work through the remaining pages of the wizard.
- 8 Run the Exchange Provisioning task to apply the retention plan to the target archives.
- 9 Synchronize the mailboxes. To do this, open the properties dialog box for the Exchange Mailbox Archiving task and then, on the **Synchronization** tab, click **Synchronize**.

About the PowerShell cmdlets for working with retention plans

Enterprise Vault comes with a number of PowerShell commands with which you can create or modify retention plans. These commands perform the same function as the equivalent facilities in the Administration Console.

Table 3-4 PowerShell commands for creating or modifying retention plans

Command	Description
<code>Get-EVRetentionPlan</code>	Returns a list of all the retention plans that you have configured in an Enterprise Vault site. You can filter the list by various properties, including the classification policies that you have associated with the plans.
<code>New-EVRetentionPlan</code>	Creates a retention plan.
<code>Remove-EVRetentionPlan</code>	Removes the specified retention plan, if it is not in use.
<code>Set-EVRetentionPlan</code>	Sets or updates the properties of an existing retention plan.

See the *PowerShell Cmdlets* guide for more information on these commands.

How retention plans affect storage expiry

Applying a retention plan to an archive can affect how Enterprise Vault deletes the items in the archive, depending on how you configure the retention plan and its associated classification policy. In particular, the following configuration options determine how storage expiry operates:

- In the properties of a retention plan, the **When expiring items, use** option on the **Expiry** tab. If you set this to **The retention category set by this Retention Plan** (abbreviated to `OverrideRetention` in the PowerShell cmdlets `New-EVRetentionPlan` and `Set-EVRetentionPlan`), the retention category that you set with the retention plan overrides the item-level retention category with which Enterprise Vault stamps each item on ingestion.
- In the properties of the associated classification policy, the option **Set retention category of items** (abbreviated to `DetermineRC` in the PowerShell cmdlets `New-EVClassificationPolicy` and `Set-EVClassificationPolicy`). If you check this option, the item-level retention category with which Enterprise Vault stamps each item overrides everything else, regardless of how you configure the associated retention plan.

As [Table 3-5](#) shows, the two configuration options above play an important role in determining how storage expiry behaves.

Table 3-5 Storage expiry behavior when retention plans are applied

Retention plan applied?	Override Retention?	Classification enabled?	Determine RC?	Expire items based on
No	Not applicable	Not applicable	Not applicable	Item-level retention category
Yes	No	No	Not applicable	Item-level retention category
Yes	No	Yes	Yes	Item-level retention category
Yes	No	Yes	No	Item-level retention category

Table 3-5 Storage expiry behavior when retention plans are applied
(continued)

Retention plan applied?	Override Retention?	Classification enabled?	Determine RC?	Expire items based on
Yes	Yes	No	Not applicable	Plan-level retention category
Yes	Yes	Yes	No	Plan-level retention category

Note: Vault stores that contain EMC Centera partitions are exempt from this behavior. In such environments, Enterprise Vault cannot expire items according to a selected retention plan.

About maintaining provisioning groups

The Exchange and Domino Provisioning tasks automatically provision new mailboxes provided that they are included in their list of targets. Mailboxes that are not included in the list of targets do not result in any warnings when the Provisioning tasks run.

If you have chosen to have mailboxes enabled automatically, remember that a mailbox is provisioned according to the first provisioning group in which it appears. Therefore, it is important that the mailbox is in the correct group before the Provisioning task runs.

Note: If you choose to use the inherited vault store or inherited Indexing service, and the provisioning group includes mailboxes from more than one server, different vault stores or Indexing services may be used for mailboxes that are enabled according to this provisioning group. Depending on the configuration options that you have chosen, it is also possible that mailboxes on a particular server cannot be enabled because no vault store or Indexing service is defined for them.

Enabling archiving for new mailboxes

You can enable archiving for a new Microsoft Exchange Server mailbox in the following ways:

- You can make Enterprise Vault automatically enable archiving for new Microsoft Exchange Server mailboxes.

If you do this, Enterprise Vault automatically creates the mailbox's archive in the default vault store.

- You can manually enable archiving for specific Microsoft Exchange Server mailboxes. If you have not set up Enterprise Vault to enable archiving for mailboxes automatically, you must use this method to enable archiving for mailboxes.

Making Enterprise Vault enable archiving for new mailboxes automatically means that you do not need to enable each mailbox manually whenever there is a new Microsoft Exchange Server mailbox.

The advantage of enabling archiving manually is that you can select a specific vault store as the location for each archive that is created.

Note that, if you make Enterprise Vault automatically enable archiving for new mailboxes, the new archives are created the next time an Exchange Mailbox task runs. If there is a new mailbox that you want to be archived somewhere other than the default vault store, you must manually enable archiving for that mailbox before the Exchange Mailbox task runs. If you do not enable the mailbox yourself, Enterprise Vault automatically enables archiving for it and creates an archive in the default location.

If you want all the new archives to be in the same vault store, making Enterprise Vault automatically create archives is the option that means the least work on your part. It is easy to turn this option on or off. For example, you can make Enterprise Vault automatically create archives on the first run of the Exchange Mailbox task, and then turn off the option and enable new mailboxes manually.

When Enterprise Vault automatically enables archiving for a mailbox, the new archive is stored in the default location.

To make Enterprise Vault enable archiving for new mailboxes automatically

- 1 In the left pane of the Administration Console, expand the vault site hierarchy until the name of the vault site is visible.
- 2 Expand the vault site and then expand **Archiving Targets**.
- 3 Expand **Exchange**.
- 4 Expand the required domain.
- 5 Click **Provisioning Group**.

If no provisioning groups are listed, create a new one as follows:

- Right-click **Provisioning Group** and, on the shortcut menu, click **New** and then **Provisioning Group**.
- Work through the **New Provisioning Group** wizard.

- 6 In the right pane, double-click the provisioning group that will contain the mailboxes that will be enabled automatically.
- 7 In the **Provisioning Group Properties**, click the **Archiving Defaults** tab.
- 8 Select **Automatically enable mailboxes**.
- 9 If you want to use a specific vault store for the new mailbox archives, click **Override the inherited Vault Store** and click **Change** to pick the vault store to use.

If you do not specify a vault store, the vault store that will be used is the one defined in the Enterprise Vault server properties. If no vault store is defined there, the vault store that is defined in the Exchange Server properties is used.

- 10 If you want to use a specific Indexing Service when archiving from the new mailboxes, click **Override the inherited Indexing Service** and click **Change** to pick the Indexing Service to use.

If you do not specify an Indexing Service, the Indexing Service that is used is the one defined in the Enterprise Vault server properties. If no Indexing Service is defined there, the Indexing Service that is defined in the Exchange Server properties is used.

- 11 Select the default retention category to use for items that are stored in the new archives.

Users can select other retention categories to use from the list of those available.

- 12 Select **OK**.

To enable archiving for mailboxes manually

- 1 On the **Tools** menu, click **Enable Mailboxes**.

The Enable Mailbox wizard starts.

- 2 Work through the wizard.

Note the following:

- You can manually disable a new mailbox. This stops Enterprise Vault from automatically enabling archiving for the mailbox. You would then have to enable the mailbox at some point, as otherwise Enterprise Vault would never archive items from it.
- When you enable a mailbox, Enterprise Vault automatically selects one of the open Indexing Locations to use to store the indexing data that is associated with that mailbox's archive. Before you enable mailboxes, make sure that the open Indexing Locations are the ones you want to use.

Enterprise Vault does not provide a way to change a mailbox's Indexing Location after you have enabled archiving for the mailbox.

- You can select an existing archive to use for a mailbox that is being enabled. This is useful when a mailbox has been migrated to a different Exchange Server in the same Enterprise Vault site and needs to be enabled for archiving to the same archive as before.

Checking for hidden mailboxes

By default, Enterprise Vault archives only the mailboxes that are listed in the Exchange Global Address List. In the Enterprise Vault Administration Console, hidden mailboxes are not listed in the Enable Mailbox wizard and do not appear in Exchange Mailbox archiving task reports. If you want Enterprise Vault to archive hidden mailboxes, you can use the registry value `ProcessHiddenMailboxes`.

Enterprise Vault does not process the mailboxes of disabled Active Directory accounts. Even if you have configured the registry value `ProcessHiddenMailboxes`, the mailboxes of hidden disabled accounts are not processed. To force Enterprise Vault to include the mailboxes of users whose accounts have been disabled, configure both of the registry values `ProcessHiddenMailboxes` and `ExcludeDisabledADAccounts`. These settings are documented in the *Registry Values* guide.

About applying or removing legal holds on selected archives

The items in an Enterprise Vault archive can be deleted when either of the following occurs:

- Enterprise Vault automatically deletes the archived items whose retention periods have expired.
- A user manually deletes one or more archived items.

In some circumstances, you may need to place the items in an archive on legal hold to stop them from being deleted. When this is the case, you can run the following PowerShell cmdlets to view and change the legal hold status of the archives:

<code>Get-EVArchive</code>	Returns a list of the Enterprise Vault archives to which a specified user has access.
<code>Set-EVArchive</code>	Sets the properties of the nominated archive.

You run the cmdlets directly in the Enterprise Vault Management Shell on the Enterprise Vault server.

To run one of the Enterprise Vault PowerShell cmdlets

- 1 Start the Enterprise Vault Management Shell.

PowerShell opens and loads the Enterprise Vault snap-in. The cmdlets are now available in the shell.

- 2 At the PowerShell command prompt, type the required command.

Help is available for all the cmdlets. For example, the following command shows the detailed Help for the Get-EVArchive cmdlet:

```
Get-Help Get-EVArchive -detailed
```

Get-EVArchive

Get-EVArchive returns a list of some or all of the archives in the Enterprise Vault site. You can filter this list to show the following:

- Archives in which a specified user has various permissions, either directly or through membership of an Active Directory group.
- Archives whose name exactly matches the specified name.

You can further filter the list by a number of archive properties. For example, you can choose to list only those archives in which a specified user has permission to delete the archived items, or only those archives that are on legal hold.

Get-EVArchive is provided by

Symantec.EnterpriseVault.PowerShell.Snapin.dll, which is loaded by the Enterprise Vault Management Shell.

Syntax

```
Get-EVArchive [-User] <String> [[-Server] <String>] [-DeleteProtected
[<Boolean>]] [-DeleteExpiredItems [<Boolean>]] [-OnHold [<Boolean>]]
[-Permissions [<String>]] [<CommonParameters>]
```

```
Get-EVArchive [[-ArchiveName] <String>] [[-Server] <String>]
[-DeleteProtected [<Boolean>]] [-DeleteExpiredItems [<Boolean>]]
[-OnHold [<Boolean>]] [<CommonParameters>]
```

Parameters

Table 3-6 Get-EVArchive parameters

Parameter	Description
-User (required if you use the first parameter set in the Syntax section)	Identifies the user for which to retrieve the archive list. Type the user's Windows logon name, user principal name, or Domino user ID. For example: <code>user@domain.com</code> , <code>domain\user</code> .
-ArchiveName	Specifies the name of an archive for which to retrieve the details.
-Server	Identifies the Enterprise Vault server for which to retrieve the archive list. For example: <code>localhost</code> , <code>evserver.domain.com</code> . If you omit this parameter, the cmdlet looks in the registry to identify the Enterprise Vault Directory service computer.
-DeleteProtected	Filters the archive list according to whether the user can manually delete the items in the archives. Set to <code>\$false</code> to list the archives in which the user can manually delete items, or <code>\$true</code> to list the archives in which the user cannot delete items.
-DeleteExpiredItems	Filters the archive list according to whether Enterprise Vault can automatically delete the archived items whose retention periods have expired. Set to <code>\$false</code> to list the archives in which Enterprise Vault does not delete expired items, or <code>\$true</code> to list the archives in which it does.
-OnHold	Filters the archive list according to the legal hold status of the archives. Set to <code>\$false</code> to list the archives in which either the user or Enterprise Vault (or both) can delete items, or <code>\$true</code> to list the archives that are on legal hold. Legal hold is equivalent to <code>DeleteProtected</code> set to <code>\$true</code> and <code>DeleteExpiredItems</code> set to <code>\$false</code> .
-Permissions	Filters the archive list according to the permissions that the user has on the archives. Specify the permissions as a combination of <code>r</code> (for read), <code>w</code> (for write), and <code>d</code> (for delete); for example, <code>rw</code> and <code>rwd</code> . A blank value (<code> </code>) denotes any permission. The default permission if not specified is <code>d</code> (delete). You can only set this parameter if you have also specified the <code>-User</code> parameter.

Examples

- `Get-EVArchive`
 Lists all the archives in the Enterprise Vault site.
- `Get-EVArchive -DeleteProtected $false`
 Filters the list of archives in the Enterprise Vault site to show only those in which users can manually delete items.
- `Get-EVArchive -User Domain\User`
 Lists the archives in which the user `Domain\User` has delete permissions.
- `Get-EVArchive -User user@domain -DeleteProtected $false -DeleteExpiredItems $false -Permissions rw`
 Lists the archives in which the user `user@domain.com` has both read and write permissions. `Get-EVArchive` filters the list to show only those archives in which the user can manually delete items but in which Enterprise Vault cannot automatically delete expired items.
- `Get-EVArchive -User Domain\User -OnHold $false | format-table -auto`
 Lists the archives in which the user `Domain\User` has delete permissions. `Get-EVArchive` excludes from the list all the archives that are on legal hold and writes the output to `format-table`.
- `Get-EVArchive -ArchiveName msmith | format-table -auto`
 Lists the archives that have the name "msmith".
- `Get-EVArchive | where-object {$_.ArchiveName -ilike "*journal*"}`
 Lists the archives whose names contain the case-insensitive string "journal".

Output

[Table 3-7](#) lists the properties that are available.

Table 3-7 Get-EVArchive properties

Name	Type	Description
ArchiveId	String	The ID of an archive to which the specified user has access.
ArchiveName	String	The name of an archive to which the specified user has access.

Table 3-7 Get-EVArchive properties (*continued*)

Name	Type	Description
ArchiveType	EV_STG_API_ARCHIVE_TYPE	<p>The Enterprise Vault archive type enumeration. The possible values are as follows:</p> <ul style="list-style-type: none"> ■ ARCHIVE_TYPE_DOMINO_JOURNAL ■ ARCHIVE_TYPE_DOMINO_MAILBOX ■ ARCHIVE_TYPE_FILE_SYSTEM ■ ARCHIVE_TYPE_INTERNETMAIL ■ ARCHIVE_TYPE_JOURNAL ■ ARCHIVE_TYPE_MAILBOX ■ ARCHIVE_TYPE_PUBLIC_FOLDER ■ ARCHIVE_TYPE_SHARED ■ ARCHIVE_TYPE_SHAREPOINT ■ ARCHIVE_TYPE_SMTP
DeleteExpiredItems	EV_STG_API_EXPIRE_ITEMS	<p>The Enterprise Vault expire items enumeration. The possible values are as follows:</p> <ul style="list-style-type: none"> ■ DONT_EXPIRE_ITEMS ■ EXPIRE_ITEMS
DeleteProtected	Boolean	Indicates whether the user can manually delete items from the archive (\$false) or not (\$true).
OnHold	Boolean	Indicates whether the archive contains items that are on legal hold (\$true) or not (\$false).
Status	EV_STG_API_STATUS	<p>The Enterprise Vault archive status enumeration. The possible values are as follows:</p> <ul style="list-style-type: none"> ■ STS_AVAILABLE ■ STS_INBACKUPMODE ■ STS_TEMPORARILY_UNAVAILABLE ■ STS_UNAVAILABLE
RetentionPlanName	String	The name of the retention plan that you have applied to the archive.

Related cmdlets

- See “[Set-EVArchive](#)” on page 92.

Set-EVArchive

`Set-EVArchive` sets a number of properties of the nominated archive, including whether users can manually delete the items in the archive and whether Enterprise Vault can automatically delete the archived items when their retention period has expired. You can also specify a description and administrative note for the archive for display in the Administration Console.

`Set-EVArchive` is provided by

`Symantec.EnterpriseVault.PowerShell.Snapin.dll`, which is loaded by the Enterprise Vault Management Shell.

Syntax

```
Set-EVArchive [[-ArchiveID] <String>] [-DeleteProtected [<Boolean>]]
[-DeleteExpiredItems [<Boolean>]] [-Description [<String>]]
[-AdminNote [<String>]] [-RetentionPlanName [<String>]]
[<CommonParameters>]
```

Parameters

Table 3-8 Set-EVArchive parameters

Parameter	Description
<code>-ArchiveID</code> (required)	Specifies the ID of the archive for which to set the properties. You can obtain the required ID with the <code>Get-EVArchive</code> cmdlet.
<code>-DeleteProtected</code>	Specifies whether to permit users manually to delete the items in the archive. Set to <code>\$false</code> to permit users to delete items, or <code>\$true</code> to prevent deletion.
<code>-DeleteExpiredItem</code>	Specifies whether to permit Enterprise Vault automatically to delete the archived items when their retention period has expired. Set to <code>\$false</code> to prevent deletion, or <code>\$true</code> to permit Enterprise Vault to delete the expired items.
<code>-Description</code>	Provides a short description for display in the archive properties in the Administration Console.
<code>-AdminNote</code>	Provides an administrative note for display in the archive properties in the Administration Console.

Table 3-8 Set-EVArchive parameters (*continued*)

Parameter	Description
-RetentionPlanName	<p>Specifies the name of a retention plan to apply to the archive.</p> <p>Note that when the archiving task next performs mailbox synchronization, it may overwrite the specified retention plan with the retention settings of the appropriate provisioning group. For an Exchange mailbox archive, this is only the case if you have unchecked the Overall lock option in the Exchange mailbox policy settings.</p>

Examples

- `Set-EVArchive 14B...EVSERVER.LOCAL -DeleteProtected:$true -DeleteExpiredItems:$false`

Stops both users and Enterprise Vault from deleting the items in the nominated archive, and so places it on legal hold.
- `Set-EVArchive 14B...EVSERVER.LOCAL -DeleteProtected:$false -AdminNote "Item deletion allowed $(get-date) by $(gc env:username) "`

Allows users manually to delete the items in the nominated archive, and modifies its administrative note.
- `Get-EVArchive localhost Domain\User -OnHold:$false | Set-EVArchive -DeleteProtected:$true -DeleteExpiredItems:$false -Description "Archive placed on legal hold $(get-date) by $(gc env:username) from $(gc env:computername) "`

With `Get-EVArchive`, generates a list of the archives on the local Enterprise Vault server which are not on legal hold and in which the user `Domain\User` has delete permissions. `Get-EVArchive` passes the list to `Set-EVArchive`, which places the archives on hold and sets the archive description accordingly.
- `Set-EVArchive 14B...EVSERVER.LOCAL -RetentionPlanName RPFForManagers`

Applies the retention plan "RPFForManagers" to the nominated archive.
- `Set-EVArchive 14B...EVSERVER.LOCAL -RetentionPlanName ""`

Removes any retention plan that was previously applied to the nominated archive.

Output

[Table 3-9](#) lists the properties that are available.

Table 3-9 Set-EVArchive properties

Name	Type	Description
Archiveld	String	The Archiveld of the archive to modify.
ArchiveName	String	The name of the archive to modify.
Updated	Boolean	Indicates whether the archive was updated by the cmdlet. Possible values are: <code>\$true</code> (archive was updated), <code>\$false</code> (archive was not updated).

Related cmdlets

- See “[Get-EVArchive](#)” on page 88.

About moving archives

Enterprise Vault’s Move Archive wizard lets you move content from existing Domino and Exchange mailbox archives, and from Domino and Exchange journal archives, to new archives or existing archives in other vault stores.

You can use the wizard to move mailbox archives between vault stores in one site, and between two sites. This includes moves between two sites that are controlled by different Enterprise Vault directories.

Move Archive supports the move of journal archives only within an Enterprise Vault site.

Note: Move Archive supports the move of archives to destination servers that run Enterprise Vault 11.0 or later.

Move Archive handles each move operation differently, depending whether the source and destination archives are associated with a mailbox at the time of the move. Move Archive considers an archive to be:

- Active if it is associated with a mailbox, regardless of whether the mailbox is enabled for archiving
- Inactive if it is not associated with a mailbox

Move Archive does not support move operations for the following archive types:

- File System Archiving (FSA) archives
- SharePoint archives
- Shared archives

- Exchange public folder archives

Move Archive also prevents moves in the following circumstances:

- The source archive exceeds its archive usage limit and the destination is a new archive.
- The destination archive exceeds its archive usage limit.

In these cases you should increase the appropriate archive's usage limit on the **Archive Properties: Archive Usage Limit** tab in the Administration Console.

How Move Archive works

When you have submitted a number of Move Archive operations using the wizard, each move is then controlled by the Move Archive task. The Move Archive task is responsible for the actions that must take place as part of an archive move. For example, the Move Archive task copies the content from the source archive to the destination. The Move Archive task also manages the wait time that is necessary while other archiving operations take place. For example, the Move Archive task waits for the mailbox archiving task to point mailbox shortcuts to the items in the destination archive.

For each Move Archive operation, the Move Archive task does the following in the order listed:

- Closes the source archive to prevent Enterprise Vault from archiving any further content to it.
- Renames the source archive.
- Copies the content from the source archive to the destination archive.
- Synchronizes the permissions from the user's mailbox to the destination archive.
- Waits for the mailbox archiving task to point shortcuts to the items in the destination archive (in the case of mailbox archives).
- Waits for the destination vault store to be backed up.
- Verifies that all the data is present in the destination archive. If any items are missing from the destination archive, the Move Archive task repeats the copy of content from the source, and all the subsequent steps. This can happen up to five times before the Move Archive task fails the move operation.

When verification has completed successfully, the move operation is complete. If necessary, you can then delete the source archive.

How Compliance Accelerator and Discovery Accelerator affect Move Archive

Using Compliance Accelerator or Discovery Accelerator in your environment can place certain restrictions on Move Archive operations. Both applications can register an interest in an archive in the following circumstances:

- Items in the archive appear in the results of a Compliance Accelerator or Discovery Accelerator search.
- Items in the archive are in a Compliance Accelerator or Discovery Accelerator review set.

When Compliance Accelerator or Discovery Accelerator has registered an interest in an archive, you can move the archive, but cannot delete it at the end of the move operation.

Discovery Accelerator also lets users place cases on legal hold to prevent the deletion of archived items that are included in the case. Move Archive prevents you from moving and deleting any archives which contain items included in Discovery Accelerator cases that have been placed on legal hold.

Move Archive and indexing levels

When you move an archive to an existing destination archive, the destination archive retains the indexing level it had before the move.

However, when you move an archive to a new destination archive, the indexing level that Move Archive sets depends on whether the archive is associated with a mailbox after the move.

If the new destination archive is associated with a mailbox after the move, the archive inherits the mailbox's indexing level. If there is no mailbox association after the move, Move Archive sets the destination site's default indexing level on the archive.

Move Archive and user-deleted items

Enterprise Vault lets you retain items that users delete from their archives so that they are available for recovery for a period of time. You can enable this feature using the **Enable recovery of user deleted items** option on the **Site Properties: Archive Settings** tab. Enterprise Vault then retains user-deleted items for the number of days that you set.

Note: During a move operation, Move Archive does not copy these deleted items from the source archive to the destination. As a result, the deleted items are not available for recovery from the destination archive.

Move Archive and retention plans

If you have assigned a retention plan to the source archive in a Move Archive operation, you must take some additional steps to ensure that the retention plan is transferred to the destination archive. Otherwise, there is a danger that Enterprise Vault will apply the wrong retention and classification settings to the items that it adds to the new archive. How you proceed depends on whether the destination archive belongs to a provisioning group.

- When the destination archive belongs to a provisioning group, Enterprise Vault assigns the retention plan to it during the next provisioning run. If you do not want to wait for this to happen, use the **Run Now** facility in the Administration Console to run the Provisioning task immediately.
- For journal archives and other types of archives that do not belong to a provisioning group, you can assign the retention plan by editing the properties of the archive with the Administration Console. You can also assign the retention plan with a PowerShell cmdlet, `Set-EVArchive`. See [“Set-EVArchive”](#) on page 92.

After you have assigned the retention plan to the destination archive, rebuild the index of the archive. This ensures that Enterprise Vault applies the correct retention and classification settings to any newly-archived items. Note that Enterprise Vault may discard certain items during this operation, if they match a discard rule in the classification policy.

See [“About the Rebuild wizard”](#) on page 153.

About moving mailbox archives within a site

Move Archive lets you move archives within an Enterprise Vault site. For example, this is useful when you want to move existing archives to a new storage device. You might also want to move archives to a newer server to take advantage of the features introduced in Enterprise Vault version 8.0, such as the optimized single instance storage model.

Within an Enterprise Vault site, Move Archive supports the following moves:

- Moving an active archive to a new archive
- Moving an inactive archive to an active archive
- Moving an active archive to an inactive archive

Moving an active archive to a new archive

This section describes the move of an archiving enabled user’s default archive in the source vault store, to a new archive in the destination vault store. In this case,

the new archive in the destination automatically becomes the default archive for subsequent archiving.

In summary, this Move Archive operation includes the following steps:

- Move Archive closes the source archive to prevent Enterprise Vault from archiving any further content to it. However, the source archive is still accessible in read-only mode.
- Move Archive renames the source archive. It appends the archive's creation date, and the date of the move operation to the archive's name.
- Move Archive copies the data from the source archive to the destination.
- Enterprise Vault synchronizes the permissions from the user's Domino or Exchange mailbox to the new archive.
From this point, Enterprise Vault archives new content to the destination archive.
- The mailbox archiving task on the destination server points all the shortcuts in the user's mailbox to the content in the new archive in the destination site. Move Archive completes this step even if you do not use mailbox shortcuts in your environment.
- Move Archive waits for the destination vault store to be backed up.
- Move Archive verifies that all the data is present in the destination archive.

The move operation is now complete and you may delete the source archive.

Moving an inactive archive to an active archive

This section describes the move of an archiving enabled user's non-default archive in the source vault store, to an existing default archive in the destination vault store.

In summary, this move operation includes the following steps:

- Move Archive closes the source archive. However, the source archive is still accessible in read-only mode.
- Move Archive renames the source archive. It appends the archive's creation date, and the date of the move operation to the archive's name.
- Move Archive copies the data from the source archive to the destination.
- The mailbox archiving task on the destination server runs and processes shortcuts if required.
Move Archive completes this step even if you do not use mailbox shortcuts in your environment.
- Move Archive waits for the destination vault store to be backed up.
- Move Archive verifies that all the data is present in the destination archive.

The move operation is now complete and you may delete the source archive.

Moving an active archive to an inactive archive

This section describes the move of an archiving enabled user's default archive in the source vault store, to an inactive archive in the destination vault store.

In summary, this Move Archive operation includes the following steps:

- Move Archive closes the source archive to prevent Enterprise Vault from archiving any further content to it. However, the source archive is still accessible in read-only mode.
- Move Archive renames the source archive. It appends the archive's creation date, and the date of the move operation to the archive's name.
- Move Archive copies the data from the source archive to the destination.
- Move Archive waits for the destination vault store to be backed up.
- Move Archive verifies that all the data is present in the destination archive.

The move operation is now complete and you may delete the source archive.

Moving other mailbox archives

You can also move other mailbox archives between vault stores, such as source archives that are not associated with archiving enabled mailboxes. You can move these archives to new destination archives, or to other existing archives that are not associated with a mailbox.

In cases like these, Move Archive moves the content from one archive to another. However, Enterprise Vault does not complete any shortcut processing because neither the source archive nor the destination archive is associated with an archiving enabled user.

About moving mailbox archives between sites

Move Archive lets you move archives between Enterprise Vault sites. This includes sites that belong to different Enterprise Vault directories. For example, a move between sites is useful when users move to a new location and you move their mailboxes to a mail server in the new site.

Note: When move operations cross two Active Directory domains, a one-way trust is required for the moves to proceed. The destination domain must trust the source domain.

Between Enterprise Vault sites, Move Archive supports the following move:

- Moving an inactive archive to an active archive

Moving active archives between sites

Move Archive lets you move archives between Enterprise Vault sites. This is useful when you want to move an individual user's mailbox to a different Domino or Exchange mail server in another Enterprise Vault site.

In this case, you must disable archiving for the user in the source site, then move the mailbox and enable it for archiving in the destination. When you have done this, you can use Move Archive to move the associated archive to the destination site.

This section describes the actions you must complete to move a user's mailbox, and the subsequent steps that are required to move the archive.

To move the user's mailbox:

- Disable archiving on the user's mailbox in the source site.
- Move the user's mailbox from the source mail server to the mail server in the destination site.
- Provision the user's mailbox on the destination Enterprise Vault server.
- Enable the user for archiving in the destination site.

Note: Ensure that you run the provisioning task before running the **Enable Mailbox** wizard to remove association of the mailbox with the original Site.

The user's mailbox is now enabled for archiving in the destination site, but the existing shortcuts in the user's mailbox still point to the source archive. New content is archived to the newly created destination archive.

When you have moved the user's mailbox and enabled it for archiving in the destination site, you can move the inactive source archive. In this case, the move operation includes the following steps:

- Move Archive closes the source archive. However, the source archive is still accessible in read-only mode.
- Move Archive renames the source archive. It appends the archive's creation date, and the date of the move operation to the archive's name.
- Move Archive copies the data from the source archive to the destination.
- The mailbox archiving task on the destination server points all the shortcuts in the user's mailbox to the content in the newly created archive in the destination site.

Move Archive completes this step even if you do not use mailbox shortcuts in your environment.

- Move Archive waits for the destination vault store to be backed up.
- Move Archive verifies that all the data is present in the destination archive.

The move operation is now complete and you may delete the source archive.

Moving other mailbox archives between sites

You can also move an inactive archive in the source site to an existing inactive archive or to a new archive in the destination site.

However Enterprise Vault completes shortcut processing only when the destination is an existing archive that is associated with a user mailbox.

In summary, these Move Archive operations include the following steps:

- Move Archive closes the source archive to prevent Enterprise Vault from archiving any further content to it. However, the source archive is still accessible in read-only mode.
- Move Archive renames the source archive. It appends the archive's creation date, and the date of the move operation to the archive's name.
- Move Archive copies the data from the source archive to the destination.
- If the destination archive is associated with a user mailbox, Enterprise Vault synchronizes the permissions from the user's Domino or Exchange mailbox to the new archive.
- If the destination archive is associated with a user mailbox, the mailbox archiving task on the destination server points all the shortcuts in the user's mailbox to the content in the destination archive.
Move Archive completes this step even if you do not use mailbox shortcuts in your environment.
- Move Archive waits for the destination vault store to be backed up.
- Move Archive verifies that all the data is present in the destination archive.

The move operation is now complete and you may delete the source archive.

About moving journal archives within a site

Move Archive lets you move Domino and Exchange journal archives only within an Enterprise Vault site, and you cannot move a journal archive that is currently in use by the journaling task. When you want to move a source journal archive that is in use, first you must configure the journaling task to use a new archive in the

destination vault store. To change the archive that is used by the journaling task, use the Administration Console to edit the journal mailbox properties.

You can move an inactive journal archive to a new archive, to an existing active archive, or to another inactive archive.

About configuring Move Archive

You can control Move Archive's behavior using two XML configuration files:

- `EvMoveArchiveTask.exe.config`, which controls the Move Archive task
- `EvTaskGuardian.exe.config`, which controls the task guardian service

Configuring the Move Archive task

`EvMoveArchiveTask.exe.config` controls the moves of any archives in the vault stores that are associated with the storage service on the server where it is present.

A basic version of this file exists in the Enterprise Vault installation folder, for example `C:\Program Files (x86)\Enterprise Vault`. The installation folder also contains another file which is called `Example EvMoveArchiveTask.exe.config`. This file contains examples of the additional settings you can change to control the Move Archive task.

To change the default behavior of the Move Archive task

- 1 Rename `EvMoveArchiveTask.exe.config` in case you need to revert to it later.
- 2 Edit the settings in `Example EvMoveArchiveTask.exe.config`, as described below.
 - `RescheduleIntervalInMins`

For each move operation, Move Archive enters a sleep state between each stage of the move. For example, Move Archive enters the sleep state while it waits for shortcut processing, and for destination archive backup. `RescheduleIntervalInMins` sets the length of this sleep state in minutes. At the end of the interval, Move Archive resumes processing if a processing slot is available.

You should consider setting a longer interval in environments where you move large numbers of archives at the same time. Specify a value between 5 and 1000. The default value is 30.
 - `SkipDuplicateItems`

If Move Archive finds that items from the source archive are duplicated in the destination vault store, it writes errors to the event log for the first 10 duplicates, and then marks the move operation as failed. It does this

because the presence of duplicates can indicate that the source archive has already been moved to the destination.

Note: All the items in one vault store must have a unique transaction ID. Move Archive considers two items in one vault store to be duplicates when they both have the same transaction ID.

You can change this behavior by setting `SkipDuplicateItems` to 1. Then, Move Archive still logs the duplicate items but skips them and proceeds with the move operation.

- `ReportVersions`

For each source archive it processes, Move Archive creates a report file in the `Reports\Move Archive` subfolder of the Enterprise Vault installation folder (for example `C:\Program Files (x86)\Enterprise Vault`). If you move the same archive a second time, following a failure for example, Move Archive creates another report when it processes the archive for the second time. `ReportVersions` sets the number of these report files it retains for each source archive, before it removes the oldest file.

Specify a value between 1 and 100. The default value is 5.

- 3 Rename the file to `EvMoveArchiveTask.exe.config`.
- 4 Restart the Move Archive task.

Configuring task guardian service

When Move Archive enters a temporary error state while it processes an archive, it waits for a period of time before it retries the archive. You can change the default retry interval using the `RetryTimeInMinutes` key in the task guardian service configuration file. `EvTaskGuardian.exe.config` controls the retry interval on each Enterprise Vault server where it is present.

A basic version of this file exists in the Enterprise Vault installation folder, for example `C:\Program Files (x86)\Enterprise Vault`. The installation folder also contains another file called `Example EvTaskGuardian.exe.config`. This file contains an example of the `RetryTimeInMinutes` key.

Default value:	30
Minimum value:	5
Maximum value:	1000

To change the default behavior of the task guardian service

- 1 Rename `EvTaskGuardian.exe.config` in case you need to revert to it later.
- 2 Edit the `RetryTimeInMinutes` setting in Example `EvTaskGuardian.exe.config`.
- 3 Rename the file to `EvTaskGuardian.exe.config`.
- 4 Restart the task guardian service.

Changing Move Archive's performance

By default, Move Archive operations are given a lower priority than other Enterprise Vault tasks on the server. You can change Move Archive's priority setting and other aspects of its performance using the **Settings** tab in **Move Archive Task properties**.

For guidance on Move Archive performance adjustment using the options on the **Settings** tab, see the Enterprise Vault *Performance Guide* which is available on the Enterprise Vault Support website:

<http://www.veritas.com/docs/000005725>

To change Move Archive's performance

- 1 In the Administration Console, right-click the Move Archive Task and click **Properties**.
- 2 Click the **Settings** tab.
- 3 Change the settings as required and click **OK**.

If you change **Priority of Move Archive operations in relation to other processes** or **Number of threads per move operation**, you must restart the Move Archive Task for the changes to take effect.

If you change **Number of concurrent move operations**, you must restart the Task Controller service for the changes to take effect.

Running Move Archive

To run the Move Archive wizard, you must log in using the vault service account, or use an account that is assigned to the power administrator role.

In the case of moves between two sites that are controlled by different Enterprise Vault directories, your source user account must be assigned to the power administrator role in the destination Enterprise Vault directory.

If the archive contains items that were archived using an Enterprise Vault extension content provider, the source user requires an additional role. In addition to the power administrator role, you need to assign the source user to the Extension Content Provider Application role in the destination directory.

See “Roles-based administration” in the *Administrator’s Guide*.

To run Move Archive

- 1 In the left pane of the Administration Console, right-click **Archives** and click **Move Archive**.
- 2 Work through the pages of the wizard and select appropriate options.

Move Archive introduction page

This page introduces the Move Archive wizard and provides important information which you should read before you proceed.

Note: Move Archive supports the move of archives to destination servers that run Enterprise Vault 11.0 or later.

Move Archive does not support move operations for the following archive types:

- Closed archives
- File System Archiving (FSA) archives
- SharePoint archives
- Shared archives
- Exchange public folder archives

Move Archive also prevents moves in the following circumstances:

- The source archive exceeds its archive usage limit and the destination is a new archive.
- The destination archive exceeds its archive usage limit.

In these cases you should increase the appropriate archive’s usage limit on the **Archive Properties: Archive Usage Limit** tab in the Administration Console.

Selecting a destination site

Move Archive lets you move mailbox and journal archives within the current Enterprise Vault site, or between two sites. Use this page to select the site into which you want to move the archives.

Note: You can move journal archives only within a site.

To move archives within a site

- ◆ Select the **Move archives within the current Enterprise Vault Site** option.

To move archives to another site

- 1 Select the **Move archives to a different Enterprise Vault Site** option.
- 2 Enter the name of the **Directory Service Computer** that controls the destination vault stores.

Selecting a site

If you have chosen to move archives to a destination that contains more than one site, this page lets you select a destination site.

To select a destination site

- ◆ Select a site from the **Destination Site** list.

Selecting archives

Use this page to select the archives you want to move, and to select destination archives.

Note: Move Archive does not let you move ineligible archives. You cannot move closed archives, FSA archives, SharePoint archives, shared archives, Exchange public folder archives, or archives that contain items placed on legal hold by Discovery Accelerator.

To add archives

- 1 Click **Add**.
- 2 Use the **Select Source** dialog box to add the archives you want to move.

When you move an archive that is currently in use by an archiving-enabled user, you can only move it to a new archive. In this case, **<New archive>** is selected automatically in the **Destination Archive** column next to the archive, and you cannot change it. You can only move active archives within a site.

When you move an inactive archive, you can select an existing archive as the destination, either in the current site or in another site.

To select a destination archive

- 1 Select the source archive for which you want to select a destination archive.
- 2 Click **Move To** and click **Select Destination**.
- 3 Use the **Select Destination** dialog box to select a destination archive.

To move archives to new destination archives

- 1 Select one or more archives.
- 2 Click **Move To** and click **New Archive**.

To remove an archive from the list

- ◆ Select an archive and click **Remove**.

You can also display more information about any pair of source and destination archives on this page.

To display the properties of a pair of source and destination archives

- 1 Select the row whose properties you want to display.
- 2 Click **Properties**.

Select destination

Use this dialog box to search for the archive you want to set as the destination.

To search for a specific archive

- 1 Enter all or part of the name of an archive in the search box.
- 2 Click the search icon.

The archives whose names contain the string you entered appear in the list.

You can display the properties of any of the archives in the list.

To show an archive's properties

- 1 Select the archive whose properties you want to see.
- 2 Click **Properties**.

To set an archive as the destination

- ◆ Select the archive and click **OK**.

Selecting destination vault stores

If you have chosen to move any archives to new destination archives, this page lets you choose a destination vault store for each. Each destination archive must be in a different vault store from the associated source archive.

To select destination vault stores

- 1 Select one or more source archives.
- 2 Click **Select Destination**.
- 3 Use the **Select Vault Store** dialog box to select a destination vault store for the selected archives.

Selecting billing accounts

Use this page to change the billing accounts assigned to the destination archives. By default, new destination archives are assigned the same billing account as the source archive. For existing destination archives, the **New Billing Account** column shows the billing account already assigned to the archive.

To change a billing account

- 1 Find the archive whose billing account you want to change.
- 2 Under the **New Billing Account** column, enter a new billing account in this format:

domain\username

You can also click the browse icon next to the billing account and use the **Select a User or Group** dialog box to select a new billing account.

Matching retention categories

When you move archives from one Enterprise Vault site to another, you can use this page to match source retention categories to destination retention categories.

For each source retention category, Move Archive tries to find a retention category in the destination site that matches the source, based on name and retention period. If it can find a matching category, it appears in the **Destination Retention Category** column. You can change the destination retention categories that Move Archive has matched automatically.

A check icon in the right column indicates that Move Archive has matched retention categories automatically. The first time you run the Move Archive wizard, this icon is green. Move Archive remembers the selections you make each time you run the wizard, and they become the defaults for next time. When you run the Move Archive wizard again, the matched retention categories are identified by a gray check icon.

In the case of Exchange managed folders, Move Archive maps all their associated retention categories in the source to just one destination retention category. You can change the destination retention category, but the change maps all the source retention categories to the single destination category you select.

For each source retention category where there is no match, you must select a destination retention category.

To select or change a destination retention category

- 1 Find the source retention category whose destination retention category you want to change.
- 2 Under the **Destination Retention Category** column, use the drop-down list by each source retention category to select a destination retention category.

You can also display more information about any pair of source and destination retention categories on this page.

To display the properties of a pair of source and destination retention categories

- 1 Select the row whose properties you want to display.
- 2 Click **Properties**.

If you do not find a suitable retention category in the destination site, you can use the Administration Console at the destination site to create one. When you have done this, click **Refresh** on this page to make the new retention category available for selection.

Reviewing the archives you have chosen to move

This page lets you review the archives you have chosen to move before you close the Move Archive wizard.

This page lists the following for each archive:

- **Type**. The icon shows the archive's type: Domino mailbox archive, Domino journal archive, Exchange mailbox archive, or Exchange journal archive.
- **Source Archive**. The name of the source archive.
- **Destination Archive**. The name of the destination archive. This column shows **<New archive>** if you are moving the source archive to a new archive.
- **Destination Vault Store**. The name of the vault store that hosts the destination archive.

Once you have reviewed the archives you have chosen to move, click **Finish**.

Displaying the status page

On this page, select the **Show the 'Move Archive Status' dialog** option if you want to monitor the progress of the archive moves.

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. If you want to start the task straight away, select the **Start the new tasks now** option. Enterprise Vault shows this option only once for each storage server.

Monitoring Move Archive

All the Move Archive operations you have submitted are displayed in the **Move Archive Status** page. If you selected the **Show the 'Move Archive Status' dialog** option when you ran the Move Archive wizard, Enterprise Vault displays the **Move Archive Status** page when you close the wizard. You can also display the page at any other time.

To display the Move Archive Status page

- ◆ In the Administration Console, right-click **Archives** and click **Move Archive Status**.

For each move operation, the **Move Archive Status** page shows the following:

- **Source Archive.** The original name of the source archive. This is the archive's name before Move Archive renames it.
- **Move Status.** The current move status for this archive.
See "[Move Archive statuses](#)" on page 111.
- **Destination Archive.** The name of the destination archive. This column shows **<New archive>** if you are moving the source archive to a new archive.
- **Source Server.** The fully qualified domain name of the source storage service computer.
- **Destination Server.** The fully qualified domain name of the destination storage service computer.
- **Start Time.** The date and time at which the archive was submitted.

To see additional information about any of the move operations in the list

- 1 Select a move operation.
- 2 Click **Properties**.

The **Move Archive Properties** dialog box shows additional information, including the names and locations of the log files associated with the move operation.

To see the latest statuses for the archives you have submitted

- ◆ Click the refresh button on the toolbar.

If you are moving large numbers of archives, you can find specific source archives using the search feature on the **Move Archive Status** page.

To search for a source archive

- 1 Enter all or part of the name of the source archive in the **Find source archive where the name contains:** box.
- 2 Click the search button.

You can also sort any of the columns on the **Move Archive Status** page by clicking the column heading.

Modifying move operations in the Move Archive Status page

The **Move Archive Status** page lets you selectively modify the move operations of archives in the queue. For example, you can sort the operations by destination site, select all the move operations, then stop them during maintenance on the site.

Note: You cannot stop a move operation during the shortcut processing stage.

You can use **Restart** when the move status is either **Completed** or **Completed with errors**.

You can use **Continue** or **Retry failed items** when the move status shows **Failed** or **Error**.

To modify the move operations

- 1 Select the archives you want to start, stop, or any other action.
- 2 Click the **Start**, **Stop**, or any other available action.
- 3 Click the **Refresh** button to see the changes in statuses for the selected archives.

Move Archive statuses

Move operations whose status is **Failed** or **Error** appear in red and require your intervention to proceed.

Archives in the **Move Archive Status** page can have the following statuses:

- **Queued.** The archive is queued for processing. Move Archive starts processing the archive when the Move Archive task runs. You can wait for the task to run to its schedule, or right-click the task and click **Run Now**.
- **Step 1 of 5 - Copying (x%).** Move Archive is processing the archive.

- **Step 2 of 5 - Waiting to update shortcuts.** Move Archive has finished moving items from the source archive to the destination, and is waiting for the Domino or Exchange mailbox archiving task to update the shortcuts in the user's mailbox. You can wait for the task to run to its schedule, or right-click the task and click **Run Now**.

Note: Shortcut processing for disabled archives occurs only when you run the mailbox archiving task for all mailboxes.

During this stage, Move Archive checks whether shortcut processing has completed and enters a sleep state if it has not completed. By default, the length of the sleep state is 30 minutes. When the sleep state ends, Move Archive again checks to see if the shortcut processing has completed.

Move Archive completes this step even if you do not use mailbox shortcuts in your environment.

- **Step 3 of 5 - Updating shortcuts.** The Domino or Exchange mailbox archiving task is updating the shortcuts in the user's mailbox.
- **Step 4 of 5 - Waiting for destination backup.** Move Archive is waiting for the vault store that contains the destination archive to be backed up. During this stage, Move Archive checks whether the destination archive has been backed up and enters a sleep state if it has not been backed up. By default, the length of the sleep state is 30 minutes. When the sleep state ends, Move Archive again checks to see if the destination archive has been backed up.
- **Step 5 of 5 - Verifying moved items (x%).** Move Archive is checking that the destination contains all the items that it moved from the source archive. This does not include items that users have deleted, and items that Enterprise Vault has expired.
- **Error.** When Move Archive encounters an error on an archive, it tries to move the archive five times before it changes the status to **Failed**. In between retries, Move Archive sets the archive's status to **Error**. Move operations whose status is **Error** appear in red and require your intervention to proceed.
- **Completed.** Move Archive has completed all processing for this archive.
- **Completed with errors.** Move Archive has completed all processing but there were some errors.
For more information on move operations that have completed with errors, see the following technical note on the Enterprise Vault Support website:
<http://www.veritas.com/docs/000041084>
- **Failed.** Move Archive has failed to process the archive.

Move operations whose status is **Failed** appear in red and require your intervention to proceed.

To find why a Move Archive operation has failed, check the Move Archive report files in the `Reports\Move Archive` subfolder of the Enterprise Vault installation folder (for example `C:\Program Files (x86)\Enterprise Vault`).

See “[Move Archive reporting and monitoring](#)” on page 115.

Move Archive lets you use **Continue** or **Retry failed items** on move operations that have a status of **Failed** or **Error**, unless the failure occurred during the verification stage. You can use **Restart** when the move status is either **Completed** or **Completed with errors**.

See “[Managing Move Archive operations with Failed and Error statuses](#)” on page 114.

Deleting archives after Move Archive

When Enterprise Vault has finished moving an archive, its status in the **Move Archive Status** page is **Completed**. You can remove the completed archives from this page, and a prompt asks if you also want to delete the source archive.

Note: You cannot delete an archive when Compliance Accelerator or Discovery Accelerator has registered an interest in it, or when Discovery Accelerator has placed items in the archive on legal hold.

See “[How Compliance Accelerator and Discovery Accelerator affect Move Archive](#)” on page 96.

At the end of a move operation, an archive’s status can be **Completed with errors**. This happens when Move Archive records errors during the move, but does not consider the errors to be serious enough to terminate the move operation. Before you remove archives that have completed with errors, you should check the Move Archive log files for the archive to ensure the errors are not serious or unexpected. For example, you might expect some items to be absent following the failure of a storage device.

For more information on move operations that have completed with errors, see the following technical note on the Enterprise Vault Support website:

<http://www.veritas.com/docs/000041084>

To remove completed archives

- 1 Select the completed archives you want to remove from the **Move Archive Status** page.
- 2 Click the **Delete** button on the toolbar.
- 3 At the prompt **Do you want to delete the source archives as well?**, click **Yes** if you want to delete the associated source archives, or **No** if you do not.

If you choose not to delete source archives when you remove them from the **Move Archive Status** page, you can remove them subsequently from the Administration Console.

Note: If you encounter errors deleting one or more source archives or vault stores due to SIS parts that are shared with another archive or vault store, do not try to delete the vault store manually through SQL. Open a case with Veritas Technical Support to investigate the problem.

Managing Move Archive operations with Failed and Error statuses

Move operations whose status is **Failed** or **Error** appear in red and require your intervention to proceed.

Move operations can fail or complete with errors due to transient problems. For example, move operations can fail because the source vault store is unavailable during the initial data copy stage. When this happens, you can retry move operations after you have resolved the problem.

Move Archive lets you retry move operations that have a status of **Failed**, or **Error** unless the errors occurred during the verification stage.

Use of **Restart**, **Continue**, and **Retry failed items**:

- Use **Restart** when the move status is either **Completed** or **Completed with errors**.
- Use **Continue** or **Retry failed items** when the move status shows **Failed** or **Error**.

For more information on move operations that have completed with errors, see the following technical note on the Enterprise Vault Support website:

<http://www.veritas.com/docs/000041084>

To retry move operations

- 1 In the **Move Archive Status** page, select one or more move operations that have the status **Failed** or **Error**.
- 2 Right-click the selected move operations and click **Retry failed items**.
- 3 Click **OK** to confirm your request.

Move Archive resubmits the move operations, and their status initially reverts to **Queued** before processing begins again.

When Move Archive starts processing a retried move operation, it begins processing from the first point of failure.

Similarly, you can use **Continue** to proceed without retrying the failed items.

Move Archive reporting and monitoring

Move Archive creates up to three report files for each move operation, in the `Reports\Move Archive` subfolder of the Enterprise Vault installation folder (for example `C:\Program Files (x86)\Enterprise Vault`).

Move Archive names the three report files using the following convention:

```
MoveArchive_archive_yyyymmddhhmmss.txt  
MoveArchive_archive_yyyymmddhhmmss_Errors.txt  
MoveArchive_archive_yyyymmddhhmmss_Verification_nnnn.txt
```

where:

- *archive* is the name of the archive.
- *yyymmddhhmmss* is the date and time when the report was generated.
- *nnnn* represents a sequential number. To produce verification files of a manageable size, Move Archive rolls over the verification report to a new file each time the maximum file size is reached. This sequential number shows the order of the files.

`MoveArchive_archive_yyyymmddhhmmss.txt` contains a summary report for the move operation. The report shows the start and end time for the move operation, including the times for the start and end of each phase. It also shows counts of the items processed.

`MoveArchive_archive_yyyymmddhhmmss_Errors.txt` reports errors that occurred during the move operation.

`MoveArchive_archive_yyyymmddhhmmss_Verification_nnnn.txt` contains a report of any differences between source items and their corresponding items in the destination archive.

For information on how to troubleshoot Move Archive verification errors, see the following technical note on the Enterprise Vault Support website:

<http://www.veritas.com/docs/000041084>

Deleting an archive

You can delete an archive, provided that the Administration Console shows a status of Available or Closed.

Note the following:

- There is no undo when you delete an archive, and you cannot stop the deletion process.
- Be careful about deleting an archive that still has an associated mailbox. There will be many errors from the Exchange Mailbox task when it tries to archive to a deleted archive. Make a note of those users who have access to the archive and then get them to change their archiving settings, so that they do not try to archive to the archive you are about to delete. Use the Permissions tab on the archive's property page to find out who has access to the archive.

To delete an archive

- 1 In the Administration Console, with the archive displayed in the listing, press F5 to refresh the view. This shows you the archive's current status.
- 2 Right-click the archive that you want to delete and, on the shortcut menu, click **Delete**.
- 3 When prompted, confirm that you do want to delete the archive.

The archive's status changes to Marked for deletion. You can no longer view the properties of the archive and shortcuts to items within the archive no longer work.

Deleting a vault store

You can delete a vault store that is no longer required. Deletion permanently removes all the partitions and archives that the vault store contains, and all the items that are stored in them.

You can delete a vault store only if all of the following conditions apply to the vault store:

- It is not a default vault store for automatically-enabled archives.
- It does not contain any archives that are associated with archiving targets.

- Its status is Available.
- It is not in backup mode.
- Its vault store database is not in a SQL AlwaysOn availability group. If it is, you must first remove it from the availability group.

Note: You can also delete vault stores by deleting the vault store group they belong to. When you delete a vault store group, all the vault stores it contains must still meet the criteria described in this section. If the vault store group's database is in a SQL AlwaysOn availability group, you must remove it from the availability group before you can delete it.

When you delete a vault store, its status changes to Marked for Deletion. Shortcuts to items within the vault store's archives no longer work.

Enterprise Vault may take a long time to complete the deletion operation. If the vault store contains any items that are on legal hold, or any SIS parts that are referenced by other vault stores, Enterprise Vault marks the vault store for deletion but it does not delete the vault store until these conditions no longer apply.

Note: If you delete a vault store, you cannot stop or undo the process. The action overrides any form of deletion protection that is applied to items or Retention Categories, other than legal hold.

To delete a vault store

- 1 In the Administration Console, select the vault store group that contains the vault store that you want to delete.
- 2 The right pane of the Administration Console displays the status of the group's vault stores. Click F5 to refresh the view. The right pane displays each vault store's current status, and indicates whether backup mode is set. You can only delete a vault store if the status is Available and backup mode is not set.
- 3 Right-click the vault store that you want to delete and, on the shortcut menu, click **Delete**.
- 4 On the warning dialog, click **Delete**.

The status of the vault store changes to Marked for Deletion.

When Enterprise Vault eventually completes the deletion, it removes the vault store from the list.

Setting a system message

Users see the system message when they use the Enterprise Vault Web Access application. For example, you can use the message to indicate periods when there is going to be an interruption to the service because of hardware changes.

The message is not visible to a user who is using a shortcut to retrieve an item, but only to a user who is searching by using the Enterprise Vault Web Access application. The message is available to all users in the Enterprise Vault site.

To change the system message from the Vault Administration Console

- 1 In the left pane of the Administration Console expand the hierarchy until the appropriate vault site is visible.
- 2 Right-click the vault site and then, on the shortcut menu, click **Properties**.
- 3 In the Site Properties dialog box, click the **General** tab.
- 4 Edit **System message** as required.
- 5 Click **OK** to accept your changes.
- 6 Stop and restart the IIS Admin service to make the change take effect.

About index volumes

When an index volume becomes full, Enterprise Vault automatically creates a new one. In the Administration Console, the Advanced tab of an archive's properties shows the number of index volumes.

Each new index volume does not have the same index root path as the previous one. The new location for the new index is a random selection from the Indexing Service's open index root paths.

If an archive has more than one index volume, the initial search is performed against the current index volume, which contains the most recently-archived items. To view search results from earlier index volumes, you must choose a date range from a list. The date ranges correspond to the archived date range of items in the index volumes.

Rollover is more likely to occur for File System Archiving archives, Journal archives, and Public Folder archives than for normal mailbox archives.

Rollover archives created before Enterprise Vault 6.0 SP1 are not merged back into the master archive. Archiving continues to the current rollover archive, and that archive's index expands to multiple index volumes as necessary.

Moving the directory database

You can move the directory database between SQL Server instances. This is useful for reconfiguration and disaster recovery.

To move the directory database

- 1 Move the directory database to the new SQL Server.
- 2 Make sure that the Vault Service account has the correct permissions to access the new database.

See the section called "Creating a SQL login account" in the *Installing and Configuring* guide.

- 3 In the left pane of the Administration Console, right-click the Enterprise Vault icon.
- 4 On the shortcut menu, click **Properties**.
- 5 Click **Change Directory SQL Server**.
- 6 Enter the new SQL Server.

Moving a vault store database

You can move a vault store database to a different SQL Server. This is useful for reconfiguration and disaster recovery.

To move the vault store database

- 1 Stop the Enterprise Vault Storage service.
- 2 Move the vault store database to the new SQL Server.
- 3 Make sure that the Vault Service account has the correct permissions to access the new database.

See the section called "Creating a SQL login account" in the *Installing and Configuring* guide.

- 4 In the Administration Console, right-click the vault store whose database you have moved, and click **Properties**.
- 5 Click the **Database** tab.
- 6 In the **SQL Server** box, enter the name of the new SQL Server.
- 7 Click **OK**.
- 8 Restart the Enterprise Vault Storage service.

Moving a fingerprint database

You can move a vault store group's fingerprint database to a different SQL Server if required, for example during disaster recovery.

For information on how to move a fingerprint database, see the following TechNote on the Enterprise Vault Support website:

<http://www.veritas.com/docs/000035817>

Moving the Monitoring database

You can move the Monitoring database between SQL Server instances. This is useful for reconfiguration and disaster recovery.

To move the Monitoring database

- 1 Move the EnterpriseVaultMonitoring database to the new SQL Server.
- 2 Make sure that the Vault Service account has the correct permissions to access the new database.

See the section called "Creating a SQL login account" in the *Installing and Configuring* guide.

- 3 Connect to the SQL server that is hosting the EnterpriseVaultMonitoring database, using SQL Enterprise Manager, SQL Query Analyzer, or a similar tool.
- 4 Enter and run the following SQL commands:

```
USE EnterpriseVaultDirectory
```

```
UPDATE MonitoringSettings SET SQLServer = "New_SQL_Server"
```

where *New_SQL_Server* is the name of the new SQL server.

Moving the auditing database

You can move the auditing database to a different SQL Server if required, for example during disaster recovery. When you have moved the database, complete the following procedure on each Enterprise Vault server on which auditing is enabled.

To move the auditing database

- 1 Move the auditing database to the new SQL Server.
- 2 On the Enterprise Vault server, use the ODBC Data Source Administrator to select the new SQL Server on the EVAudit ODBC data source.
- 3 Test the data source when the ODBC Data Source Administrator gives you the opportunity.

Changing the Vault Service account password

When you change the Vault Service account password it is important that the change is updated on all Enterprise Vault servers. The best method is to change the password while you are logged in as the Vault Service account.

To change the Vault Service account password

- 1 As the Vault Service account, start the Administration Console.
- 2 In the left pane, expand **Enterprise Vault**
- 3 Right-click **Directory** and click **Properties**.
- 4 In **Directory Properties**, click the **Service Account** tab.
- 5 Press **Ctrl+Alt+Del** and choose the option to change the password.
- 6 Change the account password and then return to the **Directory Properties** tab.
- 7 Change the password on the **Directory Properties** tab and click **OK**.

Using Enterprise Vault for records management

This chapter includes the following topics:

- [Introducing records management](#)
- [About records and non-records](#)
- [How Enterprise Vault marks items as records](#)
- [Setting up the required record types](#)
- [Setting the default record type for users](#)
- [Allowing users to change the record types of individual items](#)
- [Using the classification feature for records management](#)
- [Potential conflicts between EVPM and the classification feature](#)
- [Common configuration scenarios](#)
- [Searching archives for items marked as records](#)
- [Viewing the records management settings for one or more archives](#)
- [Exporting items from archives](#)

Introducing records management

Note: You require a license for the Enterprise Vault retention feature to implement records management.

This chapter describes how to use Enterprise Vault to mark archived items as records. By doing this you can fulfil the requirements of [Capstone](#) and similar records management systems.

Capstone is an approach to managing emails and other documents that the U.S. National Archives and Records Administration (NARA) has advocated. The aim of Capstone is to help U.S. federal agencies satisfy the requirements of the [Managing Government Records Directive \(M-12-18\)](#), which NARA issued in 2012. This directive requires federal agencies to eliminate paper and use electronic record-keeping to the fullest possible extent. The directive also requires them to manage both permanent records and temporary records in an accessible electronic format.

About records and non-records

In the Capstone approach to records management, a record is anything that documents government activities or that is used to conduct government business. Each record can be of two types: permanent or temporary. Items that do not meet the legal definition of a record are classed as non-records.

Permanent records

Permanent records are of historical value and worthy of long-term preservation in the U.S. National Archives. According to the Capstone guidelines, the following people are likely to send or receive items that are suitable for marking as permanent records:

- Officials at the higher levels of federal agencies or component organizations.
- Other staff members who regularly create or receive emails that are presumed to be of permanent value.
- Anyone else who creates or receives emails of permanent value.

The U.S. National Archives recommends that agencies consult the *United States Government Policy and Supporting Positions* (Plum Book), *U.S. Government Manual*, and other sources when assigning permanent account status. In this chapter, the term "Capstone officials" refers to those people for whom it may be appropriate to mark their emails as permanent records.

To simplify the process of records management, Capstone recommends that every email in the accounts of such people is treated as a permanent record by default. However, Capstone acknowledges that certain emails may not be worthy of preservation. In these instances, the account users have the option to mark the emails as non-permanent.

The Capstone approach requires federal agencies to make periodic transfers of permanent records to the National Archives. Depending on the security classification of the records, the National Archives may then make them publicly available.

Temporary records

Temporary records may contain government or business information but are of limited value. A federal agency does not transfer such records to the National Archives but still needs to retain them for a set period of time, based on the agency's needs.

Capstone recommends that those people who are not high-level policy makers but who may send or receive emails that constitute records have all their emails marked as temporary records by default. Again, however, Capstone gives these people the option to mark certain emails as either permanent records or non-records.

In this chapter, the term "Capstone non-officials" refers to those people for whom it may be appropriate to mark their emails as temporary records.

Non-records

Non-records are items that do not contain any government or business information, such as personal emails and charitable solicitations. Those people who have their emails marked as permanent records or temporary records by default also have the option to mark individual emails as non-records, where appropriate.

How Enterprise Vault marks items as records

By default, Enterprise Vault treats all the items that it archives as non-records. Changing this behavior, however, is simply a matter of configuring the retention categories that Enterprise Vault assigns to the archived items. You can configure each retention category so that, at the same time that Enterprise Vault assigns the retention category to an item, it also marks the item as a record of some sort. With a range of different retention categories to assign to items, you can mark each item as the appropriate type of record.

Enterprise Vault provides several ways to assign the required retention category to an item and thereby mark it as a record or non-record. For instance, you can do the following:

- Create one or more retention plans, each of which is associated with a different retention category. Then you can set up multiple provisioning groups to apply the required retention plans to selected user mailboxes.

For example, suppose that you want to mark all the items of certain Exchange users as permanent records by default. You can configure a retention category to mark items as permanent records, associate it with a retention plan, and then

apply the retention plan to the target mailboxes that you have defined in an Exchange provisioning group. You can use similar methods to mark the items of other users with a different record type, such as temporary.

See [“Setting the default record type for users”](#) on page 126.

- By using facilities such as Enterprise Vault Policy Manager (EVP), assign different retention categories to different folders in user mailboxes. Then you can allow users to mark their items as permanent records, temporary records, or non-records by dragging the items from one mailbox folder and dropping them in another.

For example, suppose that you have applied a retention plan that marks all the items of certain users as permanent records by default. To allow these users to mark selected items as temporary records or non-records, you can use EVP to add folders called "Temporary Records" and "Personal" to their mailboxes. The "Temporary Records" folder has a retention category that marks items as temporary records, whereas the "Personal" folder has a retention category that does not mark them as records. Users can then drag and drop items into the appropriate folder to change the record types of the items.

See [“Allowing users to change the record types of individual items”](#) on page 130.

- Use the Enterprise Vault classification feature to assign the appropriate retention category to items that match certain criteria.

For example, you can set up classification rules to look for items that contain personally identifiable information, such as credit card numbers, and assign to those items a retention category that marks them as non-records.

See [“Using the classification feature for records management”](#) on page 133.

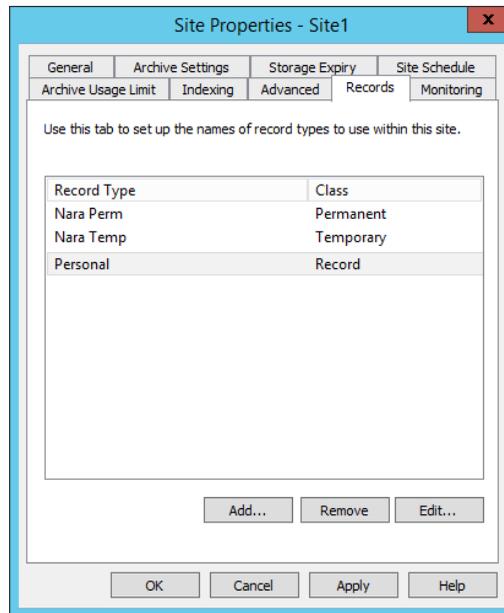
Setting up the required record types

With Capstone, it is customary to mark items as permanent records or temporary records, or not to mark them as records at all. This straightforward approach to records management works well in many cases, but if you have adopted a different methodology or have more complex requirements then it may not be sufficient. For example, you may want to mark certain items as records even though they contain personal information.

Enterprise Vault comes with two record types with which you can mark items as permanent or temporary records. You cannot set up more record types to mark items as permanent or temporary records—only one of each type is permitted—but you can set up any number of custom record types to mark items as records of other sorts. Then you can associate each additional record type with a retention category and assign this to the items that you want to mark with the record type.

To set up the required record types

- 1 In the left pane of the Administration Console, right-click your Enterprise Vault site and then click **Properties**.
- 2 In the **Site Properties** dialog box, click the **Records** tab.



- 3 Do one or more of the following:
 - Click **Add** to create a new record type. You must give the record type a unique name that contains up to 50 alphanumeric or space characters.
 - Click **Remove** to delete the selected record type. You cannot delete the permanent and temporary record types or any custom record types that you have associated with retention categories.
 - Click **Edit** to rename the selected record type.

Setting the default record type for users

An effective approach to setting the default record types for various groups of users is as follows:

- Create one or more retention categories to mark items with the required record types, such as permanent or temporary.

Note: You can edit the properties of existing retention categories so that they too mark items as records. However, any existing items to which you have assigned these retention categories will then become records automatically.

- Create one or more retention plans (or edit the properties of existing ones) and associate each plan with one of the new retention categories.
- Apply the retention plans to the target users.

The following sections describe how to perform these activities.

Creating the required retention categories

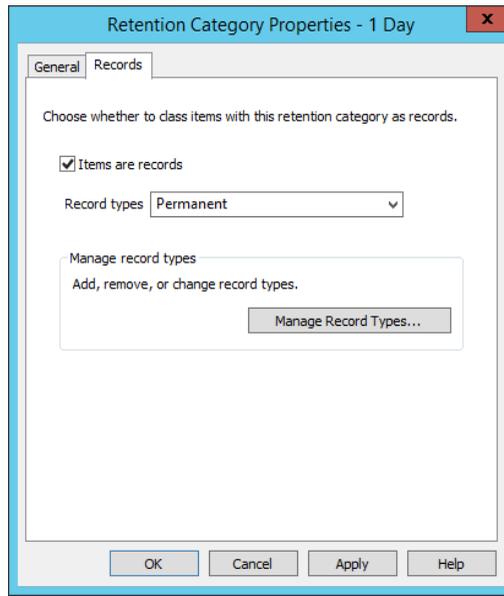
You may want to create multiple retention categories to mark items as permanent records, temporary records, and so on.

Note: You require a license for the Enterprise Vault retention feature to implement the steps below.

To create the required retention categories

- 1 In the left pane of the Administration Console, expand your Enterprise Vault site.
- 2 Expand the **Policies** container, and then expand the **Retention & Classification** container.
- 3 Right-click the **Categories** container, and then click **New > Retention Category**.
- 4 Follow the instructions in the **New Retention Category** wizard.
Depending on the purpose of the retention category, you may want to give it a name such as "Permanent Retention Category" or "Temporary Retention Category".
- 5 After you have finished the wizard, double-click the new retention category in the right pane to display its properties.

- 6 Click the **Records** tab.



- 7 If the items to which you want to apply this retention category are to be marked as records, check **Items are records** and then select the required record type. You can modify the record types from which you can select by clicking **Manage Record Types**.
- 8 Repeat steps 1 to 7 for each retention category that you want to create.

Associating the retention categories with retention plans

Retention plans are an effective way to apply a number of retention settings, including the required retention category, to the items in the mailboxes of target users. For example, suppose that you have identified a number of Capstone officials whose items you want to mark as permanent records. You can create a retention plan specifically for these users and configure it to give their items a retention category that marks the items as permanent records. You can associate other retention categories, such as those that mark items as temporary records or non-records, with additional retention plans that you will apply to Capstone non-officials and other groups of users.

To create a retention plan and associate the required retention category with it, follow the steps below.

To create a retention plan

- 1 In the left pane of the Enterprise Vault Administration Console, expand the tree view until the **Policies** container is visible.
- 2 Expand the **Policies** container and then expand the **Retention & Classification** container.
- 3 Right-click **Plans** and then point to **New** and click **Retention Plan**.
The New Retention Plan wizard appears.
- 4 Work through the pages of the wizard, which prompt you to enter the following:
 - A name for the new retention plan. The name must be unique, and it can contain up to 40 alphanumeric or space characters.
For example, you might call the retention plan "Capstone Official Plan" if it is to target users whose items are to be marked as permanent records by default. For those users whose items you want to mark as temporary records, you might create a retention plan that is called "Capstone Temporary Plan".
 - A description of the plan. The description can contain up to 127 alphanumeric, space, or special characters.
 - The required retention category: one with the record type set to Permanent or Temporary, for example.
 - Optionally, whether to allow the Enterprise Vault classification feature to classify the items that the retention plan handles. If you choose to classify the items, you must also select the required classification policy.
 - The expiry settings to assign to the affected items.

Applying the retention plans to the target users

After you have created a retention plan, you can apply it to one or more archives. The Administration Console provides many different ways to do this, as you can associate a retention plan with any of the following features:

- An Exchange, Domino, or IMAP provisioning group
- An Exchange journal archive, Domino journal archive, or SMTP archive
- An FSA volume or folder policy
- A public folder target
- A SharePoint target or site collection
- Mailboxes that you manually enable for archiving by running the Enable Mailbox wizard

The documentation for each of these features describes how to associate a retention plan with it. [Table 4-1](#) lists the more common archiving targets and the various methods for associating a retention plan with them.

Table 4-1 How to apply a retention plan to an archiving target

Archiving target	To apply a retention plan, use
Exchange mailbox	Exchange Provisioning Group, Enable Mailbox wizard, or PowerShell cmdlet <code>Set-EVArchive</code> .
Domino mailbox	Domino Provisioning Group, Enable Mailbox wizard, or PowerShell cmdlet <code>Set-EVArchive</code> .
Internet Mail	Client Access Provisioning Group, or PowerShell cmdlet <code>Set-EVArchive</code> .
SMTP	The property settings of an SMTP archive, or PowerShell cmdlet <code>Set-EVArchive</code> .

After you have assigned the retention plan, you must run the appropriate provisioning task or archiving task to apply it to the target archives. For instance, you must run the Exchange Provisioning task in the case of an Exchange provisioning group.

About retention plans and age-based archiving

The retention settings that are in force when Enterprise Vault archives a user's items determine the retention category and associated record type that Enterprise Vault assigns to these items. This may be a consideration if you have chosen to archive items when they are older than a certain age, instead of archiving them immediately.

For example, suppose that a user receives an item that will only be archived after several months have passed. Suppose also that you change the retention plan that is applied to the user in the period between the user receiving the item and Enterprise Vault archiving it. When Enterprise Vault archives the item, it assigns the retention category and associated record type that you have specified in the new retention plan rather than the old one.

Allowing users to change the record types of individual items

If you have configured Enterprise Vault to mark all the items of certain users as permanent records by default, you may want to allow these users to reclassify selected items as temporary records or non-records. Similarly, those users for whom

the default record type is temporary may need to mark selected items as permanent records or non-records. By using Enterprise Vault Policy Manager (EVPM), you can assign different retention categories to different folders in user mailboxes. Then the users can mark their items as permanent records, temporary records, or non-records by dragging them from one folder and dropping them in another.

For extensive information on how to use EVPM, see the *Utilities* guide.

Sample EVPM initialization files

Suppose that you have configured Enterprise Vault to mark all of Mike Smith's items as temporary records by default. The following EVPM initialization file creates a folder called "Permanent Records" in Mike Smith's Inbox. The "Permanent Records" folder has a retention category of "Permanent Retention Category", so he can mark items as permanent records by moving them to the new folder.

```
[Directory]
DirectoryComputerName = evserver
SiteName = Site1

[Filter]
Name = Filter1
CreateShortcut = True
DeleteOriginal = True
UnreadMail = True
UseInactivityPeriod = True
InactivityUnits = Days
InactivityPeriod = 14

[Mailbox]
LDAPQuery = (cn=Mike Smith)

[Folder]
Name = \Inbox\Permanent Records
FilterName = Filter1
RetentionCategory = Permanent Retention Category
OverrideArchiveLocks = True
```

In the following example, the initialization file creates two folders in the mailbox of a user whose items are marked as permanent records by default. One folder is for temporary records and the other is for non-records.

```
[Directory]
DirectoryComputerName = evserver
SiteName = Site1
```

```
[Filter]
Name = Filter1
CreateShortcut = True
DeleteOriginal = True
UnreadMail = True
UseInactivityPeriod = True
InactivityUnits = Days
InactivityPeriod = 14

[Mailbox]
LDAPQuery= (cn=Anne Tyler)

[Folder]
Name= \Inbox\Temporary Records
FilterName= Filter1
RetentionCategory= Temporary Retention Category
OverrideArchiveLocks= True

[Folder]
Name= \Inbox\Personal
FilterName= Filter1
RetentionCategory= Non Record Category
OverrideArchiveLocks= True
```

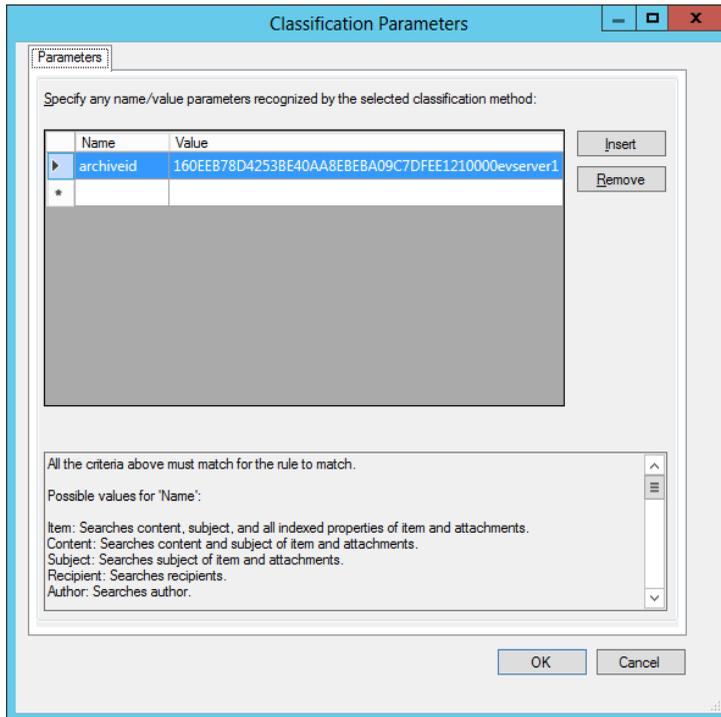
Notes on using EVPM to set up folders for records management

- If the user moves an unarchived item into one of the new folders, Enterprise Vault applies the appropriate retention category to it when the Mailbox Archiving task runs. On the other hand, if the user moves a shortcut (archived item) into one of the folders then, by default, Enterprise Vault applies the new retention category to it when shortcut processing next runs. You can restrict this behavior using the retention categories settings on the **Archive Settings** tab of site properties.
- It is important to set `OverrideArchiveLocks` to `True` in the EVPM initialization file to stop other policy settings from overriding the retention category on the folder.

Using the classification feature for records management

The Enterprise Vault classification feature lets you assign the appropriate retention category to items that match certain criteria. For example, you can set up classification rules to look for personally identifiable information in items, such as credit card numbers, and assign to those items a retention category that marks them as non-records.

Alternatively, suppose that you want to mark all the items in a specific archive as permanent records. To do this, you can set up a classification rule that checks the *archiveid* property of each item and, when this matches a specified archive identifier, assign a retention category that marks the item as a permanent record. In a rule that uses the Veritas Information Classifier method to assign the *evtag.category* property to items, you might configure the appropriate parameter like this:



By using rules such as this, you can reclassify existing items in an archive to mark them as records.

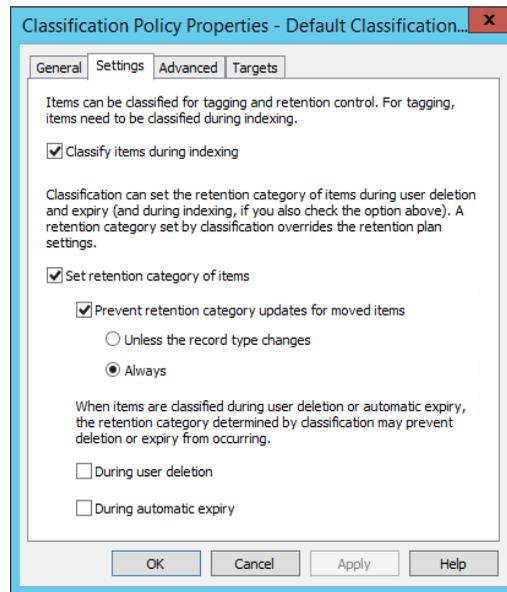
An item may sometimes match several classification rules, all of which are competing to assign a retention category to it. Where this is the case, retention categories that mark items as records take precedence over those that do not. Retention categories that mark items as permanent records take precedence over those that mark them as temporary records, and these take precedence over retention categories that mark items as any other type of record.

For more information on how to use the Enterprise Vault classification feature, see the *Classification* guide.

Potential conflicts between EVPM and the classification feature

Using Enterprise Vault Policy Manager (EVPM) to assign different retention categories to different mailbox folders is a good way to let users change the record types of individual items: users can move items between folders to change the retention category and associated record type of each item. However, a drawback of doing this is that it may override the retention categories that the classification feature has assigned to the items. For the purpose of assigning non-default retention categories to individual items, it is therefore advisable to choose either EVPM or the classification feature, but not both.

If you use the classification feature for records management, we recommend that you set your classification policies to always prevent retention category updates for moved items. [Figure 4-1](#) shows how you might achieve this.

Figure 4-1 Settings tab of Classification Policy Properties dialog box

Common configuration scenarios

This section provides several examples of how to configure users as Capstone officials, for whom you want to mark their items as permanent records by default, or Capstone non-officials, for whom the default record type is temporary.

Configuring users as Capstone officials and marking all their items as permanent records

The following procedure outlines how you might configure selected users as Capstone officials and mark all their items—both existing and newly archived items—as permanent records for submission to the U.S. National Archives. The procedure takes Microsoft Exchange users as an example, but you can readily adapt it to suit other types of users.

To configure users as Capstone officials and mark all their items as permanent records

- 1 Create a retention category that is called, for example, "Permanent Retention Category". Configure the retention category so that Enterprise Vault marks the affected items as permanent records.
- 2 Create a retention plan that is called, for example, "Capstone Official Plan". Configure the retention plan as follows:
 - Set the retention category to the one that you created in step 1 ("Permanent Retention Category").
 - Do not choose to classify the items.
 - Choose to expire items according to the retention category set by the retention plan.
- 3 Create a provisioning group that is called, for example, "Capstone Officials". Configure the provisioning group as follows:
 - Add your list of Capstone officials as targets.
 - Select an Exchange mailbox policy in which, in its **Archiving Actions** properties, you have enabled the **Overall lock** feature.
 - Select the retention plan that you created in step 2 ("Capstone Official Plan").
- 4 Run the Exchange Provisioning task to apply the retention settings to the Capstone officials.
- 5 Synchronize the mailboxes. To do this, open the properties dialog box for the Exchange Mailbox Archiving task and then, on the **Synchronization** tab, click **Synchronize**.
- 6 Enable the mailboxes for archiving, if you have not already done so.

Configuring users as Capstone officials but using classification to exclude certain items from the permanent record set

The preceding section showed how to mark all the archived items of Capstone officials as permanent records. However, it may not be appropriate to submit all these items to the U.S. National Archives because, for example, they contain unimportant information or personal information. By using the classification feature, you can instruct Enterprise Vault to look for and mark such items as temporary records or even non-records. The following procedure outlines how to do this. The procedure takes SMTP users as an example, but you can readily adapt it to suit other types of users.

When Enterprise Vault indexes and classifies items, the following procedure causes it to assign the retention category "Permanent Retention Category" to the items and mark them as permanent records. However, any items that match a classification rule receive a different retention category and are consequently marked as either temporary records or non-records.

For instructions on how to use the Enterprise Vault classification feature, see the *Classification* guide.

To configure users as Capstone officials but use classification to exclude certain items from the permanent record set

- 1 Create a retention category that is called, for example, "Permanent Retention Category". Configure the retention category so that Enterprise Vault marks the affected items as permanent records.
- 2 Create a retention category that is called, for example, "Temporary Retention Category". Configure the retention category so that Enterprise Vault marks the affected items as temporary records.
- 3 Create some classification rules to apply the appropriate retention categories to items that you do not want to mark as permanent records. These rules might include the following:
 - Rules for items that you want to mark as temporary records. For example, these might include items that have been sent to or from known addresses or domains and that do not constitute permanent records.
In this case, the rules must assign the retention category "Temporary Retention Category" as the property value to the matching items.
 - Rules for items that you do not want to mark as records at all. For example, items that contain personal information like credit card numbers may fall into this category.
In this case, the rules must assign as a property value the name of a retention category that does not mark items as records.
- 4 Create a classification policy in which both of the options **Classify items during indexing** and **Set the retention category of items** are enabled.
- 5 Create a retention plan that is called, for example, "Capstone Official Plan". Configure the retention plan as follows:
 - Set the retention category to the one that you created in step 1 ("Permanent Retention Category").
 - Choose to classify the items according to the classification policy that you created in step 4.

- 6 Create an SMTP archive, or edit the properties of an existing SMTP archive, and assign to it the retention plan that you created in step 5 ("Capstone Official Plan").
- 7 If you have not already done so, add an SMTP target address that is associated with the archive.

Configuring users as Capstone non-officials

The following procedure marks the items of Capstone non-officials as temporary records by default, but it also lets those users designate selected items as permanent records. With some modifications, you can implement a similar procedure to mark the items of Capstone officials as permanent records by default but let those officials designate selected items as temporary records or non-records.

To configure users as Capstone non-officials

- 1 Create a retention category that is called, for example, "Permanent Retention Category". Configure the retention category so that Enterprise Vault marks the affected items as permanent records.
- 2 Create a retention category that is called, for example, "Temporary Retention Category". Configure the retention category so that Enterprise Vault marks the affected items as temporary records.
- 3 Create a retention plan that is called, for example, "Capstone Temporary Plan". Configure the retention plan as follows:
 - Set the retention category to the one that you created in step 2 ("Temporary Retention Category").
 - Do not choose to classify the items.
 - Choose to expire items according to their current retention categories rather than the retention category that is set by this retention plan.
- 4 Create a provisioning group that is called, for example, "Capstone Non-Officials". Configure the provisioning group as follows:
 - Add your list of Capstone non-officials as targets.
 - Select an Exchange mailbox policy in which, in its **Archiving Actions** properties, you have enabled the **Overall lock** feature.
 - Select the retention plan that you created in step 3 ("Capstone Temporary Plan").
- 5 Run the Exchange Provisioning task to apply the retention settings to the Capstone non-officials.

- 6 Synchronize the mailboxes. To do this, open the properties dialog box for the Exchange Mailbox Archiving task and then, on the **Synchronization** tab, click **Synchronize**.
- 7 Using Enterprise Vault Policy Manager (EVP), create a folder in each target mailbox with the retention category set to "Permanent Retention Category". This is the folder to which users can move the items that they want to designate as permanent records.

See [“Allowing users to change the record types of individual items”](#) on page 130.
- 8 Enable the mailboxes for archiving, if you have not already done so.

Searching archives for items marked as records

To mark an item as a record, Enterprise Vault populates several of the item's metadata properties with record information. [Table 4-2](#) describes these properties.

Table 4-2 Metadata properties for records

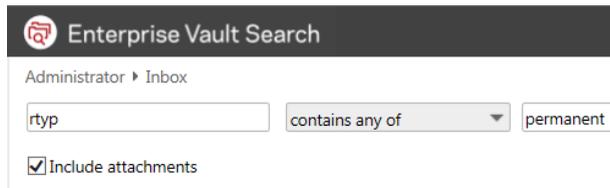
Property	Short form	Specifies
isrecord	isrc	Whether Enterprise Vault has marked the item as a record (True) or not (False).
recordid	rcid	The unique record ID of the item. This is a string of letters, numbers, and symbols, such as the following: 201602221649270000~0~9039eb282e3d4083b79f3298dc8a1e60
recordtype	rtp	The type of record, such as permanent or temporary. Only the items that Enterprise Vault has marked as records have the recordtype property; non-records do not.

When you conduct a search with Enterprise Vault Search, Compliance Accelerator, or Discovery Accelerator, you can filter the results to show only the items that Enterprise Vault has marked as records. For example, here are some queries that you can type in the simple search box of Enterprise Vault Search:

<code>isrc:True</code>	Finds all the items marked as records.
<code>isrc:False</code>	Finds all the non-records.
<code>rcid:record_id</code>	Finds the item with the specified record ID.
<code>rtp:permanent</code>	Finds all the items marked as permanent records.
<code>rtp:temporary</code>	Finds all the items marked as temporary records.

Using the advanced search facilities in Enterprise Vault Search to find records

When you conduct an advanced search with Enterprise Vault Search, you can find items marked as records by entering the required criteria in custom text fields. For example, the following query searches for all the items that Enterprise Vault has marked as permanent records:

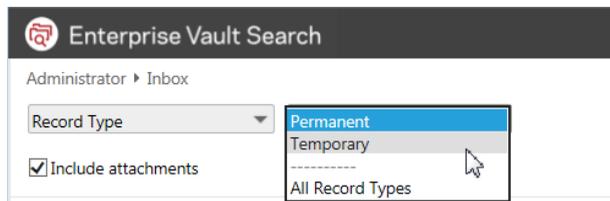


The screenshot shows the Enterprise Vault Search interface. At the top, there is a header with the Enterprise Vault logo and the text "Enterprise Vault Search". Below the header, the user is identified as "Administrator" and the current location is "Inbox". There are three input fields: a text field containing "rtyp", a dropdown menu set to "contains any of", and a text field containing "permanent". Below these fields, there is a checkbox labeled "Include attachments" which is checked.

The online Help for Enterprise Vault Search describes how to turn on the display of custom fields in advanced search, if you have yet to do so.

Helping advanced search users to find records more easily

If your Enterprise Vault role lets you define *search policies* for the other users in your organization, you can help them to search for records more easily by extending the functionality of Enterprise Vault Search. One of the facilities that you can give users through a search policy is the option to choose record properties and values from dropdown lists in advanced search, like this:



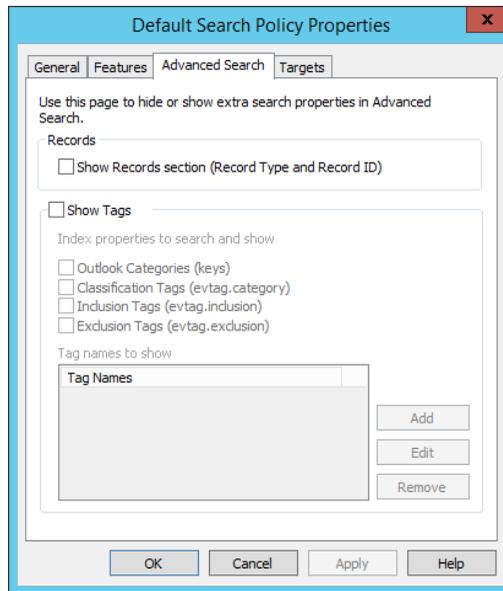
The screenshot shows the Enterprise Vault Search interface with a dropdown menu open. The header is "Enterprise Vault Search" and the user is "Administrator" in the "Inbox". The "Record Type" dropdown menu is open, showing three options: "Permanent", "Temporary", and "All Record Types". A mouse cursor is pointing at the "Permanent" option. The "Include attachments" checkbox is checked.

This saves users from having to turn on the display of custom fields and then type the property names and values for which they want to search. The following procedure describes how to make the extra options available on the dropdown lists. For more information on how to define search policies, see the *Installing and Configuring* guide.

To help advanced search users to find records more easily

- 1 In the left pane of the Administration Console, expand your Enterprise Vault site.
- 2 Expand the **Policies** container.

- 3 Click the **Search** container.
- 4 In the right pane, right-click the search policy that you want to change, and then click **Properties**.
- 5 Click the **Advanced Search** tab.



- 6 Check **Show Records** section.

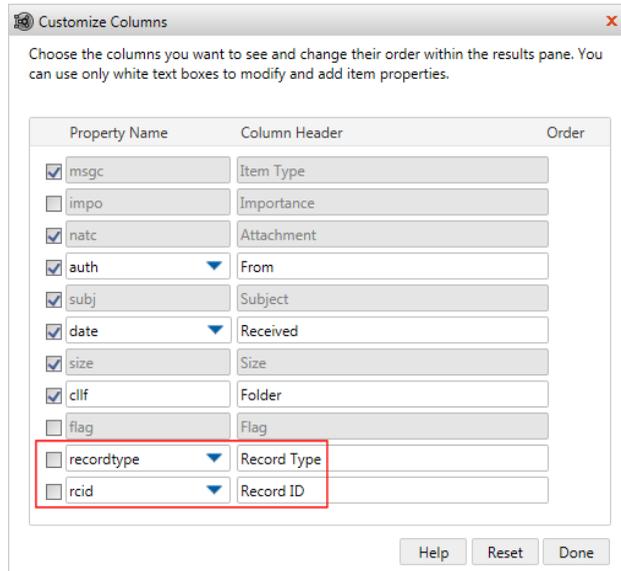
Customizing Enterprise Vault Search to show record types and IDs in the results pane

By default, the results pane in Enterprise Vault Search hides the record types and IDs of items that match your search criteria. However, by following the procedure below, you can add two columns to the results pane so that you can see the record information.

To customize Enterprise Vault Search to show record types and IDs in the results pane

- 1 Run a search to populate the results pane with some items.
 You cannot customize the columns while the results pane is empty.
- 2 In the results pane, right-click the column header and then point to **Columns**.
 A drop-down list appears.

- 3 Click **Customize Columns**.
- 4 In the **Customize Columns** dialog box, add the two properties that are shown below.



- 5 Click **Done**.

Viewing the records management settings for one or more archives

Enterprise Vault comes with a PowerShell cmdlet, `Get-EVRecordSettings`, with which you can obtain information on the records management settings in one or more archives. By running the cmdlet, you can determine the following for each archive:

- The retention plan that you have applied to the archive
- The name and ID of the retention category that you have associated with the retention plan
- The record type that you have associated with the retention category: permanent, temporary, or none

The cmdlet has various optional parameters with which you can filter the list of archives for which it provides information. For example, you can restrict the output

to archives that have a specific retention plan or retention category, or that have a default record type of permanent.

For guidelines on how to run `Get-EVRecordSettings`, see the *PowerShell Cmdlets* guide.

Exporting items from archives

The records management system that you have adopted may require you to export items from your archives for long-term retention elsewhere. For example, in the Capstone approach to records management, it is customary to make periodic transfers of permanent records to the U.S. National Archives. The following webpage provides guidance on how to make these transfers:

<http://www.archives.gov/records-mgmt/policy/transfer-guidance.html>

The National Archives does not have an interest in temporary records or non-records, so there is no need to transfer them.

Enterprise Vault comes with two PowerShell cmdlets with which you can export selected items from an archive. [Table 4-3](#) describes these cmdlets.

Table 4-3 PowerShell cmdlets for exporting items

Cmdlet	Description
<code>Export-EVArchive</code>	<p>Exports items from the specified archive. You can limit the export to items that match the specified search criteria. For example, you can export only those items that were received, sent, or created in the last month.</p> <p>You can choose to export the items in a range of formats, including EML and PST. By default, the cmdlet exports each item in its original format: MSG for Microsoft Exchange items, EML for SMTP items, TXT for text files, and so on.</p>

Table 4-3 PowerShell cmdlets for exporting items (*continued*)

Cmdlet	Description
<code>Export-EVNARAArchive</code>	<p>Exports only those items that Enterprise Vault has marked as permanent records. You can limit the export to records that fall within the specified date range and/or match the specified search criteria. As with <code>Export-EVArchive</code>, you can export the items in a range of formats.</p> <p><code>Export-EVNARAArchive</code> also creates a load file in comma-separated value (.csv) format, which you can send to the National Archives with the items. For each item that the cmdlet has successfully exported, the load file provides the following information:</p> <ul style="list-style-type: none">■ The file name of the exported item. For exports to PST, the load file shows the name of the PST file.■ The record ID.■ A title. For messages, this is the subject line; for other items, it is the original file name.■ A description, which is derived from the indexed content of the item. <p>By default, Enterprise Vault indexes the full content of each item and treats the first 128 characters as a preview string for display in search results. It is this string that appears in the load file. However, you can configure the indexing settings at the site or archive level to increase the preview length or switch to brief indexing, which does not index the contents of items at all. Any changes that you make to these settings are reflected in the description that appears in the load file.</p> <ul style="list-style-type: none">■ The creator of the item.■ The date on which the item was created.■ For exports to PST only, the location of the item in the PST folder structure.

For instructions on how to run these cmdlets, see the *PowerShell Cmdlets* guide.

Automatically filtering events

This chapter includes the following topics:

- [About filtering events](#)

About filtering events

Enterprise Vault event filtering is a mechanism that reduces the number of event log entries that Enterprise Vault creates.

When event filtering is enabled, Enterprise Vault suppresses those events that are repeats of other events that have been logged recently. Event filtering is enabled by default.

By default, event filtering does not suppress Informational events. You can choose to enable filtering for specific Informational events or for all Informational events. If you enable filtering for all events, Enterprise Vault never suppresses any events that help you to track the progress of a task. For example, event filtering does not suppress Informational events that enable you to track the progress of PST migration.

Event filtering does not affect DTrace. All events are written to DTrace, even those that have been suppressed and so do not appear in the event log. If you need to use tracing there is no need to disable event filtering.

Events generated by event filtering

When event filtering is enabled, Enterprise Vault automatically generates the following extra events:

- Event 4257 whenever the event filtering configuration is changed or when the Admin service starts. This event summarizes the event filtering configuration.
- Event 4254 (Critical Error), 4255 (Critical Warning), or 4256 (Informational). This event is generated every 15 minutes to summarize the events that have been filtered in the previous 15 minutes. The severity of the event is the same as that of the highest-severity event that has been suppressed. The event is not logged if no events have been suppressed.
- Event 4258 (Critical Informational) or 4259 (Critical Informational). This event is generated when the event filter is disabled and when the Admin service shuts down. The event summarizes the events that have been suppressed.

Configuring event filtering

By default event filtering is enabled. If you want to disable or configure event filtering you must create registry values in the following location on the appropriate Enterprise Vault server:

```
HKEY_LOCAL_MACHINE
  \SOFTWARE
    \Wow6432Node
      \KVS
        \Enterprise Vault
          \Event Filter
```

[Table 5-1](#) lists the registry values that you can create to control event filtering.

Table 5-1 Registry values that control event filtering

Name	Description	Settings
AllInfosSuppressible	Controls whether Informational events are suppressed, as follows: <ul style="list-style-type: none"> ■ If set to 0, do not suppress any Informational events except those that are named in SuppressibleInfoEventIDs. ■ If set to 1, suppress Informational events. 	<ul style="list-style-type: none"> ■ Type: DWORD ■ Default: 0 ■ Values: 0 or 1

Table 5-1 Registry values that control event filtering (*continued*)

Name	Description	Settings
Enabled	<p>Controls whether event filtering is enabled or disabled. When event filtering is enabled, Enterprise Vault suppresses those events that are repeats of other events that have been logged recently.</p> <ul style="list-style-type: none"> ■ If set to 0, event filtering is disabled. ■ If set to 1, event filtering is enabled. Event filtering is enabled by default. 	<ul style="list-style-type: none"> ■ Type: DWORD ■ Default: 1 ■ Values: 0 or 1
MaxEventsInSequence	<p>The maximum number of events that a process can generate in succession before events are suppressed.</p>	<ul style="list-style-type: none"> ■ Type: DWORD ■ Default: 12 ■ Values: 2 to 100
MaxSecsBetweenEventsInSequence	<p>The maximum time difference between events for them to be treated as part of the same sequence. Events that occur more frequently can be suppressed.</p>	<ul style="list-style-type: none"> ■ Type: DWORD ■ Default: 180 (seconds) ■ Values: 1 to 86400 (1 day)
NeverSuppressEventIDs	<p>A semicolon-delimited list of the IDs of those events that Enterprise Vault must not suppress no matter how many times they are generated.</p>	<ul style="list-style-type: none"> ■ Type: String ■ Default: None
ReportConfigPeriodMinutes	<p>A time interval in minutes that determines the following:</p> <ul style="list-style-type: none"> ■ How frequently to check for configuration changes. ■ How frequently to generate an event that summarizes the event filtering activity. 	<ul style="list-style-type: none"> ■ Type: DWORD ■ Default: 15 (minutes) ■ Values: 1 to 1440 (1 day)
SuppressibleInfoEventIDs	<p>A semicolon-delimited list of the IDs of the informational events that Enterprise Vault can suppress when AllInfosSuppressible is set to 0.</p>	<ul style="list-style-type: none"> ■ Type: String ■ Default: None

Event filtering examples

Some event filtering examples:

- To generate an event filtering summary event every 10 minutes instead of the default of 15 minutes, set `ReportConfigPeriodMinutes` to 10.
- To specify that events 1234, 5678, and 4133 must never be suppressed, set `NeverSuppressEventIDs` to the following:

```
1234;5678;4133
```

Managing indexes

This chapter includes the following topics:

- [About the indexing wizards](#)
- [Managing indexing exclusions](#)
- [Viewing details of index volumes](#)
- [About the indexing PowerShell cmdlets](#)

About the indexing wizards

Enterprise Vault provides the following wizards which you can use to manage your index volumes. All these wizards are available in the **Manage Indexes Wizard**.

Upgrade wizard	Use the Upgrade wizard to upgrade 32-bit index volumes to 64-bit.
Verify wizard	Use the Verify wizard to check that index volumes are accessible, healthy, and up to date.
Synchronize wizard	Use the Synchronize wizard to synchronize index volumes and fix known issues.
Rebuild wizard	Use the Rebuild wizard to completely rebuild index volumes. The Rebuild wizard also upgrades any 32-bit index volumes that it encounters.
Change Location wizard	Use the Change Location wizard to help you to move index volumes to a new location.

See [“Using the indexing wizards”](#) on page 155.

About indexing tasks and subtasks

When you run the indexing wizards, they create indexing tasks that complete the same action on one or more index volumes. Each task has one or more subtasks associated with it. There is one indexing subtask for each index volume to be processed.

Tasks and their subtasks are controlled by Enterprise Vault's Index Administration Task. You can display and manage indexing tasks and subtasks in the **Monitor Indexing Tasks** page.

See [“Managing indexing tasks”](#) on page 156.

Note that you cannot use the indexing wizards to create new tasks for archives, index volumes, and index locations that have other incomplete indexing subtasks associated with them. Archives, index volumes, and index locations must have either no indexing tasks associated with them, or only indexing tasks that have completed before you can submit further tasks.

The following list describes some situations in which you might not be able to add a new task:

- Any archive that has an existing task associated with it cannot be added to a new task. Note that some archives have more than one associated index volume. If just one of these index volumes has a task associated with it, you cannot add the archive to a new task.
- Index volumes that all belong to one archive can be hosted in different index locations. In this case, a task that is associated with just one archive can create tasks that make more than one index location unavailable in the indexing wizards.
- In some of the indexing wizards, you cannot select an empty index location. For example, you cannot select an empty source index location in the Change Location wizard because it contains no index volumes that can be moved.
- When you use the Change Location wizard, both the source location and the destination location are unavailable until the change location task has completed.

When you search for archives and index volumes in the indexing wizards, by default search results include archives and index volumes that already have tasks associated with them. In your searches, you can choose to exclude any archives and index volumes with associated tasks if you want to see only those that are available for you to select.

If you need to add new tasks for archives, index volumes and index locations that have associated tasks, you must first wait for the tasks to complete. Use the **Monitor Indexing Tasks** page, including its subtask view to see the progress of tasks.

In situations where you cannot wait for a task or subtasks to complete, you must first stop then delete the relevant existing tasks. Use the **Monitor Indexing Tasks** page, including its subtask view to stop and delete tasks.

Note that you must also delete failed tasks before you can submit new tasks for affected archives, index volumes and index locations.

Configuring the deletion of indexing subtasks

Enterprise Vault automatically deletes indexing subtasks that have completed with no errors, or have completed with warnings. By default, Enterprise Vault deletes these subtasks seven days after their completion. Enterprise Vault does not automatically delete subtasks that have failed.

You can change the number of days that elapse before deletion of completed subtasks in Enterprise Vault's site properties.

To change the number of days after which Enterprise Vault deletes indexing subtasks

- 1 In the Administration Console, open **Site Properties**.
- 2 Click the **Indexing** tab.
- 3 Change the **Delete indexing subtasks after** value.

About the Upgrade wizard

The Upgrade wizard lets you upgrade 32-bit index volumes to 64-bit. Use the wizard to select the archives whose index volumes you want to upgrade to 64-bit. You can select only archives that have one or more 32-bit index volumes.

The 32-bit index volumes remain searchable during the upgrade to avoid impact on users.

Note: The Upgrade wizard is absent from the **Manage Indexes Wizard** if there are no 32-bit index volumes, such as in a new installation of Enterprise Vault.

Archives that were created by Enterprise Vault 9 or earlier have one or more 32-bit index volumes. Journal archives typically have multiple index volumes. Other types of archive such as mailbox archives usually have only one index volume.

For all archive types, the Enterprise Vault upgrade closes the old 32-bit index volumes and creates a new, live 64-bit index volume for each archive. Subsequently when users search their archives, Enterprise Vault uses the content from both the 32-bit and 64-bit index volumes.

When you use the Upgrade wizard to upgrade 32-bit index volumes to 64-bit, it consolidates 32-bit index volumes if it can to create fewer 64-bit index volumes. In the case of journal archives, this consolidation excludes the new 64-bit index volume that was created during the upgrade to Enterprise Vault 10.0. For all other archive types however, the upgrade includes the new 64-bit volume in the consolidation.

Deletion of upgraded index volumes

During the upgrade of index volumes, Enterprise Vault deletes the old 32-bit index volumes as soon as it makes replacement 64-bit index volumes live and searchable.

In the case of the upgrade of multiple index volumes that are associated with one archive, the upgrade might create fewer 64-bit index volumes than there were 32-bit index volumes. When a new 64-bit volume is made live and searchable, Enterprise Vault deletes the 32-bit index volumes that the 64-bit index volume replaces. If the upgrade does not encounter any items that cannot be indexed, it continues until all the 32-bit index volumes have been replaced by 64-bit index volumes.

Each time you run the Upgrade wizard, you can choose to ignore items that cannot be indexed during the upgrade. If you choose to ignore these items, even if the upgrade encounters items that cannot be indexed it proceeds to completion in the same way.

If you do not choose to ignore items that cannot be indexed, the upgrade pauses at the end of processing for each 32-bit index volume in which it encounters these items and waits for your input in the **Monitor Indexing Tasks** page.

About the Verify wizard

The Verify wizard lets you check the health of 32-bit and 64-bit index volumes. The wizard lets you select individual archives to verify all their associated index volumes, and you can select individual index volumes. Alternatively, you can select an entire index location to verify all the index volumes it contains.

During verification, if a subtask finds no errors in an index volume that was previously marked as failed, it clears the failed status automatically.

Each time you run the wizard, you can choose one of the following verification levels:

- **Basic:** Checks that the index volume is accessible and healthy.
- **Complete:** Checks that the index volume is accessible and healthy, and completes an item level verification.

For 32-bit and 64-bit index volumes, complete verification checks for missing items in the index. These are items that are present in the archive but have not been

indexed. For 64-bit archives only, this option also checks for orphaned items, which are index entries for items that do not exist in the archive.

By default, complete verification does not log individual items that are missing content, such as attachments that have not been indexed because they are encrypted. Only the total number of items that are missing content is listed in the log file. If you want each item that is missing content to be logged individually, select the **Include content missing details** option when you initiate a complete verification task.

During complete verification, users can search their archives but no new entries are added to the index volumes.

Each time you run the Verify wizard, you can choose to create a synchronization task automatically for each index volume in which it encounters missing items and orphaned index entries.

About the Synchronize wizard

The Synchronize wizard lets you synchronize index volumes and fixes known issues.

Note: This wizard replaces the Repair Index Volume feature in versions of Enterprise Vault before version 10.0.

Synchronization tasks fix known issues including those identified by verification tasks you have run previously. For 32-bit and 64-bit index volumes, synchronization tasks index items that are present in the archive but have not been indexed. For 64-bit archives only, synchronization tasks also remove orphaned index entries for items that do not exist in the archive.

When the synchronization task has fixed known issues, it then initiates an internal synchronization to ensure the index volumes are up to date.

In addition to synchronization tasks that you create when you run the Synchronize wizard, the verification tasks can also create synchronization tasks automatically, depending on the choices you make in the Verify wizard.

About the Rebuild wizard

The Rebuild wizard lets you rebuild index volumes, and it upgrades any 32-bit index volumes that it encounters. Use the wizard to select the archives whose index volumes you want to rebuild. You can also rebuild individual index volumes.

The old index volumes remain searchable during the rebuild to avoid impact on users.

You may want to rebuild the index volumes for the following reasons:

- To fix issues that the synchronization tasks have failed to fix.
- To reindex items after setting a new indexing level.
- To reclassify items, if you have enabled classification for the associated archives.

When you use the Rebuild wizard to rebuild all the index volumes associated with an archive, the rebuild consolidates the index volumes if possible to create a smaller number of rebuilt index volumes. For all archive types, this consolidation includes the archive's live index volume.

Deletion of rebuilt index volumes

During a rebuild of index volumes, Enterprise Vault deletes the old index volumes as soon as it makes their replacements live and searchable.

In the case of a rebuild of multiple index volumes that are associated with one archive, the rebuild might create fewer new index volumes. When a new index volume is made live and searchable, Enterprise Vault deletes the old index volumes it replaces. If the rebuild does not encounter any items that cannot be indexed, it continues until all the old index volumes have been replaced by rebuilt index volumes.

Each time you run the Rebuild wizard, you can choose to ignore items that cannot be indexed during the rebuild. If you choose to ignore these items, even if the rebuild encounters items that cannot be indexed it proceeds to completion in the same way.

If you do not choose to ignore items that cannot be indexed, the rebuild pauses at the end of processing for each old index volume in which it encounters these items and waits for your input in the **Monitor Indexing Tasks** page.

About the Change Location wizard

The Change Location wizard lets you move an archive's index volumes from one physical location to another.

Change location tasks do not copy the index volumes from the source location to the target. You must copy the files manually, and use the Change Location wizard to make the necessary changes in Enterprise Vault.

When you run the Change Location wizard, you must indicate whether or not you have already copied the archive's index volumes from the source location to the target location.

If you choose to copy the index volumes before you run the wizard, you must first set the index volumes offline, then copy the files. When you run the wizard and indicate that you have already copied the files, it creates a change location task

which checks the index volumes are offline then completes the configuration of the new location.

If you choose to copy the index volumes after you run the Change Location wizard, it creates a change location task which sets the index volumes offline then pauses while you copy the files. When you have copied the files, you can use the **Monitor Indexing Tasks** page to indicate that you have copied the files for the relevant change location task. The task then completes the configuration of the new location.

Using the indexing wizards

To run the indexing wizards, your user account must be assigned the Indexing Administrator role.

See [“Roles-based administration”](#) on page 20.

The indexing wizards are all accessible from the **Indexing Summary** page in the Administration Console.

To run the Manage Indexes Wizard from Indexing Summary page

- 1 In the left pane of the Administration Console, click the **Indexing** container.
- 2 In the right pane, click **Manage Indexes**.

The **Manage Indexes Wizard** is also accessible from the following places in the Administration Console:

■ Common Tasks

- The **Indexing** container, and the containers beneath it
- The **Archive Properties: Index Volumes** tab

To run the Manage Indexes Wizard from Common Tasks

- 1 In the left pane of the Administration Console, click the name of the Enterprise Vault site.
- 2 In **Common Tasks** in the right pane, expand **Index Management**.
- 3 Click **Manage Indexes Wizard**.

To run the Manage Indexes Wizard from the Indexing container

- ◆ In the left pane of the Administration Console, right-click **Indexing** or any of the containers beneath it and click **Manage Indexes**.

To run the Manage Indexes Wizard from The Archive Properties: Index Volumes tab

- 1 In the Administration Console, right-click an archive and click **Properties**.
- 2 Click the **Index Volumes** tab.
- 3 Click **Manage Indexes**.

Managing indexing tasks

All the indexing tasks that you create using the indexing wizard are shown in the Administration Console in the **Monitor Indexing Tasks** page. The **Monitor Indexing Tasks** page is accessible from the **Indexing Summary** page in the Administration Console.

To run Monitor Indexing Tasks from Indexing Summary page

- 1 In the left pane of the Administration Console, click the **Indexing** container.
- 2 In the right pane, click **Monitor Indexing Tasks**.

The **Monitor Indexing Tasks** page is also accessible from the following places in the Administration Console:

■ Common Tasks

- The **Indexing** container, and the containers beneath it

To run the Monitor Indexing Tasks from Common Tasks

- 1 In the left pane of the Administration Console, click the name of the Enterprise Vault site.
- 2 In **Common Tasks** in the right pane, expand **Index Management**.
- 3 Click **Monitor Indexing Tasks**.

To run the Manage Indexes Wizard from the Indexing container

- ◆ In the left pane of the Administration Console, right-click **Indexing** or any of the containers beneath it and click **Monitor Indexing Tasks**.

Using the Monitor Indexing Tasks page

The **Monitor Indexing Tasks** page lists all the current indexing tasks. Use this page to monitor and manage the tasks. Use the **Search** controls to filter the tasks in the list.

For example, to list only synchronization tasks whose names contain 2011-05-05

- 1 Choose **Task** from the **Search** list.
- 2 Enter **2011-05-05** in the **search text contains** box.
- 3 Click **Deselect All** to clear the current selections.
- 4 Select **Synchronize** under **Task Type**.
- 5 Click **Search**.

If you want to include in the search results only those tasks that need attention, click **Yes** under **Show only tasks that need attention**. This includes only the tasks whose status is **Failed**, **Stopped**, and **Waiting**.

You can also click **Clear All** to clear existing search criteria before you start a new search.

For each task, the search results show the following information:

- **Task**. The name of the task.
- **Type**. The type of the task.
- **Created Date**. The date and time the task was created.
- **Not Active**. The number of inactive subtasks associated with the task. This number includes the numbers of subtasks whose status is **Inactive**, **Queued**, **Waiting**, or **Stopped**.
- **Active**. The number of active subtasks associated with the task. This is the number of subtasks whose status is **Processing**.
- **Successful**. The number of successful subtasks associated with the task. This is the number of subtasks whose status is **No errors**.
- **Unsuccessful**. The number of unsuccessful subtasks associated with the task. This number includes the numbers of subtasks whose status is **Warnings**, **Will retry**, or **Failed**.
- **Successful Subtasks**. The bar shows progress through the subtasks associated with the task.

If all the statuses of the subtasks are all in **Active** or **Successful** categories, the bar is green. If any of the subtasks have statuses in the **Not Active** category, the bar is yellow. If any of the subtasks have statuses in the **Unsuccessful** category, the bar is red.

Select tasks from the list and use the buttons on the button bar or the items on the **Actions** menu to initiate the following actions:

- **Start**. Click to start stopped tasks.

- **Stop.** Click to stop running tasks.
- **Restart.** Click to restart tasks.
- **Retry.** Click to retry failed tasks.
- **Delete.** Click to delete tasks.
- **I have copied the files** or **Process waiting subtasks.**
 For change location tasks, click **I have copied the files** when you have copied the files associated with the task to their new location.
 For all other tasks, click **Process waiting subtasks** to process the waiting subtasks.
- **Show all subtasks for the current task** (button bar only). Click to show the subtasks associated with the selected parent task.
 You can also click the name of a task to show its associated subtasks.
 See [“Using the Monitor Indexing Tasks page \(subtask view\)”](#) on page 158.
- **Copy selection to clipboard** (**Actions** menu only). Click to copy details of the selected tasks to the clipboard.
- **Refresh view.** Click to refresh the current view.

Using the Monitor Indexing Tasks page (subtask view)

In subtask view, the **Monitor Indexing Tasks** page lists all the indexing subtasks associated with a task. Use this page to monitor and manage the subtasks. Use the **Search** controls to filter the subtasks in the list.

For example, to list only unsuccessful subtasks whose archive names contain “John Doe”

- 1 Enter **John Doe** in the **search text contains** box.
- 2 Click **Deselect All** to clear the current selections.
- 3 Select **Warnings**, **Will retry**, and **Failed** under **Subtask status**.
- 4 Click **Search**.

You can also click **Clear All** to clear existing search criteria before you start a new search.

For each subtask, this page lists information in the columns described in the following table. The page includes only the columns that are relevant to the types of subtasks that are displayed.

Archive Name	The name of the archive that the subtasks are associated with.
---------------------	--

Index Volume Range	The range of sequence numbers of the items indexed in the index volume.
Items Added	<p>For upgrade and rebuild subtasks, this shows the total number of items successfully processed.</p> <p>For synchronization subtasks, this shows the number of items that have been indexed by the subtask.</p>
Items Deleted	For synchronization subtasks, this shows the number of pending deletions and other previously orphaned index entries items that have been removed from the index volume by the subtasks.
Items With Errors	<p>For upgrade, rebuild and synchronization subtasks, this shows the number of items that could not be retrieved, usually due to storage issues.</p> <p>In the case of upgrade and rebuild subtasks, items with errors cause the subtask to wait for user input if you did not select the Ignore items that cannot be indexed option when you submitted the task.</p>
Missing Items	For verification subtasks, this shows the number of items in the archive that Enterprise Vault has failed to index.
Extra Items	For verification subtasks, this shows the number of orphaned index entries it found in the index volume. These are index entries for items that do not exist in the archive.
Original Location	For change location subtasks, this shows the original location of the index volume.
Destination Location	For change location subtasks, this shows the destination location of the index volume.
Status	<p>The subtask's status.</p> <p>See "Subtask statuses" on page 160.</p>
Progress	<p>Progress. The bar shows subtask's progress. The color of the bar matches the category that subtask status belongs to. Active and Successful tasks have a green bar, Not Active subtasks have a yellow bar, and Unsuccessful subtasks have a red bar.</p>

Select subtasks from the list and use the buttons on the button bar or the items on the **Actions** menu to initiate the following actions:

- **Switch back to parent task summary view** (button bar only). Click to show the task view.

- **Start.** Click to start stopped subtasks.
- **Stop.** Click to stop running subtasks.
- **Restart.** Click to restart subtasks.
- **Retry.** Click to retry failed subtasks.
- **Delete.** Click to delete subtasks.
- **I have copied the files** or **Process waiting subtasks.**
 For change location tasks, click **I have copied the files** when you have copied the files associated with the subtask to their new location.
 For all other subtasks, click **Process waiting subtasks** to process the waiting subtasks.
- **Open report.** Click to open the report file associated with the subtask.
- **Save report.** Click to save the report file associated with the subtask.
- **Details.** Click to display details about the selected subtask.
- **Copy selection to clipboard (Actions menu only).** Click to copy details of the selected subtasks to the clipboard.
- **Refresh view.** Click to refresh the current view.

Subtask statuses

Table 6-1 Subtask statuses

Category	Status	Description
Not active	Inactive	<p>The subtask is inactive. This can happen in the following cases:</p> <ul style="list-style-type: none"> ■ The Index Administration Task on the server the subtask is associated with is not in schedule. ■ The Index Administration Task on the server the subtask is associated with has not yet picked up the subtask for processing. This can happen when you submit a task that creates a large number of subtasks. ■ Vault stores or index locations are in backup mode.
	Queued	<p>The Index Administration Task on the server the subtask is associated with has not yet picked up the subtask for processing. The statuses of these subtasks are Queued until the Index Administration tasks starts processing them.</p>

Table 6-1 Subtask statuses (*continued*)

Category	Status	Description
	Waiting	<p>The subtask is waiting for user input:</p> <ul style="list-style-type: none"> ■ For change location tasks on which you did not select The index folders have been copied to the new location, the associated subtasks complete their initial processing, then wait for you to indicate that you have copied the index folders. When you have copied the index folders, use the I have copied the files action in the Monitor Indexing Tasks page. ■ For upgrade and rebuild tasks on which you did not select Ignore items that cannot be indexed, the associated subtasks wait for your input when they encounter minor errors. Use the Process waiting subtasks action in the Monitor Indexing Tasks page to force the subtask to continue processing. ■ For Metadata Store tasks, a subtask was unable to process all items. Do one of the following: <ul style="list-style-type: none"> ■ Fix the problem and then use the Process waiting subtasks action in the Monitor Indexing Tasks page to force the subtask to continue processing. Select the option Retry the failed items and wait again if there are still errors. ■ Decide to ignore the problem and then use the Process waiting subtasks action in the Monitor Indexing Tasks page to force the subtask to continue processing. Select the option Retry the failed items and continue.
	Stopped	<p>You have stopped the subtask. The Index Administration Task does not process the subtask again until you use the Start action in the Monitor Indexing Tasks page to resume the subtask.</p>
Active	Processing	<p>The subtask is being processed.</p>
Successful	No errors	<p>The subtask completed without errors.</p>
Unsuccessful	Warnings	<p>The subtask completed with warnings.</p> <p>Examine the Subtask Details page and the subtask report file for more information.</p>

Table 6-1 Subtask statuses (*continued*)

Category	Status	Description
	Will retry	Change location and verify subtasks can have this status when errors occur. The Index Administration Task tries a subtask up to five times when it encounters errors, in case the errors are transient. After five tries, if the errors persist the subtask is marked as Failed .
	Failed	The subtask failed. Examine the Subtask Details page and the subtask report file for more information. If you can ascertain and rectify the cause of the failure, use the Retry action in the Monitor Indexing Tasks page to retry the subtask.

Managing index upgrade and index rebuild tasks

Upgrade and rebuild tasks which do not complete successfully with the status **No errors**, can have the following statuses:

- **Waiting**. If you did not select the **Ignore items that cannot be indexed** option when you submitted the upgrade or rebuild task, its subtasks wait for your input when they encounter minor errors. Use the **Process waiting subtasks** action in the **Monitor Indexing Tasks** page to force the subtask to continue processing.
- **Failed**. The upgrade or rebuild subtask has failed. This happens when the subtask encounters serious errors, or a significant number of minor errors. In the **Monitor Indexing Tasks** page, open the subtask's report file to see details of the failure. If you can ascertain and rectify the cause of the failure, use the **Retry** action in the **Monitor Indexing Tasks** page to retry the subtask.

Managing index verification tasks

Verification tasks which do not complete successfully with the status **No errors**, can have the following statuses:

- **Will retry**. The subtask has encountered errors but will retry the subtask. You do not need to take action for subtasks with this status.
- **Warnings**. When you submit a **Complete** verification task, its subtasks can complete with **Warnings**. In the **Monitor Indexing Tasks** page, open the subtask's report file to see the warnings.
- **Failed**. The verification subtask has failed. In the **Monitor Indexing Tasks** page, open the subtask's report file to see details of the failure. If you can

ascertain and rectify the cause of the failure, use the **Retry** action in the **Monitor Indexing Tasks** page to retry the subtask.

If any of your verification subtasks fail, or complete with warnings about missing items and orphaned index entries, consider submitting a synchronization task for the same archive, index volume or index location. You do not need to do this if you selected the **Auto Synchronize** option when you originally added the verification task because Enterprise Vault automatically creates synchronization tasks in this case.

Managing index synchronization tasks

Synchronization tasks which do not complete successfully with the status **No errors**, can have the following statuses:

- **Warnings.** Synchronization subtasks can complete with **Warnings**. In the **Monitor Indexing Tasks** page, open the subtask's report file to see the warnings.
- **Failed.** The synchronization subtask has failed. In the **Monitor Indexing Tasks** page, open the subtask's report file to see details of the failure. If you can ascertain and rectify the cause of the failure, use the **Retry** action in the **Monitor Indexing Tasks** page to retry the subtask.

Managing change location tasks

Change location tasks which do not complete successfully with the status **No errors**, can have the following statuses:

- **Will retry.** The subtask has encountered errors but will retry the subtask. You do not need to take action for subtasks with this status.
- **Waiting.** If you did not select the **The index folders have been copied to the new location** option when you submitted the task, after completing their initial processing, the associated subtasks wait for your input. Copy the index folder to the new location, then use the **I have copied the file** action in the **Monitor Indexing Tasks** page to complete processing.
- **Warnings.** When you submit a change location task, its subtasks can complete with **Warnings**. In the **Monitor Indexing Tasks** page, open the subtask's report file to see the warnings.
- **Failed.** The change location subtask has failed. In the **Monitor Indexing Tasks** page, open the subtask's report file to see details of the failure. If you can ascertain and rectify the cause of the failure, use the **Retry** action in the **Monitor Indexing Tasks** page to retry the subtask.

Managing indexing exclusions

Enterprise Vault's indexing exclusions feature lets you specify email content that you do not want to index, such as email disclaimers and corporate email signatures. This improves the quality of searches by avoiding unwanted search hits that would otherwise arise from the excluded text.

How indexing exclusions work

When you have created an indexing exclusion, Enterprise Vault omits from the indexes it subsequently builds any matching content that occurs in email items.

Note: Indexes that were created before you add a new indexing exclusion are not affected. Content that matches the new exclusion remains in the existing indexes unless you rebuild them.

For each Enterprise Vault site, you can add as many indexing exclusions as you need. Enterprise Vault accepts plain text exclusion content, which it then normalizes by removing leading and trailing white space, and by replacing consecutive white space characters with a single space.

During subsequent indexing, Enterprise Vault makes case-sensitive comparisons between the exclusion text and email content, and excludes from indexes any matches that occur.

When you delete an existing indexing exclusion, archived content that matches the deleted exclusion is not reinstated in indexes unless you rebuild them.

Note that it can take two hours from the time you add, edit or remove an indexing exclusion before the changes fully take effect.

Managing indexing exclusions

For each Enterprise Vault site, you can manage indexing exclusions in the Administration Console.

To manage indexing exclusions

- 1 In the Enterprise Vault Administration Console, open **Site Properties** and click the **Indexing** tab.
- 2 Click **Exclusions**.

In the **Indexing Exclusions** dialog box, you can add new indexing exclusions, and edit, rename and remove existing indexing exclusions.

Viewing details of index volumes

The Index Volumes Browser enables you to do the following:

- Search for those index volumes that meet the criteria that you specify. You can search for indexes by various attributes.
- Set individual index volumes online or offline.
- View details of individual index volumes. For example, the details of an index volume include the following:
 - The location of the index volume
 - The server or the index group that hosts the index volume
 - Details of the archive with which the index volume is associated

To display the Index Volumes Browser, do one of the following in the Administration Console:

- Click **Index Volumes Browser** in the **Indexing Summary** page.
- Right-click the **Archives** container and then click **Index Volumes Browser**.
- Right-click the **Indexing** container and then click **Index Volumes Browser**.
- Display the properties of an archive, click the **Index Volumes** tab and then click **Details**.

About the indexing PowerShell cmdlets

The Enterprise Vault Management Shell provides the following indexing cmdlets:

Table 6-2 Indexing PowerShell cmdlets

Cmdlet	Description
<code>Get-IndexServerForIndexLocation</code>	Reports the server name and server entry ID for the index server that is responsible for a specified index location.
<code>Set-IndexMetadataSyncLevel</code>	Forces the synchronization of index metadata at the next startup of the specified indexing service. This is useful after you have restored index locations during disaster recovery.

Running the indexing PowerShell cmdlets

To run one of the indexing PowerShell cmdlets

- 1 Start the Enterprise Vault Management Shell.

PowerShell opens and loads the Enterprise Vault snap-in. The cmdlets are now available in the shell.

- 2 At the PowerShell command prompt, type the required command.

Help is available for all the cmdlets. For example, the following command shows the detailed Help for the `Get-IndexServerForIndexLocation` cmdlet:

```
Get-Help Get-IndexServerForIndexLocation -detailed
```

Using Get-IndexServerForIndexLocation

Use the following syntax when you run `Get-IndexServerForIndexLocation`:

```
Get-IndexServerForIndexLocation -Location <String>
[<CommonParameters>]
```

The following examples show how `Get-IndexServerForIndexLocation` is used to report the index server that is responsible for an index location:

- `Get-IndexServerForIndexLocation -Location "F:\EVIndexes\index7"`
 This command returns the index server responsible for the index location whose path is `F:\EVIndexes\index7`.
- `Get-IndexServerForIndexLocation -Location 10AA6CBA47F403244A85E3CF172B00DEC1810000Server.Domain1.local`
 This command returns the index server responsible for the index location whose root path entry ID is `10AA6CBA47F403244A85E3CF172B00DEC1810000Server.Domain1.local`.

Using Set-IndexMetadataSyncLevel

Use the following syntax when you run `Set-IndexMetadataSyncLevel`:

```
Set-IndexMetadataSyncLevel -EntryId <String> -SyncLevel <String>
[<CommonParameters>]
```

Table 6-3 Available synchronization levels for `Set-IndexMetadataSyncLevel`

Level	Description
0	No synchronization occurs at indexing service startup.

Table 6-3 Available synchronization levels for Set-IndexMetadataSyncLevel
(continued)

Level	Description
1	At startup, the indexing service indexes items that are present in archives but have not been indexed, and removes orphaned index entries for items that do not exist in the archives.
2	At startup, the indexing service: <ul style="list-style-type: none"> ■ Indexes items that are present in archives but have not been indexed, and removes orphaned index entries for items that do not exist in the archives ■ Checks that all the index locations stored in the Directory database are correctly referenced in the index metadata

The following example shows how `Set-IndexMetadataSyncLevel` is used to force the synchronization of index metadata:

```
■ Set-IndexMetadataSyncLevel -EntryId
15B63FA16EF2BD4418934B87F2F6651A51710000.Domain1.local -SyncLevel
1
```

This command sets the synchronization level to 1 for the indexing service that has entry ID `15B63FA16EF2BD4418934B87F2F6651A51710000.Domain1.local`.

Advanced Domino mailbox and desktop policy settings

This chapter includes the following topics:

- [About the advanced policy settings for Domino mailbox and desktop policy](#)
- [Editing the advanced settings for Domino mailbox and desktop policy](#)
- [Domino mailbox policy advanced settings](#)
- [Domino desktop policy advanced settings](#)

About the advanced policy settings for Domino mailbox and desktop policy

The Domino mailbox policy advanced settings control advanced archiving behavior such as the action to take for failed items, and the method for resolving email addresses.

The Domino desktop policy advanced settings let you fine-tune the user experience provided by the Domino client desktops. The settings control advanced features and functionality of Vault Cache.

Editing the advanced settings for Domino mailbox and desktop policy

The advanced settings for a policy are provided on the Advanced tab of the policy properties.

To edit the advanced settings for a policy

- 1 In the left pane of the Administration Console, expand the hierarchy until **Policies** is visible.
- 2 Expand **Policies**.
- 3 Expand **Domino**.
- 4 Click **Mailbox** or **Desktop** as appropriate.
- 5 In the right-hand pane, double-click the name of the policy you want to edit.
The policy's properties are displayed.
- 6 Click the **Advanced** tab.
- 7 Next to **List settings from**, select the category of settings that you want to modify.
- 8 Edit the settings as required.

You can double-click a setting to edit it, or click it once to select it and then click **Modify**.

How to apply the new settings for Domino mailbox and desktop policy

Modified mailbox and desktop policy settings are applied to users' mailboxes during the next synchronization run of the Domino Provisioning task. If you want to apply the changes before the next synchronization, run Synchronize Individual Mailboxes, which is on the Synchronization tab of the Domino Provisioning task's properties.

Domino mailbox policy advanced settings

These settings control advanced aspects of Domino mailbox archiving.

There is one category of Domino mailbox policy advanced settings:

- [Archiving General: Domino mailbox policy](#)

Archiving General: Domino mailbox policy

These settings control advanced aspects of archiving behavior.

The Archiving General settings are:

- [Action for failed items \(Domino Archiving General setting\)](#)
- [Archive draft items \(Domino Archiving General setting\)](#)
- [Lookup e-mail addresses \(Domino Archiving General setting\)](#)
- [Reset archive names \(Domino Archiving General setting\)](#)
- [Strip attachments to non-shortcut items \(Domino Archiving General setting\)](#)

Action for failed items (Domino Archiving General setting)

Description	Lets you control whether items that fail three times to be archived are processed on later archiving runs.
Supported values	<ul style="list-style-type: none">■ Reprocess. Items that have failed repeatedly are reprocessed on each archiving run.■ Do not reprocess (default). Items that have failed repeatedly are not reprocessed on later archiving runs.
Legacy name	SetFailedMsgsDoNotArchive

Archive draft items (Domino Archiving General setting)

Description	Lets you control whether draft items are archived. Changes to the setting are applied to users' mail files when the Domino Provisioning task next runs. To apply the changes immediately, click Synchronize Individual Mailboxes on the Synchronization tab of the Domino Provisioning task properties.
Supported values	<ul style="list-style-type: none">■ Off (default). Draft items are not archived.■ On. Draft items are archived. When draft items are archived, they never change into shortcuts, and attachments are not removed.
Legacy name	ArchiveDraftItems

Lookup e-mail addresses (Domino Archiving General setting)

Description	Controls whether email addresses are resolved using the Domino Directory, including SMTP addresses where available.
Supported values	<ul style="list-style-type: none">■ On (default). Email addresses are resolved.■ Off. Email addresses are not resolved.

Legacy name LookupNames

Reset archive names (Domino Archiving General setting)

Description Controls whether archive names are kept synchronized with Domino user names. If the setting is On, any changes to the Domino user name are applied to the archive name when the Domino Provisioning task runs, either on a scheduled run or when the administrator clicks **Synchronize Individual Mailboxes** on the task properties.

Supported values

- On (default). Archive names are updated during synchronization.
- Off. Archive names are not updated during synchronization.

Strip attachments to non-shortcut items (Domino Archiving General setting)

Description Controls whether attachments are removed from appointments and tasks after archiving. These items are not changed into Enterprise Vault shortcuts when they are archived. If Enterprise Vault removes an attachment, it replaces it with a link to the attachment.

Supported values

- On (default). Attachments are removed from non-shortcut items after archiving.
- Off. Attachments are not removed from non-shortcut items after archiving.

Legacy name StripAttachmentsToNonShortcutItems

Domino desktop policy advanced settings

These settings allow you to fine-tune the behavior of the Enterprise Vault Notes client.

There is one category of Domino desktop policy advanced settings:

- [Vault Cache: Domino desktop policy](#)

Vault Cache: Domino desktop policy

These settings control advanced behavior of Notes with respect to Vault Cache.

The Vault Cache settings are:

- [Pause interval \(Domino Vault Cache setting\)](#)

- [Preemptive archiving threshold \(Domino Vault Cache setting\)](#)

Pause interval (Domino Vault Cache setting)

Description Specifies the number of minutes to wait before Enterprise Vault starts searching for items that need to be added to the Vault Cache.

Supported values ■ Integer value, specifying a number of minutes. The default is 3.

Preemptive archiving threshold (Domino Vault Cache setting)

Description Specifies the number of days before archiving at which Enterprise Vault copies items preemptively to the Vault Cache, in anticipation that the items will soon be archived. The copy takes place on the user's computer, with no further download required.

Supported values ■ Integer value, specifying a number of days. The default is 7.

Advanced Exchange mailbox and desktop policy settings

This chapter includes the following topics:

- [About the advanced Exchange mailbox and desktop settings](#)
- [Editing the advanced Exchange mailbox and desktop settings](#)
- [Exchange mailbox policy advanced settings](#)
- [Exchange desktop policy advanced settings](#)

About the advanced Exchange mailbox and desktop settings

The Exchange mailbox policy advanced settings control advanced aspects of archiving behavior such as whether deleted items and unexpired calendar events are archived.

The Exchange desktop policy advanced settings let you fine-tune the user experience provided by the Exchange client desktops. The settings control the advanced features and functionality provided by Vault Cache and Virtual Vault for Outlook and the Outlook and OWA clients.

Editing the advanced Exchange mailbox and desktop settings

The advanced settings for a policy are provided on the Advanced tab of the policy properties.

To edit the advanced settings for a policy

- 1 In the left pane of the Administration Console, expand the hierarchy until **Policies** is visible.
- 2 Expand **Policies**.
- 3 Expand **Exchange**.
- 4 Click **Mailbox** or **Desktop** as required.
- 5 In the right-hand pane, double-click the name of the policy you want to edit.
The policy's properties are displayed.
- 6 Click the **Advanced** tab.
- 7 Next to **List settings from**, select the category of settings that you want to modify.
- 8 Edit the settings as required.

You can double-click a setting to edit it, or click it once to select it and then click **Modify**.

How to apply the new Exchange mailbox and desktop settings

Modified mailbox and desktop policy settings are applied to users' mailboxes during the next synchronization run of the Exchange Mailbox task. If you want to apply the changes before the next synchronization, run Synchronize, which is on the Synchronization tab of the Exchange Mailbox task's properties.

Exchange mailbox policy advanced settings

These settings control advanced aspects of Exchange mailbox archiving.

There is one category of Exchange mailbox policy advanced settings:

- [Archiving General \(Exchange mailbox policy advanced settings\)](#)

Archiving General (Exchange mailbox policy advanced settings)

The Archiving General settings enable you to control advanced archiving behavior.

The Archiving General settings are:

- [Archive deleted items \(Exchange Archiving General setting\)](#)
- [Archive draft items \(Exchange Archiving General setting\)](#)
- [Archive Exchange Managed Folders \(Exchange Archiving General setting\)](#)
- [Archive naming convention \(Exchange Archiving General setting\)](#)
- [Archive unexpired Calendar Events \(Exchange Archiving General setting\)](#)
- [Code pages for right-to-left custom shortcuts \(Exchange Archiving General setting\)](#)
- [Do not archive pending reminders \(Exchange Archiving General setting\)](#)
- [Encode custom body using appropriate code pages \(Exchange Archiving General setting\)](#)
- [Future item retention category \(Exchange Archiving General setting\)](#)
- [Include default and anonymous permissions \(Exchange Archiving General setting\)](#)
- [Inherited permissions \(Exchange Archiving General setting\)](#)
- [Maximum message size to archive in MB \(Exchange Archiving General setting\)](#)
- [Pending shortcut timeout \(Exchange Archiving General setting\)](#)
- [Reset archive names \(Exchange Archiving General setting\)](#)
- [Set failed messages 'Do Not Archive' \(Exchange Archiving General setting\)](#)
- [Strip attachments to non-shortcut items \(Exchange Archiving General setting\)](#)
- [Synchronize folder permissions \(Exchange Archiving General setting\)](#)
- [Text direction indicator for custom shortcuts \(Exchange Archiving General setting\)](#)
- [Valid Enterprise Vault site aliases \(Exchange Archiving General setting\)](#)
- [Warn if default or anonymous permissions exist \(Exchange Archiving General setting\)](#)
- [Warn when mailbox not under quota after archiving run \(Exchange Archiving General setting\)](#)

Archive deleted items (Exchange Archiving General setting)

Description Controls whether items are archived from the Deleted Items folder.

- Supported values
- Off (default). Items in the Deleted Items folder are not archived.
 - On. Items in the Deleted Items folder are archived.

Legacy name ArchiveDeletedItems

Archive draft items (Exchange Archiving General setting)

Description Controls whether draft items are archived. This applies to all draft items, not just those in the Drafts folder.

Enterprise Vault does not convert archived draft items to shortcuts, even if the policy is configured to create shortcuts. Archived draft items are treated as shortcuts for purposes of shortcut deletion. Enterprise Vault does not remove attachments from archived draft items.

- Supported values
- Off (default). Draft items not archived.
 - On. Draft items are archived.

Archive Exchange Managed Folders (Exchange Archiving General setting)

Description Controls whether items are archived from Microsoft Exchange managed folders, and whether to apply managed content settings. Managed folders were introduced in Exchange Server 2007.

- Supported values
- Off. Enterprise Vault does not archive items from managed folders. Additionally, users are not allowed to archive items manually from managed folders.
 - Normal. Enterprise Vault treats managed folders as normal mailbox folders.
The value Normal lets users modify the contents of managed folders in Virtual Vault, provided the Virtual Vault policy settings allow such operations. For example, users can move items as follows:
 - From the mailbox to a managed folder in Virtual Vault
 - From a managed folder in Virtual Vault to another Virtual Vault folder
 - Managed (default). Enterprise Vault archives items from managed folders and uses retention settings that are synchronized from Exchange Server.

Legacy name ArchiveManagedFolders2

Archive naming convention (Exchange Archiving General setting)

Description	<p>By default, archives are given the same name as the associated mailbox on an Exchange Server. In some environments this may mean that the archive name is not unique. This can cause confusion when searching multiple archives, especially when items are returned from different archives that have the same name.</p> <p>The Archive naming convention setting lets you select the naming convention to use for archives. You can use this setting to ensure that the name given to an archive is unique within the organization. This setting is particularly useful if you use Veritas Discovery Accelerator to search multiple Exchange mailbox archives.</p> <p>If you modify the value of this setting, check that the value of the advanced policy setting, Reset archive names, is On. This setting is in the Archiving general list of settings.</p> <p>To update the names of existing archives so that they conform to the new naming convention, synchronize the mailboxes that use the modified policy.</p>
-------------	---

Supported values The following list describes the valid values for the setting. In the examples given, the resultant archive names assume that the user, John Doe, has the following account and mailbox details:

Account logon name in Active Directory: "JDoe"

Domain: "EXAMPLE"

Exchange Server mailbox name: "John Doe"

- *Mailbox name* (Default)
 The name of the associated Exchange mailbox.
 For example, John Doe
- *Mailbox name (account name)*
 The name of the associated mailbox, followed by the mailbox user's account logon name in Active Directory.
 For example, John Doe (JDoe)
- *Mailbox name (domain-qualified account name)*
 The name of the associated mailbox, followed by the domain and account logon name of the mailbox user (in the form DOMAIN\name).
 For example, John Doe (EXAMPLE\JDoe)
- *Account name (mailbox name)*
 The account logon name of the mailbox user, followed by the name of the associated mailbox.
 For example, JDoe (John Doe)
- *Domain-qualified account name (mailbox name)*
 The domain and account logon name of the mailbox user (in the form DOMAIN\name), followed by the name of the associated mailbox.
 For example, EXAMPLE\JDoe (John Doe)

Legacy name ArchiveNameFormat

Archive unexpired Calendar Events (Exchange Archiving General setting)

Description Controls whether unexpired calendar items are archived.

Supported values

- Off (default). Unexpired calendar items are not archived.
- On. Unexpired calendar items are archived.

Legacy name ArchiveNonExpiredCalEvents

Code pages for right-to-left custom shortcuts (Exchange Archiving General setting)

Description	A semicolon-separated list of code pages. Custom shortcuts that use these code pages are always formatted right-to-left.
Supported values	<ul style="list-style-type: none">■ A list of code pages, separated by semicolons. For example, 1255;1256. Default is 1255.
Legacy name	CustomShortcutRTLCodePages

Do not archive pending reminders (Exchange Archiving General setting)

Description	Controls whether Enterprise Vault archives items that have pending reminders.
Supported values	<ul style="list-style-type: none">■ Off. Items that have pending reminders are archived.■ On (default). Items that have pending reminders within the next five years are not archived.
Legacy name	DontArchiveItemsPendingReminder

Encode custom body using appropriate code pages (Exchange Archiving General setting)

Description	Use the appropriate ANSI code pages (rather than always using Unicode) when encoding the bodies of customized Enterprise Vault shortcuts.
Supported values	<ul style="list-style-type: none">■ Off. Use Unicode when encoding the bodies of customized Enterprise Vault shortcuts.■ On. Always use ANSI code pages when encoding the bodies of customized Enterprise Vault shortcuts.
Legacy name	EncodeCustomBodyUsingAppropriateCodePages

Future item retention category (Exchange Archiving General setting)

Description	<p>The name of the retention category to use for calendar, meeting, and task items that have end dates in the future; that is, unexpired calendar, meeting, and task items. The retention category must exist.</p> <p>If Enterprise Vault storage expiry for your site is based on the archived date of an item, then archived calendar, meeting, or task items with an end date in the future could be deleted by Enterprise Vault storage expiry before the end date of the item. To prevent this, you can create a retention category that Enterprise Vault will apply automatically to such items when they are archived, and specify this retention category in this policy setting. In the retention category properties, we recommend that you set the value of Base expiry on to Modified date, and configure the retention period as Retain items forever.</p> <p>Note: The retention category will not be applied retrospectively to items that have already been archived.</p>
Supported values	<ul style="list-style-type: none">■ The name of an existing retention category that you have set up to be used for these items. For example, Future Calendar Items.■ Leave blank to use the default retention category for the provisioning group. This is the default value.
Legacy name	FutureItemsRetCat

Include default and anonymous permissions (Exchange Archiving General setting)

Description	<p>Controls whether Enterprise Vault includes Default and Anonymous permissions when synchronizing each mailbox with its default archive.</p> <p>Enterprise Vault automatically removes existing Default and Anonymous user settings from archives unless you choose to synchronize them.</p>
Supported values	<ul style="list-style-type: none">■ Off (default). Do not synchronize Default or Anonymous permissions.■ On. Synchronize Default and Anonymous permissions. This has the side-effect that users can view each others' archives.
Legacy name	IncludeDefOrAnonPerms

Inherited permissions (Exchange Archiving General setting)

Description	Controls whether Enterprise Vault includes inherited permissions when synchronizing permissions between mailboxes or public folders and archives.
Supported values	<ul style="list-style-type: none">■ Off (default). Do not synchronize inherited permissions.■ On. Synchronize inherited permissions.
Legacy name	IncludeInheritedRights

Maximum message size to archive in MB (Exchange Archiving General setting)

Description	Controls the maximum size of messages that are archived.
Supported values	<ul style="list-style-type: none">■ 0. No restriction on maximum message size.■ Integer larger than 0. The maximum size of messages that are archived, in megabytes. Default is 250.
Legacy name	MaxMessageSizeToArchiveMB

Pending shortcut timeout (Exchange Archiving General setting)

Description	Specifies the number of days to allow items to remain in the state of archive-pending, restore-pending, or delete-pending before they are reset.
Supported values	<ul style="list-style-type: none">■ Off (default). Archive-pending, restore-pending, and delete-pending shortcuts are never reset.■ 0. When run in report mode, Exchange Mailbox tasks reset all archive-pending, restore-pending, and delete-pending shortcuts. When run in normal mode, the shortcuts are not reset.■ Any integer larger than zero. Archive-pending, restore-pending, and delete-pending shortcuts that are older than this number of days are reset. This happens in both normal archiving and in Report Mode.
Legacy name	PendingShortcutTimeout

Reset archive names (Exchange Archiving General setting)

Description	Controls whether, during synchronization, archive names are automatically changed to match mailbox names.
Supported values	<ul style="list-style-type: none">■ Off. During synchronization archive names are never changed.■ On (default). During synchronization, archive names are automatically changed if necessary to match mailbox names.
Legacy name	ResetArchiveNames

Set failed messages 'Do Not Archive' (Exchange Archiving General setting)

Description	<p>If an item cannot be archived, the default Exchange Mailbox task behavior is to reprocess the item on the next archiving run because such items can often be successfully archived on a second try.</p> <p>This setting enables you to change the behavior so items that fail archiving are marked as Do Not Archive and thus are not reprocessed on the next archiving run.</p>
Supported values	<ul style="list-style-type: none">■ Off (default). Failed items are not marked as Do Not Archive.■ On. Failed items are marked as Do Not Archive.
Legacy name	SetFailedMsgsDoNotArchive

Strip attachments to non-shortcut items (Exchange Archiving General setting)

Description	Controls whether attachments are removed from calendar items, meeting items (including requests, responses and cancellations), task and task request items, and contacts after archiving. These items are not changed into Enterprise Vault shortcuts when they are archived. If Enterprise Vault removes an attachment, it replaces it with a link to the attachment.
Supported values	<ul style="list-style-type: none">■ On (default). Attachments are removed from non-shortcut items after archiving.■ Off. Attachments are not removed from non-shortcut items after archiving.
Legacy name	StripAttachmentsToNonShortcutItems

Synchronize folder permissions (Exchange Archiving General setting)

Description	Controls whether synchronization of delegate and shared folder permissions within mailboxes are synchronized. If these are not synchronized, only mailbox owners have access to the corresponding archives. For example, this prevents delegates, from having access to mailbox archives.
Supported values	<ul style="list-style-type: none">■ Off. Folder permissions are not synchronized.■ On (default). Folder permissions are synchronized.
Legacy name	SynchronizeFolderPermissions

Text direction indicator for custom shortcuts (Exchange Archiving General setting)

Description	Specifies which code page property of a message to check when deciding whether to format its shortcut body as left-to-right or right-to-left: PR_MESSAGE_CODEPAGE or PR_INTERNET_CPID.
Supported values	<ul style="list-style-type: none">■ Use PR_MESSAGE_CODEPAGE (default).■ Prefer PR_INTERNET_CPID.
Legacy name	UsePRInternetCPIDForRTLdetermination

Valid Enterprise Vault site aliases (Exchange Archiving General setting)

Description	<p>A semicolon-separated list of the Enterprise Vault site aliases that are currently in operation in your environment.</p> <p>During shortcut processing, Enterprise Vault does not attempt to make connections to any site that is not in this list. This prevents connection attempts to Enterprise Vault sites that no longer exist in your environment.</p>
Supported values	<ul style="list-style-type: none">■ A semicolon-separated list of Enterprise Vault site aliases. You can enter unqualified aliases or fully qualified aliases, but they must match the site aliases you specified when you first ran the Enterprise Vault Configuration wizard. If you created unqualified site aliases in the Configuration wizard, you must enter unqualified aliases here.■ If this string is empty, Enterprise Vault attempts to process all shortcuts.

Legacy name WhitelistOfGoodEVConnectionPoints

Warn if default or anonymous permissions exist (Exchange Archiving General setting)

Description Controls whether Enterprise Vault places an entry in the Enterprise Vault Event Log when a folder has Default or Anonymous permissions set.

The warning looks similar to the following:

```
Date: 29/06/2004      Source: Enterprise Vault
Time: 18:00:42      Category: Archive Service
Type: Warning      Event ID: 3284
User: N/A
Computer: DEMO
```

Description:

The folder has Anonymous permissions set that grant all users access to this folder. By default, this has not been synchronized to the users archive.

```
MailboxDn: /o=Admin/ou=First Administrative
Group/cn=Recipients/cn=HardyO
FolderPath: Inbox
```

- Supported values**
- Off. Do not warn when a folder has Default or Anonymous permissions set.
 - On (default). Warn when a folder has Default or Anonymous permissions set.

Legacy name WarnWhenDefOrAnonPerms

Warn when mailbox not under quota after archiving run (Exchange Archiving General setting)

Description Controls whether a warning is entered in to the event log when too few archivable items were available to take a mailbox below the quota-free level setting.

- Supported values
- Off. Never log a warning if too few items were available to reduce the mailbox to the required usage level.
 - On (default). Log a warning if too few items were available to reduce the mailbox to the required usage level.

Legacy name WarnNotEnoughArchivedForQuota

Exchange desktop policy advanced settings

These settings control advanced aspects of Exchange desktop policy configuration.

The categories of Exchange desktop policy advanced settings are:

- [Office Mail App \(Exchange desktop policy advanced settings\)](#)
- [Outlook \(Exchange desktop policy advanced settings\)](#)
- [OWA versions before 2013 \(Exchange desktop policy advanced settings\)](#)
- [Vault Cache \(Exchange desktop policy advanced settings\)](#)
- [Virtual Vault \(Exchange desktop policy advanced settings\)](#)

Office Mail App (Exchange desktop policy advanced settings)

The Office Mail App settings let you control the availability and behavior of the Enterprise Vault Office Mail App in Outlook 2013 and OWA 2013.

The Office Mail App settings are:

- [Availability \(Exchange Office Mail App setting\)](#)
- [Behavior of Mail App Bar \(Exchange Office Mail App setting\)](#)
- [Mode \(Exchange Office Mail App setting\)](#)

Availability (Exchange Office Mail App setting)

Description Specifies the applications in which the Enterprise Vault Office Mail App is available.

Supported values	<ul style="list-style-type: none">■ OWA only (2013 or later). In Outlook, Enterprise Vault displays a message to indicate that the Office Mail App is not available. You may find this setting useful if you do not want to confuse Outlook users by providing two methods for accessing their archives (both the Enterprise Vault toolbar and the Office Mail App).■ Outlook only (2013 or later). In OWA, Enterprise Vault displays a message to indicate that the Office Mail App is not available.■ OWA and Outlook (2013 or later). This is the default setting.
Legacy name	OAAvailability

Behavior of Mail App Bar (Exchange Office Mail App setting)

Description	Determines what happens when a user clicks the Office Mail App bar in a shortcut: show the available Enterprise Vault options and immediately open the item in a new window, or show the Enterprise Vault options without opening the item.
Supported values	<ul style="list-style-type: none">■ Open immediately and show options.■ Show options (default).
Legacy name	OAMailBarBehavior

Mode (Exchange Office Mail App setting)

Description	Determines whether Outlook 2013 and OWA 2013 users have access to the full Enterprise Vault functionality.
Supported values	<ul style="list-style-type: none">■ Full. Users can choose a retention category for each item that they manually archive.■ Light (default). Users cannot choose a retention category for each item that they manually archive. Instead, Enterprise Vault archives the item with the default retention category for the mailbox folder that contains the item.
Legacy name	OAMode

Outlook (Exchange desktop policy advanced settings)

The Outlook settings enable you to control the behavior of the Enterprise Vault Outlook Add-In. Except where noted, none of the settings has any effect in the Enterprise Vault Client for Mac OS X.

The Outlook settings are:

- [Add server to intranet zone \(Exchange Outlook setting\)](#)
- [Allow script in public folders \(Exchange Outlook setting\)](#)
- [Allow script in shared folders \(Exchange Outlook setting\)](#)
- [Allow shortcut copy \(Exchange Outlook setting\)](#)
- [Alternative Web Application URL \(Exchange Outlook setting\)](#)
- [Automatically delete IE file cache \(Exchange Outlook setting\)](#)
- [Automatically re-enable Outlook add-in \(Exchange Outlook setting\)](#)
- [Deploy forms locally \(Exchange Outlook setting\)](#)
- [Display notifications \(Exchange Outlook setting\)](#)
- [Display Office Apps on original items \(Exchange Outlook setting\)](#)
- [Folder properties visible \(Exchange Outlook setting\)](#)
- [Force form reload on error \(Exchange Outlook setting\)](#)
- [Forward original item \(Exchange Outlook setting\)](#)
- [Limit automatic re-enabling of add-in \(Exchange Outlook setting\)](#)
- [Mailbox properties visible \(Exchange Outlook setting\)](#)
- [Mark PST files \(Exchange Outlook setting\)](#)
- [Message properties visible \(Exchange Outlook setting\)](#)
- [Outlook Add-In behavior \(Exchange Outlook setting\)](#)
- [Policy lookup locations \(Exchange Outlook setting\)](#)
- [Preserve message class \(Exchange Outlook setting\)](#)
- [Preserve message class \(for content class\) \(Exchange Outlook setting\)](#)
- [Prevent disabling of Outlook Add-In \(Exchange Outlook setting\)](#)
- [Printing behavior \(Exchange Outlook setting\)](#)
- [PST Import pause interval \(Exchange Outlook setting\)](#)
- [PST Import work check interval \(Exchange Outlook setting\)](#)
- [PST search interval \(Exchange Outlook setting\)](#)
- [Public Folder operations \(Exchange Outlook setting\)](#)
- [Remove PST entries \(Exchange Outlook setting\)](#)
- [Remove server from intranet zone \(Exchange Outlook setting\)](#)

- [Reply behavior \(Exchange Outlook setting\)](#)
- [RPC over HTTP restrictions \(Exchange Outlook setting\)](#)
- [Search behavior \(Exchange Outlook setting\)](#)
- [Shortcut download progress \(Exchange Outlook setting\)](#)
- [Soft deletes \(Exchange Outlook setting\)](#)
- [Use proxy settings \(Exchange Outlook setting\)](#)
- [Web Application URL \(Exchange Outlook setting\)](#)

Add server to intranet zone (Exchange Outlook setting)

Description	<p>Adds the listed servers to the browser's local intranet zone.</p> <p>If you use this setting, users are not prompted for their logon details when they search their archives or view or restore archived items.</p> <p>The change applies to the current user only, so other users of the same computer are unaffected.</p> <p>If the user does not have permission to modify the browser, the security settings are not changed and no error is generated.</p> <p>You cannot use this setting if you have applied United States Government Configuration Baseline (USGCB) group policy objects (GPO) to Windows computers in your organization. On USGCB-compliant desktops, users cannot change settings in the local intranet zone on their computers. For instructions on how you can configure the browser for these users, see the section "Publishing Enterprise Vault server details to USGCB-compliant computers" in the <i>Installing and Configuring</i> guide.</p>
Supported values	<ul style="list-style-type: none">■ A text string. Defines the computers to be added to the browser's local intranet zone. The string can contain wildcard characters, domain names, DNS aliases, or IP addresses. <p>To specify multiple computers, separate the names using a semicolon (;).</p> <p>The syntax is as follows:</p> <pre>computer1[;computer2][;computer3]...</pre> <p>Some examples of text strings are as follows:</p> <pre>webserver.mycorp.com *.mycorp.com mywebserver;*.mycorp.com</pre>
Legacy name	AddServerToIntranetZone

Allow script in public folders (Exchange Outlook setting)

Description	Controls whether the Outlook Add-In automatically sets the Allow Script In Public Folders setting. This setting is required in order for the Outlook Add-In to open shortcuts that are in public folders.
Supported values	<ul style="list-style-type: none">■ Force off. The Outlook Add-In cannot open shortcuts that are in public folders.■ Force on (default). The Outlook Add-In can open shortcuts that are in public folders.■ Keep user's setting. The user's Outlook setting of Allow Script In Public Folders is not changed.
Legacy name	AllowScriptPublicFolders

Allow script in shared folders (Exchange Outlook setting)

Description	Controls whether the Outlook setting Allow Script In Shared Folders is automatically set by the Outlook Add-In. This setting is required in order for the Outlook Add-In to be able to open shortcuts that are in shared folders.
Supported values	<ul style="list-style-type: none">■ Force off. The Outlook Add-In cannot open shortcuts that are in shared folders.■ Force on (default). The Outlook Add-In can open shortcuts that are in shared folders.■ Keep user's setting. The user's Outlook setting of Allow Script In shared Folders is not changed.
Legacy name	AllowScriptSharedFolders

Allow shortcut copy (Exchange Outlook setting)

Description	Controls the behavior when a user tries to copy a shortcut. It is possible to make Enterprise Vault restore the original item, rather than copy the shortcut. This can prevent any confusion that could arise if an archived item is later deleted, leaving orphaned shortcuts that no longer work.
-------------	---

- Supported values
- Off. When a user tries to copy a shortcut, Enterprise Vault displays a message explaining that the item can only be copied after the user has restored it.

Note that setting this option to Off does not stop users from copying shortcuts in the following ways:

- By right-clicking the shortcuts and then clicking **Move > Copy to Folder**.
- By copying an entire Outlook folder that contains one or more Enterprise Vault shortcuts into another folder.

Certain limitations in Outlook prevent Enterprise Vault from blocking these operations.

- On (default). The user is allowed to copy the shortcut. If the user later deletes the shortcut and the corresponding archived item, any copies of the shortcut no longer work.

Legacy name AllowCopyShortcut

Alternative Web Application URL (Exchange Outlook setting)

Description Specifies an alternative URL for the Enterprise Vault server, if the default Web Application URL does not resolve.

For example, clients on an external network may need to use a proxy server to contact the Enterprise Vault server. In this case, you can use the **Alternative Web Application URL** setting to specify a URL like the following:

`https://proxy_server/EnterpriseVault`

- Supported values
- A URL.

Legacy name RPCOverHTTPProxyURL

Automatically delete IE file cache (Exchange Outlook setting)

Description Controls whether the Enterprise Vault add-in to Outlook automatically deletes a user's Temporary Internet files if the Internet Explorer cache is preventing archived items from being displayed.

- Supported values
- Do not delete files (default). Temporary Internet files are never deleted.
 - Delete files and tell user. The Temporary Internet files are deleted and a message informs the user that they have been deleted.
 - Delete files silently. The Temporary Internet files are deleted and the user is not informed.
 - Ask user. The user is asked whether the Temporary Internet files should be deleted.

Legacy name AutoDeleteIECache

Automatically re-enable Outlook add-in (Exchange Outlook setting)

Description Controls whether the Enterprise Vault Outlook Add-In is automatically re-enabled if it has been disabled.

- Supported values
- Do not re-enable. The Outlook Add-In is never automatically re-enabled if it has been disabled.
 - Re-enable and tell user (default). The Outlook Add-In is automatically re-enabled if it has been disabled and a message informs the user that this has happened.
 - Re-enable silently. The Outlook Add-In is automatically re-enabled if it has been disabled and the user is not informed.
 - Ask user. The user is asked whether the Outlook Add-In should be re-enabled.

Legacy name AutoReEnable

Deploy forms locally (Exchange Outlook setting)

Description Controls how the Enterprise Vault Exchange forms are deployed to users' Personal Form Libraries.

This setting enables you to control the deployment of Enterprise Vault Exchange forms in an environment in which there is no Organizational Forms library.

If you choose to deploy forms locally, the forms are automatically updated when you upgrade to a later version of Enterprise Vault.

- Supported values
- Never. Never deploy the Enterprise Vault Exchange forms to users' Personal Form Libraries.
 - When no Org Forms. Deploy to users' Personal Form Libraries when there is no Organization Forms Library.
 - Always (default). Always deploy forms locally.
 - Delete. Delete locally-deployed forms. This may be useful if, for example, your Exchange Server environment changes so that an Organizational Forms Library becomes available. This setting enables you to remove all locally-deployed forms from users' computers.
- When upgrading to a later Enterprise Vault version, you do not need to use this option to delete existing local forms. The forms are automatically upgraded.

Legacy name DeployFormsLocally

Display notifications (Exchange Outlook setting)

Description Enables and disables Enterprise Vault Outlook Add-In user notifications. For example, when **Display notifications** is enabled, the Enterprise Vault Outlook Add-In notifies users of Vault Cache synchronization errors.

Note: You can also use the NotificationsEnabled registry value on individual computers to enable and disable user notifications. On computers where it is set, NotificationsEnabled overrides the policy setting. For more information, see "NotificationsEnabled" in the *Registry Values* guide.

- Supported values
- Off (default). Disables Enterprise Vault Outlook Add-In user notifications.
 - On. Enables Enterprise Vault Outlook Add-In user notifications.

Legacy name NotificationsEnabled

Display Office Apps on original items (Exchange Outlook setting)

Description When users open the original content of archived items from shortcuts, specifies whether to display the Enterprise Vault Office Mail App in that content. This setting applies to Outlook 2013 and later only.

Supported values	<ul style="list-style-type: none">■ Off. The Office Mail App does not appear in the original content of opened archived items.■ On (default). The Office Mail App does appear in the original content of opened archived items.
Legacy name	DisplayOfficeAppsOnOriginalItems

Folder properties visible (Exchange Outlook setting)

Description	<p>Controls whether folder properties show the Enterprise Vault property tab.</p> <p>If you have locked all the Enterprise Vault settings, you may want to hide the property tab too.</p> <p>By hiding the property tab, you are in effect locking all the settings, because users cannot get to the tab page to change them.</p>
Supported values	<ul style="list-style-type: none">■ Hide tab. Enterprise Vault folder properties are hidden.■ Show tab (default). Enterprise Vault folder properties are shown.
Legacy name	FolderPropertiesVisible

Force form reload on error (Exchange Outlook setting)

Description	<p>Controls whether the Outlook registry entry ForceFormReload is written to force Outlook to reload forms on error.</p> <p>Note that this registry entry applies to all Outlook forms, so changing this setting may affect other applications.</p>
Supported values	<ul style="list-style-type: none">■ Remove entry. Remove the registry entry. This means that Outlook does not reload forms on error.■ Write entry (default). Write the registry entry. This forces Outlook to reload forms on error.
Legacy name	SetForceFormReload

Forward original item (Exchange Outlook setting)

Description	<p>Controls the behavior when a user forwards a shortcut. The default is to forward the archived item, but it is possible to forward the contents of the shortcut itself.</p>
-------------	---

- Supported values
- Shortcut. Forward the shortcut.
 - Original (default). Forward the archived item. Items of type IPM.Document or IPM.Appointment cannot be forwarded. If a user tries to forward one of these an explanatory message is displayed.

Legacy name ForwardOriginalItem

Limit automatic re-enabling of add-in (Exchange Outlook setting)

Description Controls the maximum number of times in any seven-day period that the Outlook Add-In can re-enable itself as an Outlook add-in.

- Supported values
- An integer specify the maximum number of times that the Outlook Add-In can re-enable itself in any seven-day period. The default is 3.

Legacy name MaxAutoReEnables

Mailbox properties visible (Exchange Outlook setting)

Description Controls whether the mailbox properties show the Enterprise Vault property tab.

If you have locked all the Enterprise Vault settings, you may want to hide the property tab too.

By hiding the property tab, you are in effect locking all the settings, because users cannot get to the tab page to change them.

- Supported values
- Hide tab. Mailboxes hide the Enterprise Vault property tab.
 - Show tab (default). Mailboxes show the Enterprise Vault property tab.

Legacy name MailboxPropertiesVisible

Mark PST files (Exchange Outlook setting)

Description	<p>Controls whether the Enterprise Vault client marks PST files with details of the owning account. This setting is useful when you migrate the contents of PST files to Enterprise Vault.</p> <p>When PST file marking is switched on, the Enterprise Vault Outlook Add-In tries to open every PST that is listed in the user's Outlook profile. Users are prompted for passwords to password-protected PSTs and receive error messages for any PSTs that are inaccessible.</p> <p>Note: To avoid migration failures due to incorrect passwords or missing passwords, you may edit the General tab of the Personal Store Management properties to allow Enterprise Vault to override passwords and migrate the files.</p>
Supported values	<ul style="list-style-type: none">■ Off. The Enterprise Vault client does not mark PST files■ On (default). The Enterprise Vault client marks PST files with details of the owning account.
Legacy name	MarkPSTs

Message properties visible (Exchange Outlook setting)

Description	<p>Controls whether individual message properties show the Enterprise Vault property tab. If you have locked all the Enterprise Vault settings, you may want to hide the property tab too.</p>
Supported values	<ul style="list-style-type: none">■ Hide tab. Messages hide the Enterprise Vault property tab.■ Show tab (default). Messages show the Enterprise Vault property tab.
Legacy name	MessagePropertiesVisible

Outlook Add-In behavior (Exchange Outlook setting)

Description	<p>Controls whether the Enterprise Vault Outlook Add-In is in full mode or light mode.</p> <p>In full mode, there are no functional restrictions on the behavior of the Outlook Add-In.</p> <p>In light mode, the following restrictions apply:</p> <ul style="list-style-type: none">■ 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.
Supported values	<ul style="list-style-type: none">■ Full. The Outlook Add-In is in full mode.■ Light (default). The Outlook Add-In is in light mode. <p>If you decide to set Outlook Add-In behavior to Light, and your existing policies allow users to change Enterprise Vault folder settings, you may want to run Policy Manager to return all folders to your site settings. See the <i>Utilities</i> guide for more information on Policy Manager.</p> <p>If the Outlook Add-In version is earlier than Enterprise Vault 10.0.1, the Outlook Add-In behavior setting controls whether the Outlook Add-In behaves in exactly the same way as the HTTP-Only Outlook Add-In. In this case, the values have the following meanings:</p> <ul style="list-style-type: none">■ Full. Outlook Add-In behavior is unchanged.■ Light (default). The Outlook Add-In behaves in exactly the same way as the HTTP-Only Outlook Add-In.
Legacy name	UseSelfInstallFunc

Policy lookup locations (Exchange Outlook setting)

Description You can set Enterprise Vault Outlook Add-In registry values on a user's computer. If there is an equivalent policy value in the Exchange desktop policy in the Administration Console, the registry value overrides the Exchange desktop policy.

Policy lookup locations lets you control the use of registry values on users' computers to override the Exchange desktop policy. You can specify the following types of policy lookup:

- Look only in the Exchange desktop policy.
- Look in the registry first. If there is no registry value, use the policy value in the Exchange desktop policy.

For information about the Outlook Add-In registry values, see the *Registry Values* guide.

- Supported values
- Policy only. The Outlook Add-In looks only in the Exchange desktop policy.
 - Policy, registry HKLM. The Outlook Add-In looks in the following registry key:

```
HKEY_LOCAL_MACHINE
  \SOFTWARE
    \KVS
      \Enterprise Vault
        \Client
```

If the policy value is not in this registry key, the Outlook Add-In uses the policy value in the Exchange desktop policy. If there is no equivalent policy value in the Exchange desktop policy, the Outlook Add-In uses the registry value default.

- Policy, registry HKLM, registry HKCU (default). The Outlook Add-In looks in the following registry keys, in this order. Only the Vault Cache and Virtual Vault registry values can be located in the second of these registry keys.

```
HKEY_LOCAL_MACHINE
  \SOFTWARE
    \KVS
      \Enterprise Vault
        \Client
```

```
HKEY_CURRENT_USER
  \SOFTWARE
    \KVS
      \Enterprise Vault
        \Client
          \VaultCacheStoreID
```

```
HKEY_CURRENT_USER
  \SOFTWARE
    \KVS
      \Enterprise Vault
        \Client
```

If the policy value is not in these registry keys, the Outlook Add-In uses the policy value in the Exchange desktop policy. If there is no equivalent policy value in the Exchange desktop policy, the Outlook Add-In uses the registry value default.

Legacy name RestrictPolicyLookup

Preserve message class (Exchange Outlook setting)

Description	Preserves the message classes of archived items that have the specified classes. When a user opens a shortcut, Enterprise Vault normally appends the suffix "EnterpriseVault.Original" to its message class to indicate that the shortcut is a view of an archived item. In certain circumstances, this suffix can prevent some types of items from opening properly in Outlook. The "Preserve message class" setting lets you preserve the original message class of these items so that they open without error.
Supported values	<ul style="list-style-type: none">■ A text string. Defines the message classes that Enterprise Vault should leave unchanged when opening items that have these classes. To specify multiple classes, separate them using a semicolon (;). You can type the exact class name or append an asterisk (*) to indicate a prefix match. The default value for this setting is as follows: IPM.Note.SMime*;IPM.Report.*;REPORT.IPM* The text string is case-insensitive.
Legacy name	MessageClassesPreventingMsgClassChangeOnView

Preserve message class (for content class) (Exchange Outlook setting)

Description	Preserves the message classes of archived items that have the specified content classes. When a user opens a shortcut, Enterprise Vault normally appends the suffix "EnterpriseVault.Original" to its message class to indicate that the shortcut is a view of an archived item. In certain circumstances, this suffix can prevent some types of items from opening properly in Outlook. The "Preserve message class (for content class)" setting stops Enterprise Vault from changing the message class of any item with the specified content class.
Supported values	<ul style="list-style-type: none">■ A text string. Specifies the content classes of items whose message classes are unchangeable. To specify multiple content classes, separate them using a semicolon (;). You can type the exact class name or append a trailing asterisk (*) to indicate a prefix match. The default value is as follows: rpmsg.message The text string is case-insensitive.
Legacy name	ContentClassesPreventingMsgClassChangeOnView

Prevent disabling of Outlook Add-In (Exchange Outlook setting)

Description	Specifies whether to add the Enterprise Vault Outlook Add-In to each user's list of add-ins that Outlook may not disable. This option applies to Outlook 2013 and later only.
Supported values	<ul style="list-style-type: none">■ Add to list (default). Stops Outlook from disabling the Enterprise Vault Outlook Add-In by adding it to each user's "Do not disable Add-in" list.■ Keep user's setting. Neither add the Enterprise Vault Outlook Add-In to each user's "Do not disable Add-in" list nor remove it from the list.■ Remove from list. Remove the Enterprise Vault Outlook Add-In from each user's "Do not disable Add-in" list, if it appears in the list.
Legacy name	AddToDoNotDisableAddinList

Printing behavior (Exchange Outlook setting)

Description	This legacy setting has no effect in Outlook 2010 and later, where the behavior is always to print the contents of the shortcut. Therefore, users must first restore an archived item when they want to print its entire contents.
Supported values	<ul style="list-style-type: none">■ Shortcut. Print the contents of the shortcut.■ Archived item (default). Print the contents of the archived item.
Legacy name	PrintOriginalItem

PST Import pause interval (Exchange Outlook setting)

Description	<p>When using client-driven PST migration, this controls the amount of time the Outlook Add-In waits between completing the import of one PST file and starting the import of the next.</p> <p>This is also the time that the Outlook Add-In waits after Outlook is started before continuing with PST file import.</p>
Supported values	<ul style="list-style-type: none">■ Integer. When importing PST files, the number of minutes to wait between PST files and the number of minutes to wait after Outlook starts before continuing PST file import. The default is 1 (minute).
Legacy name	PSTImportPauseInterval

PST Import work check interval (Exchange Outlook setting)

Description	The number of minutes client-driven PST migration waits, having completed its work, before checking for more work.
Supported values	<ul style="list-style-type: none">Integer. An integer value specifying the number of minutes to wait before checking for more work. The default is 60.
Legacy name	PSTImportNoWorkPauseInterval

PST search interval (Exchange Outlook setting)

Description	When using client-driven PST migration, this controls the amount of time that the Outlook Add-In waits after searching a user's computer for PST files before searching again.
Supported values	<ul style="list-style-type: none">Integer. Indicates the number of days to wait between searches. The default is 7 (days).
Legacy name	PSTSearchInterval

Public Folder operations (Exchange Outlook setting)

Description	Controls whether users can do the following: <ul style="list-style-type: none">Manually archive from public folders.Manually restore from public folders.In public folders, delete shortcuts and their corresponding archived items.
Supported values	<ul style="list-style-type: none">Off (default). Users can archive, restore, or delete in public folders. Users must be enabled for mailbox archiving and must have Editor, Publishing Editor, or Owner permissions on the folders that they want to modify.On. Users cannot archive, restore, and delete in public folders.
Legacy name	DisablePublicFolderOps

Remove PST entries (Exchange Outlook setting)

Description	<p>Controls whether PST file entries are removed from users' profiles when the migration of the corresponding PST files is complete.</p> <p>You can combine the values as required. For example, to remove PST entries for PST files that are hidden (4) or read-only (2), you would set Remove PST Entries to 6.</p>
Supported values	<ul style="list-style-type: none">■ 0 (default). Do not remove the profile entry after migrating a PST file.■ 1. Remove the profile entry if the PST file has been deleted from the user's computer.■ 2. Remove the PST entry if the PST file is read-only.■ 4. Remove the PST entry if the PST file has the Hidden file attribute set.
Legacy name	RemovePSTEntries

Remove server from intranet zone (Exchange Outlook setting)

Description	<p>Removes the listed servers from the Internet Explorer local intranet zone.</p> <p>The effect of this is that, unless you set up appropriate access, users are prompted for their user names and passwords when they search their archives or view or restore archived items.</p> <p>The change applies to the current user only, so other users of the same computer are unaffected.</p> <p>If the user does not have permission to modify Internet Explorer the security settings are not changed and no error is generated.</p>
Supported values	<ul style="list-style-type: none">■ A text string. Defines the computers to be removed from the Internet Explorer local intranet zone. The string can contain wildcard characters, domain names, DNS aliases, or IP addresses. To specify multiple computers, separate the names using semicolons (;). The syntax is as follows: <code>computer1[;computer2][;computer3]...</code> Some examples of text strings are as follows: <code>webserver.mycorp.com</code> <code>*.mycorp.com</code> <code>mywebserver;*.mycorp.com</code>

Legacy name RemoveServerFromIntranetZone

Reply behavior (Exchange Outlook setting)

Description Controls the behavior when a user replies to a shortcut. The default is to include the contents of the archived item, but it is possible to include the contents of the shortcut itself.

Supported values

- Shortcut. Include the contents of the shortcut in the reply. (This is the same behavior as in Enterprise Vault versions before 6.0.)
- Original (default). Include the contents of the archived item.

Legacy name ReplyToOriginalItem

RPC over HTTP restrictions (Exchange Outlook setting)

Description Controls which features are available when Outlook is configured to use RPC over HTTP (Outlook Anywhere). The default value **Disable Outlook Add-In** applies only to mailboxes that are hosted on Exchange Server 2010.

If the default value is selected, all Enterprise Vault Outlook Add-In functionality is available for mailboxes that are hosted on Exchange Server 2013 or later.

Supported values

- None. All Enterprise Vault Outlook Add-In functionality is available when Outlook is configured to use RPC over HTTP.
- Disable Outlook Add-In (default). Connecting to Enterprise Vault using RPC over HTTP is not enabled in the Enterprise Vault Outlook Add-In.
- Disable Vault Cache. Vault Cache is disabled when Outlook is configured to use RPC over HTTP.
- Disable PST Import. Client-side PST migration is disabled when Outlook is configured to use RPC over HTTP.
- Disable Vault Cache and PST Import. Both Vault Cache and client-side PST migration are disabled when Outlook is configured to use RPC over HTTP.

Legacy name RPCOverHTTPRestrictions

Search behavior (Exchange Outlook setting)

Description	<p>Controls the behavior of the Search Vaults menu option and the Search Vaults button.</p> <p>This setting affects users of the Enterprise Vault Outlook Add-In only. For users of the Enterprise Vault Client for Mac OS X, the search functionality always opens in a separate browser window.</p>
Supported values	<ul style="list-style-type: none">■ Separate browser. The search functionality always opens in a separate browser window.■ In Outlook (default). The search functionality is embedded in the Outlook window, if the user has the required software, and otherwise opens in a separate browser window.
Legacy name	UseNewStyleSearch

Shortcut download progress (Exchange Outlook setting)

Description	<p>Controls the display of the progress window that appears when a user opens a shortcut and the item is being downloaded to the user's computer.</p>
Supported values	<ul style="list-style-type: none">■ 0. Do not display download dialog at all.■ An integer greater than zero. Show the progress dialog after this number of seconds. Default is 1 (second).
Legacy name	DownloadShortcutHideProgress

Soft deletes (Exchange Outlook setting)

Description	<p>Controls the behavior when a user deletes a shortcut and an archived item. The default is to perform a permanent deletion of the shortcut; that is, a deletion that is not recoverable in Exchange. If the permanent deletion fails, a recoverable deletion is performed.</p> <p>If recoverable deletion is unacceptable, set the value to Off.</p>
Supported values	<ul style="list-style-type: none">■ On (default). Allow recoverable deletion.■ Off. Do not allow recoverable deletion and display an error message instead.
Legacy name	NoSoftDeletes

Use proxy settings (Exchange Outlook setting)

Description	Controls whether the Outlook Add-In uses the proxy settings on the client computer.
Supported values	<ul style="list-style-type: none">■ Use proxy settings (default).■ Ignore proxy settings.
Legacy name	InternetOpenTypeDirect

Web Application URL (Exchange Outlook setting)

Description	<p>Specifies the address of the Web Access application in one or more different Enterprise Vault sites. The Enterprise Vault sites may be in different Enterprise Vault directories. This setting enables shortcuts from the specified Enterprise Vault sites to work.</p> <p>For example, you need to use this setting in the following cases:</p> <ul style="list-style-type: none">■ When you want users to be able to access archived items from mailbox shortcuts in other Enterprise Vault sites■ When Exchange Public Folder tasks from more than one Enterprise Vault site process a public folder hierarchy
Supported values	<ul style="list-style-type: none">■ The URLs of Web Access applications in other Enterprise Vault sites. Enter one or more addresses in the following format: <code>[vault_site_alias1]=URL;[vault_site_alias2]=URL</code> where:<ul style="list-style-type: none">■ <code>vault_site_alias1</code> and <code>vault_site_alias2</code> are the vault site aliases of the other Enterprise Vault sites. The vault site alias is displayed on the General page of site properties in the Enterprise Vault Administration Console.■ <code>URL</code> is the address of the Web Access application for the Enterprise Vault site. <p>If you specify addresses for multiple Enterprise Vault sites, separate them with a semicolon (;). The overall length of the string cannot exceed 255 characters.</p> <p>For example:</p> <pre>[UKsite]=http://UKsite.example.com/EnterpriseVault; [USAsite]=http://USAsite.example.com/EnterpriseVault</pre>
Legacy name	WebAppURL

OWA versions before 2013 (Exchange desktop policy advanced settings)

The OWA versions before 2013 settings let you control the behavior of OWA 2010 clients. For OWA 2013, use the Office Mail App settings instead.

The OWA versions before 2013 settings are:

- [Archive confirmation \(Exchange OWA versions before 2013 setting\)](#)
- [Archive subfolders \(Exchange OWA versions before 2013 setting\)](#)
- [Basic archive function \(Exchange OWA versions before 2013 setting\)](#)
- [Basic restore function \(Exchange OWA versions before 2013 setting\)](#)
- [Client connection \(Exchange OWA versions before 2013 setting\)](#)
- [Delete shortcut after restore \(Exchange OWA versions before 2013 setting\)](#)
- [External Web Application URL \(Exchange OWA versions before 2013 setting\)](#)
- [Forward mode \(Exchange OWA versions before 2013 setting\)](#)
- [Location for restored items \(Exchange OWA versions before 2013 setting\)](#)
- [Open mode \(Exchange OWA versions before 2013 setting\)](#)
- [OWA 'Archive Policy' context menu option \(Exchange OWA versions before 2013 setting\)](#)
- [Premium archive function \(Exchange OWA versions before 2013 setting\)](#)
- [Premium restore function \(Exchange OWA versions before 2013 setting\)](#)
- [Reply mode \(Exchange OWA versions before 2013 setting\)](#)
- ['Reply To All' mode \(Exchange OWA versions before 2013 setting\)](#)
- [Restore confirmation \(Exchange OWA versions before 2013 setting\)](#)
- ['Search Vaults' in Basic OWA client \(Exchange OWA versions before 2013 setting\)](#)
- ['Search Vaults' in Premium OWA client \(Exchange OWA versions before 2013 setting\)](#)
- [View mode \(Exchange OWA versions before 2013 setting\)](#)
- [Web Application alias \(Exchange OWA versions before 2013 setting\)](#)

Archive confirmation (Exchange OWA versions before 2013 setting)

Description	Specifies whether there is a confirmation prompt when a user tries to archive an item manually.
Supported values	<ul style="list-style-type: none">■ Off. No confirmation.■ On (default). Prompt for confirmation.
Legacy name	OWA2003ArchiveConfirmation

Archive subfolders (Exchange OWA versions before 2013 setting)

Description	For manual archiving, controls whether subfolders are archived if they are included in a user's selection.
Supported values	<ul style="list-style-type: none">■ Off (default). Subfolders are not archived.■ On. Subfolders are archived.
Legacy name	OWA2003ArchiveSubFolders

Basic archive function (Exchange OWA versions before 2013 setting)

Description	Controls whether users of the OWA Basic client are allowed to choose archiving settings, such as retention category and destination archive, when archiving items manually.
Supported values	<ul style="list-style-type: none">■ Basic (default). Users cannot change settings when archiving. The archive settings on Outlook folders are used, which may be set by the user in Outlook or by the administrator.■ Enhanced. Users can select archiving settings when they perform manual archives.
Legacy name	OWA2003BasicArchiveFunction

Basic restore function (Exchange OWA versions before 2013 setting)

Description	Controls whether the OWA context menu for the OWA Basic client has a Restore option.
-------------	---

- Supported values
- Basic (default). There is no **Restore** option on the context menu.
 - Enhanced. There is a **Restore** option on the context menu.

Legacy name OWA2003BasicRestoreFunction

Client connection (Exchange OWA versions before 2013 setting)

Description This setting is no longer used.

Legacy name OWAClientUseDirectConnection

Delete shortcut after restore (Exchange OWA versions before 2013 setting)

Description Controls whether a shortcut is deleted when it is used to restore the corresponding archived item.

- Supported values
- Retain. The shortcut is not deleted when the archived item is restored.
 - Delete (default). The shortcut is deleted when the archived item is restored.

Legacy name OWA2003RestoreDeleteShortcut

External Web Application URL (Exchange OWA versions before 2013 setting)

Description Specifies an external URL for Enterprise Vault; that is, a URL that is used outside the corporate network to access the Enterprise Vault server through a firewall.

For more information on the use of this setting, see the following technical note on the Veritas Support website:

<http://www.veritas.com/docs/000035132>

The technical note also provides other information about configuring internal and external web application URLs for OWA. The information includes configuration file settings that let you refine which users access Enterprise Vault using the External Web Application URL.

- Supported values
- A text string. The external URL for Enterprise Vault. The URL can be either a fully qualified URL to the Web Access application virtual directory, or a relative URL. An example of a fully qualified URL is:
`http://evserver1.external.name/enterprisevault`
An example of a relative URL is:
`/enterprisevault`
The default value of this setting is:
`<https>/enterprisevault`
The optional component `<https>` at the start of the relative URL indicates that the HTTPS protocol should be used. If the optional component is not present, then the HTTP protocol is used.

Legacy name ExternalWebAppURL

Forward mode (Exchange OWA versions before 2013 setting)

Description Controls the behavior when a user chooses to forward an Enterprise Vault shortcut. It is possible to forward either the shortcut itself, or the archived item. The recipients cannot access the archived item unless they have access to the archive.

- Supported values
- Shortcut. The shortcut contents are forwarded.
 - Archived item (default). The archived item is forwarded.

Legacy name OWA2003ForwardMode

Location for restored items (Exchange OWA versions before 2013 setting)

Description Controls the destination for an item that is restored using a shortcut. The destination can be either of the following:

- The current location (the same folder as the shortcut).
- The Enterprise Vault Restored Items folder.

- Supported values
- Current location (default). Restore to the same folder as the shortcut.
 - Restored items. Restore to the Restored Items folder.

Legacy name OWA2003RestoreToRestoredItems

Open mode (Exchange OWA versions before 2013 setting)

Description	Controls the behavior when a user opens an Enterprise Vault shortcut.
Supported values	<ul style="list-style-type: none">■ Shortcut. The shortcut itself is opened.■ Archived item (default). The archived item is opened.
Legacy name	OWA2003OpenMode

OWA 'Archive Policy' context menu option (Exchange OWA versions before 2013 setting)

Description	<p>In Exchange Server 2010 the OWA archive policy enables users to archive items to the secondary Exchange Server mailbox. This setting lets you hide the OWA archive policy options in OWA 2010 Premium clients. Setting the value to On removes the OWA archive policy option from the following menus:</p> <ul style="list-style-type: none">■ Folder context menu■ Item context menu (non-conversation view)■ Item context menu (conversation view)■ Conversation Actions menu
Supported values	<ul style="list-style-type: none">■ On. The option is not displayed in the menus.■ Off (default). The option is displayed on the menus.
Legacy name	OWA2010HideOWAArchivePolicy

Premium archive function (Exchange OWA versions before 2013 setting)

Description	Controls whether users of the OWA Premium client are allowed to choose archiving settings, such as retention category and destination archive, when archiving items manually.
Supported values	<ul style="list-style-type: none">■ Basic. Users cannot change settings when archiving. The archive settings on Outlook folders are used, which may be set by the user in Outlook or by the administrator.■ Enhanced (default). Users can select archiving settings when they perform manual archives.
Legacy name	OWA2003PremiumArchiveFunction

Premium restore function (Exchange OWA versions before 2013 setting)

Description	Controls whether users of the OWA Premium client are allowed to choose archiving settings, such as retention category and destination archive, when archiving items manually.
Supported values	<ul style="list-style-type: none">■ Basic. Users cannot change settings when archiving. The archive settings on Outlook folders are used, which may be set by the user in Outlook or by the administrator.■ Enhanced (default). Users can select archiving settings when they perform manual archives.
Legacy name	OWA2003PremiumRestoreFunction

Reply mode (Exchange OWA versions before 2013 setting)

Description	Controls the behavior when a user chooses to reply to an Enterprise Vault shortcut.
Supported values	<ul style="list-style-type: none">■ Shortcut. The shortcut is replied to.■ Archived item (default). The archived item is replied to.
Legacy name	OWA2003ReplyMode

'Reply To All' mode (Exchange OWA versions before 2013 setting)

Description	Controls the behavior when a user selects a shortcut and chooses Reply to All .
Supported values	<ul style="list-style-type: none">■ Shortcut. The shortcut is replied to.■ Archived item (default). The archived item is replied to.
Legacy name	OWA2003ReplyToAllMode

Restore confirmation (Exchange OWA versions before 2013 setting)

Description	Controls whether the user is asked for confirmation after choosing to restore an archived item.
-------------	---

- Supported values
- Off. The item is restored without asking the user for confirmation.
 - On (default). There is a confirmation prompt before an item is restored.

Legacy name OWA2003RestoreConfirmation

'Search Vaults' in Basic OWA client (Exchange OWA versions before 2013 setting)

Description Controls whether the archive search option is available in the OWA Basic client.

- Supported values
- Off. The archive search option is not available.
 - On (default). The archive search option is available.

Legacy name OWA2003SearchFromBasicNavbar.

'Search Vaults' in Premium OWA client (Exchange OWA versions before 2013 setting)

Description Controls whether the archive search option is available in the OWA Premium client.

- Supported values
- Off. The archive search option is not available.
 - On (default). The archive search option is available.

Legacy name OWA2003SearchFromPremiumNavbar

View mode (Exchange OWA versions before 2013 setting)

Description Controls whether when a user clicks **Open the Original Item** in the banner of a custom shortcut, the original item is rendered by OWA (and looks like an Outlook message), or by Enterprise Vault (and looks like a web browser page).

- Supported values
- Enterprise Vault. Enterprise Vault renders the original item.
 - OWA (default). OWA renders the original item.

Legacy name OWA2003ViewMode

Web Application alias (Exchange OWA versions before 2013 setting)

Description	Specifies the name of the virtual directory for anonymous connections, EVAnon. This is synchronized to the hidden settings in each mailbox.
Supported values	<ul style="list-style-type: none">■ A text string. The name of the virtual directory to use for anonymous connections.
Legacy name	OWAWebAppAlias

Vault Cache (Exchange desktop policy advanced settings)

The Vault Cache advanced settings let you control the behavior of Vault Cache.

The Vault Cache settings are:

- [Download item age limit \(Exchange Vault Cache setting\)](#)
- [Lock for download item age limit \(Exchange Vault Cache setting\)](#)
- [Manual archive inserts \(Exchange Vault Cache setting\)](#)
- [Offline store required \(Exchange Vault Cache setting\)](#)
- [Pause interval \(Exchange Vault Cache setting\)](#)
- [Per item sleep \(Exchange Vault Cache setting\)](#)
- [Preemptive archiving in advance \(Exchange Vault Cache setting\)](#)
- [Root folder \(Exchange Vault Cache setting\)](#)
- [Root folder search path \(Exchange Vault Cache setting\)](#)
- [Show Setup Wizard \(Exchange Vault Cache setting\)](#)
- [Synchronize archive types \(Exchange Vault Cache setting\)](#)
- [WDS search auto-enable \(Exchange Vault Cache setting\)](#)

Download item age limit (Exchange Vault Cache setting)

Description	<p>Specifies the maximum age of items, in days, at which items are considered too old to be initially downloaded to the Vault Cache.</p> <p>For example, if Download item age limit is set to 30 then items up to 30 days old are downloaded. If Download item age limit is set to 0 then all items are downloaded.</p>
-------------	---

- Supported values
- 0. No age limit. All items are downloaded.
 - Integer. The maximum age, in days, of items that will be downloaded. All items up to this age will be downloaded.

Legacy name OVDownloadItemAgeLimit

Lock for download item age limit (Exchange Vault Cache setting)

Description Controls whether users can change the download age limit.

- Supported values
- On. Locked.
 - Off. Not locked.

Legacy name OVLlockDownloadItemAgeLimit

Manual archive inserts (Exchange Vault Cache setting)

Description Controls whether an item that is manually archived is also automatically added to the Vault Cache.

- Supported values
- On (default). Automatically add manually archived items to the Vault Cache.
 - Off. Do not add to the Vault Cache.

Legacy name OVNoManualArchiveInserts.

Offline store required (Exchange Vault Cache setting)

Description Controls whether Vault Cache can be enabled when no offline store is present.

Users have offline store (OST) files if Outlook Cached Exchange Mode is enabled. If a user does not have an OST file, Enterprise Vault cannot perform preemptive caching.

If there is no preemptive caching, there is an increased load on Vault Cache content synchronization for newly archived items. The increased load is only a consideration if the Vault Cache content strategy is **Store all items**.

- Supported values
- Yes (default). An offline store is required for Vault Cache to be enabled.
 - No. An offline store is not required for Vault Cache to be enabled.

Legacy name OVRequireOfflineStore

Pause interval (Exchange Vault Cache setting)

Description The number of minutes to wait before Enterprise Vault starts searching for items that need to be added to the Vault Cache.

Supported values ■ An integer value. The default is 3 (minutes).

Legacy name OVPauseInterval

Per item sleep (Exchange Vault Cache setting)

Description The delay, in milliseconds, that will be used between items when updating the Vault Cache.

Supported values ■ Integer. The number of milliseconds to use between items when updating the Vault Cache Default is 100 (milliseconds).

Legacy name OVPerItemSleep

Preemptive archiving in advance (Exchange Vault Cache setting)

Description	<p>The Outlook Add-In copies items from the user's Outlook .OST file to the Vault Cache before the items are due to be archived. The process is known as preemptive caching. Preemptive caching takes place on the user's computer. It reduces the number of items that need to be downloaded from the mailbox archive to the Vault Cache when the two are synchronized.</p> <p>Preemptive caching obeys the settings in the Exchange mailbox policy's archiving rules.</p> <p>The Outlook Add-In uses the Preemptive archiving in advance value when it determines the age of items on which to perform preemptive caching. To determine the age, it deducts the Preemptive archiving in advance value from the Archive items when they are older than value in the Exchange mailbox policy's archiving rules.</p> <p>For example, you do not change Preemptive archiving in advance from its default value. You set the Archive items when they are older than mailbox policy setting to six weeks. The Outlook Add-In deducts the Preemptive archiving in advance default value of seven days from six weeks, and preemptively caches the items that are five weeks old or older.</p> <p>Note that if you use an archiving strategy that includes quotas, it is difficult to predict the age at which items are archived. It is then usually advantageous to preemptively cache items as soon as possible. Enterprise Vault therefore uses 0 days as the age at which to perform preemptive caching if both of the following are true:</p> <ul style="list-style-type: none">■ The mailbox policy uses an archiving strategy that is based on quota or age and quota.■ You do not change the Preemptive archiving in advance setting from its default value.
Supported values	<ul style="list-style-type: none">■ An integer, specifying a number of days. The default is 7.
Legacy name	OVPreemptAdvance

Root folder (Exchange Vault Cache setting)

Description	<p>The location in which to place Vault Caches. This value is used when a user enables Vault Cache. Changing this value has no effect on existing Vault Caches.</p>
-------------	---

Supported values	<ul style="list-style-type: none">■ Path. A path to a folder that Enterprise Vault can create on the user's local computer. If you do not specify Root Folder, Enterprise Vault uses an Enterprise Vault subfolder in the user's Application Data folder.
Legacy name	OVRootDirectory

Root folder search path (Exchange Vault Cache setting)

Description	<p>Enables you to supply a list of possible locations for the Vault Cache. The first such location that is valid on a user's computer is the one that will be used at the time the Vault Cache is created. This enables you to specify a list that is likely to be suitable for computers with different configurations.</p> <p>For example, if you specify <code>E:\vault;C:\vault</code> then the Vault Cache would be created in <code>E:\vault</code> if that was valid on the user's computer and, if it was not valid, then in <code>C:\vault</code>.</p> <p>If none of the locations is valid, the one specified by Root folder is used, if possible.</p> <p>See "Root folder (Exchange Vault Cache setting)" on page 216.</p>
Supported values	<ul style="list-style-type: none">■ A text string. A semicolon-separated list of possible locations for the Vault Cache.
Legacy name	OVRootDirectorySearchPath

Show Setup Wizard (Exchange Vault Cache setting)

Description	<p>Controls whether the client shows the Vault Cache setup wizard.</p> <p>The setup wizard does the following:</p> <ul style="list-style-type: none">■ Summarizes what Vault Cache does and what is about to happen.■ Asks whether the user wants to start a download automatically after the initial scan has finished. The default is to start the download. <p>If the wizard is turned off, Vault Cache waits for the amount of time that is specified in Pause interval and then automatically begins looking for items to download.</p> <p>See "Pause interval (Exchange Vault Cache setting)" on page 215.</p>
Supported values	<ul style="list-style-type: none">■ 0. Do not show the setup wizard.■ 1 (default). Show the setup wizard.
Legacy name	OVSetupWizard

Synchronize archive types (Exchange Vault Cache setting)

Description	Controls what is synchronized by Vault Cache.
Supported values	<ul style="list-style-type: none">■ Default mailbox. Synchronize the primary mailbox only.■ All mailbox archives. Synchronize the primary mailbox archive, and any delegate mailbox archives to which the user has access.■ All mailbox and shared archives. Synchronize the primary mailbox archive, and any delegate or shared mailbox archives to which the user has access.
Legacy name	OVSynArchiveTypes

WDS search auto-enable (Exchange Vault Cache setting)

Description	Controls whether the Vault Cache search plug-in for Windows Desktop Search is automatically enabled for users. This plug-in, which is installed with the Outlook Add-In, enables users to search their Vault Cache using Windows Desktop Search.
Supported values	<ul style="list-style-type: none">■ Force off. Disable this feature.■ Force on. Enable this feature.■ Keep user's setting. Retain the user's setting for this feature.
Legacy name	OVWDSAutoEnable

Virtual Vault (Exchange desktop policy advanced settings)

The Virtual Vault settings let you control the behavior of Virtual Vault.

The Virtual Vault settings are:

- [Max archive requests per synchronization \(Exchange Virtual Vault setting\)](#)
- [Max attempts to archive an item \(Exchange Virtual Vault setting\)](#)
- [Max data archived per synchronization \(Exchange Virtual Vault setting\)](#)
- [Max delete requests per synchronization \(Exchange Virtual Vault setting\)](#)
- [Max item size to archive \(Exchange Virtual Vault setting\)](#)
- [Max item updates per synchronization \(Exchange Virtual Vault setting\)](#)
- [Max total size of contentless operations \(Exchange Virtual Vault setting\)](#)
- [Max total size of items to archive \(Exchange Virtual Vault setting\)](#)
- [Show content in Reading Pane \(Exchange Virtual Vault setting\)](#)

- [Threshold number of items to trigger synchronization \(Exchange Virtual Vault setting\)](#)
- [Threshold total size of items to trigger synchronization \(Exchange Virtual Vault setting\)](#)
- [Users can archive items \(Exchange Virtual Vault setting\)](#)
- [Users can copy items to another store \(Exchange Virtual Vault setting\)](#)
- [Users can copy items within their archive \(Exchange Virtual Vault setting\)](#)
- [Users can hard delete items \(Exchange Virtual Vault setting\)](#)
- [Users can reorganize items \(Exchange Virtual Vault setting\)](#)

Max archive requests per synchronization (Exchange Virtual Vault setting)

Description	<p>Controls the maximum number of archive requests during a Vault Cache synchronization. Any remaining requests are made at the next synchronization.</p> <p>When a user stores unarchived items in Virtual Vault, the archive operation does not take place until after the next Vault Cache header synchronization.</p> <p>No limit or a high value can increase the time that is required to complete a Vault Cache synchronization. This effect is a consideration if the additional load affects the Enterprise Vault server.</p> <p>Also, until the items that a user has stored in Virtual Vault are archived in the online archive, moved and copied items exist only on the user's computer. You can set two thresholds that trigger automatic Vault Cache synchronization based on the number or total size of pending archive items in Virtual Vault.</p> <p>See "Threshold number of items to trigger synchronization (Exchange Virtual Vault setting)" on page 224.</p> <p>See "Threshold total size of items to trigger synchronization (Exchange Virtual Vault setting)" on page 225.</p>
Supported values	<ul style="list-style-type: none"> ■ An integer value. The default is 0 (no limit).
Legacy name	OVMaXItemArchivesPerSync

Max attempts to archive an item (Exchange Virtual Vault setting)

Description	<p>Specifies how many times Enterprise Vault tries to archive an item.</p> <p>The archive operation is tried this number of times before the item is listed in the Virtual Vault Search folder named Could Not Archive.</p>
Supported values	<ul style="list-style-type: none">■ An integer value. The default is 3.
Legacy name	OVItemArchiveAttempts

Max data archived per synchronization (Exchange Virtual Vault setting)

Description	<p>Controls the maximum amount of data in megabytes that can be uploaded during a Vault Cache synchronization. Any remaining data is uploaded at the next synchronization.</p> <p>No limit or a high value can increase the time that is required to complete a Vault Cache synchronization. This effect is a consideration if the additional load affects the Enterprise Vault server.</p> <p>Also, until the items that the user stores in Virtual Vault have been archived in the online archive, moved and copied items exist only on the user's computer. You can set two thresholds that trigger automatic Vault Cache synchronization based on the number or total size of pending archive items in Virtual Vault.</p> <p>See “Threshold number of items to trigger synchronization (Exchange Virtual Vault setting)” on page 224.</p> <p>See “Threshold total size of items to trigger synchronization (Exchange Virtual Vault setting)” on page 225.</p> <p>The value of this setting must be greater than or equal to the value of Max item size to archive. If not, the value of Max item size to archive is used.</p>
Supported values	<ul style="list-style-type: none">■ An integer value. The default is 512 (MB). The value 0 specifies no limit.
Legacy name	OVMaxToArchivePerSyncMB

Max delete requests per synchronization (Exchange Virtual Vault setting)

Description	<p>Controls the maximum number of delete requests during a Vault Cache synchronization. Any remaining requests are made at the next synchronization.</p> <p>Deletion requests use relatively few resources on the Enterprise Vault server.</p>
Supported values	<ul style="list-style-type: none">■ An integer value. The default is 0 (no limit).
Legacy name	OVMMaxItemDeletesPerSync

Max item size to archive (Exchange Virtual Vault setting)

Description	<p>Controls the maximum size in megabytes of an item that can be moved or copied into Virtual Vault.</p> <p>If this value is similar to the value of Max total size of items to archive, a full synchronization can consist of one item.</p> <p>The Max item size to archive value may be used automatically for Max data archived per synchronization or Max total size of items to archive. It is used if the value of those settings is less than the Max item size to archive value.</p> <p>You can set two thresholds that trigger automatic Vault Cache synchronization based on the number or total size of pending archive items in Virtual Vault.</p> <p>See “Threshold number of items to trigger synchronization (Exchange Virtual Vault setting)” on page 224.</p> <p>See “Threshold total size of items to trigger synchronization (Exchange Virtual Vault setting)” on page 225.</p>
Supported values	<ul style="list-style-type: none">■ An integer value. The default is 256 (MB). The value 0 specifies no limit.
Legacy name	OVMMaxMessageSizeToArchiveMB

Max item updates per synchronization (Exchange Virtual Vault setting)

Description	<p>Controls the maximum number of property change requests during a Vault Cache synchronization. Any remaining requests are made at the next synchronization.</p> <p>Update requests use relatively few resources on the Enterprise Vault server.</p>
Supported values	<ul style="list-style-type: none">■ An integer value. The default is 0 (no limit).
Legacy name	OVMMaxItemUpdatesPerSync

Max total size of contentless operations (Exchange Virtual Vault setting)

Description	<p>Controls the maximum total size in megabytes of copy and move operations when items have no content in Vault Cache. This setting does not apply to documents that are placed directly in the mailbox. It only applies to standard Outlook mail types, for example, mail items, calendar items, tasks, and contacts.</p> <p>This setting only applies when two or more items with no content are involved in the operation. Retrieval of one item is allowed regardless of its size.</p>
Supported values	<ul style="list-style-type: none">■ An integer value. The default is 64 (MB). The value 0 specifies no limit.
Legacy name	VVDenyMultiContentlessOpsAboveMB

Max total size of items to archive (Exchange Virtual Vault setting)

Description	<p>Controls the maximum total size in megabytes of pending archive data in Vault Cache.</p> <p>Pending archive data consists of items that the user has moved or copied into Virtual Vault. These items are pending archive until Vault Cache synchronization has successfully uploaded and archived them.</p> <p>The value of this setting must be greater than or equal to the value of Max item size to archive. If not, the value of Max item size to archive is used.</p> <p>You can set two thresholds that trigger automatic Vault Cache synchronization based on the number or total size of pending archive items in Virtual Vault.</p> <p>See “Threshold number of items to trigger synchronization (Exchange Virtual Vault setting)” on page 224.</p> <p>See “Threshold total size of items to trigger synchronization (Exchange Virtual Vault setting)” on page 225.</p>
Supported values	<ul style="list-style-type: none">■ An integer value. The default is 512 (MB). The value 0 specifies no limit.
Legacy name	OVMaxTotalToArchiveMB

Show content in Reading Pane (Exchange Virtual Vault setting)

Description	<p>Controls whether the content of an item that is selected in Virtual Vault is shown in the Outlook Reading Pane.</p> <p>If the item itself is a document, it is not displayed in the Reading Pane. A message in the Reading Pane advises the user to open the item to read the item's contents.</p>
-------------	---

Supported values	<ul style="list-style-type: none">■ Never show content. The Reading Pane always shows only the selected item's header. A banner provides a link to open the original item.■ When in Vault Cache (default). The Reading Pane shows the selected item's header. If the item is in Vault Cache, it also shows the content. If the content is not shown, a banner provides a link to open the original item. When the Vault Cache content strategy is Store only items that user opens, the effect of this value is that the Reading Pane only shows the content of previously opened items.■ Always show content. The Reading Pane always shows the header and content of the item that is selected in Virtual Vault. <p>Show content in Reading Pane can only have the value Always show content if the following conditions apply:</p> <ul style="list-style-type: none">■ You have upgraded from an earlier release.■ In the earlier release, Show content in Reading Pane had the value Always show content. <p>Always show content is not available in the Modify Setting dialog box. So if Always show content is the current value and you change it, you cannot go back to it.</p>
Legacy name	VVReadingPaneContent

Threshold number of items to trigger synchronization (Exchange Virtual Vault setting)

Description	<p>Specifies the total number of pending archive items in Virtual Vault that triggers automatic Vault Cache synchronization.</p> <p>Pending archive data consists of items that the user has moved or copied into Virtual Vault. These items are pending archive until Vault Cache synchronization has successfully uploaded and archived them.</p> <p>If you enable this setting, consider how it interacts with other settings, as follows:</p> <ul style="list-style-type: none">■ Max item size to archive and Max total size of items to archive can prevent the user from adding items to Virtual Vault, so that the threshold is never reached.■ Max archive requests per synchronization may have a value that is lower than the value of Threshold number of items to trigger synchronization. In this case, automatic synchronization may occur but not all the pending archive items are archived.
-------------	--

- Supported values
- 0 (default). The threshold is inactive.
 - Non-zero integer. The total number of pending archive items in Virtual Vault that triggers automatic Vault Cache synchronization.

Legacy name VVAutoSyncltemThreshold

Threshold total size of items to trigger synchronization (Exchange Virtual Vault setting)

Description Specifies the total size in megabytes of pending archive items in Virtual Vault that triggers automatic Vault Cache synchronization.

Pending archive data consists of items that the user has moved or copied into Virtual Vault. These items are pending archive until Vault Cache synchronization has successfully uploaded and archived them.

If you enable this setting, consider how it interacts with other settings, as follows:

- **Max item size to archive** and **Max total size of items to archive** can prevent the user from adding items to Virtual Vault, so that the threshold is never reached.
- **Max data archived per synchronization** may have a value that is lower than the value of **Threshold total size of items to trigger synchronization**. In this case, automatic synchronization may occur but not all the pending archive items are archived.

- Supported values
- 0 (default). The threshold is inactive.
 - Non-zero integer. The total size in megabytes of pending archive items in Virtual Vault that triggers automatic Vault Cache synchronization.

Legacy name VVAutoSyncltemsSizeThresholdMB

Users can archive items (Exchange Virtual Vault setting)

Description	<p>Controls whether users can archive items manually by adding new items to Virtual Vault using standard Outlook actions. Examples of these standard Outlook actions are drag and drop, move and copy, and Rules.</p> <p>If you disable this setting, users can still create folders if Users can reorganize items is enabled.</p> <p>If you enable this setting, consider setting the thresholds that trigger automatic Vault Cache synchronization.</p> <p>See “Threshold number of items to trigger synchronization (Exchange Virtual Vault setting)” on page 224.</p> <p>See “Threshold total size of items to trigger synchronization (Exchange Virtual Vault setting)” on page 225.</p> <p>Note: By default there are no safety copies for those items that users archive from Virtual Vault. If you require safety copies you can configure the vault stores that host the users' archives so that Enterprise Vault keeps safety copies in the Storage queue. This configuration change affects all archiving to those vault stores.</p>
Supported values	<ul style="list-style-type: none">■ Yes (default). Users can archive items manually in Virtual Vault.■ No. Users cannot archive items manually in Virtual Vault.
Legacy name	VVAllowArchive

Users can copy items to another store (Exchange Virtual Vault setting)

Description	<p>Controls whether users can copy and move items from a Virtual Vault to another message store.</p> <p>If users can copy or move items out of Virtual Vault and the content is available in Vault Cache, the items are retrieved from Vault Cache.</p> <p>If the Vault Cache content strategy is Do not store any items in cache, the items are retrieved from the online archive. In this case, use the Virtual Vault advanced setting Max total size of contentless operations to control the maximum total size of view, copy, and move operations.</p>
Supported values	<ul style="list-style-type: none">■ Yes (default). Users can copy and move items to another message store.■ No. Users cannot copy and move items to another message store.
Legacy name	VVAllowInterStoreCopyAndMove

Users can copy items within their archive (Exchange Virtual Vault setting)

Description	<p>Controls whether users can copy items within their archive.</p> <p>If users can copy items within their archive and the content is available in Vault Cache, the items are retrieved from Vault Cache.</p> <p>If the Vault Cache content strategy is Do not store any items in cache, the items are retrieved from the online archive. In this case, use the Virtual Vault advanced setting Max total size of contentless operations to control the maximum total size of view, copy, and move operations.</p> <p>If you enable this setting, consider setting the thresholds that trigger automatic Vault Cache synchronization.</p> <p>See “Threshold number of items to trigger synchronization (Exchange Virtual Vault setting)” on page 224.</p> <p>See “Threshold total size of items to trigger synchronization (Exchange Virtual Vault setting)” on page 225.</p>
Supported values	<ul style="list-style-type: none">■ Yes. Users can copy items within their archive.■ No (default). Users cannot copy items within their archive.
Legacy name	VVAllowIntraStoreCopy

Users can hard delete items (Exchange Virtual Vault setting)

Description	<p>Controls whether users can hard delete items from Virtual Vault.</p> <p>For this setting to take effect, the option Users can delete items from their archives must be enabled on the Archive Settings tab in the Site Properties dialog box.</p> <p>If you disable this setting, users can still move items to the Deleted Items folder if Users can reorganize items is enabled.</p>
Supported values	<ul style="list-style-type: none">■ Yes (default). Users can hard delete items from Virtual Vault.■ No. Users cannot hard delete items from Virtual Vault.
Legacy name	VVAllowHardDelete

Users can reorganize items (Exchange Virtual Vault setting)

Description	<p>Controls whether users can reorganize items in Virtual Vault.</p> <p>This setting can enable users to move items between folders and to create, move, rename, or delete folders.</p> <p>If folders still exist in the mailbox, users cannot move, rename, or delete them.</p> <p>Users can hard delete only empty folders, unless Users can hard delete items is enabled.</p>
Supported values	<ul style="list-style-type: none">■ Yes (default). Users can reorganize items in Virtual Vault.■ No. Users cannot reorganize items in Virtual Vault.
Legacy name	VVAllowReOrg

Advanced Exchange journal policy settings

This chapter includes the following topics:

- [Editing the advanced Exchange journal policy settings](#)
- [Archiving General \(Exchange journal policy advanced settings\)](#)

Editing the advanced Exchange journal policy settings

The settings are available in the properties of Exchange journal policies. For details of the various settings, see the individual sections.

To edit the settings for a policy

- 1 In the left pane of the Administration Console, expand the hierarchy until **Policies** is visible.
- 2 Expand **Policies**.
- 3 Expand **Exchange**.
- 4 Click **Journaling**.
- 5 In the right-hand pane, double-click the name of the policy you want to edit.
The policy's properties are displayed.
- 6 Click the **Advanced** tab.

- 7 Next to **List settings from**, select the category of settings that you want to modify.
- 8 Edit the settings as required.
You can double-click a setting to edit it, or click it once to select it and then click **Modify**.

Archiving General (Exchange journal policy advanced settings)

The Archiving General settings enable you to control archiving behavior.

The Archiving General settings are:

- [ClearText copies of RMS Protected items \(Exchange Archiving General setting\)](#)
- [Expand distribution lists \(Exchange Archiving General setting\)](#)
- [Failed DL expansion behavior \(Exchange Archiving General setting\)](#)
- [Inherited permissions \(Exchange Archiving General setting\)](#)
- [Journal delay \(Exchange Archiving General setting\)](#)
- [Maximum message size to archive in MB \(Exchange Archiving General setting\)](#)
- [Pending shortcut timeout \(Exchange Archiving General setting\)](#)
- [Queue Journal items \(Exchange Archiving General setting\)](#)
- [Reset archive names \(Exchange Archiving General setting\)](#)
- [Return failed items to inbox \(Exchange Archiving General setting\)](#)

ClearText copies of RMS Protected items (Exchange Archiving General setting)

Description

If journal report decryption is configured on Exchange, then two messages are attached to the journal report: the original RMS-protected message and a clear text version. This policy setting controls whether Enterprise Vault uses the clear text message or the RMS-protected message as the primary message during archiving.

Enterprise Vault stores both versions of the message and the journal report in the message saveset. However, Enterprise Vault does not currently support the retrieval of the secondary message or the journal report from the archive.

Supported values	<ul style="list-style-type: none"> ■ Treat as Primary (default) <ul style="list-style-type: none"> ■ The clear text message is returned in response to retrieval requests from Enterprise Vault clients and Veritas Discovery Accelerator. As Exchange Server does not decrypt any attachments that have been individually protected, Enterprise Vault cannot preview these attachments. ■ Enterprise Vault indexes the content and properties of the clear text message, and any attachments that are not encrypted. With this option, single instance sharing between Exchange mailbox and journal archiving is not possible. ■ Custom filters that process RMS-protected messages must explicitly retrieve the RMS-protected message from the attachments to the journal report message (P1 message). ■ Treat as Secondary <ul style="list-style-type: none"> ■ The RMS-protected message is returned in response to retrieval requests from Enterprise Vault clients and Veritas Discovery Accelerator. Enterprise Vault cannot preview these messages unless an application is used to decrypt them. ■ Information available for indexing is restricted to Subject, Recipients, and other message metadata. The item can be shared between Exchange mailbox and journal archiving. The message content and attachments are not indexed unless an application is used to decrypt them. ■ Custom filters that do not decrypt RMS-protected messages cannot read the message content.
Legacy name	ClearTextPrimary

Expand distribution lists (Exchange Archiving General setting)

Description	Controls whether the Exchange Journaling Task expands distribution lists.
Supported values	<ul style="list-style-type: none"> ■ Off. Do not expand distribution lists. ■ On (default). Expand distribution lists.
Legacy name	ExpandDistributionLists

Failed DL expansion behavior (Exchange Archiving General setting)

Description	Controls the behavior when an Exchange Journaling Task fails to expand a distribution list.
Supported values	<ul style="list-style-type: none"> ■ Move to 'Failed DL Expansion' folder. Move the item without archiving it. ■ Archive item (default). Archive the item.
Legacy name	FailedDLExpansion

Inherited permissions (Exchange Archiving General setting)

Description	Controls whether Enterprise Vault includes inherited permissions when synchronizing permissions between mailboxes and archives.
Supported values	<ul style="list-style-type: none"> ■ Off (default). Do not synchronize inherited permissions. ■ On. Synchronize inherited permissions.
Legacy name	IncludedInheritedRights

Journal delay (Exchange Archiving General setting)

Description	<p>During journal archiving, Enterprise Vault groups journal reports that have the same message ID.</p> <p>To allow time for all the messages in a group to be received, journal archiving waits for a period of time after the receipt of the last message with a given ID before it archives the group. Journal delay sets the length of the delay in minutes.</p> <p>In normal circumstances, the default delay of five minutes allows sufficient time for the last message of a related group to arrive in the journal mailbox.</p>
Supported values	<ul style="list-style-type: none"> ■ Integer. An integer value that specifies the journal delay in minutes. Set Journal delay to 0 to disable journal grouping for this policy. Default is 5.
Legacy name	JournalDelay

Maximum message size to archive in MB (Exchange Archiving General setting)

Description	Controls the maximum message size to archive.
Supported values	<ul style="list-style-type: none"> Integer. An integer value specifying the maximum size of messages that can be archived, in megabytes. Default is 250.
Legacy name	MaxMessageSizeToArchiveMB

Pending shortcut timeout (Exchange Archiving General setting)

Description	Specifies the number of days to allow items to remain in an archive-pending state before being reset.
Supported values	<ul style="list-style-type: none"> Off (default). Archive-pending shortcuts are never reset. 0. When run in report mode, Exchange Mailbox tasks reset all archive-pending shortcuts. When run in normal mode, archive-pending shortcuts are not reset. Any integer larger than zero. Archive-pending shortcuts that are older than this number of days are reset. This happens in both normal archiving and in Report Mode.
Legacy name	PendingShortcutTimeout

Queue Journal items (Exchange Archiving General setting)

Description	Controls the Exchange Journaling Tasks' use of MSMQ, thus improving performance.
Supported values	<ul style="list-style-type: none"> All single threaded. Use if all your tasks are single threaded. Multiple threads (default). Improves performance if any Journaling Task uses multiple threads.
Legacy name	QueueJournalItems

Reset archive names (Exchange Archiving General setting)

Description	Controls whether, during synchronization, archive names are automatically changed to match mailbox names.
-------------	---

- Supported values
- Off. During synchronization archive names are never changed.
 - On (default). During synchronization, archive names are automatically changed if necessary to match mailbox names.

Legacy name ResetArchiveNames

Return failed items to inbox (Exchange Archiving General setting)

Description Controls whether, when the Journaling task starts, messages that are stored in the failed folders are automatically moved back into the Inbox to be reprocessed.

- Supported values
- Off (default). Do not move items in the failed folders to the Inbox when the task starts.
 - On. Move items the failed folders to the Inbox when the task starts.

Legacy name MoveFailedItemsToInbox

Advanced Exchange public folder policy settings

This chapter includes the following topics:

- [Editing advanced Exchange public folder settings](#)
- [Archiving General \(Exchange public folder policy advanced settings\)](#)

Editing advanced Exchange public folder settings

The settings are available in the properties of Exchange public folder policies. For details of the various settings, see the individual sections.

To edit the settings for a policy

- 1 In the left pane of the Administration Console, expand the hierarchy until **Policies** is visible.
- 2 Expand **Policies**.
- 3 Expand **Exchange**.
- 4 Click **Public Folder**.
- 5 In the right-hand pane, double-click the name of the policy you want to edit.
The policy's properties are displayed.
- 6 Click the **Advanced** tab.
- 7 Next to **List settings from**, select the category of settings that you want to modify.
- 8 Edit the settings as required.

You can double-click a setting to edit it, or click it once to select it and then click **Modify**.

Archiving General (Exchange public folder policy advanced settings)

The Archiving General settings enable you to control archiving behavior.

The Archiving General settings are:

- [Archive unexpired Calendar Events \(Exchange Archiving General setting\)](#)
- [Code pages for right-to-left custom shortcuts \(Exchange Archiving General setting\)](#)
- [Do not archive pending reminders \(Exchange Archiving General setting\)](#)
- [Inherited permissions \(Exchange Archiving General setting\)](#)
- [Maximum message size to archive in MB \(Exchange Archiving General setting\)](#)
- [Pending shortcut timeout \(Exchange Archiving General setting\)](#)
- [Set failed messages 'Do Not Archive' \(Exchange Archiving General setting\)](#)
- [Strip attachments to non-shortcut items \(Exchange Archiving General setting\)](#)

Archive unexpired Calendar Events (Exchange Archiving General setting)

Description	Controls whether unexpired calendar items are archived.
Supported values	<ul style="list-style-type: none"> ■ Off (default). Unexpired calendar items are not archived. ■ On. Unexpired calendar items are archived.
Legacy name	ArchiveNonExpiredCalEvents

Code pages for right-to-left custom shortcuts (Exchange Archiving General setting)

Description	A semicolon-separated list of code pages. Custom shortcuts that use these code pages are always formatted right-to-left.
Supported values	<ul style="list-style-type: none"> ■ A list of code pages, separated by semicolons. For example, 1255;1256. Default is 1255.
Legacy name	CustomShortcutRTLCodePages

Do not archive pending reminders (Exchange Archiving General setting)

Description	Controls whether Enterprise Vault archives items that have pending reminders.
Supported values	<ul style="list-style-type: none"> ■ Off. Items that have pending reminders are archived. ■ On (default). Items that have pending reminders within the next five years are not archived.
Legacy name	DontArchiveItemsPendingReminder

Inherited permissions (Exchange Archiving General setting)

Description	Controls whether Enterprise Vault includes inherited permissions when synchronizing permissions between public folders and archives.
Supported values	<ul style="list-style-type: none"> ■ Off (default). Do not synchronize inherited permissions. ■ On. Synchronize inherited permissions.
Legacy name	IncludeInheritedRights

Maximum message size to archive in MB (Exchange Archiving General setting)

Description	Controls the maximum size of messages that are archived.
Supported values	<ul style="list-style-type: none"> ■ 0. No restriction on maximum message size. ■ Integer larger than 0. The maximum size of messages that are archived, in megabytes. Default is 250.
Legacy name	MaxMessageSizeToArchiveMB

Pending shortcut timeout (Exchange Archiving General setting)

Description	Specifies the number of days to allow items to remain in the state of archive-pending, restore-pending, or delete-pending before they are reset.
-------------	--

Supported values	<ul style="list-style-type: none"> ■ Off (default). Archive-pending, restore-pending, and delete-pending shortcuts are never reset. ■ 0. When run in report mode, the archiving tasks reset all archive-pending, restore-pending, and delete-pending shortcuts. When run in normal mode, the shortcuts are not reset. ■ Any integer larger than zero. Archive-pending, restore-pending, and delete-pending shortcuts that are older than this number of days are reset. This happens in both normal archiving and in report mode.
Legacy name	PendingShortcutTimeout

Set failed messages 'Do Not Archive' (Exchange Archiving General setting)

Description	<p>If an item cannot be archived, the default archiving task behavior is to reprocess the item on the next archiving run because such items can often be successfully archived on a second try.</p> <p>This setting enables you to change the behavior so items that fail archiving are marked as Do Not Archive and thus are not reprocessed on the next archiving run.</p>
Supported values	<ul style="list-style-type: none"> ■ Off (default). Failed items are not marked as Do Not Archive. ■ On. Failed items are marked as Do Not Archive.
Legacy name	SetFailedMsgsDoNotArchive

Strip attachments to non-shortcut items (Exchange Archiving General setting)

Description	<p>Controls whether attachments are removed from calendar items, meeting items (including requests, responses and cancellations), task and task request items, and contacts after archiving. These items are not changed into Enterprise Vault shortcuts when they are archived. If Enterprise Vault removes an attachment, it replaces it with a link to the attachment.</p>
Supported values	<ul style="list-style-type: none"> ■ On (default). Attachments are removed from non-shortcut items after archiving. ■ Off. Attachments are not removed from non-shortcut items after archiving.
Legacy name	StripAttachmentsToNonShortcutItems

Advanced SMTP policy settings

This chapter includes the following topics:

- [Editing advanced SMTP policy settings](#)
- [Journal Reports settings](#)

Editing advanced SMTP policy settings

The settings are available in the properties of SMTP Archiving policies. For details of the various settings, see the individual sections.

To edit the settings for a policy

- 1 In the left pane of the Administration Console, expand the hierarchy until **Policies** is visible.
- 2 Expand **Policies**.
- 3 Click **SMTP**.
- 4 In the right-hand pane, double-click the name of the policy you want to edit.
The policy's properties are displayed.
- 5 Click the **Advanced** tab.
- 6 Edit the settings as required.

You can double-click a setting to edit it, or click it once to select it and then click **Modify**.

Journal Reports settings

The Journal Reports settings enable you to control the processing behavior for journal reports.

The Journal Reports settings are as follows:

- [ClearText copies of RMS Protected items \(Advanced SMTP policy setting\)](#)
- [Journal report processing \(Advanced SMTP policy setting\)](#)

ClearText copies of RMS Protected items (Advanced SMTP policy setting)

Description	<p>If journal report decryption is configured on Exchange, then two messages are attached to the journal report: the original RMS-protected message and a clear text version. This policy setting controls whether Enterprise Vault uses the clear text message or the RMS-protected message as the primary message during archiving.</p> <p>Enterprise Vault stores both versions of the message and the journal report in the message saveset. However, Enterprise Vault does not currently support the retrieval of the secondary message or the journal report from the archive, except by using the Content Management API.</p>
Supported values	<ul style="list-style-type: none">■ Treat as Primary (default)<ul style="list-style-type: none">■ The clear text message is returned in response to retrieval requests from Enterprise Vault clients and Veritas Discovery Accelerator.■ Enterprise Vault indexes the content and properties of the clear text message, and any attachments that are not encrypted.■ Treat as Secondary<ul style="list-style-type: none">■ The RMS-protected message is returned in response to retrieval requests from Enterprise Vault clients and Veritas Discovery Accelerator. Enterprise Vault cannot preview these messages unless an application is used to decrypt them.■ Information available for indexing is restricted to Subject, Recipients, and other message metadata. The message content and attachments are not indexed.
Legacy name	ClearTextPrimary

Journal report processing (Advanced SMTP policy setting)

Description	Controls whether journal reports are processed and stored with the message.
Supported values	<ul style="list-style-type: none">■ Process journal reports (default). Journal reports are processed and archived in addition to the original messages. Select this option for journal archives.■ Discard journal reports. Journal reports are discarded and only the original messages are processed and archived. Select this option for archives that users can access.

Site properties advanced settings

This chapter includes the following topics:

- [About site properties advanced settings](#)
- [Editing site properties advanced settings](#)
- [Site properties advanced settings](#)

About site properties advanced settings

Site properties advanced settings control advanced aspects of Enterprise Vault's behavior for the whole Enterprise Vault site.

The advanced settings that apply to a single Enterprise Vault server are available in the computer properties.

See [“About computer properties advanced settings”](#) on page 263.

Editing site properties advanced settings

The advanced settings for the Enterprise Vault site are provided on the **Advanced** tab of the site properties.

To edit the site properties advanced settings

- 1 In the left pane of the Administration Console, expand the hierarchy until the name of the site is visible.
- 2 Right-click the name of the site. Then click **Properties**. The site properties are displayed.

- 3 Click the **Advanced** tab.
- 4 Edit the settings as required.

How to apply new settings for site properties

To apply the changes that you have made, you must restart the IMAP server, or the Indexing service or Storage service, depending on which settings you have changed.

Site properties advanced settings

Site properties advanced settings control advanced aspects of Enterprise Vault's behavior for the whole Enterprise Vault site.

You can change advanced settings in the following categories:

- [Content Conversion \(site properties advanced settings\)](#)
- [IMAP \(site properties advanced settings\)](#)
- [Indexing \(site properties advanced settings\)](#)
- [SQL Server \(site properties advanced settings\)](#)
- [SMTP \(site properties advanced settings\)](#)
- [Storage \(site properties advanced settings\)](#)

Content Conversion (site properties advanced settings)

Before Enterprise Vault can index the content of an item, the content needs to be converted to HTML or text. The Content Conversion settings let you control how different file types are converted, and the conversion events that are reported in the Enterprise Vault Converters event log.

Content Conversion settings apply to files, attachments, files in archive and container files such as zip, tar, and pst files, and message bodies (specifically RTF format message bodies).

To apply Content Conversion setting changes, restart all Enterprise Vault Storage Services in the site.

The Content Conversion settings are:

- [File types excluded from conversion \(site properties Content Conversion setting\)](#)
- [File types converted to text \(site properties Content Conversion setting\)](#)
- [File types for Postscript conversion \(site properties Content Conversion setting\)](#)

- [File types for OCR conversion \(site properties Content Conversion setting\)](#)
- [File types for IFilter conversion \(site properties Content Conversion setting\)](#)
- [Conversion timeout \(site properties Content Conversion setting\)](#)
- [Conversion timeout for archive file types \(site properties Content Conversion setting\)](#)
- [Include hidden text \(site properties Content Conversion setting\)](#)
- [Include hidden spreadsheet data \(site properties Content Conversion setting\)](#)
- [Show spreadsheet border \(site properties Content Conversion setting\)](#)
- [Show metadata properties \(site properties Content Conversion setting\)](#)
- [Maximum conversion size \(site properties Content Conversion setting\)](#)
- [OCR language \(site properties Content Conversion setting\)](#)
- [OCR optimization \(site properties Content Conversion setting\)](#)
- [Log conversion failure events \(site properties Content Conversion setting\)](#)
- [Log fallback to text events \(site properties Content Conversion setting\)](#)
- [Log conversion timeout events \(site properties Content Conversion setting\)](#)
- [Log file type not recognized events \(site properties Content Conversion setting\)](#)
- [Log maximum conversion size exceeded events \(site properties Content Conversion setting\)](#)

File types excluded from conversion (site properties Content Conversion setting)

Description The list of file types that are not converted to HTML or text.

Note that Enterprise Vault can neither display a preview of items of the listed file types, nor index the content of such items.

Supported values You can modify the list of file types to exclude from conversion. Add file types in the format:

.filetype[filetype]

If you specify the wildcard value "*", or include it in the list, all content conversion is effectively disabled. In this situation, no content is indexed for items that are archived, and all other conversion settings are redundant.

By default, the following file types are not converted:

```
.ABS .AIF .AIFC .AIFF .ASC .ASF .ASX .AU .AVI .BIN
.BMP .BP .C2D .CBT .CCD .CD .CDI .CHM .CIF .CUR
.DAO .DVS .DWI .ENC .ENT .EVT .FCD .FDM .FP .GCD
.GI .GTS .HLP .ICO .IMG .ISO .JFI .JFIF .JIF .JPE
.JTF .JP2 .JPX .JPF .MJ2 .M1V .M2V .M3U .MDF .MDS
.MID .MKV .MMM .MOD .MODV .MOO .MOOV .MOV .MP2
.MP3 .MP4 .MPA .MPE .MPEG .MPEGA .MPEGV .MPG .MPM
.MPP .MPV .MSO .NRG .OLE .PAB .PDI .PF .PGP .PJPEG
.PLS .POI .PUB .PXI .QT .QTM .QTW .RA .RAM .RAW .RM
.RMI .RMJ .RMX .RP .RV .SND .SNP .SWA .SWF .TAO
.VDO .VIV .VSF .WAV .WMA .WMV .Z01 .Z02 .Z03 .Z04
.Z05 .Z06 .Z07 .Z08 .Z09 .Z10
```

- Legacy registry settings**
- Enterprise Vault\ExcludedFileTypesFromConversion
 - Enterprise Vault\BypassConversions

File types converted to text (site properties Content Conversion setting)

Description The list of file types to convert to text instead of HTML.

Note that this setting does not override the setting, **File types excluded from conversion**. For example, if the file type .xyz is included in both setting values, then instances of the file type xyz are not converted.

Supported values You can list file types in the format:

.filetype[filetype]

Specify the wildcard value "*" to convert all file types to text.

- Legacy registry settings**
- Enterprise Vault\TextConversionFileTypes
 - Enterprise Vault\ConvertWordToText
 - Enterprise Vault\ConvertExcelToText
 - Enterprise Vault\ConvertRTFCoverToText

File types for Postscript conversion (site properties Content Conversion setting)

Description	<p>The list of file types to convert using Enterprise Vault Postscript conversion.</p> <p>Note that this setting does not override the setting, File types excluded from conversion. For example, if the file type .xyz is included in both setting values, then instances of the file type xyz are not converted.</p>
Supported values	<p>You can list file types in the format:</p> <p>.filetype[filetype]</p> <p>By default, the following file types are converted using Enterprise Vault Postscript conversion:</p> <p>.PS.EPS</p>

File types for OCR conversion (site properties Content Conversion setting)

Description	<p>The list of file types to convert using OCR conversion.</p> <p>Note that this setting does not override the setting, File types excluded from conversion. For example, if the file type .xyz is included in both setting values, then instances of the file type xyz are not converted.</p>
Supported values	<p>You can list file types in the format:</p> <p>.filetype[filetype]</p> <p>By default, the following file types are configured for OCR conversion:</p> <p>.GIF.JPG.JPEG.PNG.TIF.TIFF</p> <p>Setting the value to an empty string effectively disables OCR conversion of images.</p>

File types for IFilter conversion (site properties Content Conversion setting)

Description	<p>The list of file types to convert using Windows IFilter conversion.</p> <p>The relevant 64-bit IFilter for each configured file type must be installed on all the Enterprise Vault servers in the site that host a Storage Service.</p> <p>Note that this setting does not override the setting, File types excluded from conversion. For example, if the file type .xyz is included in both setting values, then instances of the file type xyz are not converted.</p>
-------------	---

Supported values You can list file types in the format:
 .filetype[.filetype]

Conversion timeout (site properties Content Conversion setting)

Description The conversion timeout in minutes.

Supported values The value is specified as an integer.
 The default value is 10.

Legacy registry setting ■ Enterprise Vault\ConversionTimeout

Conversion timeout for archive file types (site properties Content Conversion setting)

Description The conversion timeout in minutes for archive file types, for example, ZIP files.

Supported values The value is specified as an integer.
 The default value is 10.

Legacy registry setting ■ Enterprise Vault\ConversionTimeoutArchiveFiles

Include hidden text (site properties Content Conversion setting)

Description Controls whether hidden text is included when converting document items to HTML.
 PDF and Microsoft Word are example file types that can contain hidden text.

Supported values ■ On (default). Hidden text is included in the conversion.
 ■ Off. Hidden text is not included in the conversion.

Legacy registry setting ■ Enterprise Vault\ConversionIncludeHiddenText

Include hidden spreadsheet data (site properties Content Conversion setting)

Description	Controls whether the contents of hidden cells, columns, and sheets are included when converting spreadsheet items to HTML.
Supported values	<ul style="list-style-type: none">■ On (default). Hidden data is included in the conversion.■ Off. Hidden data is not included in the conversion.
Legacy registry setting	<ul style="list-style-type: none">■ Enterprise Vault\Conversion\IncludeHiddenSpreadsheetData

Show spreadsheet border (site properties Content Conversion setting)

Description	Controls the display of cell borders when converting spreadsheet items to HTML. Setting the value to On improves the display of the converted content, but significantly increases both the conversion output size and the time taken to convert the spreadsheet.
Supported values	<ul style="list-style-type: none">■ On. Cell borders are displayed when previewing converted spreadsheet items.■ Off (default). Cell borders are not displayed in converted spreadsheet items.
Legacy registry setting	<ul style="list-style-type: none">■ Enterprise Vault\Conversion\SpreadsheetBorder

Show metadata properties (site properties Content Conversion setting)

Description	When converting items to HTML, controls the display of metadata properties for file types that contain embedded metadata. The set of metadata properties depends on whether the file type content contains embedded properties, and the content converter that is configured for the file type. For example the metadata properties for a photo file could include camera details. For PDF and Microsoft Office documents the metadata properties could include author, subject, and created and last modified dates.
-------------	--

- Supported values
- On. Metadata properties are visible at the end of conversion output HTML.
 - Off (default). Metadata properties are hidden at the end of conversion output HTML. The metadata properties are still present in the HTML, and are searchable as part of the item content.

Maximum conversion size (site properties Content Conversion setting)

- Description The maximum size (MB) of the content conversion output that can be indexed for an item. If an item's conversion output exceeds this value, then its attributes are indexed, but the content is not indexed.
- Supported values The value is specified as an integer.
- The default value is 30.
- Note that if you increase the value, and the conversion output exceeds the default size but is less than the set size, then the item might not be indexed at all; not even the attributes.
- Legacy registry setting ■ Enterprise Vault\MemLimitForTextConversionFallback

OCR language (site properties Content Conversion setting)

- Description The language used during Optical Character Recognition (OCR) conversion of images.
- To maximize OCR accuracy, the language selected should match the expected most common language of archived images for the site.
- The set of languages supported is defined by the Windows TIFF IFilter technology. The language set applies to all conversions on the server; a different language cannot be selected for specific conversion operations.
- Supported values The following languages are currently supported: Chinese (Simplified), Chinese (Traditional), Czech, Danish, Dutch, English, Finnish, French, German, Greek, Hungarian, Italian, Japanese, Korean, Norwegian, Polish, Portuguese, Russian, Spanish, Swedish, and Turkish.
- The default language is based on the administration language that you selected for your Enterprise Vault installation: English, Japanese, Chinese (Simplified).
- Legacy registry setting ■ Enterprise Vault\OCRUseLocalServerSettings

OCR optimization (site properties Content Conversion setting)

Description	Controls whether optimization is enabled for Optical Character Recognition (OCR) conversion. Windows TIFF IFilter performance optimization mechanisms are designed to skip the OCR processing for images that do not contain text. OCR optimization improves the conversion performance, but may reduce accuracy during OCR conversion. Reduced accuracy may result in Enterprise Vault not indexing text that OCR does not recognize.
Supported values	<ul style="list-style-type: none">■ On. OCR optimization is enabled.■ Off (default). OCR optimization is disabled. This value forces Windows IFilter to perform OCR on every page of a TIFF document.
Legacy registry setting	<ul style="list-style-type: none">■ Enterprise Vault\OCRUseLocalServerSettings

Log conversion failure events (site properties Content Conversion setting)

Description	Controls whether conversion failures are written to the Enterprise Vault Converters event log.
Supported values	<ul style="list-style-type: none">■ On (default). Conversion failures are recorded in the event log.■ Off. Conversion failures are not recorded in the event log. This effectively disables all of the other log conversion event settings.
Legacy registry setting	<ul style="list-style-type: none">■ Storage\FailedConversionEvents

Log fallback to text events (site properties Content Conversion setting)

Description	Controls whether to record in the event log successful conversions to text after a failed conversion to HTML. These entries are recorded in the Enterprise Vault Converters event log. Note that the value of this setting does not override the Log conversion failure events setting.
Supported values	<ul style="list-style-type: none">■ On (default). Successful fallback conversions to text are recorded in the event log.■ Off. Successful fallback conversions to text are not recorded in the event log.

Legacy registry setting ■ Storage\FallbackConversionEvents

Log conversion timeout events (site properties Content Conversion setting)

Description Controls whether to record conversion timeout events in the Enterprise Vault Converters event log. Conversion timeout events include conversion failures or fallback to text conversions.

This setting is only effective if either **Log conversion failure events**, or **Log fallback to text events** is set to **On**.

Supported values

- On (default). Conversion timeout events are recorded in the event log.
- Off. Conversion timeout events are not recorded in the event log.

Legacy registry setting ■ Storage\ConversionTimeoutEvents

Log file type not recognized events (site properties Content Conversion setting)

Description Controls whether to record in the Enterprise Vault Converters event log conversion failures that result from an unrecognized file type.

This setting is only effective if either **Log conversion failure events**, or **Log fallback to text events** is set to **On**.

Supported values

- On (default). File type not recognized conversion failures are recorded in the event log.
- Off. File type not recognized conversion failures are not recorded in the event log.

Legacy registry setting ■ Storage\UnrecognisedFileTypeEvents

Log maximum conversion size exceeded events (site properties Content Conversion setting)

Description	<p>Controls whether to record in the event log conversion failures in which the maximum conversion output size is exceeded. These entries are recorded in the Enterprise Vault Converters event log.</p> <p>This setting is only effective if either Log conversion failure events, or Log fallback to text events is set to On.</p>
Supported values	<ul style="list-style-type: none"> ■ On (default). Maximum conversion size exceeded events are written to the event log. ■ Off. Maximum conversion size exceeded events are not written to the event log.
Legacy registry setting	<ul style="list-style-type: none"> ■ Storage\RequestedAllocationSizeTooLargeEvents

File System Archiving (site properties advanced settings)

These settings enable you to control aspects of File System Archiving.

There is one category of File System Archiving advanced settings:

- [Name of the folder shortcut file \(site properties File System Archiving setting\)](#)

Name of the folder shortcut file (site properties File System Archiving setting)

Description	<p>Allows you to change the name of the folder shortcut file (.url), which contains a hypertext link to the archived folder. The file name would be <code>[NewFileName].url</code>. The default name is <code>[View Archived Files].url</code>. Note that if you have customized the folder shortcut name, you may see multiple folder shortcut files. The File System Archiving task does not delete old .url files.</p>
Supported values	<p>Any string value that contains characters supported by the file system. Note that the folder shortcut file name cannot contain any of the following characters:</p> <p>< (less than), > (greater than), :(colon), " (double quote), / (forward slash), \ (backslash), (vertical bar or pipe), ? (question mark), * (asterisk), and characters whose integer representations are in the range from 1 through 31.</p>

IMAP (site properties advanced settings)

The IMAP settings let you control advanced IMAP behavior.

The IMAP settings are:

- [Folder limit \(site properties IMAP setting\)](#)
- [Caching duration \(site properties IMAP setting\)](#)
- [Caching duration when disk space is low \(site properties IMAP setting\)](#)
- [Send Email Timeout \(site properties IMAP setting\)](#)

Folder limit (site properties IMAP setting)

Description Limits the number of archived items that Enterprise Vault returns to IMAP clients from each archive folder. Enterprise Vault returns the most recently archived items, up to the limit you set.

Supported values ■ An integer that sets the folder limit. The default is **10000**.

Caching duration (site properties IMAP setting)

Description Defines the number of minutes for which retrieved items are cached.

Note: Do not change this advanced setting unless your technical support provider advises you to do so.

Supported values ■ An integer that sets the duration. The default is **30**.

Caching duration when disk space is low (site properties IMAP setting)

Description Defines the number of seconds for which retrieved items are cached when the cache is running out of space.

Note: Do not change this advanced setting unless your technical support provider advises you to do so.

Supported values ■ An integer that sets the duration. The default is **900**.

Send Email Timeout (site properties IMAP setting)

Description	<p>Defines the number of seconds that the Client Access Provisioning task waits for confirmation that newly-provisioned users have received the IMAP notification email.</p> <p>The email is sent as soon as the task runs. If the specified time period elapses, and no confirmation of receipt arrives, the client access provisioning task report shows the error message <code>Error sending notification: The operation has timed out.</code> The process is repeated the next time the task is run.</p>
Supported values	<ul style="list-style-type: none">■ An integer in the range 1 to 300 that sets the duration. The default is 30.

Indexing (site properties advanced settings)

The Indexing settings enable you to control advanced indexing behavior.

Note: Do not change the Indexing settings unless your technical support provider advises you to do so.

The Indexing settings are as follows:

- [Allowed index location characters \(Site Properties Indexing setting\)](#)
- [Index Group server preference for mailboxes \(Site Properties Indexing setting\)](#)
- [Maximum concurrent indexing tasks \(Site Properties Indexing setting\)](#)
- [Maximum consecutive failed items \(Site Properties Indexing setting\)](#)
- [Maximum update errors \(Site Properties Indexing setting\)](#)
- [Search Cache Permissions \(Site Properties Indexing setting\)](#)
- [Search Max Attempts When Engine Busy \(Site Properties Indexing setting\)](#)
- [Search Max Folders For Specific Folder Optimization \(Site Properties Indexing setting\)](#)
- [Search Specific Folder Optimization \(Site Properties Indexing setting\)](#)
- [Search VSA Can Search All Archives \(Site Properties Indexing setting\)](#)
- [Text limit for custom properties \(Site Properties Indexing setting\)](#)

Allowed index location characters (Site Properties Indexing setting)

Description	<p>Characters that can be used in index location folder paths.</p> <p>Note: Do not change this advanced setting unless your technical support provider advises you to do so.</p> <p>This setting specifies a regular expression that describes which characters are valid in index location folder paths. The default value allows only ASCII characters.</p> <p>The Indexing service validates index locations when it starts. If any index location folder paths contain invalid characters, the locations are listed in an Enterprise Vault event log message. The message lists the locations that were closed earlier, and the locations that have been closed during the current validation.</p> <p>If any locations were closed during the current validation, the Indexing service is stopped. An error is written to the Enterprise Vault event log. The error says that open index locations contained invalid characters, and that the Indexing service will stop.</p>
Supported values	<ul style="list-style-type: none">■ A regular expression. The default is: <code>[!x00-!x7f]+</code>

Index Group server preference for mailboxes (Site Properties Indexing setting)

Description	<p>Specifies the preferred index group server to use for mailboxes.</p> <p>Note: Do not change this advanced setting unless your technical support provider advises you to do so.</p> <p>Enterprise Vault allocates the location of an index volume by a process that first selects an Index Server within an Index Server group. The process then selects an index location on that Index Server.</p> <p>This allocation method distributes the index volumes amongst all the available Index Servers, which is suitable for large archives such as journal archives. By default, Enterprise Vault does not use this allocation method for the index volumes for mailbox archives. Instead, it keeps these index volumes together on the same Index Server.</p> <p>This setting lets you override the default so that index volumes for mailbox archives are distributed amongst all the available Index Servers.</p>
-------------	---

- Supported values
- Local server (default). The index volumes for mailbox archives are kept together on the Index Server that is local to the associated storage server.
 - None. Index volumes for mailbox archives are distributed amongst all the available Index Servers.

Maximum concurrent indexing tasks (Site Properties Indexing setting)

Description Specifies the maximum number of concurrent indexing tasks.
Note: Do not change this advanced setting unless your technical support provider advises you to do so.

- Supported values
- An integer in the range 1 to 25. The default is 20.

Maximum consecutive failed items (Site Properties Indexing setting)

Description The maximum number of consecutive items that cannot be fetched from the Storage service before the index volume is marked as failed.
Note: Do not change this advanced setting unless your technical support provider advises you to do so.

- Supported values
- An integer specifying a number of consecutive items. The default is 25.

Maximum update errors (Site Properties Indexing setting)

Description The maximum number of errors that are allowed when making index changes before the index volume is marked as failed.
Note: Do not change this advanced setting unless your technical support provider advises you to do so.

- Supported values
- An integer specifying a number of errors. The default is 3.

Search Cache Permissions (Site Properties Indexing setting)

Description	<p>Specifies whether or not user permissions are cached in the Index Query Server.</p> <p>Note: Do not change this advanced setting unless your technical support provider advises you to do so.</p>
Supported values	<ul style="list-style-type: none"> ■ On (default). User permissions are cached in the Index Query Server. ■ Off. User permissions are not cached in the Index Query Server.

Search Max Attempts When Engine Busy (Site Properties Indexing setting)

Description	<p>The maximum number of attempts for searches that fail due to the search engine being temporarily too busy to handle the search.</p> <p>Note: Do not change this advanced setting unless your technical support provider advises you to do so.</p>
Supported values	<ul style="list-style-type: none"> ■ An integer specifying a number of search attempts. The default is 3.

Search Max Folders For Specific Folder Optimization (Site Properties Indexing setting)

Description	<p>The maximum number of folders a search can target, in order for the search query to benefit from applying the specific folder performance optimization.</p> <p>See “Search Specific Folder Optimization (Site Properties Indexing setting)” on page 258.</p> <p>Note: Do not change this advanced setting unless your technical support provider advises you to do so. Changing this value may adversely affect search performance, system performance, or both.</p>
Supported values	<ul style="list-style-type: none"> ■ An integer specifying a number of folders. The default is 10.

Search Specific Folder Optimization (Site Properties Indexing setting)

Description	<p>Specifies whether or not to apply a performance optimization to searches that target a small number of folders. The Search Max Folders For Specific Folder Optimization setting determines the limit for what is considered small.</p> <p>See “Search Max Folders For Specific Folder Optimization (Site Properties Indexing setting)” on page 257.</p> <p>Note: Do not change this setting unless your Technical Support provider advises you to do so.</p>
Supported values	<ul style="list-style-type: none">■ On (default). Applies the performance optimization.■ Off. Performance optimization is not applied.

Search VSA Can Search All Archives (Site Properties Indexing setting)

Description	<p>Specifies whether or not the Index Query Server allows the Vault Service account to search all archives.</p> <p>Note the following:</p> <ul style="list-style-type: none">■ Enabling this setting does not make all the archives visible to the Vault Service account in end-user applications like Enterprise Vault Search. The setting is designed for use with applications that must search across all the archives, such as Compliance Accelerator, Discovery Accelerator, and the EVSVR utility.■ Do not change this advanced setting unless your technical support provider advises you to do so. Compliance Accelerator, Discovery Accelerator, and some of the indexing tools in particular require this option to be on, otherwise they fail.
Supported values	<ul style="list-style-type: none">■ On (default). The Index Query Server allows the Vault Service account to search all archives.■ Off. The Index Query Server does not allow the Vault Service account to search all archives.

Text limit for custom properties (Site Properties Indexing setting)

Description The maximum number of characters in a custom property that can be stored, indexed, retrieved, or searched.

Note: Do not change this advanced setting unless your technical support provider advises you to do so.

Supported values

- An integer specifying a number of characters. The default is 1000; the maximum is 65535.

SQL Server (site properties advanced settings)

The SQL Server settings let you control advanced aspects of Enterprise Vault's interaction with SQL servers.

The SQL Server settings are:

- [SQL AlwaysOn checks \(site properties SQL Server setting\)](#)
- [SQL server connection timeout \(site properties SQL Server setting\)](#)

SQL AlwaysOn checks (site properties SQL Server setting)

Description Use to enable and disable checks for availability groups and failover cluster instances on a SQL server when you create Enterprise Vault databases. Set to Enabled to show informational messages, and Disabled to hide them.

Supported values

- Enabled (default).
- Disabled.

SQL server connection timeout (site properties SQL Server setting)

Description Sets the SQL server connection timeout in seconds. Increase the connection timeout to give applications more time to connect to SQL server.

Supported values

- An integer in the range 5 to 300. The default is 120.

SMTP (site properties advanced settings)

The SMTP settings enable you to control SMTP archiving behavior.

The SMTP settings are as follows:

- [Delete messages without recipients or a matching target \(Site Properties SMTP setting\)](#)
- [List of internal SMTP domains \(Site Properties SMTP setting\)](#)
- [Log action when a message does not contain any archiving-enabled target \(Site Properties SMTP setting\)](#)
- [Selective Journal Archiving \(Site Properties SMTP setting\)](#)

Delete messages without recipients or a matching target (Site Properties SMTP setting)

Description	Controls what action to take when messages in the holding folder do not have recipients or a matching target.
Supported values	<ul style="list-style-type: none"> ■ No. Do not delete. Messages that do not contain a matching target address that is enabled for archiving are moved to the folder <code>NoMatchingTarget</code>, which is in the holding folder. In the <code>NoMatchingTarget</code> folder, subfolders for day, hour, and minute are created as needed. The message file is placed in the appropriate minute folder. ■ Yes (default). Delete messages without recipients or a matching target

List of internal SMTP domains (Site Properties SMTP setting)

Description	<p>Specifies a list of SMTP domains that are to be considered internal to the company. For example, "ourcompany.com;ourcompany.co.ie;ourcompany.co.uk". These domains are supplemental to those detected from the Vault Admin account's email addresses. Alternatively you can use an asterisk (*) to specify that all SMTP domains are internal.</p> <p>This setting complements the following registry value:</p> <p>HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KVS\Enterprise Vault\Agents\InternalSMTPDomains</p> <p>Enterprise Vault automatically combines any domains that you specify through the registry value with those that you specify through the advanced setting.</p>
Supported values	<ul style="list-style-type: none"> ■ A list of domains separated by semi-colons.

Log action when a message does not contain any archiving-enabled target (Site Properties SMTP setting)

- Description** This setting controls whether the SMTP Archiving task logs an event in the SMTP Archiving task error log when it processes a message that does not contain any matching target. The event indicates whether the message has been deleted or moved.
- The SMTP Archiving task error log is in the `Reports\SMTP` subfolder of the Enterprise Vault installation folder.
- Supported values**
- No (default). Do not log actions.
 - Yes. Log actions in the SMTP Archiving task error log.

Selective Journal Archiving (Site Properties SMTP setting)

- Description** Selective Journal Archiving configures the SMTP Archiving task to search all of the sender and recipient fields (X-RCPT-TO, To, CC, BCC, From, Sender) in each message.
- To optimize performance for SMTP Journaling, ensure that this advanced site setting is set to No.
- Supported values**
- No (default). Do not match recipients in the message headers.
 - Yes. Match recipients in the message headers.

Storage (site properties advanced settings)

The Storage settings enable you to control advanced storage behavior.

The Storage settings are as follows:

- [Additional StorageOnlineOpns instances](#)
- [Maximum expiry errors per archive \(Site Properties Storage setting\)](#)
- [Transaction history \(Site Properties Storage setting\)](#)

Additional StorageOnlineOpns instances

On an Enterprise Vault storage server there can never be less than one StorageOnlineOpns process. This setting controls the number of extra processes StorageOnlineOpns to run. The default is for four extra processes, making a total of five StorageOnlineOpns processes.

Note: Do not change this advanced setting unless your technical support provider advises you to do so.

Maximum expiry errors per archive (Site Properties Storage setting)

Description Specifies the maximum number of errors per archive that may occur while processing items for automatic expiry. When this limit is exceeded, Enterprise Vault abandons expiry for the archive. However, it tries again when automatic expiry next runs.

Supported values ■ An integer in the range 0 through 100000. The default is 20.

Transaction history (Site Properties Storage setting)

Description **Transaction history** enables you to control how long to maintain the details of updates to archives. Updates include adding new items, deleting items, and moving items. This transaction history significantly improves the performance of Vault Cache synchronization by providing records of the changes to an archive since the last Vault Cache synchronization. If a user has not synchronized their Vault Cache within the transaction history period, then Enterprise Vault processes the archive to determine the updates.

Transaction history records are held in the SQL Server, so you need to ensure that the database can accommodate this data.

Supported values ■ An integer that specifies the number of days to retain the transaction history of each archive. The default is **32**

Computer properties advanced settings

This chapter includes the following topics:

- [About computer properties advanced settings](#)
- [Editing computer properties advanced settings](#)
- [Computer properties advanced settings](#)

About computer properties advanced settings

The computer properties advanced settings control advanced aspects of Exchange archiving, IMAP access, and indexing and storage behavior on a single Enterprise Vault server.

The advanced settings that apply to the Enterprise Vault site are available in the site properties.

See [“About site properties advanced settings”](#) on page 242.

Editing computer properties advanced settings

The advanced settings for an Enterprise Vault server are provided on the **Advanced** tab of the computer properties.

To edit the computer properties advanced settings

- 1 In the left pane of the Administration Console, expand the hierarchy until **Enterprise Vault Servers** is visible.
- 2 Click **Enterprise Vault Servers**.

- 3 In the right pane, right-click the name of the server whose properties you want to edit. Then click **Properties**. The computer properties are displayed.
- 4 Click the **Advanced** tab.
- 5 Edit the settings as required.

How to apply new settings for computer properties

To apply the changes that you have made, you must restart the Exchange archiving tasks, the IMAP server, or the Indexing service or Storage service, depending on which settings you have changed.

Computer properties advanced settings

Computer properties advanced settings let you configure advanced aspects of some Enterprise Vault server functionality.

Note that the changes you make apply only to the Enterprise Vault server on which you make the changes. To make changes that apply to the whole Enterprise Vault site, use the Site properties advanced settings.

You can change advanced settings in the following categories:

- [Agents \(computer properties advanced settings\)](#)
- [IMAP \(computer properties advanced settings\)](#)
- [Indexing \(computer properties advanced settings\)](#)
- [Storage \(computer properties advanced settings\)](#)

Agents (computer properties advanced settings)

The Agents settings enable you to control advanced agents behavior on an Enterprise Vault server.

The Agents settings are:

- [Send compressed bytes \(Computer Properties Agents setting\)](#)

Send compressed bytes (Computer Properties Agents setting)

Description Controls whether Enterprise Vault agents that archive from Exchange Server compress data before sending it to the storage queue. The compression can reduce network traffic on a WAN. On fast networks the performance overhead of the compression is more significant than the network traffic gain.

This option is not recommended for fast networks.

Supported values

- Yes.
- No (default).

IMAP (computer properties advanced settings)

The Indexing settings are:

- [Generate transcripts \(Computer Properties IMAP setting\)](#)
- [Maximum concurrent connections \(Computer Properties IMAP setting\)](#)
- [Thread pool algorithm \(Computer Properties IMAP setting\)](#)
- [Thread pool maximum size \(Computer Properties IMAP setting\)](#)

Generate transcripts (Computer Properties IMAP setting)

Description Use this property to generate transcripts for IMAP sessions on this Enterprise Vault server, when DTrace is running against IMAP. This can be useful to troubleshoot users' connection problems. Enterprise Vault writes transcripts to the Vault Service account's `TEMP` directory, in files whose extension is `.X`.

Enterprise Vault deletes transcript files when you stop the IMAP server.

Note: IMAP transcripts contain sensitive information from users' email.

Supported values

- No (default).
- Yes.

Maximum concurrent connections (Computer Properties IMAP setting)

Description Use this property to configure the maximum number of concurrent IMAP connections to this Enterprise Vault server.

Supported values ■ An integer in the range 5000 to 100000. The default is 15000.

Thread pool algorithm (Computer Properties IMAP setting)

Description Use this property to set the method this Enterprise Vault server uses to determine the maximum number of CPU threads that are available to service requests.

See [“Thread pool maximum size \(Computer Properties IMAP setting\)”](#) on page 266.

Note: Do not change this advanced setting unless your technical support provider advises you to do so.

Supported values ■ Hardware (default). Use the physical properties of the computer to determine the maximum number of threads. Note however, that the maximum is still constrained by the value in **Thread pool maximum size** if that is lower than the computer would otherwise allow.

■ Setting. Use the value in **Thread pool maximum size**, irrespective of the computer’s physical properties.

Thread pool maximum size (Computer Properties IMAP setting)

Description Use this property to configure the maximum number of CPU threads that are available to service IMAP requests.

Note that the actual number of threads can be further constrained if the **Thread pool algorithm** is set to **Hardware**, and the computer’s physical thread pool size is lower than the limit you set.

See [“Thread pool algorithm \(Computer Properties IMAP setting\)”](#) on page 266.

Note: Do not change this advanced setting unless your technical support provider advises you to do so.

Supported values ■ An integer in the range 20 to 400. The default is 100.

Indexing (computer properties advanced settings)

The Indexing settings enable you to control advanced indexing behavior on an Enterprise Vault server.

Note: Do not change the Indexing settings unless your technical support provider advises you to do so.

The Indexing settings are:

- [Create multiple Index Locations \(Computer Properties Indexing setting\)](#)
- [Empty index volume deletion limit \(Computer Properties Indexing setting\)](#)
- [Force Indexing Engine Shutdown \(Computer Properties Indexing setting\)](#)
- [Frequency of checks for failed volumes \(Computer Properties Indexing setting\)](#)
- [Frequency of checks for index volumes to process \(Computer Properties Indexing setting\)](#)
- [Frequency of full checks for index volumes to process \(Computer Properties Indexing setting\)](#)
- [Indexing Engine Query Service Port \(Computer Properties Indexing setting\)](#)
- [Indexing Execution Timeout \(Computer Properties Indexing setting\)](#)
- [Indexing Max Request Length \(Computer Properties Indexing setting\)](#)
- [Indexing memory throttling threshold \(Computer Properties Indexing setting\)](#)
- [Maximum child process shutdown time \(Computer Properties Indexing setting\)](#)
- [Maximum child process startup time \(Computer Properties Indexing setting\)](#)
- [Maximum concurrent indexing capacity \(Computer Properties Indexing setting\)](#)
- [Maximum indexing application pool start time \(Computer Properties Indexing setting\)](#)
- [Maximum indexing engine shutdown time \(Computer Properties Indexing setting\)](#)
- [Maximum indexing engine startup time \(Computer Properties Indexing setting\)](#)
- [Maximum item wait time \(Computer Properties Indexing setting\)](#)
- [Maximum items in a file system index volume \(Computer Properties Indexing setting\)](#)
- [Maximum items in a journal index volume \(Computer Properties Indexing setting\)](#)
- [Maximum items in a mailbox index volume \(Computer Properties Indexing setting\)](#)
- [Maximum items in a public folder index volume \(Computer Properties Indexing setting\)](#)
- [Maximum items in a shared index volume \(Computer Properties Indexing setting\)](#)

- [Maximum items in a SharePoint index volume \(Computer Properties Indexing setting\)](#)
- [Maximum items in an index volume \(Computer Properties Indexing setting\)](#)
- [Maximum items in an internet mail index volume \(Computer Properties Indexing setting\)](#)
- [Search HTTP Service Path \(Computer Properties Indexing setting\)](#)
- [Search HTTP Service Port \(Computer Properties Indexing setting\)](#)
- [Search HTTP Service Requires SSL \(Computer Properties Indexing setting\)](#)
- [Search Log Queries \(Computer Properties Indexing setting\)](#)
- [Search Log Results \(Computer Properties Indexing setting\)](#)
- [Search Logs Folder \(Computer Properties Indexing setting\)](#)
- [Search Maximum Threads \(Computer Properties Indexing setting\)](#)
- [Search Minimum Threads \(Computer Properties Indexing setting\)](#)
- [Search Performance Counters Enabled \(Computer Properties Indexing setting\)](#)

Create multiple Index Locations (Computer Properties Indexing setting)

Description	<p>Specifies whether Enterprise Vault creates multiple index locations or one index location.</p> <p>Note: Do not change this advanced setting unless your technical support provider advises you to do so.</p> <p>On the Index Locations tab in the Indexing service properties, you can add a folder that is used for index storage. By default, Enterprise Vault automatically creates eight index location subfolders beneath the folder that you add.</p> <p>This setting lets you specify that Enterprise Vault creates only one index location subfolder.</p>
Supported values	<ul style="list-style-type: none">■ Yes (default). Enterprise Vault creates eight index location subfolders.■ No. Enterprise Vault creates one index location subfolder.

Empty index volume deletion limit (Computer Properties Indexing setting)

Description	<p>At regular intervals, the Indexing service checks for empty index volumes, and deletes them. This setting configures the maximum number of empty index volumes that the Indexing service can delete in one pass.</p> <p>By default, the Indexing service checks for empty index volumes every 10 hours. The frequency of these checks is defined by the setting Frequency of full checks for index volumes to process.</p> <p>See “Frequency of full checks for index volumes to process (Computer Properties Indexing setting)” on page 270.</p>
Supported values	<ul style="list-style-type: none">■ An integer configuring the maximum number of empty index volumes. The default is 20. This value can be increased, but we recommend that you do not change this advanced setting unless your technical support provider advises you to do so.

Force Indexing Engine Shutdown (Computer Properties Indexing setting)

Description	<p>Forces indexing engine shutdown.</p> <p>Note: Do not change this advanced setting unless your technical support provider advises you to do so.</p>
Supported values	<ul style="list-style-type: none">■ On (default).■ Off.

Frequency of checks for failed volumes (Computer Properties Indexing setting)

Description	<p>The time between the Indexing service's attempts to process failed index volumes, in hours.</p> <p>Note: Do not change this advanced setting unless your technical support provider advises you to do so.</p>
Supported values	<ul style="list-style-type: none">■ An integer specifying a number of hours. The default is 6.

Frequency of checks for index volumes to process (Computer Properties Indexing setting)

Description The time between the Indexing service's checks for index volumes to process, in hours.

Note: Do not change this advanced setting unless your technical support provider advises you to do so.

Supported values ■ An integer specifying a number of hours. The default is 1.

Frequency of full checks for index volumes to process (Computer Properties Indexing setting)

Description The time between the Indexing service's full checks for index volumes to process, in hours.

Note: Do not change this advanced setting unless your technical support provider advises you to do so.

Supported values ■ An integer specifying a number of hours. The default is 10.

Indexing Engine Query Service Port (Computer Properties Indexing setting)

Description The internal communication port for the Indexing Engine Query Service.

Note: Do not change this advanced setting unless your technical support provider advises you to do so.

Supported values ■ An integer specifying a port number. The default is 7215.

Indexing Execution Timeout (Computer Properties Indexing setting)

Description The indexing HTTP runtime execution timeout, in hours.

Note: Do not change this advanced setting unless your technical support provider advises you to do so.

Supported values ■ An integer specifying a number of hours. The default is 6.

Indexing Max Request Length (Computer Properties Indexing setting)

Description The indexing HTTP runtime maximum request length, in kilobytes.

Note: Do not change this advanced setting unless your technical support provider advises you to do so.

Supported values ■ An integer specifying a number of kilobytes. The default is 76800.

Indexing memory throttling threshold (Computer Properties Indexing setting)

Description The maximum memory usage ratio for the indexing engine. If the total virtual memory in use exceeds this ratio multiplied by the RAM, indexing reduces its memory consumption. The normal range is 1.5 to 2.0. Higher ratios may increase disk paging.

Note: Do not change this advanced setting unless your technical support provider advises you to do so.

Supported values ■ A text value specifying the maximum memory usage ratio. The default is 1.5.

Maximum child process shutdown time (Computer Properties Indexing setting)

Description The maximum time the Indexing service waits for each child process to shut down, in minutes.

Note: Do not change this advanced setting unless your technical support provider advises you to do so.

Supported values ■ An integer specifying a number of minutes. The default is 15.

Maximum child process startup time (Computer Properties Indexing setting)

Description The maximum time the Indexing service waits for each child process to start (minutes).

Note: Do not change this advanced setting unless your technical support provider advises you to do so.

Supported values ■ An integer specifying a number of minutes. The default is 1.

Maximum concurrent indexing capacity (Computer Properties Indexing setting)

Description The maximum total of index volumes and subtasks that can be processed concurrently.

Note: Do not change this advanced setting unless your technical support provider advises you to do so.

Supported values ■ An integer specifying a number of index volumes and subtasks. The default is 30.

Maximum indexing application pool start time (Computer Properties Indexing setting)

Description Maximum time to wait for the Indexing application pool to start, in milliseconds.

Note: Do not change this advanced setting unless your technical support provider advises you to do so.

Supported values ■ An integer specifying a number of milliseconds. The default is 800.

Maximum indexing engine shutdown time (Computer Properties Indexing setting)

Description The maximum time the Indexing service waits for the collection broker and search service to shut down, in minutes.

Note: Do not change this advanced setting unless your technical support provider advises you to do so.

Supported values ■ An integer specifying a number of minutes. The default is 5.

Maximum indexing engine startup time (Computer Properties Indexing setting)

Description The maximum time the Indexing service waits for the collection broker and search service to start (minutes).

Note: Do not change this advanced setting unless your technical support provider advises you to do so.

Supported values ■ An integer specifying a number of minutes. The default is 2.

Maximum item wait time (Computer Properties Indexing setting)

Description The maximum time the Indexing service waits for an item to be fetched from the Storage service (minutes).

Note: Do not change this advanced setting unless your technical support provider advises you to do so.

Supported values ■ An integer specifying a number of minutes. The default is 15.

Maximum items in a file system index volume (Computer Properties Indexing setting)

Description The maximum number of items in a file system index volume. The index volume rolls over to a new volume when it contains approximately this number of items.

Note: Do not change this advanced setting unless your technical support provider advises you to do so.

Supported values ■ An integer specifying a number of items. The default is 5000000.

Maximum items in a journal index volume (Computer Properties Indexing setting)

Description The maximum number of items in a journal index volume. The index volume rolls over to a new volume when it contains approximately this number of items.

Note: Do not change this advanced setting unless your technical support provider advises you to do so.

Supported values ■ An integer specifying a number of items. The default is 5000000.

Maximum items in a mailbox index volume (Computer Properties Indexing setting)

Description The maximum number of items in a mailbox index volume. The index volume rolls over to a new volume when it contains approximately this number of items.

Note: Do not change this advanced setting unless your technical support provider advises you to do so.

Supported values ■ An integer specifying a number of items. The default is 5000000.

Maximum items in a public folder index volume (Computer Properties Indexing setting)

Description The maximum number of items in a public folder index volume. The index volume rolls over to a new volume when it contains approximately this number of items.

Note: Do not change this advanced setting unless your technical support provider advises you to do so.

Supported values ■ An integer specifying a number of items. The default is 5000000.

Maximum items in a shared index volume (Computer Properties Indexing setting)

Description The maximum number of items in a shared index volume. The index volume rolls over to a new volume when it contains approximately this number of items.

Note: Do not change this advanced setting unless your technical support provider advises you to do so.

Supported values ■ An integer specifying a number of items. The default is 5000000.

Maximum items in a SharePoint index volume (Computer Properties Indexing setting)

Description The maximum number of items in a SharePoint index volume. The index volume rolls over to a new volume when it contains approximately this number of items.

Note: Do not change this advanced setting unless your technical support provider advises you to do so.

Supported values ■ An integer specifying a number of items. The default is 5000000.

Maximum items in an index volume (Computer Properties Indexing setting)

Description The maximum number of items in an index volume. The index volume rolls over to a new volume when it contains approximately this number of items.

Note: Do not change this advanced setting unless your technical support provider advises you to do so.

Supported values ■ An integer specifying a number of items. The default is 5000000.

Maximum items in an internet mail index volume (Computer Properties Indexing setting)

Description The maximum number of items in an internet mail index volume. The index volume rolls over to a new volume when it contains approximately this number of items.

Note: Do not change this advanced setting unless your technical support provider advises you to do so.

Supported values ■ An integer specifying a number of items. The default is 5000000.

Search HTTP Service Path (Computer Properties Indexing setting)

Description The path part of the URL for the Index Query Server HTTP service, as used by IndexClient.

Note: Do not change this advanced setting unless your technical support provider advises you to do so.

- Supported values
- A text value specifying a path. The default is:
`/enterprisevault/search/indexserversearchservice/`

Search HTTP Service Port (Computer Properties Indexing setting)

Description The port part of the URL for the Index Query Server HTTP service, as used by IndexClient.

Note: Do not change this advanced setting unless your technical support provider advises you to do so.

- Supported values
- An integer specifying a port number. The default is 80.

Search HTTP Service Requires SSL (Computer Properties Indexing setting)

Description Specifies whether or not the Index Query Server HTTP service requires SSL (HTTPS) connections. If this setting is on, a certificate must be bound to the appropriate port on the Index Query Server HTTP service host.

Note: Do not change this advanced setting unless your technical support provider advises you to do so.

- Supported values
- Off (default).
 - On.

Search Log Queries (Computer Properties Indexing setting)

Description Specifies whether or not the Index Query Server logs queries to disk. The Search Logs Folder setting specifies the location for the files.

See [“Search Logs Folder \(Computer Properties Indexing setting\)”](#) on page 277.

Note: Do not change this advanced setting unless your technical support provider advises you to do so.

- Supported values
- Off (default).
 - On.

Search Log Results (Computer Properties Indexing setting)

Description	<p>Specifies whether or not the Index Query Server logs results to disk. The Search Logs Folder setting specifies the location for the files.</p> <p>See “Search Logs Folder (Computer Properties Indexing setting)” on page 277.</p> <p>Note: Do not change this advanced setting unless your technical support provider advises you to do so.</p>
Supported values	<ul style="list-style-type: none">■ Off (default).■ On.

Search Logs Folder (Computer Properties Indexing setting)

Description	<p>A local folder to store log files that are generated by the Index Query Server.</p> <p>Note: Do not change this advanced setting unless your technical support provider advises you to do so.</p> <p>These logs are only written if the Search Log Queries setting or the Search Log Results setting is turned on.</p> <p>See “Search Log Queries (Computer Properties Indexing setting)” on page 276.</p> <p>See “Search Log Results (Computer Properties Indexing setting)” on page 277.</p>
Supported values	<ul style="list-style-type: none">■ A text value specifying a local folder. The default is that no folder is specified and the Vault Service account <code>TEMP</code> folder is used.

Search Maximum Threads (Computer Properties Indexing setting)

Description	<p>Controls the maximum number of concurrent searches that the server is able to perform.</p> <p>Note: Do not change this advanced setting unless your technical support provider advises you to do so. Changing this value may adversely affect search performance, system performance, or both.</p>
-------------	--

- Supported values
- An integer value specifying a number of threads. The default is 200. The value must be greater than the **Search Minimum Threads** value.
See [“Search Minimum Threads \(Computer Properties Indexing setting\)”](#) on page 278.

Search Minimum Threads (Computer Properties Indexing setting)

Description The minimum number of threads that are used to perform searches within the Index Query Server.

Note: Do not change this advanced setting unless your technical support provider advises you to do so.

- Supported values
- An integer value specifying a number of threads. The default is 4. The value must be less than the **Search Maximum Threads** value.
See [“Search Maximum Threads \(Computer Properties Indexing setting\)”](#) on page 277.

Search Performance Counters Enabled (Computer Properties Indexing setting)

Description Specifies whether or not the Index Query Server performance counters are enabled.

Note: Do not change this advanced setting unless your technical support provider advises you to do so.

- Supported values
- On (default).
 - Off.

Storage (computer properties advanced settings)

The Storage settings enable you to control advanced storage behavior on an Enterprise Vault server

The Storage settings are:

- [Compress savesets \(Computer Properties Storage setting\)](#)
- [Keep classification files \(Computer Properties Storage setting\)](#)
- [Maximum concurrent active connections \(Computer Properties Storage setting\)](#)
- [Threshold for number of queued items \(Computer Properties Storage setting\)](#)

- [Threshold for remaining disk space \(Computer Properties Storage setting\)](#)

Compress savesets (Computer Properties Storage setting)

Description	<p>Controls whether the Enterprise Vault Storage Service compresses savesets before placing them on the storage queue.</p> <p>If you are using the storage queue to store safety copies this option can save a significant amount of disk space. The compression overhead can cause a performance reduction.</p>
Supported values	<ul style="list-style-type: none">■ Off (default).■ On.

Keep classification files (Computer Properties Storage setting)

Description	<p>Controls whether to keep the temporary files that the Enterprise Vault classification component makes when it classifies items. These files may contain sensitive data, so it is normally a good idea to delete them. On the other hand, if Enterprise Vault does not classify items as you expect, you may be able to find out why by examining the files.</p>
Supported values	<ul style="list-style-type: none">■ Off (default).■ On.

Maximum concurrent active connections (Computer Properties Storage setting)

Description	<p>Controls the maximum number of concurrent connections to the storage server.</p>
Supported values	<ul style="list-style-type: none">■ An integer specifying the maximum number of connections to use. The default is 50.

Threshold for number of queued items (Computer Properties Storage setting)

Description	<p>Controls the maximum number of unprocessed savesets that can be on the storage queue. When this limit is reached Enterprise Vault automatically waits until more items can be placed on the queue.</p>
-------------	---

- Supported values
- An integer specifying the maximum number of pending items that are allowed on the queue. The default is 50000.

Threshold for remaining disk space (Computer Properties Storage setting)

Description

The minimum percentage of disk space that must be available at the storage queue location. If its limit is reached, Enterprise Vault does not place any new items on the queue until more space is available.

If you keep safety copies on the storage queue and this limit is reached, the cause may be that there has been no recent backup of the vault store.

- Supported values
- An integer specifying the minimum percentage of free disk space. The default is 10.

Task properties advanced settings

This chapter includes the following topics:

- [Editing task properties advanced settings](#)
- [Advanced SMTP Archiving task properties](#)

Editing task properties advanced settings

The advanced settings for an Enterprise Vault task are provided on the **Advanced** tab of the task properties.

To edit the task properties advanced settings

- 1 In the left pane of the Administration Console, expand the hierarchy until **Enterprise Vault Servers** is visible.
- 2 Expand **Enterprise Vault Servers**.
- 3 Expand the server whose task properties you want to edit.
- 4 Click **Tasks**.
- 5 In the right pane, double-click the task whose properties you want to modify.
- 6 Click the **Advanced** tab.
- 7 Edit the settings as required.

Advanced SMTP Archiving task properties

The advanced SMTP Archiving task properties control advanced aspects of SMTP Archiving tasks.

The advanced SMTP Archiving task properties are as follows:

- [Checkpoint interval for the SMTP Archiving task](#)
- [Frequency to update SMTP Archiving task Summary Report](#)
- [Maximum occurrences of unchanged checkpoints](#)

Checkpoint interval for the SMTP Archiving task

Description	<p>The time between the SMTP Archiving task checkpoints, in minutes.</p> <p>The SMTP Archiving task performs checkpointing at regular intervals. If the task is stopped for any reason, the checkpoint information enables it to resume from the most recent checkpoint position.</p> <p>This setting controls how frequently the task saves checkpoint information.</p>
Supported values	<ul style="list-style-type: none">■ An integer number of minutes. The default is 720 (minutes).

Frequency to update SMTP Archiving task Summary Report

Description	<p>The time interval between updates of the SMTP Archiving task summary information in the task report file (minutes).</p> <p>The SMTP Archiving task generates summary reports and error log reports in the following folder:</p> <p><i>Enterprise_Vault_installation_folder\Reports\SMTP\SMTP_task_name</i></p>
Supported values	<ul style="list-style-type: none">■ An integer value. The default is 60 (minutes).

Maximum occurrences of unchanged checkpoints

Description	<p>The SMTP Archiving task performs checkpointing at regular intervals. If the checkpoint information remains unchanged then it is likely that there is a problem with the task. This setting specifies the maximum number of times an unchanged checkpoint is allowed before the SMTP Archiving task logs a warning event.</p> <p>The SMTP Archiving task generates summary reports and error log reports in the following folder:</p> <p><i>Enterprise_Vault_installation_folder\Reports\SMTP\SMTP_task_name</i></p>
Supported values	<ul style="list-style-type: none">■ An integer number. The default is 6.

Advanced Personal Store Management properties

This chapter includes the following topics:

- [About the advanced Personal Store Management properties settings](#)
- [Editing the advanced Personal Store Management properties settings](#)
- [PST Message Sampling \(Personal Store Management properties advanced settings\)](#)

About the advanced Personal Store Management properties settings

The Personal Store Management properties advanced settings control advanced aspects of ownership identification of PST files.

Editing the advanced Personal Store Management properties settings

The advanced settings for configuring message sampling to identify possible owners of PST files are provided on the **Advanced** tab of the Personal Store Management properties.

To edit the advanced Personal Store Management properties settings

- 1 In the left pane of the Administration Console, expand the hierarchy until you see the **Personal Store Management** node.
- 2 Right-click **Personal Store Management**, and then click **Properties**. The Personal Store Management properties are displayed.

- 3 Click the **Advanced** tab.
- 4 Edit the settings as required.

PST Message Sampling (Personal Store Management properties advanced settings)

The PST Message Sampling settings enable you to control the behavior of PST message sampling.

The PST Message Sampling settings are as follows:

- [Change migration state percentage \(Personal Store Management properties advanced settings\)](#)
- [Message type exclude list \(Personal Store Management properties advanced settings\)](#)

Change migration state percentage (Personal Store Management properties advanced settings)

Description	The percentage of associated mails that decides whether the PST file moves to the "Ready to copy" state. If the percentage criteria is not met, the file remains in its current state.
Supported values	<ul style="list-style-type: none"> ■ Value in the range 80% through 100%.

Message type exclude list (Personal Store Management properties advanced settings)

Description	The list containing MAPI message classes for each message that you want to exclude during the ownership identification scan. By default, this is set to IPM.Note.Microsoft.Conversation. All messages with this message class MAPI property are excluded from the PST during the ownership identification process. This will be a comma-separated list.
Supported values	<ul style="list-style-type: none"> ■ Any string value containing MAPI message class. For example, IPM.Note.SMIME.MultipartSigned.

Classification policy advanced settings

This chapter includes the following topics:

- [Editing the classification policy advanced settings](#)
- [Classification Settings \(Classification Policy advanced settings\)](#)

Editing the classification policy advanced settings

To edit the classification policy advanced settings

- 1 In the left pane of the Administration Console, expand the hierarchy until **Policies** is visible.
- 2 Expand **Policies > Retention & Classification > Classification**.
- 3 In the right-hand pane, double-click the name of the policy you want to edit.
The policy's properties are displayed.
- 4 Click the **Advanced** tab.
- 5 Edit the settings as required.

You can double-click a setting to edit it, or click it once to select it and then click **Modify**.

Classification Settings (Classification Policy advanced settings)

The classification settings let you control advanced classification policy behavior. The Classification Settings are:

- [Retention category selection \(Classification Policy setting\)](#)

Retention category selection (Classification Policy setting)

Description	Specifies the retention category to use when classification tags match multiple retention categories. Enterprise Vault uses the retention category that retains the item for the longest or shortest duration, depending on this setting value.
Supported values	<ul style="list-style-type: none"> ■ Longest (default) ■ Shortest
Legacy name	RetentionCategorySelection

Managing the Storage queue

This chapter includes the following topics:

- [About the Storage queue](#)
- [How the Storage queue keeps safety copies](#)
- [Checking how many safety copies are on the Storage queue](#)
- [Viewing or changing Advanced settings](#)
- [Changing the Storage queue location](#)
- [Closing or opening a Storage queue location](#)

About the Storage queue

The storage queue holds the items that Enterprise Vault is in the process of archiving.

When Enterprise Vault archives an item, it keeps a safety copy as part of the archiving process. You can choose to make Enterprise Vault keep the safety copies on the storage queue. The advantage is that the space soon becomes available at the original location. For example, a user who archives an item sees the quota usage reduce almost immediately instead of waiting until the next backup.

The storage queue location should be on a fault-tolerant device (RAID 1 or higher). The device must have sufficient space for all items on the queue. If you intend to use the storage queue for safety copies then there must be enough space to keep them until after the next backup.

For performance information about the Storage queue see the Enterprise Vault *Performance Guide* at the following location:

<http://www.veritas.com/docs/000005725>

Applications may use the storage queue for safety copies regardless of the vault store properties settings in the Administration Console. Therefore it is not safe to assume that the storage queue is never used for safety copies.

If you use a building blocks environment the Storage queue location must be shared with the associated servers.

There is one Storage queue on each server that runs an Enterprise Vault Storage service.

How the Storage queue keeps safety copies

When the safety copies are kept on the Storage queue, the mailbox archiving process is as follows:

- 1 An item is marked as archive pending.
- 2 The item is added to .EVSQ file in the Storage queue location.
- 3 Storage takes the item from the .EVSQ file and adds it to the appropriate archive.
- 4 Enterprise Vault changes the archive pending item in the mailbox to a shortcut.
- 5 Enterprise Vault scans to make sure that each SIS part and DVS file have been secured.
- 6 When all the archived versions of all the items in the .EVSQ file are secured, Enterprise Vault deletes the .EVSQ file.

Enterprise Vault creates empty .EVSQ files and then populates them as required. The Storage queue location may contain files with zero size. Such files are part of the normal operation. The files are deleted when they are not longer needed.

Checking how many safety copies are on the Storage queue

When Enterprise Vault keeps safety copies on the Storage queue they are removed automatically after the corresponding archive has been secured.

You can check the Storage queue at any time to see how many safety copies are on queue.

To check how many items are on the Storage queue

- 1 In the left pane of the Administration Console, expand the vault site.
- 2 Expand **Enterprise Vault Servers**.
- 3 Expand the server whose Storage queue you want to view.
- 4 Click **Services**.
- 5 Double-click the Storage service.
- 6 Click the **Storage Queue** tab.
- 7 Under details, look at the value of **Number of safety copies on the queue**.

Viewing or changing Advanced settings

The Advanced Storage settings are in the computer properties.

The Advanced Storage settings are as follows:

- **Compress savesets.** Controls whether the Enterprise Vault Storage service compresses savesets before placing them on the Storage queue.
See [“Compress savesets \(Computer Properties Storage setting\)”](#) on page 279.
There is a separate option that controls whether Enterprise Vault sends compressed data to the Storage queue. By default this option is disabled because on fast networks the performance overhead of the compression is more significant than the network traffic gain.
See [“Send compressed bytes \(Computer Properties Agents setting\)”](#) on page 265.
- **Maximum concurrent active connections.** Controls the maximum number of concurrent connections to the Storage server.
See [“Maximum concurrent active connections \(Computer Properties Storage setting\)”](#) on page 279.
- **Threshold for number of queued items.** Controls the maximum number of unprocessed savesets that can be on the storage queue. When this limit is reached Enterprise Vault automatically waits until more items can be placed on the queue.
See [“Threshold for number of queued items \(Computer Properties Storage setting\)”](#) on page 279.
- **Threshold for remaining disk space.** The minimum percentage of disk space that must be available at the storage queue location. If its limit is reached, Enterprise Vault does not place any new items on the queue until more space is available.
See [“Threshold for remaining disk space \(Computer Properties Storage setting\)”](#) on page 280.

To view or modify the Advanced settings

- 1 In the left pane of the Administration Console, expand the vault site.
- 2 Expand **Enterprise Vault Servers**.
- 3 Right-click the server whose settings you want to view or modify and on the shortcut menu click **Properties**.
- 4 In **Computer Properties** click the **Advanced** tab.
- 5 Next to **List settings from** select **Storage**.
- 6 Double-click any setting that you want to modify.

Changing the Storage queue location

You can change the Storage queue location in the properties of the Storage service. The existing location may contain safety copies of those archived items that have not yet been secured.

Note: The storage queue location should be on a fault tolerant device (RAID 1 or higher). The device must have sufficient space for all items on the queue. If you intend to use the storage queue for safety copies then there must be enough space to keep them until after the next backup.

You may want to close the Storage queue before you change its location. When the Storage queue is closed Enterprise Vault cannot add new items but can still process those items that are already on the queue.

See [“Closing or opening a Storage queue location”](#) on page 291.

To change the Storage queue location

- 1 In the left pane of the Administration Console, expand the vault site.
- 2 Expand **Enterprise Vault Servers**.
- 3 Expand the server whose Storage queue you want to modify.
- 4 Click **Services**.
- 5 In the right pane check that the Enterprise Vault Storage service is stopped. If the service is not stopped, right-click the service and on the shortcut menu click **Stop**.
- 6 When you have ensured that the Storage service is stopped, double-click the Storage service.
- 7 Click the **Storage Queue** tab.

- 8 In the **Queue Location** section click the browse button.
If there are safety copies in the current Storage queue location there is prompt for you to copy the existing files to the new location.
- 9 Click **I want to copy the files now** to open the current Storage queue location.
- 10 Copy the existing files to the new location.
- 11 Click **I'm ready to select the new storage location**, select the folder that you want to use and then click **OK**. Click **OK** to close the Storage service properties dialog.
- 12 Right-click the service and on the shortcut menu click **Start**.

Closing or opening a Storage queue location

You can close or open a Storage queue location to control whether Enterprise Vault is allowed to add new items to the queue, as follows:

When the Storage queue is open Enterprise Vault can add new items to the Storage queue.

When the Storage queue is closed Enterprise Vault cannot add new items but can still process those items that are already on the queue.

You may find it useful to close a Storage queue if you intend to move the queue to another location. You can then wait for the number of items on the queue to reduce before you move the queue.

To close or open the Storage queue location

- 1 In the left pane of the Administration Console, expand the vault site.
- 2 Expand **Enterprise Vault Servers**.
- 3 Expand the server whose Storage queue you want to modify.
- 4 Click **Services**.
- 5 Double-click the Storage service.
- 6 Click the **Storage Queue** tab.
- 7 In the **Queue Status** section select the option you require, as follows:
 - To close the location, select **Closed**
 - To open the location, select **Open**
- 8 Click **OK**.

Automatic monitoring

This chapter includes the following topics:

- [About automatic monitoring](#)
- [Monitoring in Site Properties](#)
- [About monitoring using Enterprise Vault Operations Manager](#)
- [About monitoring using MOM](#)
- [About monitoring using SCOM](#)

About automatic monitoring

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

- The **Monitoring** tab in Site Properties lets you turn on performance monitoring of important aspects of Enterprise Vault. If a monitored item reaches its threshold, a message is logged in the Application Event log and in the **Status** section of the Administration Console.
If you have other tools to monitor the event log, you can use them to alert you when monitoring messages are logged.
- If you have installed the Enterprise Vault Operations Manager Web Application, you can use it to monitor Enterprise Vault remotely from any computer on which Internet Explorer is installed.
- If you have Microsoft Operations Manager (MOM), you can use the supplied Enterprise Vault Management Pack to monitor Enterprise Vault operations and performance.

- If you have Microsoft System Center Operations Manager (SCOM), you can use the supplied Enterprise Vault Management Pack, to monitor Enterprise Vault operations and performance.

Monitoring in Site Properties

When you enable monitoring in Site Properties you can then select any number of available alerts. When an alert you have selected reaches its threshold level, Enterprise Vault writes an appropriate entry in the Application Event Log. Enterprise Vault also shows the alert in the **Status** section of the Administration Console.

Additionally, when you enable any of the alerts, Enterprise Vault turns on a performance counter for that alert. Thus you can monitor the counter using the Windows Performance Monitor or any other programs that you use to monitor performance counters.

To enable monitoring

- 1 In the left pane of the Administration Console, right-click the vault site and, on the shortcut menu, click **Properties**.
- 2 Click the **Monitoring** tab of Site Properties.
- 3 Select the items for which you want to receive notifications.

For each item, you can click the following to modify them:

Threshold	This is the level at which Enterprise Vault issues a notification. For example, if Directory Backup has a threshold of 2 Days, then a warning is issued if the Enterprise Vault has not been backed up after 2 Days.
Frequency	This is how often Enterprise Vault checks this item. In the case of performance-related items, this is the frequency with which Enterprise Vault writes the associated performance counter.
Start At	The time at which measuring starts. If you do not select a time, the statistics are collected when the monitoring process starts and then at the interval that is defined in the Frequency column.

- 4 Click **OK**.

About monitoring using 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 you monitor the following:

- The status of Enterprise Vault services and tasks.
- Performance counters for vault stores, disk space, memory, and processors.
- The status of Exchange Server journal mailbox target archiving targets, including item counts for Inbox, Archive Pending, and failed operations such as Failed DL Expansion.
- The status of Domino Server journaling location archiving targets, including item counts for Inbox, Archive Pending, and failed operations.

Enterprise Vault includes a Monitoring agent on each Enterprise Vault server. The Monitoring agents collect monitoring data at scheduled intervals, typically every few minutes, and store it in the Enterprise Vault Monitoring database.

Operations Manager displays the most recent data collected by the Monitoring agents. It provides summary tables for at-a-glance status assessment, and detailed data to help identify problems or bottlenecks. Status indicators warn when values breach chosen thresholds.

From the Configuration page you can enable or disable monitoring, adjust the monitoring frequency of the Monitoring agents, and set the status indicator thresholds.

Accessing Operations Manager

Enterprise Vault Operations Manager is a separately installable feature. To monitor the Enterprise Vault servers in an Enterprise Vault site, you must have installed the Operations Manager web application component on at least one Enterprise Vault server in that site.

If you have not already installed Enterprise Vault Operations Manager, you can install it as described in the *Installing and Configuring* manual.

To access Enterprise Vault Operations Manager

- 1 Enter the following URL in Internet Explorer:

```
http://host_ipaddress/MonitoringWebApp/default.aspx
```

where *host_ipaddress* is the IP address of the computer that is hosting the Enterprise Vault server on which the Enterprise Vault Operations Manager web application feature is installed.

Alternatively, if you are accessing Operations Manager from the computer on which it is installed, you can use the following URL, which does not require step 2:

```
http://localhost/MonitoringWebApp/default.aspx
```

- 2 In the Connect to IP *Address* dialog box, enter the user name and password of an account in the host computer's domain. Then click **OK**.

Note: Any user other than the Vault Service account must be assigned to a suitable role to access Operations Manager. Users can view only the tabs and tables in Operations Manager that are applicable to the role to which they are assigned.

See "[Roles-based administration](#)" on page 20.

If the user credentials are valid, Operations Manager displays its site Summary page.

About monitoring using MOM

The Enterprise Vault Management Pack contains rules that enable Microsoft Operations Manager (MOM) to monitor critical Enterprise Vault events in the Application Event Log.

You can also use MOM to monitor all the alerts that are on the Monitoring tab in **Site Properties**. To do so, you start by enabling the monitoring in **Site Properties**. The alerts are written as critical events to the Application Event Log. There are MOM rules defined, and enabled by default, to monitor those same events in the Event Log.

This section assumes that you have some familiarity with MOM administration. See the MOM documentation if you need help with using MOM.

Caution: You must already have a working Microsoft MOM installation before you can install the Enterprise Vault Management Pack. If you experience monitoring issues, contact Microsoft Support for assistance.

Installing MOM

The Enterprise Vault installation copies the MOM Management Pack to the MOM subfolder of the Enterprise Vault program folder (for example `C:\Program Files (x86)\Enterprise Vault\MOM`).

The Management Pack is `EnterpriseVault.akm`.

Configuring MOM

You must do the following:

- Import the Enterprise Vault Management Pack.
- Add operators to the Enterprise Vault Notifications Group, Enterprise Vault Administrators.
- Enabled monitoring in the Enterprise Vault Administration Console.

To import the Enterprise Vault Management Pack

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

To add operators to the Enterprise Vault notifications group

- 1 In the left pane of the MOM Administrator Console, expand **Rule Groups**.
- 2 Click **Notification Groups**.
- 3 In the right pane, double-click **Enterprise Vault Administrators**.
- 4 Add the operators who should receive alerts.
- 5 Click **OK**.

Optional MOM configuration

The Enterprise Vault MOM Management Pack defines many rules for Enterprise Vault monitoring, some of which are enabled by default and some of which are disabled. Review the rules and enable or disable as required.

When you have configured your Enterprise Vault MOM management pack, you may need to configure some of the rules before you can use them.

For example, if you want to use the following rule you must configure it to specify which SQL server to monitor:

```
Sample value of the performance counter SQL Server - Checkpoint pages / sec is greater than the defined threshold
```

Note that some MOM rules concern events that are themselves enabled by the Enterprise Vault Administration Console. In the case of these events, they must be enabled in the Administration Console.

[Table 18-1](#) lists the events that can be enabled from the Administration Console that have corresponding MOM rules.

By default, all the events in this table are enabled.

Table 18-1 MOM rules and corresponding events

Event ID	Administration Console name	MOM rule name
41008	New items awaiting backup	Backup warning: Saveset files not backed up or replicated
41011	Vault Store database backup	Backup overdue for vault store SQL database.
41012	Vault Store transaction log backup	Backup overdue for vault store SQL database transaction log.
41013	Vault Store transaction log size	Space allocation warning for vault store SQL database.
41014	Directory database backup	Backup overdue for Enterprise Vault directory database.
41015	Directory transaction log backup	Backup overdue for Enterprise Vault directory database.
41016	Directory transaction log size	Space allocation warning for Enterprise Vault Directory SQL database.
41021	Archived items waiting to be indexed	Backup, indexing, or replication operations not completed.
41022	Deleted items waiting to be deleted from indexes	Delete operations not completed.

Table 18-1 MOM rules and corresponding events (*continued*)

Event ID	Administration Console name	MOM rule name
41023	Items waiting to be restored	Restoration queue length warning.
41203	Vault Store fingerprint database backup	Backup overdue for Vault Store Group SQL database.
41204	Vault Store fingerprint database log backup	Backup overdue for Vault Store Group SQL database transaction log.
41205	Vault Store fingerprint database log size	Space allocation warning for Vault Store Group Log size.
41256	Vault Store in backup mode	Vault Store(s) in backup mode (All)
41258	Vault Store partition backup scan	Partition(s) not scanned (All)
41260	Partition items secured	Partition(s) contain items that have not been secured for a while (All)
41262	Index location in backup mode	Index locations in backup mode (All)
41264	Tasks in report mode	Task(s) in report mode (All)
41265	Unscheduled task	Task schedule is set to 'Never'

About monitoring using SCOM

Enterprise Vault includes a management pack for System Center Operations Manager (SCOM) 2012 SP1 and later. This pack defines rules that enable SCOM to monitor Enterprise Vault components and critical Enterprise Vault events in the Application Event Log on Enterprise Vault servers.

You can also use SCOM to monitor all the alerts that are on the **Monitoring** tab in **Site Properties**. To do so, you start by enabling the monitoring in **Site Properties**. The alerts are written as critical events to the Application Event Log. SCOM monitors the event log for those events. The SCOM monitoring rules are enabled by default.

In a cluster, you can monitor the Enterprise Vault cluster resource group but not individual servers.

Caution: You must already have a working Microsoft SCOM installation before you can install the Enterprise Vault management pack. If you experience monitoring issues, contact Microsoft Support for assistance.

Setting up SCOM monitoring for Enterprise Vault servers

The following procedure summarizes the process of setting up SCOM monitoring for Enterprise Vault. Follow the links to see the details.

To set up SCOM monitoring for Enterprise Vault

- 1** Create or choose a domain account that you want to use as the Run As account for SCOM monitoring.
See [“Creating a Run As account”](#) on page 299.
- 2** Assign the Enterprise Vault Monitoring Application role to the account that you want to use as the Run As account for SCOM monitoring.
See [“Assigning the Monitoring Application role to an account”](#) on page 300.
- 3** Distribute the Run As account details to the Enterprise Vault servers that will be managed by SCOM.
See [“Distributing the Run As account credentials”](#) on page 300.
- 4** Import the Enterprise Vault SCOM pack.
See [“Importing the Enterprise Vault SCOM management pack”](#) on page 301.
- 5** Associate the Run As account with the Run As profile that is included in the Enterprise Vault SCOM pack.
See [“Associating the Run As account with the Run As profile”](#) on page 302.
- 6** Enable Agent Proxy for the installed agents.
See [“Enabling Agent Proxy for the installed agents”](#) on page 302.

Creating a Run As account

You must create or choose a domain account that you want to use as the Run As account for SCOM monitoring.

To create a Run As account

- 1** Start System Center Operations Manager
- 2** Click the **Administration** tab.

- 3 In the left pane, right-click **Accounts** under **Run As Configuration** and click **Create Run As Account**.
- 4 Work through the **Create Run As Account Wizard** as follows:
 - On the General Properties page:
 - Select **Windows** as the **Run As Account Type**.
 - Enter your own choice of **Display Name** and **Description**.
 - On the Credentials page:
 - Enter the details of the account to which you assigned the Monitoring Application role in the Enterprise Vault Administration Console.
 - On the Distribution Security page:
 - Select **Less Secure** or **More Secure** as required.
 - Select **Less Secure** to distribute the account details to all SCOM Agent servers.
 - Select **More Secure** to distribute the account details to specific servers.

Assigning the Monitoring Application role to an account

You must assign the Monitoring Application role to the account you want to use as the Run As account for SCOM monitoring.

See [“Roles-based administration”](#) on page 20.

Distributing the Run As account credentials

This section describes how to distribute the Run As account details to the Enterprise Vault servers that will be managed by SCOM.

To distribute the Run As account credentials

- 1 Start System Center Operations Manager
- 2 Click the **Administration** tab.
- 3 In the left pane, click **Accounts** under **Run As Configuration**.
- 4 In the Accounts list, right-click the Run As account that you intend to use for Enterprise Vault monitoring and then click **Properties**.
- 5 Click the **Distribution** tab.
- 6 Click **More secure**.
- 7 Click **Add** then select each Enterprise Vault server that you intend to monitor.
- 8 Click **Apply**.

Importing the Enterprise Vault SCOM management pack

The SCOM management pack is provided in a self-extracting executable file, `Veritas Enterprise Vault Management Pack.exe`. The file is on the Enterprise Vault media.

To import the Enterprise Vault management pack

- 1 Load the Enterprise Vault media.
- 2 If Windows AutoPlay is enabled on the server, Windows shows an AutoPlay dialog box. Click **Run Setup.exe**.

If AutoPlay is not enabled, use Windows Explorer to open the root folder of the installation media and then double-click the file **Setup.exe**.
- 3 In the list in the left pane of the **Veritas Enterprise Vault Install Launcher** window, click **Enterprise Vault**.
- 4 Click **Client Installation**.
- 5 In the right pane, click **SCOM Management Pack**.
- 6 Click **Open Folder**. Windows Explorer starts in the folder that contains the management pack.
- 7 Double-click the following file:
`Veritas Enterprise Vault Management Pack.exe`
- 8 Read the displayed license and click **Yes** to agree to the terms.
- 9 Specify the folder where you want to place the management pack and click **OK**.
- 10 In System Center Operations Manager select **Administration**.
- 11 In the left pane, right-click **Administration** and click **Import Management Packs**.
- 12 In the Import Management Packs Wizard, click **Add** and then click **Add from disk**.
- 13 If there is a prompt that asks whether you want to search the online catalog for dependencies, click **No**.
- 14 Navigate to the folder that contains the management packs that you extracted.
- 15 Click `Veritas.EnterpriseVault.Library.mp` and `Veritas.EnterpriseVault.12.mp` and then click **Open**. The wizard adds the management packs to the **Import list**.
- 16 Click **Install**. The wizard imports the management packs.
- 17 Click **Close**.

Associating the Run As account with the Run As profile

This section describes how to associate the Run As account with the Run As profile that is included in the Enterprise Vault SCOM pack.

To associate the Run As account with the Run As profile

- 1 In System Center Operations Manager, click **Administration**.
- 2 In the left pane, click **Profiles**.
- 3 In the right pane, double-click **Veritas Enterprise Vault Monitoring Profile**.
- 4 Work through the **Run As Profile Wizard** as follows:

On the Run As Accounts screen:

- Click **Add** and then select the Run As account that you created.
- Under **This Run As Account will be used to manage the following objects**, select **All targeted objects**.

Enabling Agent Proxy for the installed agents

This section describes how to enable Agent Proxy for the installed agents.

To enable Agent Proxy

- 1 In the SCOM management console, click the **Administration** tab.
- 2 Under **Device Management**, click **Agent Managed**.
- 3 Do the following for each Enterprise Vault server in the Agent Managed list:
 - Right-click the server and then click **Properties**.
 - Click the **Security** tab.
 - Select **Allow this agent to act as a proxy and discover managed objects on other computers**
 - Click **OK**.

Using or removing an earlier SCOM management pack

When you import the Enterprise Vault SCOM management pack, any SCOM pack from Enterprise Vault versions earlier than 11.0.1 is not removed.

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

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

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

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

To delete the previous Enterprise Vault management packs

- 1 In the Operations console, click the **Administration** button.
- 2 In the **Administration** list, click **Management Packs**.
- 3 In the **Management Packs** pane, right-click the Enterprise Vault management pack and then click **Delete**.

If any other management packs depend on the Enterprise Vault pack, a "Dependent Management Packs" error message appears. Before you can continue, you must first take a backup copy of the dependent packs and then either delete them or edit them to remove their dependency on the Enterprise Vault pack.

Optional SCOM configuration

The Enterprise Vault SCOM management pack defines many rules for Enterprise Vault monitoring, some of which are enabled by default and some of which are disabled. Review the rules and enable or disable as required.

When you have configured your Enterprise Vault SCOM management pack, you may need to configure some of the rules before you can use them.

Note that some SCOM rules concern events that are themselves enabled by the Enterprise Vault Administration Console. In the case of these events, they must be enabled in the Administration Console.

Points to note about SCOM monitoring

By default SCOM discovers the Enterprise Vault Index Service every 24 hours. If you want to override this default you must change the setting in both of the following two objects:

- **Discover server dependencies (Discovered type: Indexing).**
- **Discover server indexing dependencies (Discovered Type: Indexing Service).**

The SCOM monitoring has the following known limitations:

- When a monitored Enterprise Vault server is not reachable, the SCOM Operations Console may show the server status incorrectly. In the Site State view an unreachable server should be shown as disabled (gray) but is instead

shown as enabled (green). The Server State view correctly shows an unreachable server as disabled (gray).

- When Enterprise Vault is installed on a Microsoft Cluster, the health status of individual servers may take a long time to be updated in the Enterprise Vault Site health status. The update may take more than 30 minutes. The health status of individual servers is always up to date
- If the connection to the Directory database is lost then the health statuses of vault store databases and fingerprint databases are not refreshed and so may be incorrect. The health status is reported correctly when the connection to the Directory database is fixed.
- If the Storage service is unavailable or the Storage service loses a database connection then the performance counter values for vault store partitions are not updated. This means that the health shown for vault store partitions may be incorrect. The counters are updated automatically when the Storage service connections are restored.

Managing extension content providers

This chapter includes the following topics:

- [About extension content providers](#)
- [Extension content provider properties](#)
- [Assigning the Extension Content Provider Administrator role](#)
- [Assigning the Extension Content Provider Application role](#)
- [Enabling an extension content provider](#)
- [Viewing the content provider reports](#)

About extension content providers

The Enterprise Vault Extensions feature enables partners to develop solutions that extend the standard functionality of Enterprise Vault.

In the Administration Console navigation pane, installed extensions are listed below the Extensions container.

Access to extensions in the Administration Console is controlled using Enterprise Vault roles-based administration. This control enables you to designate specific individuals or groups as extension administrators.

Each extension content provider has its own schedule. You can modify the schedule by editing the properties of the extension content provider.

Extension content provider properties

The properties of an extension content provider enable you to do the following:

- Enable or disable the extension. When the extension is enabled it archives according to the settings on the Schedule tab.
- Set the default vault store. You must select a default vault store. This vault store may be used by the extension but there is no requirement for it to do so.
- Manage extra options that may have been provided by the partner who created the extension.
- Define the archiving schedule.
- Modify settings that fine tune the behavior of the extension.

For additional information on managing an extension, see the documentation that was provided partner who created that extension.

Assigning the Extension Content Provider Administrator role

If you intend to use an account other than the Vault Service account to manage the Content Provider extensions then you must assign that account to the Extension Content Provider Administrator role.

See [“Roles-based administration”](#) on page 20.

The Extension Content Provider Administrator role allows assigned accounts to view and manage extensions.

Assigning the Extension Content Provider Application role

The account under which an extension runs must be assigned to the Extension Content Provider Application role.

See [“Roles-based administration”](#) on page 20.

The Extension Content Provider Application role lets the application to run as an Enterprise Vault extension, to create, read, and update extension entries in the directory, and to archive items.

This role does not allow full update permission on all extension properties. For example an extension cannot enable or disable itself, nor can it modify or override its own schedule.

Enabling an extension content provider

To enable an extension content provider

- 1 In the left pane of the Administration Console, expand the Enterprise Vault site until the Extensions container is visible.
- 2 Expand the Extensions container and then click **Content Providers**. The right-hand pane shows the extensions that have been installed.
- 3 Right-click the extension and on the shortcut menu click **Properties**.
- 4 On the properties **General** tab, select **Enable**.
- 5 Under **Default Vault Store** click **Browse** and select that vault store that you want the extension to use.
- 6 Click the **Schedule** tab.
- 7 Select **Always** or set a schedule as required.
- 8 Click **OK** to close the properties.

Viewing the content provider reports

From the Administration Console you can view the following extension content provider reports:

- Content Providers Licensing and Usage Summary. This report provides the following information:
 - The Veritas Enterprise Vault capacity license usage.
 - The total amount of data that has been ingested into Enterprise Vault by all content providers, both capacity licensed and per-user licensed.
- Content Provider Ingest History. This report shows the number and total size of the items that a single content provider or content provider instance has presented to Enterprise Vault for archiving over a chosen time period.

To view the Content Providers Licensing and Usage Summary report

- 1 In the left pane of the Administration Console, expand **Directory**.
- 2 Expand **Extensions**.
- 3 Right-click **Content Providers** and on the shortcut menu click **Content Providers Licensing and Usage Summary report**.

To view the Content Provider Ingest History report

- 1** In the left pane of the Administration Console, expand **Directory**.
- 2** Expand **Extensions**.
- 3** Click **Content Providers**.
- 4** In the right pane, right-click the extension for which you want a report and on the shortcut menu click **Content Provider Ingest History Report**.

You can also run the reports from the **Common Tasks** section in the Administration Console.

To view reports from Common Taskks

- 1** In the left pane of the Administration Console, click the name of the Enterprise Vault site.
- 2** In **Common Tasks** in the right pane, expand **Enterprise Vault Server Management**.
- 3** Click **Run operation reports**.

For more information about the reports and how to use them, see the *Reporting* guide.

Exporting archives

This chapter includes the following topics:

- [About the Export Archive wizard](#)
- [Importing \(migrating\) exported files](#)
- [Starting the export with the Export Archive wizard](#)

About the Export Archive wizard

Export Archive can be used to export archived items from the following archive types:

- Exchange Mailbox archive
- Exchange Journal archive
- File System archive
- Shared archive

Export Archive can be used with Exchange Server mailbox archiving only. If you want to export items from Domino archives, see the description of Domino Archive Exporter in the *Utilities* guide.

The Export Archive wizard lets you export archived items as follows:

- Archives to PST files. This is useful when the following apply:
 - You want to give a user a personal copy of archived items, perhaps to use when out of the office.
 - You want to send individual mailbox archives somewhere for safekeeping.
- Archives to their original mailboxes. This is useful when the following apply:
 - You are transferring mailboxes and want to send the users' archived items too.

- You have been running a pilot installation of Enterprise Vault and now want to copy everything that has been archived back to the original mailboxes.
- A single archive to a chosen mailbox. This could be useful when the following apply:
 - A person takes over an existing role within the company. For example, You could export to the new mailbox everything that was archived from the old mailbox with a particular retention category.
 - There is a legal investigation. You may want to copy everything that has been archived from a particular mailbox to a new mailbox, ready for subsequent investigation.

When you export, you can filter the output by date and by retention category. For example, you can export items less than a year old that were archived with a particular retention category.

When you export to PST files, the wizard lets you control the maximum size of the output files. The default maximum of 600 MB is ideal for writing to CD. If a file reaches the maximum size, the wizard automatically creates a numbered sequence of files, none of which exceeds the maximum size.

Folders in PST files can contain a maximum of 16,383 items. This is a PST file limitation. If a folder reaches this limit the Export Archive wizard automatically creates a new folder of the same name but with a number suffix. For example, if folder 'Inbox' is full, the Export Archive wizard automatically creates 'Inbox 1' to hold further items.

For each PST file, the wizard creates a configuration file that you may need if you intend to import the PST file contents back into Enterprise Vault. You can import files that have been exported, so it is possible to move someone's archived items to another Enterprise Vault system.

Importing (migrating) exported files

When you migrate exported PST files to an archive, it is best to locate the destination archive on a different vault store from the original archive. If these archives are on the same vault store, then you must delete the original archive before migrating the PST files. Failure to do this results in duplicate entries in the vault store database.

The following steps summarize the procedure for migrating PST files when the destination archive is on the same vault store as the original archive.

To migrate PST files to an archive on the same vault store as the original archive

- 1 After you have exported the archive to PST files using the Export Archive wizard, ensure that the export was successful.
- 2 If the destination archive is to be associated with the same mailbox, then disable the mailbox using the Enterprise Vault Administration Console.
- 3 In the Enterprise Vault Administration Console, delete the original archive.
- 4 To create the destination archive, enable the associated mailbox.
- 5 Use PST Migration to import the PST files into the new archive. To fix any broken shortcuts in the mailbox, configure PST migration as follows:
 - Do not create shortcuts to newly-archived items.
 - Import items to the root folder .
 - Merge the folder structures.

PST configuration files and exported archives

When you export archives to PST files, a configuration file is automatically created for each PST file. This configuration file contains information that is needed if you intend to import the PST file contents back into Enterprise Vault, including the following:

- The retention category that was applied to all the items in the PST file.
- The Vault ID, which is needed to correct the shortcuts that the move has broken.

At the bottom of the configuration file there is a section called [RETENTION_CATEGORY] that shows details of the retention category that applies to all the items in the corresponding PST file. The [RETENTION_CATEGORY] section is present only if they were exported with **Split PST files by retention category** selected in the Export Archive wizard. When you import, the wizard tries to match the existing retention categories to the ones in the PST configuration file. If the section is not present, there is no way to determine the original retention category of the items.

Example PST configuration file with an exported archive

This example configuration file shows that the retention category Personal was used when all the items in `JohnSmith_Export_0001.pst` were archived.

```
[PST]
FILENAME = JohnSmith_Export_0001.pst
DESCRIPTION = John Smith
```

```
CREATED = 22Aug2002 10:01 AM
ORIGIN = EXPORT_ARCHIVE
[MAILBOX]
NAME = John Smith
MAILBOXDN = /O=ACME/OU=LEGAL/CN=RECIPIENTS/CN=JOHNS
EXCHANGESERVER = EXCH01
[USER]
FIRSTNAME = John
LASTNAME = Smith
DEPT = Legal
TITLE = Audit Manager
[VAULT]
NAME = John Smith
DESCRIPTION = Created by Enable Mailbox Wizard
VAULTID =
19A33926632EA274B9822FDBCA82CA09B1110000laguna3.win.kvsinc.com
VAULTSTORENAME = CCV4VS
[RETENTION_CATEGORY]
NAME = Personal
DESCRIPTION = Personal items
PERIOD = 60
PERIODUNITS = MONTHS
```

It is possible that the retention category does not match any retention category in your Enterprise Vault site. In this case you must decide on a suitable action, as follows:

- You can use an existing retention category that most closely matches the retention category in the configuration file.
- You can create a new retention category to match the one in the configuration file. However, this new retention category is then available to all users and you may find that its name is likely to confuse existing users.

Starting the export with the Export Archive wizard

When you are ready to export archived items to PST files or mailboxes, follow the instructions below to start the Export Archive wizard.

To start the export

- 1** In the left-hand pane of the Administration Console, right-click the **Archives** icon.
- 2** On the shortcut menu, click **Export**.
- 3** Work through the Export Archive wizard to complete the export.

Enterprise Vault message queues

This chapter includes the following topics:

- [Accessing Enterprise Vault message queues](#)
- [MSMQ queue summary](#)
- [Exchange Mailbox task queues](#)
- [Exchange Journaling task queues](#)
- [Exchange Public Folder task queues](#)
- [Retrieval queues](#)
- [Storage service queues](#)

Accessing Enterprise Vault message queues

Enterprise Vault uses Microsoft Message Queue (MSMQ) Server to transfer information between Enterprise Vault components.

You must clear all Enterprise Vault queues before you carry out any Microsoft Exchange maintenance. If you check or repair the Microsoft Exchange database when an Exchange Mailbox task still has work outstanding, that work cannot be done.

Normally you should allow the Enterprise Vault tasks and services to clear message queues. If there is a significant build-up of messages on particular queues, it is important to investigate the cause of the problem. In certain circumstances support may advise you to clear specific message queues manually.

To access the message queues

- 1 If you have yet to install Message Queuing, see the Windows documentation for instructions on how do so with the **Add or Remove Programs** applet in Control Panel.
- 2 In Control Panel, first click **Administrative Tools** and then click **Computer Management**.
- 3 In the left pane of the Computer Management console, first expand **Services and Applications**, then expand **Message Queuing**, and finally expand **Private Queues**.

MSMQ queue summary

[Table 21-1](#) gives a brief description of what goes on to each of the Enterprise Vault queues. Here, *server* is the name of the server that the Exchange Mailbox task is processing, and *queue* is a number that uniquely identifies the queue.

Table 21-1 Summary of MSMQ queues

Queue name	Contains information about
Enterprise Vault Exchange Mailbox task for <i>server queue A1</i>	Pending items to update. Also failed operations.
Enterprise Vault Exchange Mailbox task for <i>server queue A2</i>	Individual items to process. Used for manual archive requests and whenever Enterprise Vault cannot directly communicate with the Storage Archive queue of the Storage service.
Enterprise Vault Exchange Mailbox task for <i>server queue A3</i>	Mailboxes to process. Used if you start archiving using the Run Now option in the Administration Console.
Enterprise Vault Exchange Mailbox task for <i>server queue A4</i>	Individual items to process. Only used for retries when Enterprise Vault cannot directly communicate with the Storage Archive queue of the Storage service.
Enterprise Vault Exchange Mailbox task for <i>server queue A5</i>	Mailboxes to process. Used during scheduled archive runs. This queue is not processed outside the scheduled archiving times, so you cannot use Run Now to clear a backlog on this queue.

Table 21-1 Summary of MSMQ queues (*continued*)

Queue name	Contains information about
Enterprise Vault Exchange Mailbox task for <i>server queue A6</i>	<p>Requests to update folders with items that have been moved inside a mailbox.</p> <p>Enterprise Vault compresses the moved and copied item data that is placed in requests on queue A6. It also limits message storage on this queue to 100 MB. A compressed request to update 1,000 items occupies approximately 50 KB. So, about 2,000 requests can be placed on the queue.</p> <p>When the queue is full, further requests are rejected. These moved and copied items have to wait for another shortcut processing run.</p>
Enterprise Vault Exchange Mailbox task for <i>server queue A7</i>	Synchronization requests.
Enterprise Vault Journaling task for <i>server queue J1</i>	Pending items to update. Also failed operations.
Enterprise Vault Journaling task for <i>server queue J2</i>	Items to process.
Enterprise Vault Journaling task for <i>server queue J3</i>	Instructs the Exchange Journaling task to examine the journal mailbox for new messages. Up to 500 new messages are marked as archive pending, and a message is placed on queue J2 for each such message.
Enterprise Vault Journaling task for <i>server queue J4</i>	Synchronization requests.
Enterprise Vault Public Folder task for <i>server queue P1</i>	Pending items to update. Also failed operations.
Enterprise Vault Public Folder task for <i>server queue P3</i>	Folders to process. Used if you start archiving using the Run Now option in the Administration Console.
Enterprise Vault Public Folder task for <i>server queue P5</i>	<p>Folders to process. Used during scheduled archive runs.</p> <p>This queue is not processed outside the scheduled archiving times, so you cannot use Run Now to clear a backlog on this queue.</p>
Enterprise Vault Exchange Mailbox task for <i>server queue R1</i>	Notifications of item retrieval requests.

Table 21-1 Summary of MSMQ queues (*continued*)

Queue name	Contains information about
Enterprise Vault Exchange Mailbox task for <i>server queue R2</i>	Retrieval requests.
Enterprise Vault restore spool admin queue	Items that the Storage service has retrieved and that are now ready for the Exchange Mailbox task to process (for retrieval).
Enterprise Vault storage archive for <i>server</i>	Items to be stored in vault stores.
Enterprise Vault storage restore for <i>server</i>	Items to be retrieved from vault stores.

Exchange Mailbox task queues

[Table 21-2](#) describes the queues that the Exchange Mailbox task uses. Here, *server* is the name of the server that the Exchange Mailbox task is managing, and *queue* is a number that uniquely identifies the queue.

Table 21-2 Exchange Mailbox task queues

Queue name	Messages placed on the queue
Enterprise Vault Exchange Mailbox task for <i>server queue A1</i>	Update Shortcut, Operation Failed.
Enterprise Vault Exchange Mailbox task for <i>server queue A2</i>	Process Item (Explicit Archives).
Enterprise Vault Exchange Mailbox task for <i>server queue A3</i>	Process Mailbox, Process System (Run Now), Check System, Check Mailbox.
Enterprise Vault Exchange Mailbox task for <i>server queue A4</i>	Only used for retries where Enterprise Vault cannot communicate directly with the Storage Archive queue.
Enterprise Vault Exchange Mailbox task for <i>server queue A5</i>	Process Mailbox, Process System (Schedule only).
Enterprise Vault Exchange Mailbox task for <i>server queue A6</i>	Process Moved Items in Folder.
Enterprise Vault Exchange Mailbox task for <i>server queue A7</i>	Synchronization requests.

Table 21-3 provides more information on the messages that the Exchange Mailbox task may place in queues A1 through A7.

Table 21-3 Messages in the Exchange Mailbox task queues

Message	Notes
Operation Failed	Informs the Exchange Mailbox task that an error has occurred and that it should change the message from archive pending back into a message. The message is reprocessed later. This message is sent if an error occurs during archiving and storage.
Process Item	<p>Asks the Exchange Mailbox task to archive a specific message from the Exchange server to the Storage service. The item in Exchange is turned into a shortcut when the storage returns an Update Shortcut message.</p> <p>Process Item messages are produced by a user explicitly archiving an item (placed on A2) or by retry requests for items that failed during normal processing. Retry requests from Run Now are placed on the A2 queue, whereas those from scheduled archiving are placed on the A4 queue.</p>
Process Mailbox	Asks the Exchange Mailbox task to examine a mailbox and find any messages that match the archiving criteria. The items are placed on the Storage Archive queue for storage processing.
Process Moved Items in Folder	<p>Asks the Exchange Mailbox task to update the items that have been moved or copied to the specified folder.</p> <p>Process Moved Items in Folder messages are only placed on queue A6.</p>
Process System	<p>Asks the Exchange Mailbox task to determine which mailboxes on the Exchange server are eligible for archiving. The Exchange Mailbox task reads the list of all provisioned mailboxes and sends a Process Mailbox message (on the same queue) for each mailbox.</p> <p>A Process System message is placed immediately on queue A3 if the administrator selects Run Now from the task properties, or it is placed on queue A5 at the start of a scheduled archive period (provided that there are no other Process System messages that are already waiting to be done).</p>

Table 21-3 Messages in the Exchange Mailbox task queues (*continued*)

Message	Notes
Synchronize System	<p>Synchronization requests for an Exchange Mailbox task are placed on the A7 queue. When synchronization is run, a Synchronize System request is placed on this queue. This generates a Synchronize Mailbox request for each mailbox that needs to be synchronized. Having multiple Synchronize Mailbox requests means that multiple threads can service the requests.</p> <p>The A7 queue is processed at all times but is always the lowest priority task. This means that scheduled background archives always take precedence over synchronization requests.</p>
Update Shortcut	<p>Notifies the Exchange Mailbox task that it can turn an archive pending item into a shortcut. It occurs after a message has been stored by the Storage service, and backed up.</p>

Notes on the Exchange Mailbox task queues

- Each queue has a suffix of *Apriority number*, where A1 is the highest priority. The message queues are treated as FIFO (First In, First Out), and new messages are always added to the end of the queue.
- The Exchange Mailbox task processes the queues in order of priority. The task scans through each queue, starting with the highest priority. If it finds a message on a queue, it processes the message and then starts the scan again from the highest priority queue. Therefore, queues A2 through A7 are not processed until queue A1 is empty. When A1 is empty, A2 requests are processed before A3 requests.
However, queues A4 and A5 are special queues that are used by the archiving schedule only. The Exchange Mailbox task processes messages on the A5 queue only during a scheduled archive period. Outside the scheduled periods, messages on these queues are ignored until the next schedule period.
- Using performance monitor, you can monitor the changes in the queues to assess the progress of the task.
For example, at the start of a scheduled period, the number of messages on queue A5 rises (to the number of enabled mailboxes on the Exchange server). These are Process Mailbox messages. The Exchange Mailbox task takes the first message off queue A5, finds all the eligible messages in the mailbox, and changes them to archive pending. A Process Item message is then placed on

the Storage Archive queue of the Storage service for each message to be archived.

- After the vault store has been backed up, Update Shortcut messages are placed on queue A1. The messages are processed immediately because the queue has a higher priority.
- Queue A3 performs the same function as queue A5, but for an immediate process system. This queue also performs shortcut expiry and deletion. Explicit user archives from the Outlook client extension are placed on queue A2.
- Queue A5 is only processed during a scheduled period, but queues A1 through A3, A6, and A7 are always processed. If a queue has not been processed for more than 10 minutes, and there are no messages in a higher priority queue, there may be a problem with the task. Check the Enterprise Vault event log on the Exchange Mailbox task computer for any additional information.
- Monitoring queue A1 indicates that a backup has correctly updated shortcuts. However, if A1 is being used during normal use (before a backup), this may indicate a problem with tasks. Check the Enterprise Vault event log for errors.

Exchange Journaling task queues

Table 21-4 describes the queues that the Exchange Journaling task uses. Here, *server* is the name of the server that the Exchange Journaling task is managing, whereas *queue* is a number that uniquely identifies the queue.

Table 21-4 Exchange Journaling task queues

Queue name	Messages placed on the queue
Enterprise Vault Journaling task for <i>server queue J1</i>	Post Process Archived Item, Operation Failed.
Enterprise Vault Journaling task for <i>server queue J2</i>	Process Item.
Enterprise Vault Journaling task for <i>server queue J3</i>	Process Mailbox.
Enterprise Vault Journaling task for <i>server queue J4</i>	Synchronize System.

Table 21-5 provides more information on the messages that the Exchange Journaling task may place in queues J1 through J4.

Table 21-5 Messages in the Exchange Journaling task queues

Message	Notes
Operation Failed	<p>Notifies the Exchange Journaling task that an error has occurred and that it should do the following:</p> <ul style="list-style-type: none">Change the message from archive pending back into a message. The message is reprocessed later.Move the message to the Failed to Store folder. <p>This message is sent if an error occurs during archiving and storage.</p>
Post Process Archived Item	<p>Notifies the Exchange Journaling task to delete an archive pending item from the journal mailbox. It occurs after a message has been stored by the Storage service, and backed-up.</p>
Process Mailbox	<p>Asks the Exchange Journaling task to examine the journal mailbox, finding any messages that have arrived. Up to 500 new messages are turned into archive pending, and a message is placed on the Storage Archive queue of the Storage service for each message to be archived.</p> <p>The process mailbox message is issued every minute onto queue J3. This allows for continuous scanning of the journal mailbox while the Journaling task is running.</p>
Synchronize System	<p>Synchronization requests for an Exchange Journaling task are placed on the J4 queue. When synchronization is run, a Synchronize System request is placed on this queue. This generates a Synchronize Mailbox request for each mailbox that needs to be synchronized. Having multiple Synchronize Mailbox requests means that multiple threads can service the requests.</p> <p>The J4 queue is processed at all times but is always the lowest priority task. This means that scheduled background archives always take precedence over synchronization requests.</p>

Notes on the Exchange Journaling task queues

- Each queue has a suffix of *Jpriority number*, where J1 is the highest priority. The message queues are treated as FIFO (First In, First Out), and new messages are always added to the end of the queue.

- An Exchange Journaling task processes the queues in order of priority. The task scans through each queue, starting with the highest priority. If it finds a message on a queue, it processes the message and then starts the scan again from the highest priority queue. Therefore, if there are messages on queue J1, queue J2 and J3 are not processed until queue J1 is empty.
- Monitoring queue J1 will indicate that a vault store backup is correctly deleting the messages. However, if J1 is being used during normal use (before a backup), this may indicate a problem with tasks. Check the Enterprise Vault event log for errors.
- Monitoring queue J3 will indicate that at least every minute a process mailbox message is on the queue (a new message will only be added if the queue is empty). There should never be more than one message on this queue. The message should appear on the queue and then disappear as soon as queue J1 is clear. Any new messages in the journal mailbox will be processed.
- If a queue has not been processed for more than 10 minutes, and there are no messages in a higher priority queue, there may be a problem with the tasks. Check the Enterprise Vault event log on the Exchange Journaling task computer for any additional information.

Exchange Public Folder task queues

[Table 21-6](#) describes the queues that each Exchange Public Folder task uses. Here, *server* is the name of the server that the Public Folder task is managing, whereas *queue* is a number that uniquely identifies the queue.

Table 21-6 Exchange Public Folder task queues

Queue name	Messages placed on the queue
Enterprise Vault Public Folder task for <i>server queue</i> P1	Update Shortcut, Operation Failed.
Enterprise Vault Public Folder task for <i>server queue</i> P3	Process Folder, Process Folders (Run Now), Check Folders, Check Folder.
Enterprise Vault Public Folder task for <i>server queue</i> P5	Process Folder, Process Folders (Schedule only).

Note that Enterprise Vault has not used queues P2 and P4 since version 3.6.

[Table 21-7](#) provides more information on the messages that the Exchange Public Folder task may place in queues P1, P3, and P5.

Table 21-7 Messages in the Exchange Public Folder task queues

Message	Notes
Operation Failed	Informs the Exchange Public Folder task that an error has occurred and that it should change the message from archive pending back into a message. The message is reprocessed later. This message is sent if an error occurs during archiving and storage.
Process Folder	Asks the Exchange Public Folder task to examine a specific folder and find any messages that match the archiving criteria. These messages are then turned into archive pending, and a message is placed on the process item queue for each message to be archived.
Process Folders	<p>Asks the Exchange Public Folder task to determine which folders on the Exchange Server are eligible for archiving. The Exchange Public Folder task reads the list of all the public folders that are hosted on the Exchange server and sends a Process Folder message (on the same queue) for each top-level folder that is eligible.</p> <p>Process Folders messages are placed immediately on queue P3 if the administrator selects Run Now from the task properties, or it is placed on queue P5 at the start of a scheduled archive period (provided that there are no other process folders messages already waiting to be done).</p>
Update Shortcut	Instructs the Exchange Public Folder task to turn an archive pending item into a shortcut. It occurs after a message has been stored by the Storage service, and backed up.

Notes on the Exchange Public Folder task queues

- Each queue has a suffix of *Ppriority number*, where P1 is the highest priority. The message queues are treated as FIFO (First In, First Out), and new messages are always added to the end of the queue.
- The Exchange Public Folder task processes the queues in order of priority. The task scans through each queue, starting with the highest priority. If it finds a message on a queue, it processes the message and then starts the scan again from the highest priority queue. Therefore, if there are messages on queue P1, the other queues are not processed until queue P1 is empty.

However, the P5 queue is a special queue only used during the public folder archiving schedule. The Exchange Public Folder task processes only messages on queue P5 during a scheduled archive period. Outside of the schedule, any messages on these queues are ignored.

- Queue P3 performs the same function as queue P5, but for an administrator Run Now. This queue also performs shortcut expiry and deletion.
- Queue P5 is only processed during a scheduled period, but queues P1 and P3 are always processed. If a queue has not been processed for more than 10 minutes, and there are no messages in a higher priority queue, there may be a problem with the task. Check the Enterprise Vault event log on the Exchange Public Folder task computer for any additional information.
- Monitoring queue P1 will indicate that a backup has correctly updated shortcuts. However, if P1 is being used during normal use (before a backup), it may indicate a problem with tasks. Check the Enterprise Vault event log for errors.

Retrieval queues

[Table 21-8](#) describes the queues with which the Exchange Mailbox task carries out retrieval. Here, *server* is the name of the server that the Exchange Mailbox task is processing, whereas *queue* is a number that uniquely identifies the queue.

Table 21-8 Retrieval queues

Queue name	Messages placed on the queue
Enterprise Vault Exchange Mailbox task for <i>server queue</i> R1	Item Ready, Operation Failed.
Enterprise Vault Exchange Mailbox task for <i>server queue</i> R2	Restore Item, Update Basket.
Enterprise Vault Storage Spool	Message content. The messages on this queue are items restored from the Storage service. The Exchange Mailbox task reads the messages as it processes the queue R1.

[Table 21-9](#) provides more information on the messages that the Exchange Mailbox task may place in queues R1 and R2 when it carries out retrieval.

Table 21-9 Messages in the Retrieval queues

Message	Notes
Item Ready	This message informs the Exchange Mailbox task that a previously requested message is now available on the storage spool queue. The Exchange Mailbox task collects the message from the storage spool queue and places it into the mailbox. The Storage service generates these messages as required.
Operation Failed	This message informs the Exchange Mailbox task there was a problem restoring the message. If the retrieval was started from the web application, the Exchange Mailbox task updates the basket to indicate the item was not restored.
Restore Item	This message is a request to restore an item from the Storage service back into Exchange Server. The Exchange Mailbox task prompts for the message from the Storage service and places it into the mailbox. Messages are placed on this queue from both the user extension and the web page restore functions.
Update Basket	<p>When a restore succeeds or fails, the retrieval task tries to update the shopping basket directly. If this fails, the retrieval task posts an Update Basket request so that it is tried again.</p> <p>This message instructs the Exchange Mailbox task to update a web basket with the successful restoration of an item.</p>

Notes on the retrieval queues

- Each queue has a suffix of *Rpriority_number*, where R1 is the higher priority. The message queues are treated as FIFO (First In, First Out), and new messages are always added to the end of the queue.
- The Exchange Mailbox task processes the queues in order of priority. The task scans through each queue, starting with the highest priority. If it finds a message on a queue, it processes the message and then starts the scan again from the highest priority queue. Therefore, if there are messages on queue R1, queue R2 is not processed until queue R1 is empty.
- If a queue has not been processed for more than 10 minutes, and there are no messages in a higher priority queue, there may be a problem with the task.

Check the Enterprise Vault event log on the Exchange Mailbox task computer for any additional information.

Storage service queues

[Table 21-10](#) describes the queues that the Storage service uses.

Table 21-10 Storage service queues

Queue name	Messages placed on the queue
Enterprise Vault storage archive	Store Item.
Enterprise Vault storage restore	Restore an Item.

[Table 21-11](#) provides more information on the messages that the Storage service may place in the queues.

Table 21-11 Messages in the Storage service queues

Message	Notes
Restore an Item	The Exchange Mailbox task places a message in the Storage Restore queue, requesting an item to be restored from an archive. When the Storage service has located the item, it places it in the Storage Spool queue and notifies the Exchange Mailbox task on queue R1.
Store Item	<p>The Exchange Mailbox task places a compressed email message on the Storage Archive queue, to be stored in an archive. If the compressed message is larger than 4 MB, it is divided into 4-MB chunks (each labeled with a part number, such as "Part 1 of 5"). The message is reconstructed by the Storage service before storing.</p> <p>The Exchange Mailbox task places all emails to be stored onto the appropriate Storage service archive queue. Multiple Storage services may be configured, so the Exchange Mailbox task must select the correct Storage service for the vault store in which the archive resides.</p>

Notes on the Storage service queues

- Monitoring the storage archive queue will indicate the Storage service is processing items. If the number of items in this queue does not change for at least 30 minutes, there is likely to be a problem. Check the Enterprise Vault event log on the storage computer for any errors and, if necessary, restart the Storage service.
- When all the vault stores on an Enterprise Vault server are in backup mode, the Storage Archive queue is not processed.
- Monitoring the restore queue will indicate the number of restores required by the users. Again, if the number of items on the queue does not change, there is likely to be a problem.

Customizations and best practice

This chapter includes the following topics:

- [Mailbox archiving strategies](#)
- [Public folder archiving best practice](#)
- [About performance tuning](#)

Mailbox archiving strategies

This section covers the following:

- [About mailbox archiving strategies](#)
- [Notes on archiving based on age](#)
- [Notes on archiving based on quota or age and quota](#)
- [Notes on archiving items from Exchange managed folders](#)
- [Archiving items only if they have attachments](#)
- [How to customize the Enterprise Vault settings for a journal mailbox](#)
- [Disabling archiving for mailboxes](#)

About mailbox archiving strategies

You define an archiving strategy for a mailbox policy on the **Archiving Rules** tab. 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.
The age of a mail message is taken from the date when it was received or sent. The age of a document is taken from the date when it was last modified.
- **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 based on age and archiving based on quota or age and quota are the main strategies for selection of items to archive. You can also configure the policy so that Enterprise Vault archives large items first. Archiving large items first operates in addition to the main archiving strategy. Archiving large items first has the following advantages:

- Initial archiving performance is improved.
- Mailbox space is recovered by archiving relatively few items.

You can also select the following options:

- Items younger than an age that you specify are never archived.
- Only messages with attachments are archived.

Notes on archiving based on age

Archiving based on age is the default archiving strategy.

When you configure archiving based on age, the following recommendations apply:

- Consider a policy that uses the setting "Start with items larger than" so that archiving has the greatest benefits early on.
- Larger, less frequent runs make backups easier. For example, it is easier to do one large run on Friday and then a full backup of the Enterprise Vault system than daily archives and backups.

Notes on archiving based on quota or age and quota

You can choose archiving based on quota on its own, or as part of the archiving by age and quota option. The same configuration and best practice considerations apply.

You need to decide first whether you need to base archiving on quota. The default strategy of archiving based on age is more efficient, and avoids the possibility of archiving too many items.

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.

Enterprise Vault calculates the amount of data it needs to archive to achieve the quota percentage target. It bases the calculation on estimates of the size of shortcuts. The estimates take account of any items that already have a status of pending archive. For information about how the estimates are calculated, see the following TechNote on the Enterprise Vault Support website:

<http://www.veritas.com/docs/000035815>

You can use the following registry values to override the values that Enterprise Vault uses in the shortcut size estimates:

- ShortcutCalcAverageBodySize
- ShortcutCalcBannerSize
- ShortcutCalcBaseItemSize
- ShortcutCalcBodySizeMultiplier
- ShortcutCalcOverride
- ShortcutCalcRecipientSize

See *Enterprise Vault Registry Values*.

See [“Recommendations for quota-based archiving”](#) on page 330.

Recommendations for quota-based archiving

When you configure archiving based on quota, or on age and quota, consider the recommendations given here. These recommendations help you to avoid setting the quota percentage too high for your Enterprise Vault configuration. If the quota percentage is too high, Enterprise Vault may archive too many items as it tries to achieve the quota target.

The recommendations are as follows:

- Review your shortcut settings and consider using smaller shortcuts. With smaller shortcuts, Enterprise Vault saves more space in a mailbox for each item that it archives. The result is that Enterprise Vault needs to archive fewer items to achieve the percentage of free space that you require.
If you use large shortcuts when the average item is small, Enterprise Vault saves less space for each item that it archives.

To find out the average shortcut size, run the Exchange Mailbox Archiving task in **Report** run mode.

You specify the settings that determine what information is left in a shortcut on the mailbox policy **Shortcut Content** tab.

- Consider making shortcuts expire earlier. When shortcuts expire earlier, you save mailbox space and avoid archiving too many items. You set the age at which Enterprise Vault deletes shortcuts on the mailbox policy **Shortcut Deletion** tab.
- Specify that Enterprise Vault starts by archiving large items. Enterprise Vault then archives items that use the most mailbox space first.
- Start with a low quota percentage, and increase it gradually until you get the results you require.
- Make sure that there is enough archiving each night so that users have sufficient space for the following day.
- Check the mailbox policy Advanced settings **Archive deleted items** and **Archive Exchange Managed Folders**.

Items in the Deleted Items folder are included in the Exchange Server mailbox storage limit calculation. By default Enterprise Vault does not archive items from the Deleted Items folder. So items in the Deleted Items folder can prevent Enterprise Vault from reaching the quota percentage target.

Managed folders are also included in the Exchange Server mailbox storage limit calculation. By default Enterprise Vault archives from managed folders, but you can configure it so that it does not archive from managed folders. In this case, Enterprise Vault may not be able to achieve the quota percentage target.

- Check the mailbox policy Advanced setting **Strip attachments to non-shortcut items**. By default, Enterprise Vault removes attachments from calendar, meeting, task, and contact items after it archives these items. If attachments are not removed from these items, then archiving them does not save space in the mailbox.

Further points to note are as follows:

- If no Microsoft Exchange storage limit applies to a mailbox, Enterprise Vault cannot process the mailbox with quota-based archiving.
- In Exchange, you can specify the maximum space that a mailbox can occupy before the user is prohibited from sending or receiving messages. If you archive by quota and this storage limit has been exceeded, then Enterprise Vault cannot process the mailbox with quota-based archiving.

The solution is to remove or raise the limit, archive until a suitable storage level is reached, and then reimpose the limit if necessary. Enterprise Vault normally keeps users within quota, so you may decide to remove the limit.

Notes on configuring archiving based on age and quota with a script

You can use an Enterprise Vault Policy Manager script to configure your archiving strategy for a mailbox.

For information about Policy Manager, see the *Utilities Guide*.

An example script is shown here. This script applies settings for archiving based on age and quota to a mailbox. It also configures a special folder to override the mailbox-level settings.

The first part of the script configures the mailbox as follows:

- Archive items that are older than three months.
- Archive items that are larger than 4 MB immediately.
- If necessary, continue quota-based archiving until 30% of the mailbox storage limit is free. Quota-based archiving starts with any items that are larger than 1 MB and more than one day old.
- Create shortcuts, and delete the original items.

The second part of the script configures a mailbox folder that is named `\Inbox\Special Project` as follows:

- Archive items that are older than 0 days.
- Do not create shortcuts, and delete the original items.

You might want to configure a special folder as shown here as an alternative to manual archiving. Users can move items into the folder, and Enterprise Vault automatically archives the items soon afterwards.

The example script is as follows:

```
[directory]
directorycomputername=evserver
sitename=evsite

[mailbox]
distinguishedname=/o=First Organization/ou=First Administrative Group/
cn=Recipients/cn=recipient_1

; Using Age & Quota based archiving
;
[filter]
name=AGEANDQUOTA
```

```
; Quota settings
; Archive to 30% of quota is available
; Start with large items >1MB that are more than 1 day old
UsePercentageQuota=true
PercentageQuota=30
UseInactivityPeriod=true
QMinimumAgeThresholdPeriod=1
QMinimumAgeThresholdUnits=Days
QPrioritizeItemsOver=1024
QPrioritizeLargeItems=true

; Age settings
; Archive all items older than 3 months
; Archive all items >4MB immediately.
UseInactivityPeriod=true
InactivityPeriod=3
InactivityUnits=Months
ALargeItemThresholdPeriod=0
ALargeItemThresholdUnits=Days
APrioritizeItemsOver=4096
APrioritizeLargeItems=true

; Create shortcuts and delete the original item
;
CreateShortcut=true
DeleteOriginal=true

; Do not archive unread items
Unreadmail=false

; Special case zero day folder to override Age & Quota settings
;
[filter]
name=ZeroDaysNoShortcut

; Archive Items after 0 days, delete the original and
; do not leave a shortcut
;
UseInactivityPeriod=true
UsePercentageQuota=false
InactivityPeriod=0
InactivityUnits=Days
CreateShortcut=false
```

```
DeleteOriginal=true
Unreadmail=true

; Set the mailbox to use Age & Quota based archiving as
; defined in the policy above
;
[folder]
name=MailboxRoot
filtername=AGEANDQUOTA
Overridearchivelocks=true

; Apply the ZeroDaysNoShortcut policy to a special project folder
;
[folder]
name=\Inbox\Special Project
filtername=ZeroDaysNoShortcut
Overridearchivelocks=true
```

Notes on archiving items from Exchange managed folders

Caution: The following information applies only to managed folders and not to the messaging records management (MRM) features that replace managed folders in later versions of Exchange Server. When archiving from Exchange Server 2007, which supports managed folders, the following information applies. When archiving from Exchange Server 2010, which supports both the newer MRM features and managed folders, the following information applies only to the latter. When archiving from Exchange Server 2013, which does not support managed folders, the following information does not apply.

Exchange Server 2007 and 2010 let you set up Exchange managed folders and apply managed content settings to them. The managed content settings let you control the retention of items of the specified message class.

Enterprise Vault can apply special retention categories to items that it archives from managed folders. These managed folder retention categories are based on settings that are synchronized from Exchange managed content settings. Managed folder retention categories are created and updated automatically. They have a different icon and different properties from normal retention categories. You can change the name and description of a managed folder retention category, but not its retention period. Synchronization with Exchange managed content settings prevents Enterprise Vault managed folder retention category settings from conflicting with the managed content settings.

For example, the managed content settings may specify that items in the managed folder are deleted after 180 days. If synchronization with managed content settings is active, Enterprise Vault automatically creates a managed folder retention category. Enterprise Vault gives the managed folder retention category the same name as the managed content settings. Enterprise Vault sets the retention period so that archived items expire at the same time that they are due to expire from Exchange.

In the Enterprise Vault Exchange mailbox policy, the advanced setting **Archive Exchange Managed Folders** controls whether Enterprise Vault archives items from managed folders.

The possible values of **Archive Exchange Managed Folders** are as follows:

Off	Enterprise Vault does not archive items from managed folders. Users cannot archive items manually from managed folders.
Normal	<p>Enterprise Vault treats managed folders in the same way as any other folder.</p> <p>The value Normal lets users modify the contents of managed folders in Virtual Vault, provided the Virtual Vault policy settings allow such operations. For example, users can move items as follows:</p> <ul style="list-style-type: none">■ From the mailbox to a managed folder in Virtual Vault■ From a managed folder in Virtual Vault to another Virtual Vault folder
Managed	Default value. Enterprise Vault archives items from managed folders and uses managed folder retention category settings that are synchronized from Exchange.

The Enterprise Vault Exchange Provisioning task performs the synchronization with Exchange managed content settings. Synchronization is automatic when there is an Exchange 2013 or 2010 server in the domain. So the Exchange Provisioning task performs synchronization and creates managed folder retention categories even if you have not set **Archive Exchange Managed Folders** to Managed.

If synchronization fails, it causes the entire Provisioning task to fail. To prevent synchronization, you can place a configuration file in the Enterprise Vault server installation folder.

See [“Preventing synchronization with Exchange managed folders”](#) on page 338.

When archiving from managed folders is active, users of the Enterprise Vault Outlook Add-In in full mode see the following:

- They cannot specify a retention category or an archive when they archive items manually from managed folders.
- The Enterprise Vault tab in the folder properties does not include the **Change** option.
- Enterprise Vault always creates shortcuts and deletes the original items.

Enterprise Vault auditing records details of creation, modification, and deletion of Exchange managed content settings.

Requirements for synchronized archiving from Exchange managed folders

To archive items from an Exchange managed folder and synchronize managed content settings with a managed folder retention category, all the following conditions must apply:

- In the Enterprise Vault Exchange mailbox policy, the advanced setting **Archive Exchange Managed Folders** must be set to **Managed**.
- The item's message class must match the **Message type** setting in one set of managed content settings that are defined for the managed folder. (In Exchange, you can define multiple sets of managed content settings for a single managed folder. Each set of managed content settings can specify a different message type.)
- The managed content settings must define the action to take at the end of the retention period as **Delete and Allow Recovery** or **Permanently Delete**.
- The Enterprise Vault filter that applies to the managed folder must be the system default.
See "[Setting the system default filter on Exchange managed folders](#)" on page 336.
- The Vault Service account must have the Exchange View-Only Administrator role assigned to it. For details of how to assign this role, see *Installing and Configuring Enterprise Vault*.

Setting the system default filter on Exchange managed folders

One requirement for synchronizing managed content settings is that the Enterprise Vault filter applied to the managed folder must be set to **Use the system default**. If the filter on a managed folder is set to **Use custom settings**, Enterprise Vault does not apply managed content settings.

Custom settings on a managed folder may be inherited, or set with Enterprise Vault Policy Manager.

If necessary, you can use the PowerShell cmdlet `Remove-EVExchangeFolderPolicy` to remove all existing custom settings from managed folders. You can then use Policy Manager to set managed folders to use the system default filter.

For information about Policy Manager, see the *Utilities Guide*.

To remove Policy Manager policies from managed folders

- 1 Start the Enterprise Vault Management Shell.
- 2 In the Enterprise Vault Management Shell window, enter the following command if you want to see detailed Help for `Remove-EVExchangeFolderPolicy`:

```
Get-Help Remove-EVExchangeFolderPolicy -detailed
```

- 3 Enter the `Remove-EVExchangeFolderPolicy` command with the required parameters.

For example:

- To remove any Enterprise Vault filter settings from managed folders in a mailbox, enter the following command:

```
Remove-EVExchangeFolderPolicy -PrimarySMTPAddress  
user_name@domain -ManagedFolders
```

where `user_name@domain` is the name of the mailbox.

- You can run the following script to remove any Enterprise Vault filter settings from managed folders in all mailboxes on a specified Exchange 2013 or 2010 server.

Run the script in the Enterprise Vault Management Shell window.

```
$Session = New-PSSession -ConfigurationName Microsoft.Exchange  
-ConnectionUri http://Exchange_server/PowerShell/  
-Authentication Kerberos -Credential Exchange_administrator
```

```
Import-PSSession $Session -CommandName Get-Mailbox
```

```
$UserList = Get-Mailbox |  
where-object{$_ .ServerName -like "Exchange_server"}  
foreach($Entry in $UserList)  
{ $Address = $Entry.PrimarySMTPAddress;  
Remove-EVExchangeFolderPolicy -PrimarySMTPAddress $Address }
```

where `Exchange_server` is the name of the Exchange server, and `Exchange_administrator` the name of the Exchange administrator account.

To set a managed folder to use the system default filter

- 1 Create a Policy Manager initialization file that contains the following [Folder] section:

```
[Folder]
NAME=\Managed Folders\managed_folder
filtername = systemdefault
overridearchivelocks=true
```

where *managed_folder* is the name of the managed folder that you want to use the system default filter.

- 2 Run Policy Manager with the initialization file.

Preventing synchronization with Exchange managed folders

The Enterprise Vault Exchange Provisioning task performs synchronization with managed folders. The task checks for Exchange 2013 and 2010 servers in the domain. The task also checks for new managed folders, and for new or changed managed content settings in existing managed folders.

You can prevent the Exchange Provisioning task from synchronizing with managed folders by using a configuration file in the Enterprise Vault server installation folder.

The configuration file setting that is described in this section only prevents synchronization with managed folders and their managed content settings. Enterprise Vault does not create new managed folder retention categories, or update existing managed folder retention categories. Archiving from managed folders continues if the necessary conditions apply.

You may want to prevent or temporarily suspend synchronization in the following circumstances:

- You have problems with synchronization, possibly because permissions on the Exchange server are not set correctly.
- You do not require Enterprise Vault to synchronize managed content settings with managed folder retention categories.

To prevent synchronization with managed folders

- 1 In the Enterprise Vault installation folder, take a backup copy of the file, `EvExchangePolicySyncTask.exe.config`. The installation folder is typically `C:\Program Files (x86)\Enterprise Vault`.
- 2 Open the file with a text editor.

- 3 Add the following lines to the **<configuration>** section in the file:

```
<appSettings>  
    <add key="SkipManagedFolderSynch" value="true" />  
</appSettings>
```

- 4 Save and close the file.
- 5 The change will take effect the next time the Exchange Provisioning task runs.

Archiving items only if they have attachments

Enterprise Vault can be configured so that a mailbox or public folder item is archived only if the item has an attachment, assuming all other archiving criteria are met. This is not the same as archive attachments only.

The advantages of archiving only items with attachments are as follows:

- A significant performance improvement, since many fewer items are being archived.
- Fewer problems generally, because fewer items are being archived. For example, users open fewer archived items, there are fewer problems archiving items, and so on.
- Normally, using the "leave cover note text" option means Exchange store growth for messages without attachments. However, if you set this and also configure Enterprise Vault to archive items only if they have attachments, then Enterprise Vault leaves cover note text only for items that do have attachments. This means that there is always a space gain.

The disadvantages of archiving only items with attachments are as follows:

- You cannot use this method if you are archiving for legal reasons because you cannot be sure of what will be archived.
- Users will not be sure of where to find older items. Should they search in the mailbox or in Enterprise Vault?
- Such a policy may be harder for users to understand than a simple age-based one.

Note: If you decide to archive only items with attachments, consider having occasional archiving runs with it turned off and with an age-based policy of, say, two years. This ensures that any really old items are eventually archived, even though they have no attachments. This frees space in the Exchange database. You could do this using, for example, a simple, scheduled SQL script running once each month.

To enable archiving only items with attachments

- 1 Start the Administration Console.
- 2 In the left pane, expand the vault site.
- 3 Expand **Policies** and then **Exchange**.
- 4 Click the **Mailbox** container.
- 5 In the right pane, double-click the Exchange Mailbox Policy you want to modify.
- 6 Click the **Archiving Rules** tab.
- 7 Select **Archive messages with attachments only**.
- 8 Click **OK**.

How to customize the Enterprise Vault settings for a journal mailbox

You can customize the journal mailbox so that items are archived to different archives and with different retention categories.

By default, Enterprise Vault uses the same archive and retention category for every item that is archived from a journal mailbox. If this is not what you want, you can customize the journal mailbox and send items to different archives with different retention categories.

You can override the parent folder settings by changing the Enterprise Vault properties for a folder. If a folder contains other folders then, by default, those folders inherit the properties of the parent folder. However, you can change the settings for individual folders.

By default, all folders in the journal mailbox have the Enterprise Vault property Use Parent Folder Settings selected. This means that all folders inherit the same settings, retention category, and archive that are set up for the journal mailbox. Until you change the values for a particular folder, Enterprise Vault archives all items with the same retention category and stores them in the same archive.

To modify the settings, use Microsoft Outlook or Microsoft Exchange Client to do the following:

- Define rules to redirect mail to the appropriate folders within the journal mailbox. The Exchange Journaling task will then archive items from those folders.
- Set the mailbox and folder properties in the journal mailbox.

The journal mailbox is enabled with the following settings:

- Vault: from the Journal Mailbox Target properties
- Retention Category: from the Journal Mailbox Target properties

The following tables list the Enterprise Vault settings that you can change to modify the behavior of the Exchange Journaling task, together with those that the Exchange Journaling task ignores.

Table 22-1 Journal mailbox settings

Setting	Comment
Vault	Can be changed from the default.
Retention Category	Can be changed from the default.
Do not archive this folder	Ignored.
Archive items older than	Ignored (always 0 days).

Table 22-2 Journal mailbox folder settings

Setting	Comment
Vault	Overrides parent folder
Retention Category	Overrides parent folder
All other settings	Ignored (uses mailbox settings)

Table 22-3 Journal mailbox message settings

Setting	Comment
Do not archive this item	Ignored
Retention Category	Ignored (uses folder setting)

Disabling archiving for mailboxes

There may be occasions when you want to disable archiving for a mailbox. If you disable archiving for a mailbox, you can later enable it again at any time.

To disable archiving for one or more mailboxes

- 1 In the left pane of the Administration Console, expand **Enterprise Vault Servers**.
- 2 Expand the name of the computer that runs the Exchange Mailbox task.
- 3 Click **Tasks**.
- 4 In the right pane, click the Mailbox Archiving task.

- 5 On the **Tools** menu, click **Disable Mailboxes**.
- 6 When the Disable Mailbox wizard starts, follow the on-screen instructions to select the mailboxes that you want to disable.

Public folder archiving best practice

When setting up Public Folder archiving, consider the following:

- When you specify a public folder root path then, by default, all folders underneath that path are archived.
- If you want a setting to be applied to a whole section of a public folder tree, use Enterprise Vault Policy Manager.
- An Exchange Public Folder task takes its settings from the site that the Exchange Public Folder task is in and applies those settings to every folder under its root path.

If you change any archiving policy using Outlook, the change applies only to that folder, even if the folder is the root path.

So, for example, you could have three root paths archived under one site and you want to change the policy for one of those paths. You could use the Enterprise Vault folder properties in Outlook. However only that folder and not its subfolders will have the new archive policy. If you want to have folder policy inheritance you must use Policy Manager to set up the policy. Policy Manager will set the new policy on all subfolders.

- Any new public folder is archived using the site settings until you change the settings for that folder. The new folder does not inherit any settings from its parent.
For example, if you set a particular part of the public folder tree as Do Not Archive, any new folder created in there will archived until you change its settings. The same is true for a folder move.
To correct this you would run Policy Manager every day to ensure that the correct folder policies are being applied.
- If you use Policy Manager to apply settings to a folder and its subfolders, Policy Manager applies those settings to all folders underneath the folder you specify. So, for example, if there is a lower-level folder that has a different policy, you need to run Policy Manager to reapply the correct policy to the lower-level folder. For a complicated folder hierarchy you can may have a Policy Manager entry for each folder. To be safe you'd have a policy setting that archives only very old items, perhaps as old as 10 years. By doing this you turn off archiving for new folders that have not yet had a Policy Manager policy applied to them.

- "Default" access permissions are not applied to vaults. Thus, anyone accessing a shortcut in a Public Folder using the default permission cannot access archived items.
- It is best to make Enterprise Vault archive the home server for the public folder because this reduces complications of replication and bandwidth. However, this might mean that you need extra Enterprise Vault servers.
- If there is public folder replication then, when a user opens a shortcut, View Online goes to the vault server where the item is located.
- To view items, a user's mailbox must be enabled for Enterprise Vault archiving. Consider where users may be when viewing these archived items in Public Folders. Will those users have Enterprise Vault? Will their mailboxes be enabled?

About performance tuning

Knowing how well Enterprise Vault is performing helps you decide whether it is necessary to change the configuration by adding or moving components, or by modifying existing components.

Hierarchical Storage Management (HSM) software, if available, may provide the following information to help you improve the performance of Enterprise Vault:

- The time newly-archived items wait to be backed-up. If this is too long, the Archiving Agent and the Storage service will have many uncompleted archive requests.
- The time newly-archived items wait to be moved to offline storage. If this is too short, and items are being moved offline quickly, then more recalls from offline storage may be generated.
- The number of times an archived item is restored from online storage. If too many items are being restored too many times, they may be being archived too soon. If the same items are being continually transferred between the Microsoft Exchange Server store and Enterprise Vault, you may need to increase the size of the Microsoft Exchange Server message store relative to the size of the Enterprise Vault online store.
- The number of times an archived item is recalled from offline storage. If too many items are being recalled too many times, the online storage area may be too small.
- The time taken to recall items from offline storage. This time is dependent on the HSM but can be used to give Enterprise Vault users expected recall times.

Moving the Windows Temp folder

Enterprise Vault services write temporary files to the Windows `Temp` folder. If the `Temp` folder is on the system disk, this can cause the following problems:

- There may not be much space on the system disk. This means that Enterprise Vault services may stop because they have run out of temporary storage space.
- Performance may be affected because of the access needed to both system files and temporary files.

We recommend that, on every computer that is running an Enterprise Vault service, you move the Windows `Temp` folder to a disk other than the system disk.

If you choose to move the `Temp` folder to a non-system disk, you must ensure that it still has the correct permissions assigned to it after the move. For more information, see the section called “TEMP folder security requirements” in the *Installing and Configuring* guide.

Improving performance on Storage service computers

This section includes the following topics:

- [How to control content conversion](#)
- [How to deal with items that stay a long time on the Archive Queue](#)
- [How to exclude items from content conversion](#)

How to control content conversion

Enterprise Vault converts Microsoft Excel and Microsoft Word documents to HTML. If Enterprise Vault performs many such conversions, or if the documents are complex, you may suffer performance problems. In such cases, you can significantly improve performance by making Enterprise Vault convert the documents to text instead of HTML.

Enterprise Vault provides the following registry values with which you can use control whether Enterprise Vault converts documents to text instead of HTML:

- To convert Excel documents to text instead of HTML, set the following registry key to 1:

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

- To convert Word documents to text instead of HTML, set the following registry key to 1:

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

- To list a number of file types that must be converted to text, edit the following registry key:

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

This registry key contains a list of file types, separated by periods, of the file types that are converted to text. The list must end in a period.

For example, if the list is currently `.PPT.POT.PPS.ZIP.` and you want to add file type `XYZ`, you would change the list to the following:

```
.PPT.POT.PPS.ZIP.XYZ.
```

How to deal with items that stay a long time on the Archive Queue

One reason for items to stay on the Microsoft Message Queue Enterprise Vault Storage Archive queue for a long time is that they really are taking a long time to be converted. When the maximum time for the conversion is reached, the item is archived but no HTML version is created. The item is archived and a message is written to the Windows Application Event Log.

If many items are taking longer than the default 10 minutes allowed, you can change the timeout value. To change the timeout, edit the following registry key:

```
HKEY_LOCAL_MACHINE
  \SOFTWARE
    \Wow6432Node
      \KVS
```

```
\Enterprise Vault  
  \ConversionTimeout
```

The units for this key are minutes.

How to exclude items from content conversion

If you decide that some types of items are causing problems when they are being converted, you can exclude them from being converted. The item attributes are indexed in the usual way and the item is archived in its native format but not converted to HTML. The user will not be able to preview an item that has not had its content converted to HTML.

To exclude items from conversion, add the item's file extension to the following registry key:

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

The format for the key is as follows:

```
.filetype[.filetype].
```

For example, to exclude *.JPG and *.CAD files from conversion, set the key to the following:

```
.JPG.CAD.
```

The registry key lists all the file types that are not currently converted.

Auditing

This chapter includes the following topics:

- [About auditing](#)
- [Creating the auditing database](#)
- [Configuring audit categories](#)
- [Starting or stopping auditing](#)
- [Viewing the audit log](#)
- [Tuning auditing](#)

About auditing

Enterprise Vault auditing records activity in a number of different categories. You select the categories in which you want to record activity, and Enterprise Vault stores the audit log entries in the Enterprise Vault auditing database.

Auditing is disabled by default. [Table 23-1](#) summarizes the tasks required to set up auditing, and provides links to the sections where you can find more information.

Table 23-1 Steps to set up auditing

Steps	Task	More information
Step 1	Create the auditing database.	One auditing database is created for all of the Enterprise Vault servers in the site. See “Creating the auditing database” on page 349.

Table 23-1 Steps to set up auditing (*continued*)

Steps	Task	More information
Step 2	Select the categories to audit.	You configure audit categories on each Enterprise Vault server in the site. See “Configuring audit categories” on page 350.
Step 3	Start or stop auditing.	You need to start or stop auditing on each Enterprise Vault server in the site. See “Starting or stopping auditing” on page 353.
Step 4	View audit entries.	See “Viewing the audit log” on page 353.

You can use scripting to customize the processing of audit log entries. An example PowerShell script is provided in the Enterprise Vault kit.

See [“Converting archive permissions to text”](#) on page 354.

If necessary, you can tune auditing by changing the number of connections that Enterprise Vault services can make to the auditing database.

See [“Tuning auditing”](#) on page 355.

You can also move the auditing database to a different SQL Server.

See [“Moving the auditing database”](#) on page 120.

Recommended practice when configuring auditing

Consider the following points when you plan the auditing configuration for your environment:

- Auditing database security. It is important to apply appropriate security to the auditing database. You should consider limiting the access to the database for very privileged users, such as the Vault Service account. For example, you may want to prevent the Vault Service account from removing or modifying Archive Permissions records in the auditing database.

The Enterprise Vault databases contain roles that you can use to increase the database security in your environment. For information on how to use database roles to improve security on the auditing database, see the following technical note on the Veritas Support website:

<http://www.veritas.com/docs/000070503>

- Auditing configuration across multiple servers. If your environment contains multiple Enterprise Vault servers, we recommend that you configure audit

categories consistently across all of the servers in the sites that are associated with the Enterprise Vault directory. Failure to do this will result in inconsistent audit log information in your environment.

If you select the category, **Archive Permissions**, it is particularly important to select this category on all of the Enterprise Vault servers.

- The **Archive Permissions** audit category enables you to record manual changes to an archive's access permissions that an Enterprise Vault administrator makes using the Enterprise Vault Administration Console. However, Enterprise Vault auditing does not capture changes to automatic access permissions on an archive. Automatic archive permissions are permissions that are set on the original content source, and synchronized to the Enterprise Vault archive. To capture this information, you must enable and configure auditing in the content source application.

For example, access permission changes that a user makes on an Exchange Server mailbox are automatically synchronized to the associated Enterprise Vault archive. To capture these permission changes, you must enable and configure Exchange Server auditing on the Exchange Server that hosts the mailbox.

- Enterprise Vault Auditing does not capture changes to Enterprise Vault Auditing registry settings on the Enterprise Vault server. If you want to record this information, configure Windows Registry Auditing for the settings under the key, `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KVS\Enterprise Vault\Admin\Auditing`.

Creating the auditing database

This section describes how to use the Administration Console to create the auditing database.

Note: The auditing database can grow to a large size, and it may sometimes be necessary to perform a rollover to a new database or remove entries from the database to reclaim some disk space. For instructions on how to do this, see the following article on the Veritas Support website:

<http://www.veritas.com/docs/000028295>

To create the auditing database

- 1 In the left pane of the Administration Console, right-click the Enterprise Vault Directory and then, on the context menu, click **Enable Auditing**.
- 2 Under **Audit Database location**, click **Browse** to display the available locations for the auditing database.
- 3 If you want to create a new folder for the auditing database, click **New Folder**.
- 4 Click the location to use for the auditing database, and then click **OK**.
- 5 Under **Transaction log location**, click **Browse** to display the available locations for the auditing database transaction log.
- 6 If you want to create a new folder for the transaction log, click **New Folder**.
- 7 Click the location to use for the log, and then click **OK**.
- 8 Click **OK** to close the Configure Auditing dialog box.
- 9 Wait a few moments for Enterprise Vault to create the database.
- 10 When Enterprise Vault displays a message confirming that it has created the auditing database, click **OK** to dismiss the message.

The auditing database is created on the same SQL Server as the Enterprise Vault Directory database. However, you can move the auditing database to another server, if required.

See [“Moving the auditing database”](#) on page 120.

Configuring audit categories

Audit categories identify the different types of information that auditing can collect. After you have created the auditing database, you can use the Enterprise Vault Administration Console to select audit categories. All categories can record summary audit data, and some can also record detailed data.

You can modify the audit categories when auditing is running or stopped. When an Enterprise Vault administrator changes the auditing configuration, an event ID 4288 reports whether auditing is running (enabled) or stopped (disabled), the status of each audit category, and the identity of the administrator who made the changes. An audit log entry is also created with the same information.

Audit log entries and the following event messages are also created when the Enterprise Vault Admin service starts:

- Event ID 4286 is reported when the Enterprise Vault Admin service starts and auditing is enabled. The message includes the status of each audit category.

- Event ID 4287 is reported when the Enterprise Vault Admin service starts and auditing is disabled. The message includes the status of each audit category.

Audit categories apply to the Enterprise Vault server that you select in the **Enterprise Vault Servers** container in the Administration Console. If there are multiple Enterprise Vault servers, you need to select each server in turn, and configure the audit categories for each server. It is good practice to set the audit categories consistently on all of the Enterprise Vault servers in the sites that are associated with the Enterprise Vault directory.

If you select **Archive Permissions** on one server, it is important that you select it on all of the Enterprise Vault servers.

To configure audit categories

- 1 In the Administration Console, expand the tree in the left pane until the Enterprise Vault Servers container is visible.
- 2 Click the **Enterprise Vault Servers** container.
- 3 Right-click the computer for which you want to configure auditing, and click **Properties** on the context menu.
- 4 Click the **Auditing** tab.
- 5 Check or uncheck the required audit categories.

AdminActivity	Configuration changes made in the Enterprise Vault Administration Console, such as adding a new service, creating archives, or enabling mailboxes.
Advanced Search	Searches performed, including the terms used and the number of items found.
Archive	Items being archived, either manually or on a scheduled run.
Archive Folder Updates	Archived items being moved to a different mailbox folder.
Archive Permissions	Manual changes to user or group access permissions on an archive. Manual permissions are set on an archive using the archive properties dialog, or the Enterprise Vault Policy Manager (EVPM) utility.
Classification	Classification of archived items.
Delete	Archived items being deleted, either manually or through automatic expiry.
Domino Archive	Any Domino archiving activity.
Domino Restore	Any Domino restore activity.

Exchange Synchronization	Records details of creation, modification, and deletion of Exchange managed content settings. Enterprise Vault records relevant details when it is configured to archive from Exchange managed folders and to synchronize with their managed content settings.
FS Archive	File System Archiving activity.
GetOnlineXML	Document retrieval into SharePoint Portal Server.
Indexing operations	When indexing subtasks for managing index volumes start and stop. Also records any critical errors that the subtasks encounter when processing indexes. The Manage Indexes wizard enables you to manage index volumes.
Move Archive	Details of individual Move Archive operations.
NSF Migration	Items being migrated from NSF files.
PST Migration	Items being migrated from PST files.
Restore	Archived items being restored.
Retention Category Updates	Changes to the retention category of archived items.
SPS Archive	SharePoint archiving activity.
Saveset Status	(For Support use.) Rarely used. Records whether a saveset file is available.
Subtask Control	The creation and modification of subtasks, such as the subtasks that control Move Archive operations.
Undelete	Deleted items that are recovered using the option Recover items on the Deleted Items tab of Archive Properties. Shortcuts recovered using the FSAUndelete utility are also recorded.
User	Your own auditing entries.
View	Viewing archived items, either as HTML or in their original formats.
View Attachments	Viewing of archived items from within SharePoint Portal Server.

6 Click **OK** to save the changes you have made.

Starting or stopping auditing

To start or stop auditing you need to perform the following procedure on each Enterprise Vault server.

To start or stop auditing

- 1 In the Administration Console, expand the tree in the left pane until the Enterprise Vault Servers container is visible.
- 2 Click the **Enterprise Vault Servers** container.
- 3 Right-click the computer on which you want to start or stop auditing, and click **Properties** on the context menu.
- 4 Click the **Auditing** tab.
- 5 To start auditing on the Enterprise Vault server, check **Audit entries based on the following categories**.

To stop auditing on the server, uncheck this setting.

When an Enterprise Vault administrator changes the auditing configuration, an event ID 4288 reports whether auditing is enabled or disabled, the status of each audit category, and the identity of the administrator who made the changes. An audit log entry is also created with the same information.

- 6 Click **OK** to save the changes you have made.

Viewing the audit log

Enterprise Vault provides the Audit Viewer utility, which lets you view and filter the data that is logged in the auditing database. For more information on Audit Viewer, see the *Utilities* guide.

You can also view the audit log entries using SQL queries. To customize how audit log entries are processed, you can use scripting.

See [“Converting archive permissions to text”](#) on page 354.

To view the audit log entries using SQL Server Management Studio

- 1 Start the SQL Server Management Studio.
- 2 On the Standard toolbar, click **New Query**.
- 3 On the SQL Editor toolbar, select **EnterpriseVaultAudit** from the list of available databases.

- 4 Type the following command in the query window:

```
SELECT * FROM EVAuditView ORDER BY AuditDate DESC
```

- 5 Click **Execute** on the SQL Editor toolbar, or press F5 to run the command.

Converting archive permissions to text

An administrator can change the manual permissions on an archive using the Permissions tab on the Archive properties, or using Enterprise Vault Policy Manager (EVPM) utility. In audit log entries, changes to manual archive access permissions are shown as Security Descriptor Definition Language (SDDL) strings for Windows permissions, and XML for Domino permissions. An example PowerShell script, `ExampleEvPermissionsAuditHelper.ps1`, is included in Enterprise Vault to show you how you can convert these strings to an array of permissions in a more user-friendly format. The following information is included in the script output:

- Identity details of the archive.
- Name of the Enterprise Vault administrator who changed the permissions.
- A list of the old and new permissions for each administrator who has manual permissions set on the archive.

The example script is located in the folder, *Enterprise Vault_installation\Auditing*. You can run the script on your auditing database, or modify it to use as part of your auditing database processing. The Enterprise Vault Management Shell is not required to run this script.

The comments in the example script explain what the script does, the permissions needed to run the script, and the limitations of this example. You need to change values in the script for your environment.

The permissions available in the Archive properties dialog and in EVPM are Read, Write, and Delete. These permissions equate to more granular permissions in audit log entries. [Table 23-2](#) shows the mapping between the permissions that are available to administrators, and the underlying permissions that are displayed in the audit log entries that are output by the example script.

Table 23-2 Mapping of available permissions to permissions output by script

Permissions in Archive properties and EVPM	Permissions output by example script
Read	READ_FOLDER READ_ITEM

Table 23-2 Mapping of available permissions to permissions output by script
(continued)

Permissions in Archive properties and EVPM	Permissions output by example script
Write	ADD_FOLDER ADD_ITEM CONTROL_FOLDER
Delete	DELETE_FOLDER DELETE_ITEM

Tuning auditing

Each computer on which you enable auditing has a limited number of connections that it can make to the auditing database. These connections are reused as needed. Auditing uses a pool of connections to the auditing database. You can make Enterprise Vault log the level of usage of these connections and then, if necessary, you can modify the number of connections as required.

To turn connection information logging on or off

- 1 In the Administration Console, expand the tree in the left pane until the **Enterprise Vault Servers** container is visible.
- 2 Click the **Enterprise Vault Servers** container.
- 3 Right-click the computer for which you want to enable or disable connection information logging, and click **Properties** on the context menu.
- 4 Click the **Auditing** tab.
- 5 Click **Advanced**.
- 6 Check or uncheck **Log database information** to turn logging on or off.
- 7 Click **OK**.
- 8 Restart the Enterprise Vault Admin service on the computer.

Modifying the connection pool sizes

When an Enterprise Vault service that has auditing turned on stops, it logs an event that shows the number of connections it used and the maximum number of connections available to it. You can use this information to decide whether to change the connection pool sizes.

To change the connection pool sizes

- 1** In the Administration Console, expand the tree in the left pane until the **Enterprise Vault Servers** container is visible.
- 2** Click the **Enterprise Vault Servers** container.
- 3** Right-click the computer for which you want to change the connection pool sizes, and click **Properties** on the context menu.
- 4** Click the **Auditing** tab.
- 5** Click **Advanced**.
- 6** Set the number of connections for each Enterprise Vault service.
- 7** Click **OK**.
- 8** Restart the Enterprise Vault Admin service on the computer.

Failover in a building blocks configuration

This chapter includes the following topics:

- [About Enterprise Vault services in building blocks configurations](#)
- [Extra requirements for building blocks](#)
- [Updating service locations after failover](#)
- [Additional actions after failover for SMTP Archiving](#)

About Enterprise Vault services in building blocks configurations

In a building blocks configuration, each Enterprise Vault server operates as a discrete unit providing the following Enterprise Vault functionality for a particular set of users:

- Archiving and retrieval of data. Each building blocks server includes a Directory service and the required archiving tasks and services.
- Web access. Each building blocks server includes the Web Access application, which provides users with an interface to search and retrieve archived items. This can only be accessed correctly if there is a non-specific URL in the site properties, for example, /EnterpriseVault

The failover functionality of building blocks (**Update Service Locations**) passes the duties of the failed server to another building blocks server. If a required service or task does not yet exist on the new active server, then Update Service Locations creates it.

The building blocks system also contains a number of shared system components. These include the following:

- SQL databases for directory and archive data. These are typically deployed on a dedicated SQL server, allowing the inherent scalability and high availability features of SQL to be fully exploited.
- Centralized storage. Vault store partition data and index locations are shared by each of the building blocks servers.

A building block server may or may not include an Indexing service, depending on the indexing configuration used. The following indexing configurations are supported in building blocks:

- Both the active and failover servers are Index Servers that belong to the same Index Server Group.
- Both the active and failover servers are ungrouped Index Servers.
- Neither the active nor failover servers host an Indexing service.
- The active server is an ungrouped Index Server, and the failover server does not host an Indexing service. On failover, an ungrouped Indexing service is created on the failover computer.

For an introduction to Index Servers, Index Server Groups and Enterprise Vault building blocks, see *Introduction and Planning*.

The planning of building block configurations is beyond the scope of this manual. Contact your Veritas solution provider if you need a highly-available installation of Enterprise Vault.

Extra requirements for building blocks

The following extra requirements apply to building blocks configurations:

- If the active server hosts an Indexing service, then the failover server must have an Enterprise Vault server cache configured.
- The Enterprise Vault Storage queue location must be on a file system that is shared with the associated building blocks servers.
- The Enterprise Vault cache location must have the same path on each Enterprise Vault server. The cache location is local to each server but the name must be the same to prevent errors after a failover. For example, all servers could have a cache location of `D:\MyCache`.
- Each building blocks server can include a local Storage service. The storage and index files must be stored on a file system that is shared with the associated building blocks servers.

See “[About the Storage queue](#)” on page 287.

- You must install and configure the Enterprise Vault SMTP Archiving components on any building blocks server that is to support SMTP Archiving.
If an SMTP Archiving task is running on both the active server and the failover server, then two SMTP Archiving tasks will run on the failover server after you run Update Service Locations. For this reason, the SMTP holding folder path on the active and failover servers must be different.
- You must log on to the active Enterprise Vault server using the Vault Service account, or an account that has been assigned to the Power Administrator role. If Enterprise Vault needs to create a service on the failover server, you are prompted to log on using the Vault Service account, even if you are using an account assigned to the Power Administrator role.
- You must assign the user account the `SC_MANAGER_ALL_ACCESS` access right for the Service Control Manager (SCM) on all Enterprise Vault servers in the Enterprise Vault site. For more information, see *Service Security and Access Rights*, available at the following address on the Microsoft website:
[https://msdn.microsoft.com/en-gb/library/windows/desktop/ms685981\(v=vs.85\).aspx](https://msdn.microsoft.com/en-gb/library/windows/desktop/ms685981(v=vs.85).aspx)

Updating service locations after failover

This section describes the procedure to follow when an Enterprise Vault server that is part of a building blocks solution has failed or been replaced.

Before you use this procedure it is essential that you have configured a working building blocks solution. The failover will not work unless you have already run Update Service Locations on the correctly-configured Enterprise Vault site.

To update service locations after failover

- 1 Change the DNS alias of the failed Enterprise Vault server so that it maps to a working server. You must make this change on all the remaining servers in the Enterprise Vault site.

The method you use to do this depends on the procedures within your organization, as follows:

- Using a host file. Update the host files on all the remaining server computers in the Enterprise Vault site.
 - Using DNS zones. Update the DNS zones to reflect the new alias, and clear the DNS cache using the command line `ipconfig /flushdns`.
- 2 Log on to a working Enterprise Vault server using the Vault Service account, or an account that has been assigned to the Power Administrator role.

- 3 Start the Administration Console.
- 4 In the left pane, expand the tree until the **Enterprise Vault Servers** container is visible.
- 5 Right-click the **Enterprise Vault Servers** container and, on the shortcut menu, click **Update Service Locations**.

If Enterprise Vault needs to create a service, you are prompted for the Vault Service account password.
- 6 If you are prompted, enter the password for the Vault Service account and click **OK**.

Enterprise Vault updates the service locations and creates new services as necessary.

At the end of the update a summary screen appears, listing the services on each computer in the site.
- 7 If the Update Service Locations has created any services, start them.

What to do when a server comes back online

When a server fails, Update Service Locations installs the services that were running on the server onto a working server in the site. When the failed server is restored, run Update Service Locations again. Next, restart the server that was temporarily running the services now hosted by the restored server.

Note: It is important to restart the server as described above. Update Service Locations deletes services that are no longer required on the temporary server. When it does this, a restart ensures the deletion process completes successfully.

Additional actions after failover for SMTP Archiving

On each Enterprise Vault SMTP server, a local SMTP holding folder is configured for the SMTP Archiving task on that computer. After you run Update Service Locations, you need to take the following actions to ensure that the SMTP Archiving task on the failover server can access the correct SMTP holding folder location:

- If the holding folder is on a movable disk, then move the disk to the failover server.

If the holding folder is not on a movable disk, then copy the SMTP holding folder tree from the original server to the failover server.

- On the failover server, open the properties of the SMTP Archiving task and change the location of the holding folder to the new location.
- Restart the SMTP Archiving task.
When you stop the archiving task, click **Yes** to the request to stop the SMTP service. The SMTP service is automatically restarted when the SMTP Archiving task starts.

If an SMTP Archiving task is running on both the original server and the failover server in a Building Blocks environment, then both SMTP Archiving tasks are hosted on the failover server after you run Update Service Locations. Note the following points in this configuration:

- There is only one SMTP service on the failover server. The SMTP service places any messages that it receives in the holding folder of the SMTP Archiving task that was originally running on the failover server.
- The SMTP Archiving task that has failed over from the original server processes messages that are in its configured holding folder. The SMTP service does not place any new messages in this folder. When the archiving task finishes processing the messages in the folder, Enterprise Vault monitoring generates low usage alerts for the archiving task.
- In the properties of each of the SMTP Archiving tasks, the holding folder information shows whether the SMTP service is using the specified holding folder.

Ports used by Enterprise Vault

This appendix includes the following topics:

- [About the ports used by Enterprise Vault](#)
- [Firewall settings for Enterprise Vault programs](#)

About the ports used by Enterprise Vault

On all Enterprise Vault servers you need to open the normal ports that are required for authentication within a Windows domain. For example, Kerberos (port 88), DNS (port 53 UDP), Active Directory (port 445).

Enterprise Vault servers and the servers with which they communicate may require other ports to be open, depending on the functionality that you require.

See <http://www.veritas.com/docs/000040649> for information about the ports that File System Archiving requires to be open on target file servers.

Enterprise Vault servers use DCOM for communication between software components. DCOM is based on the Remote Procedure Call (RPC) protocol, which uses the RPC end-point mapper port (port 135) for connection set up and then ports are dynamically allocated from the range of dynamic RPC ports.

See <http://www.veritas.com/docs/000038099> for information on configuring Enterprise Vault for restricted DCOM access.

See [“Firewall settings for Enterprise Vault programs”](#) on page 362.

Firewall settings for Enterprise Vault programs

[Table A-1](#) lists the ports that are required by specific Enterprise Vault programs.

Table A-1 Firewall settings for Enterprise Vault programs

Server	Inbound ports	Target program	Comments
Enterprise Vault server	TCP 135	svchost.exe component RPCSS service	RPC Endpoint Mapper. Obtain RPC (DCOM) connection.
Enterprise Vault server	RPC dynamic ports.	svchost.exe component Winmgmt service	RPC (DCOM) connection ports for WMI.
Enterprise Vault server	RPC dynamic ports.	Directoryservice.exe	Remote Administration Console access.
Enterprise Vault server	RPC dynamic ports.	AdminService.exe	Access server properties from Administration Console.
Enterprise Vault server	RPC dynamic ports.	TaskController.exe	Task management.
Enterprise Vault server	RPC dynamic ports.	AuthServer.exe	User authentication.
Enterprise Vault server	TCP 445	System	Browse shares from remote server. For example, from remote Administration Console
Enterprise Vault server	TCP 5114	System	Communication between Enterprise Vault services.
Enterprise Vault server	TCP ports defined by the administrator.	IMAPServer.exe	The default IMAP ports are 143 (IMAP) and 993 (IMAPS), but administrators may choose to use other ports.
Enterprise Vault server	TCP ports defined by the administrator.	isode.pp.smtp.exe	The default SMTP ports are 25 and 465 (SSL), but administrators may choose to use other ports.
Enterprise Vault storage server	RPC dynamic ports.	StorageManagement.exe	Create Vault Stores (on storage server).
Enterprise Vault storage server	RPC dynamic ports.	StorageOnlineOpns.exe	Create archives (on storage server).
Enterprise Vault storage server	RPC dynamic ports.	StorageCrawler.exe	Allow remote index servers to retrieve data (from storage server).

Table A-1 Firewall settings for Enterprise Vault programs *(continued)*

Server	Inbound ports	Target program	Comments
Enterprise Vault storage server	RPC dynamic ports.	StorageDelete.exe	Delete Vault Stores/archives (on storage server).
Enterprise Vault storage server	TCP 2103, 2105	mqsvc.exe	Task monitoring of storage message queues. Ports 2103, and 2105 are incremented by 11 if the initial choice is in use when Message Queuing initializes.
Enterprise Vault storage server	RPC dynamic ports.	EVIndexAdminService.exe	Contact index server.
Enterprise Vault server with Exchange Server task	TCP 1801	mqsvc.exe (in Windows\System32\)	Message Queue message transfer.
Enterprise Vault server with Exchange Server task	UDP 1801	mqsvc.exe (in Windows\System32\)	Message Queue server discovery.
Enterprise Vault Domino Gateway	RPC dynamic ports.	nserver.exe (in Lotus\Domino\ or IBM\Domino)	Retrieve archived Domino messages.
Enterprise Vault Domino Gateway	TCP 1352	nserver.exe (in Lotus\Domino\ or IBM\Domino)	From Notes client. Retrieve archived Domino messages.
Enterprise Vault Shopping server	RPC dynamic ports.	ShoppingService.exe	Web restore to Exchange Server.
Enterprise Vault with Exchange archiving task.	RPC dynamic ports.	AgentClientBroker.exe	Client restore to Exchange Server.
Web server	TCP 80	System	Web search.
Web server	TCP 443	System	Secure Web search (HTTPS).
Centera	3218 UDP and TCP	Not applicable	Connection to Centera storage device.
Exchange Server	TCP 135	svchost.exe component RPCSS service	RPC Endpoint Mapper. Obtain RPC (DCOM) connection.

Table A-1 Firewall settings for Enterprise Vault programs *(continued)*

Server	Inbound ports	Target program	Comments
Exchange Server	TCP 445	System	Required for the period when the Administration Console is used to add Exchange Server as a target.
Exchange Server (OWA)	TCP 80	System	HTTP.
Exchange Server (OWA)	TCP 443	System	HTTPS.
Exchange Server 2010 (CAS)	RPC dynamic ports	Microsoft.Exchange.AddressBook.Service.exe	For Exchange archiving task.
Exchange Server 2010 (CAS)	RPC dynamic ports	Microsoft.Exchange.RpcClientAccess.Service.exe	Access to Exchange store.
Exchange Server 2016 and 2013 (CAS)	TCP 80	System	HTTP.
Exchange Server 2016 and 2013 (CAS)	TCP 443	System	HTTPS.
FSA target server	TCP 135	svchost.exe component RPCSS service	RPC Endpoint Mapper. Obtain RPC (DCOM) connection.
FSA target server	RPC dynamic ports	svchost.exe component Winmgmt service	RPC (DCOM) connection ports for WMI.
FSA target server	TCP 445	System	SMB file sharing
Enterprise Vault Domino Gateway	TCP 1352	nserver.exe (in Lotus\Domino\ or IBM\Domino)	From Notes client.
Enterprise Vault Domino Gateway	As configured on Domino server. For example, TCP 8080.	nhhttp.exe	For HTTP to Domino server.
Enterprise Vault Domino Gateway	As configured on Domino server.	nhhttp.exe	For HTTPS to Domino server.
Enterprise Vault Domino Gateway	TCP 80	System	For HTTP to IIS.

Table A-1 Firewall settings for Enterprise Vault programs (*continued*)

Server	Inbound ports	Target program	Comments
Enterprise Vault Domino Gateway	TCP 443	System	For HTTPS to IIS.
Domino server	TCP 1352	nserver.exe (in Lotus\Domino\ or IBMDomino)	From Notes client.
Domino server	TCP 80	nhttp.exe	HTTP for iNotes.
Domino server	TCP 443	nhttp.exe	HTTPS for iNotes.
SharePoint server	TCP 80	System.	For HTTP access by SharePoint archiving task.

Useful SQL queries

This appendix includes the following topics:

- [About the SQL queries](#)

About the SQL queries

In SQL Query Analyzer, choose a vault store database and then do the following:

- Use the following SQL query to show how much has been archived in a certain period as well as time the first and last items were stored during that period. Replace the dates and times in this example with those you want to use.

```
Select count(*),min(archiveddate),max(archiveddate) from saveset
where archiveddate >'2002-04-26 18:00' and archiveddate <
'2002-04-27 5:00'
```

- Use the following SQL Query to obtain the number of different vaults processed in a specified period.

```
Select distinct(vaultidentity) from saveset where
archiveddate >'2002-04-26 18:00' and
archiveddate < '2002-04-27 5:00'
```

- Use the following SQL Query to obtain the number of vaults with items stored in them.

```
Select count(*) from vault
```

Troubleshooting

This appendix includes the following topics:

- [Installation problems](#)
- [Microsoft SQL Server problems](#)
- [Server problems](#)
- [Client problems](#)
- [Problems enabling or processing mailboxes](#)
- [Problems with Vault Cache synchronization](#)
- [Problems with Enterprise Vault components](#)
- [Techniques to aid troubleshooting](#)
- [About moving an Indexing service](#)

Installation problems

The problems in this category can include the following:

- [Enterprise Vault servers: installation problems](#)
- [Desktop clients: installation problems](#)

Enterprise Vault servers: installation problems

This section includes the following topics:

- [Problems when running the installation procedure](#)

Problems when running the installation procedure

If the Enterprise Vault installation fails when trying to register files, restart your system and run the installation again.

Desktop clients: installation problems

If you install the Enterprise Vault Outlook Add-In and then later remove it and reinstall to a different location, the following problems occur:

- When starting Outlook, the following error message appears:

```
The add-in \original_location\valkyrie.dll
could not be installed or loaded.
```

- Double-clicking a shortcut produces error messages about being unable to load custom forms.

The problem occurs because Outlook maintains a cache file of settings, called `extend.dat`, which contains a pointer to the original location of the Outlook Add-In.

You can stop the problem from occurring by taking the following steps:

- Do not change the location of the Outlook Add-In.
- If you do need to change the location of the Outlook Add-In, run Outlook after you remove it. This forces Outlook to rebuild the `extend.dat` file without the original location of the Outlook Add-In. You can then exit from Outlook and reinstall the Outlook Add-In.

If the problem already exists, the solution is to delete the `extend.dat` file so that it is automatically rebuilt when Outlook is next started. As the location of this file varies, you need to search for it. One copy of the file exists for each user who uses Outlook on the computer, so there can be several copies of the file to delete.

You can also use the `ResetEVClient` command-line tool to fix problems with the Enterprise Vault add-in to Microsoft Outlook. For information on how to use `ResetEVClient`, see the *Utilities* manual.

Note: `ResetEVClient` deletes `extend.dat` only for the user who runs it.

Microsoft SQL Server problems

The problems in this category can include the following:

- [Error: ODBC SQL Server Driver Connection is Busy](#)

- [Number of SQL Server licenses exceeded](#)
- [How to reset passwords after moving an Enterprise Vault database](#)

Error: ODBC SQL Server Driver Connection is Busy

Read this section if you see the following MSSQLServer error and Enterprise Vault database error messages in the Windows log:

```
Event ID: 17060 Source: MSSQLServer Type: Error Category:
ODS Error: 17832, Severity: 18, State: 0 Unable to read login
packet(s) . . .
```

```
Event ID: 13344 Source: Enterprise Vault Type: Error
Category: Database An error was detected whilst accessing
the Vault database _EnterpriseVaultDirectory_:
[Microsoft][ODBC SQL Server Driver][DBNMPTW]Connection is
busy_
```

These errors are caused by a known SQL Server problem. How you fix the problem depends on how you have set up access to SQL. The two most common methods of access are TCP/IP and named pipes. For more information, see the most up-to-date articles on the Microsoft Support website. In particular, you may find the following article useful:

<http://support.microsoft.com/?kbid=109787>

Number of SQL Server licenses exceeded

The following message is displayed when you have exceeded the number of SQL Server licenses that you have registered:

```
An error was detected whilst accessing the Vault Database
'name': [Microsoft][ODBC SQL Server Driver][SQL Server]Login
failed- The maximum simultaneous user count of n licenses
for this server has been exceeded. Additional licenses
should be obtained and registered using the Licensing
application in the NT Control Panel.
```

If you are running SQL Enterprise Manager remotely, you require an extra SQL Server license.

Enterprise Vault creates and accesses the Vault Directory Database and the vault store databases. The number of licenses depends on your licensing type. For example, if you are using per-server licensing, and both databases are located on

the same computer, you require one Client Access License. If the two databases are on different computers, you require two Client Access Licenses.

How to reset passwords after moving an Enterprise Vault database

If you are using SQL Server for Enterprise Vault only, we do not recommend that you move either the Vault Directory database or the vault store databases.

Instructions in this section are for experienced SQL Server administrators who may need to know what impact moving the databases has on Enterprise Vault.

When you move the databases using the SQL Transfer Database method, the encrypted passwords are not moved. You must therefore set up your Enterprise Vault passwords to these databases again, and point the DSN at the new server.

Using the Administration Console, set the SQL login password for the following:

- The Vault Directory database. You must use the Administration Console that is running on the same computer as the database.
- Each vault store database. Right-click each vault store and then, on the context menu, click Properties. On the General tab, type a new password.

Server problems

The following sections list errors that you may encounter while running Enterprise Vault.

The problems in this category can include the following:

- [Fixing errors when opening MSMQ dead letter queue](#)

Here are a few tips for making sure that you avoid some common problems:

- It is very important to set up the Vault Service account correctly and to ensure that the Enterprise Vault services run under this account.
- The Vault Service account must have the Microsoft Exchange Server permission Service Account Admin at the Site and Configuration level. See the *Installing and Configuring* manual for detailed information on setting up the Vault Service account.
- When you change the Vault Service account password using Windows, you must update the password in the Vault Directory Database using the Administration Console. The password is encrypted in the Vault Directory Database. See the online help for the Administration Console for more information.

Fixing errors when opening MSMQ dead letter queue

If you receive the following error message:

```
Error opening MSMQ Dead Letter Queue - Access is Denied for
queue MACHINE=98b76660-4198-11d2-bb6f-0000f8789ea8;DEADXACT
```

then you should grant the Local Administrator group full control of the message queues on all computers running the following:

- Exchange Mailbox Task
- Exchange Public Folder Task
- Exchange Journaling Task
- Storage Service

To grant full control to the Local Administrator group

- 1 Run Microsoft Message Queue Explorer.
- 2 Expand the required site.
- 3 Select the appropriate computer.
- 4 Right-click the computer and then, on the context menu, select **Properties**.
- 5 On the **Security** tab, click **Permissions**.
- 6 In the Computer Permissions dialog box, select **Add**.
- 7 In the Add Users and Groups dialog box, select the Administrators group in the **List Names From** box.
- 8 Click **Add**, and then click **OK** until you have returned to the main Message Queue Explorer dialog box.

Client problems

The problems in this category can include the following:

- [Problems logging on to the Enterprise Vault Web Access application](#)
- [MAPISVC.INF problems \(client\)](#)
- [Problems seen by Enterprise Vault users](#)

Problems logging on to the Enterprise Vault Web Access application

When users start the Enterprise Vault Web Access application from Microsoft Outlook or Microsoft Exchange Client, they may be prompted for both their Windows

username and password. If there is no separate box for the domain name, the username must be supplied in the following format:

domain_name\username

When users start the Enterprise Vault Web Access application from Microsoft Outlook or Microsoft Exchange Client, they are prompted for both their Windows user name and password. Normally, Windows passwords have a limit of 14 characters. If a user has set a password containing more than 14 characters, IIS fails to recognize it, and the user cannot log on to use the Enterprise Vault Web Access application. The user must change the password to 14 characters or fewer. This is a known IIS restriction.

MAPISVC.INF problems (client)

If there is an invalid version of `MAPISVC.INF` in the `%windir%\System32` folder, either of the following problems can occur:

- The Enterprise Vault Outlook client cannot display the contents of shortcuts.
- Outlook displays an error message informing you that it is unable to resolve the conflict between a recently installed program and Microsoft Office or other email-enabled programs.

To fix MAPISVC problems

- 1 Run the program `fixmapi.exe`, which is normally in the folder `%windir%\System32`. Note that the program does not appear to do anything when you run it.
- 2 Restart the computer.
- 3 Test whether the problem has been fixed.

If you continue to have problems

- 1 Rename the existing `MAPISVC.INF` in the folder `%windir%\System32`.
- 2 Copy the version of `MAPISVC.INF` supplied with Outlook to the `System32` folder. This file is normally as follows:

```
c:\program files\common
files\system\mapi\1033\nt\MAPISVC.INF
```

- 3 Restart the computer.
- 4 Try the failing operation again.

Problems seen by Enterprise Vault users

The problems that Enterprise Vault users may encounter include the following:

- [Items can no longer be accessed from shortcuts: user problem](#)
- [RPC server is unavailable, or call to the retrieval task failed: user problem](#)
- [Out of date vault index data: user problem](#)
- [Timeouts when restoring large baskets: user problem](#)
- [PowerPoint conversions](#)

Items can no longer be accessed from shortcuts: user problem

If you have changed the protocol or port used for the Web Access application, shortcuts to existing archived items will no longer work.

Shortcuts in email clients like Outlook and Notes can be updated with the new protocol or port information using Synchronize mailboxes in the Enterprise Vault Administration Console, but customized shortcuts, FSA shortcuts, and SharePoint shortcuts cannot be updated.

For more information, see "Customizing the port or protocol for the Enterprise Vault Web Access components" in *Installing and Configuring*.

RPC server is unavailable, or call to the retrieval task failed: user problem

If users receive either message when trying to archive or restore an item, make sure that their DNS Server TCP/IP address in the TCP/IP Properties dialog box is correct.

Out of date vault index data: user problem

The index of items stored in a user's archive may become out of date if, for example, there is a power failure or an out-of-date system backup is restored.

If there is a problem with the index, Enterprise Vault rebuilds it automatically the next time that an item is archived in that archive. This means that there may be a short period when the index contains out-of-date information about the items that are in the archive. Users searching an archive may not be able to find items until the index is updated.

If you believe that this is the problem, the user can archive an item to force Enterprise Vault to rebuild the index.

Timeouts when restoring large baskets: user problem

There is no limit to the number of items that a user can try to restore from a basket. However, if the number of items in the restoring basket is very large, IIS may time out before all of the items have been restored. If most items have been restored, the user can run the restore again, as Enterprise Vault only tries to restore the items that have not been restored yet. If many of the items were not restored, we recommend that the user creates additional baskets and ensures that there are fewer items in each basket before retrying the restore.

PowerPoint conversions

The Microsoft PowerPoint text conversion applies only to text contained within a slide. Speaker notes text is not converted.

Problems enabling or processing mailboxes

This section describes how to diagnose and fix problems with enabling archiving for mailboxes.

Work through the following checks to correct the problem:

- Is the Exchange Mailbox Task for the Exchange Server running?
 The Exchange Mailbox Task does the work of enabling mailboxes, so it must be running.
- Does the Enterprise Vault mailbox still exist, or has it been created incorrectly?
 A problem here normally means that, when you try to enable a mailbox, the message "Failed to enable the mailbox" appears.
 See "[Checking the Enterprise Vault system mailbox](#)" on page 376.
- Is the Enterprise Vault mailbox hidden from the address book?
 Use Microsoft Exchange Server Administrator to look at the properties of the Enterprise Vault mailbox. Make sure that, on the Advanced tab, you have not selected the option to hide the mailbox from the address book.
- Is the Microsoft Exchange Information Store service running on the Exchange System?

To check and modify the Vault Service account permissions

- 1 Start Active Directory Users and Computers.
- 2 Right-click the domain, and then click **Properties**.
- 3 Click the **Security** tab.
- 4 Click **Advanced**, and then click **Add**.

- 5 Double-click the account to which you want to add the permission.
- 6 In the Permission Entry dialog box, click the Properties tab.
- 7 Next to **Apply onto**, select **User objects**.
- 8 In the **Permissions** list, next to both **Read extensionData** and **Write extensionData**, check **Allow**.
- 9 Click **OK** repeatedly to close the dialog boxes.

Checking the Enterprise Vault system mailbox

If you suspect that there may be a problem with the Enterprise Vault system mailbox, work through this section.

To check the Enterprise Vault mailbox

- 1 Start Active Directory Users and Computers.
- 2 Double-click the user to display the properties.
- 3 Click the **Email Addresses** tab, and check that an email address is present.
- 4 If there is no email address, run the Recipient Update Service as follows:
 - Select the **Recipient Update Services** container, which is under the **Recipients**.
 - Right-click the domain, and then click **Update Now**.

To create the mailbox when it does not exist

- 1 Right-click the **Users** container, and then click **New > User**.
- 2 In the **Full name** box, type a name such as *EV System mailbox for server*, where *server* is the name of the Exchange server.
- 3 Type a user logon name, and then click **Next**.
- 4 Type a password, and then confirm it.
- 5 Uncheck **Account is disabled**. It does not matter what the other settings are.
- 6 Click **Next**.
- 7 Make sure that the correct server is selected.
- 8 Check **Create an Exchange mailbox**, and then click **Next**.
- 9 Click **Finish** to create the user and mailbox.

Note that it may take some time for the mailbox to be available.

Problems with Vault Cache synchronization

In Enterprise Vault 9.0.4, 10.0.2 and later, the Outlook Add-In communicates the results of Vault Cache synchronization attempts to the Enterprise Vault server. Earlier versions of the Outlook Add-In do not report this information.

An administrator can browse to the Vault Cache Diagnostics web page to view these results. The Vault Cache Diagnostics page is hosted on an Enterprise Vault server. The server version must be Enterprise Vault 10.0.2 or later.

Viewing the Vault Cache Diagnostics page

The requirements for viewing the Vault Cache Diagnostics page are as follows:

- The DWORD registry value ClientDiagnosticsEnabled must be enabled on the Enterprise Vault server. It is enabled by default for Enterprise Vault 11.0 or later. For information about ClientDiagnosticsEnabled, see the Enterprise Vault *Registry Values* guide.
You must restart the Admin service after you have changed the registry value for the change to take effect.
- To view the Vault Cache Diagnostics page, the administrator must belong to an Enterprise Vault role that allows administration on Enterprise Vault servers. Typical roles for this purpose are Power Administrator, Messaging Administrator, and Exchange Administrator.
- You must select the Windows option to run your browser as an administrator to open the Vault Cache Diagnostics page on an Enterprise Vault server.

To view the Vault Cache Diagnostics page

- ◆ Enter the following address in your browser:
http://your_ev_server/EnterpriseVault/ClientDiagnostics.aspx
 where *your_ev_server* is the name of the Enterprise Vault server.

About Vault Cache Diagnostics

The Vault Cache Diagnostics page shows the last Vault Cache synchronization attempt from each user, and for each archive that they synchronize. The reporting information that is displayed on the page is posted by client computers immediately after they attempt a synchronization, and regardless of the outcome. The default view is to show only the attempts that failed.

To view all synchronization attempts, uncheck **Only show failed synchronizations** at the top of the page.

[Table C-1](#) shows the information that is available for each recorded synchronization attempt.

Table C-1 Information for synchronization attempts

Information	Description
Time since last sync	The elapsed time since the last synchronization attempt (this record).
Client Host	The name of the host computer that the synchronization attempt originated from.
User Domain	The logon domain of the user.
User Name	The logon name of the user.
Status	The last synchronization status. The possible values are Pending, Healthy, Failed, and Unknown.
Header Sync State	The status of Vault Cache Header synchronization.
Content Cache Sync State	The status of the user's Content Cache.
Items to Download	The number of items pending download to the user's Content Cache.
Items Failed to Archive	The number of items that have failed to be archived as part of Vault Cache synchronization.

In addition, you can click an individual record on the page to display more detailed information about it at the bottom of the page. [Table C-2](#) shows the information that is available.

Table C-2 Detailed information for each record

Information	Description
Header Synchronization status	A more detailed explanation of the status of Vault Cache Header (item stubs) synchronization.
Content Cache Synchronization Status	A more detailed explanation of the user's Content Cache synchronization status.
Last Synchronization Occurred	The date and time of the last synchronization attempt (UTC).
Items in Content Cache	The total number of items in the user's content cache. Depending on policy configurations, this number may be 0.

Table C-2 Detailed information for each record (*continued*)

Information	Description
Archive Name	The name of the archive that was synchronized.
Archive Id	The archive ID of the archive that was synchronized.
Enterprise Vault Server	The name of the Enterprise Vault server that handled the synchronization attempt.
Add-in Version	The version and build number of the Enterprise Vault Outlook Add-In.
Outlook Version	The version and build number of Outlook .

Advanced use of Vault Cache Diagnostics

The Vault Cache Diagnostics page lets you perform additional actions to help identify and locate individual client issues. At the top of the page, you can apply a filter to show results for a particular user or Windows domain. You can also sort table columns into descending or ascending order.

The following example shows how to check for users from a particular domain who have not synchronized for over a week.

To show users from a domain who have not synchronized for over a week

- 1 Navigate to:
http://your_ev_server/EnterpriseVault/ClientDiagnostics.aspx
 where *your_ev_server* is the name of the Enterprise Vault server.
- 2 Uncheck **Only Show failed synchronizations**.
- 3 In the **Apply filter** box, enter the domain name.
- 4 On the **User name/User domain** menu to the right of **Apply filter**, select **User domain**.
- 5 Click **Search**.
- 6 In the search results, examine the **Time since last sync** column to identify the users whose last synchronization was over a week ago.

Exporting results

You can export the results on the Vault Cache Diagnostics page to a CSV file for further analysis and reporting. Any filter, search, or ordering is honored in the exported results.

To export the current results

- 1 Click **Export** at the top right of the page.
- 2 Save the results file.

Client synchronization status text

A client can report numerous possible statuses for both Content Cache synchronization and Header synchronization to the Enterprise Vault server.

[Table C-3](#) explains the Content Cache synchronization statuses and the steps you can take to remedy any issues on the client computer.

Table C-3 Content Cache synchronization status

Status	Meaning and steps to remedy
Initializing	Content Cache is initializing. This is a normal phase for newly enabled clients before a first synchronization occurs, and is not a cause for concern.
Not yet downloading	Content Cache has finished initializing but has not yet started downloading files. Again, this is a normal part of the Content Cache download process, and is not a cause for concern.
Complete	Content Cache synchronization has completed successfully. Depending on your Desktop policy settings, this may or may not have involved downloading item content to the user's Content Cache.
Waiting for file on server	Content Cache is waiting for a file to be built on the Enterprise Vault server. Content Cache waits for a PST file to be built on the Enterprise Vault server and downloads the same file to the user's local Content Cache.
Downloading	Content Cache is currently downloading a file from the Enterprise Vault server.
Retrying	Content Cache is retrying a download following an error communicating with the Enterprise Vault server. The client may have lost connectivity momentarily.
BITS not available	The Microsoft Windows BITS service is not installed or not available. On the affected client computer, check to see if the Background Intelligent Transfer Service is listed as a service and is started.

Table C-3 Content Cache synchronization status (*continued*)

Status	Meaning and steps to remedy
Build failed	<p>A failure occurred on the Enterprise Vault server while building a file or as part of integrating a built file with a local Content Cache. The Enterprise Vault Outlook Add-In should retry the Content Cache download as part of the next scheduled synchronization. If this status occurs regularly for a number of users then you should investigate any possible issues on the Enterprise Vault server or client.</p> <p>See "Identifying and resolving Vault Cache issues on the Enterprise Vault server" on page 383.</p> <p>See "Identifying and resolving Vault Cache issues on an end-user computer" on page 385.</p>
BITS download error	<p>The Microsoft Windows BITS feature reported an error while downloading a file from the Enterprise Vault server. The download will be retried during the next scheduled synchronization. If this status occurs regularly for an individual user then you should investigate the BITS feature on that client computer.</p>
Failed to add archive	<p>The Content Cache component encountered an error when attempting to process an additionally available archive. A retry will occur during the next synchronization attempt. If this status occurs regularly for an individual user, then you should examine a client log file from the affected computer to help diagnose the underlying issue.</p> <p>See "Viewing the Enterprise Vault client log file" on page 387.</p>
Could not connect	<p>Content Cache could not connect to the target Enterprise Vault server for the selected archive. It is unlikely that this status will ever be seen, since a connection to the Enterprise Vault server is a requirement for the Outlook Add-In to report the synchronization state.</p>
File locked	<p>A client-side file that Content Cache depends on (<code>DatabaseList.ini</code>) is locked or in use. Restarting Outlook may fix this issue. If not, restarting the affected client computer should ensure that the file becomes unlocked and usable again.</p>
Unspecified error	<p>Content Cache has encountered an unspecified error.</p> <p>See "Identifying and resolving Vault Cache issues on an end-user computer" on page 385.</p>
Unknown error	<p>Content Cache has encountered an unknown error.</p> <p>See "Identifying and resolving Vault Cache issues on an end-user computer" on page 385.</p>

[Table C-4](#) explains the Header synchronization statuses and the steps you can take to remedy any issues on the client computer.

Table C-4 Header synchronization status

Status	Meaning and steps to remedy
Archive changed	The archive information for the user changed while Header synchronization was in progress. This should be resolved by the next scheduled synchronization.
Failed (server synchronizing)	Header synchronization failed because the server was synchronizing the archive hierarchy on the Enterprise Vault server. This is a temporary state for an archive on an Enterprise Vault server and the next scheduled synchronization should complete as normal.
Synchronization prevented	Header synchronization was prevented by user activity in Virtual Vault. While a user is performing certain actions within Virtual Vault (for example, moving folders) synchronization cannot occur. Synchronization will be retried during the next scheduled synchronization.
Insufficient disk space	There is insufficient disk space on the client computer for header synchronization to occur. You need to increase the amount of available disk space before synchronization can complete. The Enterprise Vault Outlook Add-In needs 100MB by default to be able to synchronize.
Failed to acquire slot	Header synchronization failed to acquire a synchronization slot from the Enterprise Vault server. This synchronization slot is in place to limit the number of concurrent header synchronizations occurring on the Enterprise Vault server. If this status occurs regularly for a large number of users, consider altering your server configuration to allow for a larger number of concurrent synchronizations. See “Performance tuning Vault Cache and Virtual Vault” on page 387.
Could not connect	Header synchronization could not occur because the Enterprise Vault Outlook Add-In could not connect to the Enterprise Vault server. It is unlikely that this status will ever be seen, since a connection to the Enterprise Vault server is a requirement for the Outlook Add-In to report the synchronization state.
Offline	The Enterprise Vault Outlook Add-In does not currently have a connection to the Enterprise Vault server. It is unlikely that this status will ever be seen, since a connection to the Enterprise Vault server is a requirement for the Outlook Add-In to report the synchronization state.
Corrupt MDC	Header synchronization could not proceed due to a corrupt MDC file. You will need to delete the MDC file from the affected user’s computer. See “Fixing issues caused by a corrupt MDC file” on page 386.
Unknown failure	Header synchronization encountered an unknown error. See “Identifying and resolving Vault Cache issues on an end-user computer” on page 385.
Complete	Header synchronization completed successfully.

Table C-4 Header synchronization status (*continued*)

Status	Meaning and steps to remedy
Not yet synchronizing	Header synchronization has not yet started. This might be an additionally available archive that the user has not yet selected to synchronize with Enterprise Vault.
Pending	Header synchronization is pending, but not yet started. You should not see this status on the Vault Cache Diagnostics page, but it may be seen on client computers before synchronization has started.
In progress	Header synchronization is in progress. You should not see this status on the Vault Cache Diagnostics page, but it may be seen on client computers during synchronization.
Acquiring slot	The Enterprise Vault Outlook Add-In is trying to acquire a synchronization slot from the Enterprise Vault server to proceed with synchronization. You should not see this status on the Vault Cache Diagnostics page, nor on client computers. It is an internal, transient state that is replaced with another status when the synchronization slot has been either acquired or not acquired.
Waiting for slot	The Enterprise Vault Outlook Add-In is trying to acquire a synchronization slot from the Enterprise Vault server to proceed with synchronization. You should not see this status on the Vault Cache Diagnostics page, nor on client computers. It is an internal, transient state that is replaced with another status when the synchronization slot has been either acquired or not acquired.
Reset	Header synchronization was reset manually by the user. You should not see this status on the Vault Cache Diagnostics page, nor on client computers. It is an internal, transient state that is replaced with another status when synchronization is resumed.
Suspended	Header synchronization was suspended by the user. You should not see this status on the Vault Cache Diagnostics page, nor on client computers. It is an internal, transient state that is replaced with another status when synchronization is resumed.
Client Shutdown	Header synchronization was stopped due to a shutdown by the user. You should not see this status on the Vault Cache Diagnostics page, nor on client computers. It is an internal, transient state that is replaced with another status when Outlook is restarted.
Unknown	Header synchronization encountered an unknown error. See “Identifying and resolving Vault Cache issues on an end-user computer” on page 385.

Identifying and resolving Vault Cache issues on the Enterprise Vault server

A number of components on an Enterprise Vault server are used as part of Vault Cache synchronization.

Table C-5 lists these components, and describes their use and how to identify any issues.

Table C-5 Components on an Enterprise Vault server

Component	Use	Identifying issues
IIS	Hosts a number of Enterprise Vault webpages that are used during synchronization. Serves built Content Cache files to the client BITS service and receives files archived through Virtual Vault.	DTrace the process <code>w3wp.exe</code> on the affected server. Examine IIS log files for any issues. See “Examining IIS log files” on page 388.
EVMonitoring.exe (Cache Manager)	Location on disk for the Content Cache builder component to assemble and build PST files to be downloaded by client computers. The Cache Manager component manages configured disk space as specified under the Cache tab of individual server properties.	The Veritas Enterprise Vault event log describes any serious issues concerning lack of disk space. Any other issues require a DTrace of the <code>EVMonitoring.exe</code> process. See “Tracing Vault Cache server components” on page 384.
EVMonitoring.exe (Content Cache Request Manager)	Handles client requests to build files for Content Cache. Performs throttling of number of concurrent builds.	The Veritas Enterprise Vault event log describes any serious issues. Any other issues require a DTrace of the <code>EVMonitoring.exe</code> process. See “Tracing Vault Cache server components” on page 384.
MigratorServer.exe (Content Cache Builder)	Builds files as the result of requests from client computers through the Content Cache Request Manager component. These files are later downloaded via BITS from the cache location.	Any severe issues should appear in the Veritas Enterprise Vault event log. Any other issues or investigation require a DTrace of <code>MigratorServer.exe</code> . See “Tracing Vault Cache server components” on page 384.
EVMonitoring.exe (Content Cache File Server)	Serves up completed files to client computers that are performing downloads via BITS.	Any severe issues should appear in the Veritas Enterprise Vault event log. Any other issues or investigation require a DTrace of <code>EVMonitoring.exe</code> . See “Tracing Vault Cache server components” on page 384.

Tracing Vault Cache server components

You can trace the following components on an Enterprise Vault server with the DTrace tool, which is supplied with Enterprise Vault. For more information about DTrace, see the Enterprise Vault *Utilities* guide.

- IIS (*w3wp.exe*)
- Content Cache Request Manager (*EVMonitoring.exe*)
- Cache Manager (*EVMonitoring.exe*)
- Content Cache Builder (*MigratorServer.exe*)
- Content Cache File Server (*EVMonitoring.exe*)

For example, by targeting *EVMonitoring.exe* with DTrace and setting a filter to list only lines that contain the word **cache**, you might see a line such as the one below, which could help in diagnosing issues with cache sizing:

```
232 11:20:49.508 [3,044] (EVMonitoring) <5944> EV-H {CacheManager}
Updating cache Size: New:271360
```

Identifying and resolving Vault Cache issues on an end-user computer

After identifying an issue with synchronization on a client computer, determine what manual intervention is required, if any. Some statuses require no intervention and will be resolved as part of the next scheduled synchronization.

See [“Client synchronization status text”](#) on page 380.

Next, if Virtual Vault is enabled but does not appear in the user's Outlook Navigation Pane, check that the *MAPISVC.INF* file that describes message stores in the user's profile is correctly configured. The easiest way to confirm that the file is correctly configured is to use the Outlook Add-In Enterprise Vault Information feature as described in the procedure below. If the *MAPISVC.INF* file is not configured correctly, run the *ResetEVClient* utility as described in the Enterprise Vault *Utilities* guide.

For more serious issues, examine the client log file. For persistent synchronization issues, ensure that the log file captures tracing during a synchronization attempt. Issues that occur in a scheduled synchronization should also be visible in the log file after a manual synchronization.

See [“Viewing the Enterprise Vault client log file”](#) on page 387.

To check that *MAPISVC.INF* is correctly configured

- 1 In Outlook, press Ctrl and Shift and click one of the Enterprise Vault Outlook Add-In buttons.
- 2 In the **Enterprise Vault Diagnostics** dialog box, click **Vault Information**.
- 3 In the **Enterprise Vault Information** window, scroll to the section **VIRTUAL VAULT CONFIGURATION** and confirm that **EVMSD configuration in *MAPISVC.INF*** has the result **OK**.

Fixing issues caused by a corrupt MDC file

A metadata cache (MDC) file contains the item header information and folder structure that Enterprise Vault uses in Vault Cache synchronization. If an MDC file is corrupt, the Enterprise Vault Outlook Add-In is unable to synchronize the archive that it represents, although in some cases the Vault Cache remains usable, and the client reports the Header synchronization status as Corrupt MDC.

If an MDC file is corrupt, do one of the following:

- (This is the preferred action.) Perform a partial reset of Vault Cache. See [“Resetting Vault Cache on a client computer”](#) on page 387.
- If a partial reset is not possible or does not fix the issue with the corrupt MDC file, delete the MDC file.
The MDC file is recreated the next time the Enterprise Vault Outlook Add-In tries to synchronize.

To delete an MDC file

- 1 Open the Enterprise Vault Information window.
See [“Identifying and resolving Vault Cache issues on an end-user computer”](#) on page 385.
- 2 Scroll to the section VIRTUAL VAULT STORES IN PROFILE and find the **File name** line for the affected archive. This line gives a path to the MDC file.
- 3 Click **Send To Clipboard** and paste the information into a text editor, so that you can refer to the path and the file name after you close Outlook.
- 4 Click **OK**.
- 5 Close Outlook.
- 6 Delete the MDC file.

Fixing issues caused by a corrupt DatabaseList.ini file

Vault Cache uses the `DatabaseList.ini` file to track files that contain cached message data. This file can sometimes become corrupt if you use an older version of the Enterprise Vault Outlook Add-In. When this happens, Vault Cache is not able to download items and the Content Cache synchronization status on the Vault Cache Diagnostics page is "Unspecified error" or "Unknown error".

You must close Outlook before you check if the `DatabaseList.ini` file is corrupt.

`DatabaseList.ini` is located in the folder

`%HOMEPATH%\AppData\Local\KVS\Enterprise Vault.`

If the `DatabaseList.ini` file is corrupt, do one of the following:

- Upgrade to the latest version of the Outlook Add-In. This is the preferred action.

- If it is not possible to upgrade, or if you have upgraded but the issue occurred before you upgraded, reset the Vault Cache.
 See [“Resetting Vault Cache on a client computer”](#) on page 387.

Resetting Vault Cache on a client computer

For severe client Vault Cache issues where all other means of resolution have failed, you can reset Vault Cache.

The following types of Vault Cache reset are possible:

- A partial reset, which ensures that the next Header synchronization is a full synchronization.
- A full reset, which forces an initial synchronization of both the Header information and the Content Cache. The effect is the same as if the user has just been enabled for Vault Cache.

Note: We recommend that wherever possible you avoid a full reset, because the initial build of a user’s Content Cache incurs a significant overhead on the Enterprise Vault server.

To reset Vault Cache

- 1 In Outlook, press Ctrl and Shift and click one of the Outlook Add-In buttons.
- 2 See the note above about full resets.
 In the **Enterprise Vault Diagnostics** dialog box, click **Partial Reset**, or **Reset** for a full reset.
- 3 On the prompt that appears, click **Yes** to continue with the reset.

Viewing the Enterprise Vault client log file

The Enterprise Vault client log file provides information about Vault Cache synchronization.

To view the Enterprise Vault client log file

- 1 In Outlook, press Ctrl and Shift and click one of the Enterprise Vault Outlook Add-In buttons.
- 2 In the **Enterprise Vault Diagnostics** dialog box, click **Open Log**.

Performance tuning Vault Cache and Virtual Vault

Several policy settings on the Enterprise Vault server affect the performance of Vault Cache synchronization. For more information, see the *Virtual Vault Best*

Practice Guide, which is available from the following address on the Veritas Support website:

<http://www.veritas.com/docs/000040409>

Examining IIS log files

As a final step in diagnosing client synchronization issues, you can examine the IIS log files on an Enterprise Vault server. The files show the interaction between individual client computers and the various web pages that are used during synchronization.

The IIS log files are typically located at `C:\inetpub\logs\LogFiles\W3SVC1`.

The following example shows a typical line in the log file:

```
2012-08-19 09:29:59 10.12.128.42 GET /EnterpriseVault/Slot.aspx
ArchiveID=10F4ECDC3CF80D240B591162DC0F122321110000ECTO1-EVSVR-VM.mail2.lab&Timeout=0
80 MAIL2\mike_smith 10.12.128.36 EnterpriseVaultOutlookExt-V10.0.2.658 200 0 0 6474
```

In the example:

- A request was made to `Slot.aspx` at 09:29 A.M. on August 19, 2012.
- The request included the archive ID, which in this case was the Archive ID of a client attempting to synchronize.
- The requesting user was `MAIL2\mike_smith`.
- The response code was 200 (success).

[Table C-6](#) shows the web pages that are used during synchronization, with their uses and their possible effect on synchronization. A response code of 200 indicates success.

Table C-6 Web pages used during synchronization

Web page	Use	Notes
DeleteArchivedItems.aspx	The client may call this web page, passing it a list of items to be deleted as the result of items being deleted from Virtual Vault.	A response code of 500 indicates an issue. DTrace <code>w3wp.exe</code> for more detailed information on the cause of the response.
DeleteJob.aspx	Called by the client to indicate that one or more files have been downloaded successfully, so that the Enterprise Vault server can remove the files from the cache location.	A response code of 500 or 501 indicates an issue. DTrace <code>w3wp.exe</code> for more detailed information on the cause of the response.

Table C-6 Web pages used during synchronization (*continued*)

Web page	Use	Notes
DownloadContent.aspx	Used by the BITS component on the client to download completed files from the cache location to the client.	<p>HTTP response codes can indicate issues with the download, as follows:</p> <ul style="list-style-type: none"> ■ 403: Access Denied ■ 404: File not found (it may have been removed from the cache) ■ 408: Transient/Timeout ■ 505/501: Fatal error <p>DTrace <code>w3wp.exe</code> for more detailed information on the cause of the response.</p>
FullSync.aspx	Performs an index query and returns data to the client to facilitate an initial, full header synchronization.	A response code of 500 indicates an issue, possibly with the underlying index query being performed. DTrace <code>w3wp.exe</code> for more detailed information on the cause of the response.
GetArchiveFolderHierarchy.aspx	Gets the archive hierarchy (a list of archive folders). Used for header synchronization.	A response code of 500 indicates an issue. DTrace <code>w3wp.exe</code> for more detailed information on the cause of the response.
GetIncrSlotWithServer.aspx	Used to obtain a slot with the server to perform an incremental build for Content Cache.	A response code of 500 indicates an issue. DTrace <code>w3wp.exe</code> or <code>EVMonitoring.exe</code> for more detailed information on the cause of the response.
GetSlotWithServer.aspx	Used to obtain a slot with the server to perform an initial (full) build for Content Cache.	A response code of 500 indicates an issue. DTrace <code>w3wp.exe</code> or <code>EVMonitoring.exe</code> for more detailed information on the cause of the response.
GetVaultInformation.aspx	Used during Content Cache synchronization to get information such as the date range of the archive.	A response code of 500 indicates an issue. DTrace <code>w3wp.exe</code> for more detailed information on the cause of the response.

Table C-6 Web pages used during synchronization (*continued*)

Web page	Use	Notes
HasJobBuiltYet.aspx	The client polls the server through calling this web page to determine when a file being built on the server is ready to be downloaded.	A response code of 500 indicates an issue. DTrace <code>w3wp.exe</code> or <code>EVMonitoring.exe</code> for more detailed information on the cause of the response.
IncrSync.aspx	Gets the data for incremental header synchronization.	A response code of 500 indicates an issue. DTrace <code>w3wp.exe</code> for more detailed information on the cause of the response.
ListArchives.aspx	Returns a list of accessible archives to the client before a synchronization.	A response code of 500 indicates an issue. DTrace <code>w3wp.exe</code> for more detailed information on the cause of the response.
Slot.aspx	Called by the client to obtain a slot to proceed with header synchronization.	Repeated response codes of 500 indicate a potential bottleneck in the number of users attempting to synchronize. See “Performance tuning Vault Cache and Virtual Vault” on page 387.
SyncPoint.aspx	Used by the client to determine the type of synchronization needed (full or incremental).	A response code of 500 indicates an issue. DTrace <code>w3wp.exe</code> for more detailed information on the cause of the response.
UpdateArchivedItemMetadata.aspx UpdateArchivedFolderHierarchy.aspx	Used to inform the Enterprise Vault server of any user updates that have been performed in Virtual Vault.	A response code of 500 indicates an issue. DTrace <code>w3wp.exe</code> for more detailed information on the cause of the response.
UploadItem.aspx	Used to upload (that is, to archive) items that have been dragged into Virtual Vault.	A response code of 500 or 520 indicates an issue. DTrace <code>w3wp.exe</code> or <code>EVMonitoring.exe</code> for more detailed information on the cause of the response.

Problems with Enterprise Vault components

This section includes information on the following topics:

- [Troubleshooting: All tasks and services](#)
- [Troubleshooting: File System Archiving](#)
- [Troubleshooting: Directory service](#)
- [Troubleshooting: Exchange archiving or Journaling tasks](#)
- [Troubleshooting: Restoring items](#)
- [Troubleshooting: Indexing](#)
- [Troubleshooting: Storage service](#)
- [Troubleshooting: Shopping service](#)
- [Troubleshooting: Web Access application](#)
- [Troubleshooting: Enterprise Vault Operations Manager and the Monitoring database](#)
- [Troubleshooting: Enterprise Vault Reporting and FSA Reporting](#)
- [Specific problems](#)
- [Restoring items for users](#)

Troubleshooting: All tasks and services

This section describes problems with Enterprise Vault tasks and services and covers the following topics:

- [Task or service fails to start: all tasks and services](#)
- [Failed to create MAPI session: all tasks and services](#)
- [Error creating or opening an MSMQ message: all tasks and services](#)
- [User does not have access to an archive: all tasks and services](#)
- [Tasks or services stop because of low system resources: all tasks and services](#)

Task or service fails to start: all tasks and services

If an Enterprise Vault task or service fails to start, check that the following are running:

- Enterprise Vault Directory Service
- Either the MSMQ Primary Enterprise Controller or the Message Queuing service
- If connection to the SQL Server is lost, and you need to shutdown Enterprise Vault services, stop the individual services manually, finishing with the Directory

service and the Admin service. You should stop the services in this way, rather than stopping the Admin service, and relying on it to stop the other services.

If an Exchange task fails to start, check also that you have installed Microsoft Outlook on the Enterprise Vault server.

Failed to create MAPI session: all tasks and services

Except for the Directory service and the Admin service, the Enterprise Vault services and tasks run under the Vault Service account. If you have set up a service or task to run under a different account, or if you have not given the Vault Service account the required Microsoft Exchange Server permissions, an Exchange Journaling task continues to log errors until you stop it.

The Exchange Journaling task continues to try to process the Microsoft Exchange Server Journal mailbox at one-minute intervals. This problem shows up in the Windows Event Viewer as follows:

```
* retry count:
Could not get a MAPI session from the session pool
whilst processing mailbox /o=ACME/ou=Site2000/
cn=Recipients/cn=lvservice
```

and:

```
Could not scan user mailbox
/o=ACME/ou=Site2000/cn=Recipients/cn=lvservice,
unable to get the state of the users mailbox
```

Check the following:

- Is the Exchange Server computer running (private message store)?
- Has the Enterprise Vault mailbox been deleted?
- Have the Vault Service account permissions been set on the Exchange tree?

Error creating or opening an MSMQ message: all tasks and services

- Check that the task or service has permissions to access its MSMQ queues.
- Is the MSMQ Primary Enterprise Controller or Backup Enterprise Controller running?

User does not have access to an archive: all tasks and services

Users require write access to an archive in order to archive, and read access in order to retrieve. This applies even for background archiving. A user must also be the owner of the mailbox or be a member of the local Administrators group on the system that is running the Exchange Mailbox task.

Tasks or services stop because of low system resources: all tasks and services

When the Admin service detects that your system is low on resources, it stops Enterprise Vault tasks and services residing on that system. Occasionally, this may result in additional events being logged. The comment in the log states that the task or service could not be stopped in a timely manner. Before restarting the task or service, ensure that all processes associated with the stopped task or service have been terminated.

To check the status of the processes, right-click the Windows taskbar and then, on the context menu, select Task Manager.

Troubleshooting: File System Archiving

File System Archiving automatically configures the Internet Explorer settings so that the Web Access application computer is in the Internet Explorer trusted sites list. File System Archiving checks this setting each time the file server is processed on an archiving run.

If the computer that runs the Placeholder service has incorrect Internet Explorer security settings, users cannot open any placeholder shortcuts. Each attempt to do so produces an entry on the Windows Application log on the placeholder computer, saying that there was an error downloading a file.

To configure the Internet Explorer security settings

- 1** Log on as the Vault Service account to the computer that is running the Placeholder service.
- 2** In Control Panel, double-click **Internet Options**.
- 3** Click the **Security** tab.
- 4** In the list of zones, click **Local intranet**.
- 5** Click **Sites**.
- 6** Click **Advanced**.

- 7 Enter the name of the Web Access application computer, without the DNS domain, and then click **Add**.
- 8 Click **OK**.
- 9 Click **OK** to close the local intranet settings.
- 10 On the **Security** tab of the Internet Options dialog box, click **Custom Level**.
- 11 Under **User Authentication** in the Security Settings dialog box, select either **Automatic logon only in Intranet zone** or **Automatic logon with current username and password**.
- 12 Click **OK** to close the Security Settings dialog box.
- 13 Click **OK** to close the Internet Options dialog box.

Troubleshooting: Directory service

The Directory service has a client that runs on every system that runs Enterprise Vault software. The Directory service and client both log events to the Enterprise Vault event log. When you have a problem with the Directory Service, the first step is to look for events to determine where the problem lies.

This section includes information on the following topics:

- [Client problems: Directory service](#)
- [Service problems: Directory service](#)
- [SQL problems: Directory service](#)
- [Security problems: Directory service](#)
- [Setting tracing levels: Directory service](#)

Client problems: Directory service

- Events in the log may refer to service-related problems that have been reported to the client. If so, check the computer that is running the service.
- The network between the client and service may be down. Run ping from a Command Prompt window to check that the Directory service computer is available. Run the test in both directions.
- Check that the Directory service is running. If it is not, the client cannot make a connection.

Service problems: Directory service

- Check that prerequisite software is available. The Directory service must have all its required software. ADO (which is installed as part of MDAC) and SQL must be installed and be operational.
- Check that the EnterpriseVaultDirectory ODBC DSN is set up correctly. The Directory Service depends upon an ODBC System DSN called EnterpriseVaultDirectory. This is added automatically by the Configuration Wizard, but it can be modified by anyone using ODBC from Control Panel. Check that this is configured correctly.
- Check that the SQL passwords match. You may see an event informing you that the SQL login has failed. This is because the Directory service depends upon a SQL login ID called EnterpriseVault and an associated password. Ensure that the passwords match. You can use the Administration Console to set the SQL password in Enterprise Manager and the Directory Service.

SQL problems: Directory service

- SQL event data is included in Enterprise Vault events. SQL can report an event for several reasons, such as a database that has run out of disk space.
- You should become familiar with SQL Enterprise Manager. This tool lets you manage the SQL Server and the Enterprise Vault Directory database.
- Use SQL Profiler to see what commands have been sent to the SQL database engine.
- SQL may not recognize the SQL command it has been given. You can use SQL Profiler to check the commands. The event logged by the Directory Service tells you the command, but only if SQL returned control back to the Directory service. Start SQL Profiler from within SQL Enterprise Manager.

Security problems: Directory service

- Create, Update, and Delete must be used by an account that belongs to the local group Administrators on the Directory service computer.
- Any component has permission to read from the Directory service but, to write data, you must have write permissions. The user who tries to modify the data that is maintained by the Directory service must be a member of the local group called Administrators on the Directory Computer.
- SQL database permissions must be correct.
- When the SQL database is created, all the correct permissions are applied to the tables. That is, the SQL login ID EnterpriseVault has access to all of the

tables. If someone inadvertently modifies these permissions, access may be denied. The Application Event Log should indicate such a problem.

- The password stored by the Directory must match the password set in SQL. Always use the Administration Console to change the password.

Setting tracing levels: Directory service

- For problems with tasks and services, use the Vault Administration Console to change the level of tracing. When you are trying to diagnose a problem, set the tracing level higher.
- For problems with clients, create a new DWORD value called Trace Level under the following registry key:

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

where the possible values for Trace Level are as follows:

0	None
1	Low
2	Medium
3	High

Troubleshooting: Exchange archiving or Journaling tasks

This section covers problems with Exchange Mailbox, Public Folder and Journaling tasks.

The archiving task scans through Microsoft Exchange Server mailboxes or public folders and select items for archiving using the selection criteria that you have specified. If you have allowed users to override the selection criteria that you have set, individual users may have set different criteria.

This section includes information on the following topics:

- [Archiving fails completely: Exchange archiving or Journaling tasks](#)
- [Archiving fails partially: Exchange archiving or Journaling tasks](#)

- [Setting up cross-domain archiving: Exchange archiving or Journaling tasks](#)

Archiving fails completely: Exchange archiving or Journaling tasks

Archiving can fail for any of the following reasons:

- Configuration problems. Check through the Application Event Log to find out whether there are any messages there that help with solving the problem.
- Communication or access problems. Check through the Application Event Log to find out whether there are any messages there that help with solving the problem.
- There may be no archiving schedule set. If you have not set such a schedule, the Exchange Mailbox and Public Folder tasks do not run unless you use Run Now. Check the Application Event Log for entries made by the Exchange Mailbox task. Does archiving work when you use Run Now?
- No mailboxes have had archiving enabled. This does not apply to an Exchange Journaling task.
- Use tracing so that you can follow the decisions made by the Exchange Mailbox or Journaling task.

If you have just started using Enterprise Vault, it may take several archiving runs before the system reaches a normal state. This is because a new installation may have more items to archive than can be processed in a single run of the Exchange Mailbox task. Enterprise Vault takes a few items from each mailbox and then, if there is still time in its schedule, goes around again to take more. So some items may have to wait for the next run of the Exchange Mailbox task.

This balancing process ensures that archiving is carried out evenly across all mailboxes. However, it can appear that Enterprise Vault is ignoring some items when, in fact, it is not.

Microsoft Exchange Server can monitor processes for you; see the Microsoft Exchange Server documentation.

Archiving fails partially: Exchange archiving or Journaling tasks

There are several reasons why archiving fails completely for some Microsoft Exchange Server mailboxes but still works for others, or why not all the items that you expect to be archived are archived.

If Enterprise Vault fails to archive anything from some Microsoft Exchange Server mailboxes then the following may apply:

- The most likely cause is that those mailboxes have not been enabled for archiving.
- It is possible that the clock on the computer that is running the Exchange Mailbox task is wrong by a large amount, such as weeks or days. The Exchange Mailbox task uses the local clock to determine the date and time. If this clock has a very different time from that on the Microsoft Exchange Server computer, archiving is affected. On a test system you might be more aware of this problem and so notice it even if the clocks are only a few minutes different.

If Enterprise Vault is archiving some items from a mailbox and is missing others, the problem could be any of the following:

- The user has overridden the archiving settings so that the items are never going to be archived, or are not yet ready to be archived.
- You have a new Enterprise Vault installation and the system has not yet reached its normal state. It may take several runs of the Exchange Mailbox task before all items that are ready to be archived are actually processed.
- The user has no access to the archive. Check through the Application Event Log to find out if there are any messages that help with solving the problem.
- The user has changed the amount of time before an item is ready for archiving, and items are consequently not yet eligible for archiving.
- The item's message class has not been added to the list of those that Enterprise Vault archives. To add more messages classes, use the Directory Properties: Exchange Message Classes tab.
- The Enterprise Vault mailbox has been deleted.

If items never turn into shortcuts, check the following:

- The Exchange Mailbox task is running.
- The Storage service is running.
- The settings on the **Safety Copies** tab of the vault store properties. If the vault store retains safety copies in the original location, items do not become shortcuts until the vault store has backed up or replicated.

Setting up cross-domain archiving: Exchange archiving or Journaling tasks

If you plan to add an Exchange Mailbox or Journaling task for an Exchange Server computer that is in a different domain from that of the Enterprise Vault server, you must set the E2KAutoCreateMailboxContainerADsPath registry value before you add the task.

To set the E2KAutoCreateMailboxContainerADsPath registry value

- 1** Log on to the computer on which you are going to use the Enterprise Vault Configuration Program or Administration Console to add the task for the Exchange Server computer that is in the remote domain.
- 2** Start the Registry Editor.
- 3** Find the following key:

On a 32-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
  \Software
    \KVS
      \Enterprise Vault
        \Admin
```

On a 64-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
  \Software
    \Wow6432Node
      \KVS
        \Enterprise Vault
          \Admin
```

- 4** If the string value E2KAutoCreateMailboxContainerADsPath does not exist, create it.
- 5** Give E2KAutoCreateMailboxContainerADsPath a value of Users.

You can now add the task for the remote Exchange Server computer. After you have added the task, you can change the value of E2KAutoCreateMailboxContainerADsPath back to the default value of Default or leave it as Users.

Troubleshooting: Restoring items

If you encounter problems when restoring items, do the following:

- Check the Application Event Log for more information.
- Check that the Exchange Mailbox task is running.
- Check that the Storage service is running.
- If the items are offline, check that the HSM software is running properly.
- Check that you have the correct archive and Exchange mailbox permissions. To restore items, you must have at least Read access to the archive.

Troubleshooting: Indexing

For the Indexing service to function correctly, you must install it on a computer whose year format is equivalent to the Gregorian year (currently 2017). For example,

setting the computer's regional format to Thai causes the Indexing service to fail, as the current year in the Thai solar calendar falls outside the date range that the service supports.

Indexing tools are available to enable you to manage indexes and index volumes:

See [“About the indexing wizards”](#) on page 149.

Several documents and articles, including the following, are available on the Enterprise Vault Support website to assist in troubleshooting indexing:

- Troubleshooting and monitoring index tasks at <http://www.veritas.com/docs/000094484>
- Troubleshooting index volume error codes at <http://www.veritas.com/docs/000082103>

Troubleshooting: Storage service

Storage service errors are logged in the Windows Application Event Log under the Storage and Database categories.

This section includes information on the following topics:

- [Storage Service does not start: Storage service](#)
- [Failing to create queues: Storage service](#)
- [Failure to access queues: Storage service](#)
- [Cannot create vault stores: Storage service](#)
- [Cannot perform archive, restore, replay, online operations: Storage service](#)
- [Cannot archive: Storage service](#)
- [Exchange messages stay as Archive pending: Storage service](#)
- [Messages are not restored: Storage service](#)
- [Error creating a vault store: Storage service](#)

Storage Service does not start: Storage service

Do the following:

- Check the Application Event Log for more information.
- Check that the Directory service is running.
- Check that the Indexing service is running.

Failing to create queues: Storage service

Do the following:

- Check the Application Event Log for more information.
- Check that the MSMQ Primary Enterprise Controller or Backup Enterprise Controller is running.
- Using Message Queue Explorer, check that the entries for the computers running the Exchange Mailbox and Journaling tasks or Storage services have the correct permissions.

To check the permissions

- 1 In Windows, start Computer Management.
- 2 In the left-hand pane, expand the **Computer Management** node and then expand the **Services and Applications** node.
- 3 Right-click **Message Queuing** and then, on the context menu, click **Properties**. The appears.
- 4 In the Message Queuing Properties window, click **Add**.
- 5 In the Select Users, Computers, or Groups window, next to **Look In**, select **Entire Directory**.
- 6 In the list, click **Administrators** and then click **Add**.
- 7 Click **OK** to return to the Message Queuing Properties window.
- 8 Click **Administrators**.
- 9 Under **Permissions**, check **Allow** next to **Full Control**.
- 10 Click **OK**.
- 11 Close Computer Management.

Failure to access queues: Storage service

Check queue access permissions.

Cannot create vault stores: Storage service

Do the following:

- Check the Application Event log for more information.
- Check that SQL Server is running.
- Check disk space on the NTFS volumes for the vault store database files.
- Examine SQL logs and trace output for more information about the problem.

Cannot perform archive, restore, replay, online operations: Storage service

Do the following:

- Check the Application Event Log for more information.
- Check that the vault store databases are accessible.
- Check that SQL Server is running.
- Examine SQL logs and trace output for more information about the problem.

Cannot archive: Storage service

Check that the Indexing service is running.

Exchange messages stay as Archive pending: Storage service

Do the following:

- Check the settings on the **Safety Copies** tab of the vault store properties. If the vault store retains safety copies in the original location, items do not become shortcuts until the vault store has backed up or replicated. Check that the vault store is being backed up or replicated.
- Check that the Exchange Mailbox task is running.

Messages are not restored: Storage service

Do the following:

- Check that the Exchange Mailbox task is running.
- If you are using HSM software, check that it is running.
- Check the Application Event Log to find out whether Enterprise Vault is reconstructing vault indexes.
 If Enterprise Vault is reconstructing indexes for some archives, it rejects all archive and retrieval operations for those archives until the reconstruction is complete. Other archives are unaffected, so archive and retrieval operations can continue normally for those other archives.

Error creating a vault store: Storage service

If you receive an error when creating a vault store, try restarting the Storage service.

The Application Event Log entries associated with the problem are as follows:

Event ID 13360

An error was detected while accessing the Vault Database 'FasterVS':

Description:

[Microsoft][ODBC SQL Server Driver][SQL Server]Unable to connect. The maximum number of '30' configured user connections are already connected. System Administrator can configure to a higher value with sp_configure.

Event ID 13336

Unable to create Device EVFasterVS on path D:\mssql\data

Event ID 13360

An error was detected while accessing the Vault Database 'FasterVS':

Troubleshooting: Shopping service

This section includes the following topics:

- [Common problems: Shopping service](#)
- [Poor performance: Shopping service](#)
- [Recovering lost disk space: Shopping service](#)
- [Moving shopping data: Shopping service](#)

Common problems: Shopping service

If anything goes wrong with Shopping, check first that all the appropriate services have started. All the following must be running for Shopping to work:

- IIS Admin service
- World Wide Web Publishing service
- Enterprise Vault Shopping service
- Enterprise Vault Directory service
- Enterprise Vault Exchange Mailbox task

If all the tasks and services are running, check the Application Event log on the computer that hosts the Shopping service and the computer that hosts the Exchange Mailbox task. Most high-level errors are self-explanatory, and the solution is straightforward.

Table C-7 lists the error messages that you may receive.

Table C-7 Log messages

Message	What to do
The Shopping Service root directory (<...>) does not exist	Create the folder and try again.
Failed to connect to the Shopping Service	Make sure that the Shopping service is started.
Failed to create new basket <i>BasketName</i> Failed to create file: <i>filespec</i> . Failed to open file <i>filespec</i>	<p>Check the access permissions on the Shopping folders, as follows:</p> <ul style="list-style-type: none"> ■ Enterprise Vault\Shopping\. All Enterprise Vault users who use Shopping require Write access to the Shopping folder. One way to ensure that users have this access is to grant the Authenticated Users group Write access to the Shopping folder. You may prefer to grant access to a smaller group that contains only Enterprise Vault users. ■ Enterprise Vault\Shopping Access. Everyone must have Full Control. ■ Enterprise Vault\Shopping\Domain. Everyone must have Full Control ■ Enterprise Vault\Shopping\Domain\user. Both the user (<i>Domain\user</i>) and the Administrators group on the web server computer (<i>WebServerComputer\Administrators</i>) must have Full Control.
Failed to open file: <filespec>	Check the access permissions on the file. Both the user (<i>Domain\user</i>) and the Administrators group on the web server computer (<i>WebServerComputer\Administrators</i>) must have Full Control.
Failed to retrieve the Shopping Service directory information	Make sure that the Directory service is started.

If there are no errors in the Application Event Log, or the errors listed do not point to an obvious solution, try stopping and then restarting all the Enterprise Vault tasks and services. If restarting the tasks and services does not fix the problem, try increasing the tracing level to see whether that produces any additional information in the Application Event Log.

Poor performance: Shopping service

Bigger shopping baskets mean poorer performance and a greater chance of locking problems during retrieval confirmations. There is no enforced limit on the size of a basket but, in general, users should try to keep baskets to a moderate size (typically fewer than a hundred or so items).

Recovering lost disk space: Shopping service

When a user selects items to restore, a record of these items is kept in a `.des` file on the Shopping Service computer. As the user retrieves more items, the `.des` file gradually increases in size, even if the user deletes all shopping baskets.

If this size increase becomes a problem, do the following:

- 1 Ask the affected users to delete all their baskets.
- 2 As an administrator, delete each `.des` file manually.

New, empty `.des` files are created automatically as needed.

Moving shopping data: Shopping service

We recommend that you do not move the shopping data when users have started shopping. If you do move the data to another volume, all the individual file permissions are lost and must be reapplied manually.

If you move rather than copy the data to somewhere else on the same volume, the file permissions are retained.

To move the data to another location on the same volume

- 1 Stop IIS.
- 2 Stop the Shopping service.
- 3 Move the data. (Do not copy it.)
- 4 Change the data location in the Vault Administration Console by performing the following steps in the order listed:
 - In the Administration Console, expand the left pane until the appropriate Vault Site is visible.
 - Expand the Vault Site until **Computers** is visible.

- Expand **Computers**.
 - Expand the computer that runs the Shopping service.
 - In the right pane, double-click the Shopping service that you want to modify.
 - On the **General** tab of the Shopping Service property page, click **Change**.
 - If you are prompted for the password to the Vault Service account, type it and then click **OK**.
 - In the Choose Folder dialog box, select the new folder and then click **OK**.
- 5** Start the Shopping service and IIS.

Troubleshooting: Web Access application

This section includes the following topics:

- [Users do not see the web page: Web Access application](#)
- [Web Access application does not work: Web Access application](#)
- [Other problems: Web Access application](#)

Users do not see the web page: Web Access application

If the IIS virtual directory settings are wrong, users do not see the web page. The default URL for the Web Access application is **/EnterpriseVault**; the name of the Web Access application virtual directory in IIS.

Check the Web Access application settings on the General tab of the Site Properties dialog box in the Administration Console. The protocol and port shown must match the protocol and port set for the Default Web Site in IIS which contains the **/EnterpriseVault** virtual directory.

Web Access application does not work: Web Access application

The following must all be running for the Web Access application to work:

- IIS
- World Wide Web Publishing service
- Enterprise Vault Directory service
- Enterprise Vault Shopping service
- Enterprise Vault Indexing service

Errors that can occur because the services are not started are as follows:

- The message `The Enterprise Vault Service is not available` appears when the Web Access application is first accessed.
- The message `Failed to perform search request` appears when performing a search.
- Shopping baskets are not created.

Other problems: Web Access application

- English text is displayed instead of text in the language of the web browser. The language file needs to be in the same folder as the English language file (`en.lan`) and the Active Server Page (`.asp`) files. The language is that of the user's web browser and not that of the IIS computer. If the correct language file does not exist, English is used. The name of the language file is `language.lan`.
- Incorrect user name/password entry format. The user name must be in the form `domain\username` for the log on to work correctly.
- A message is unexpectedly restored with all attachments. When a user selects an attachment to restore, Enterprise Vault restores the whole message, with all its attachments. This is the correct behavior.
- An item cannot be added to a basket twice. When adding an item that has already been added to a basket, the item is not added again and there is no warning message.
- Error: ASP 0115. If one of the services that the Web Access application is using causes an access violation, this error is logged. Look at the Application Event log on the web server computer and find out on which service the error occurred and what the error was.
- Error: ASP 0177. This could be the result of either of the following:
 - A Shopping, Indexing, or Storage service has not been registered on the web server computer.
 - The wrong permissions have been set on the virtual directory.

Troubleshooting: Enterprise Vault Operations Manager and the Monitoring database

If you see an error page when attempting to access Enterprise Vault Operations Manager, or when using it to monitor your system, see the following TechNote on the Veritas Support website:

<http://www.veritas.com/docs/000033198>

The TechNote provides detailed troubleshooting information related to installing and using Operations Manager

For information on troubleshooting the Monitoring database and Monitoring agents, see the following TechNote on the Veritas Support website:

<http://www.veritas.com/docs/000033005>

Troubleshooting: Enterprise Vault Reporting and FSA Reporting

If you have problems with installing Enterprise Vault Reporting, or when accessing or viewing its reports, see the following TechNote on the Enterprise Vault Support website:

<http://www.veritas.com/docs/000033199>

This TechNote gives detailed troubleshooting information for Enterprise Vault Reporting.

If you have problems when configuring or using FSA Reporting, refer to the troubleshooting advice in the following Enterprise Vault TechNote:

<http://www.veritas.com/docs/000088358>

Specific problems

- Enterprise Vault tasks and services do not start (login failure).
 If Enterprise Vault tasks and services do not start and report a login failure, the most likely cause of the problem is that the password that has been supplied for the Vault Service account is wrong. If you supply an incorrect password, there will be login failures from all Enterprise Vault tasks and services.
- Error while enabling mailbox for user /o=aaaa/ou=bbbb/cn=Recipients/cn=cccc, error sending enabled message.
 Enterprise Vault cannot send the enable mailbox message. This message is stored in a file called `EnableMailboxMessage.msg` on the Exchange Mailbox task computer.
- Changes to an Enterprise Vault task or service do not take effect.
 For many of the settings that you can change, you must stop and restart the appropriate Enterprise Vault task or service so that it can obtain the new settings. There are some settings that affect more than one task or service, so you may need to stop and restart multiple tasks and services.
- Mailboxes with no associated Windows account are not archived.
 This is the correct behavior. The Exchange Mailbox task automatically disables archiving for such mailboxes.

- BCC recipients are missing from a message.
 If you archive an unsent message with BCC recipients and then restore it, the BCC recipients are missing from the restored message.
- Re-installing the Outlook Add-In to a different folder does not work.
 If you remove the Outlook Add-In and then install it to a different folder, Outlook may not refresh its cache and so may not recognize the new location.
 To force Outlook to see the new installation, do the following in the order listed:
 - Exit Outlook.
 - Remove the Enterprise Vault Outlook Add-In from the computer.
 - Start and then exit from Outlook.
 - Reinstall the Enterprise Vault Outlook Add-In.
 - Start Outlook.
- Items cannot be deleted from archives.
 This may not be a problem at all. There is a five-minute delay before the Index service catches up with a user deleting something from an archive, so users should wait some time before checking that items have been deleted.
- Extra copy of an item when archive fails.
 If an item cannot be archived for some reason, and you have chosen not to delete the original item after archiving on the Archiving Actions tab of the Enterprise Vault Exchange policy properties, it is possible that the user may have an extra copy of the item.
- User cannot store items in an archive.
 Following a power or disk failure, Enterprise Vault may need to reconstruct indexes for one or more archives. If Enterprise Vault is reconstructing indexes for some archives, it rejects all archive and retrieval operations for those archives until the reconstruction is complete, so users of those archives cannot archive or retrieve items. A user whose archive index is being reconstructed cannot archive items, but does not receive any error message. Other archives are unaffected by the replay operations, so archive and retrieval operations can continue normally. The solution is to wait until Enterprise Vault has finished reconstructing the indexes.
- Archiving appears to work, but the log shows an error.
 If the error message is `An error was detected whilst accessing the Vault Database "vaultstore"`, the password to the vault store may have been changed but the Storage service has not been stopped and restarted. Stop the Storage service and restart it so that the service uses the new password.
- Error: `RPC Server is Unavailable`.

You can receive a message that an RPC Server is unavailable in the following situations:

- When you are using the Administration Console to add Enterprise Vault tasks or services.
- When you are running the Enterprise Vault Configuration Program to configure your system.
- When you are remotely managing a computer that is running Enterprise Vault tasks and services.

Each Enterprise Vault computer requires a registered IP address, and the DNS properties for the TCP/IP protocol must be defined.

You may see this problem if the computer on which you are configuring the Enterprise Vault tasks and services does not have any WINS servers defined, and you have chosen not to enable DNS for Windows Resolution on the TCP/IP Protocol property page for WINS. You can either use DNS for service control management or enable DNS for Windows resolution.

If this does not solve the problem, set up the Administration Console computer to use LanMan names instead of DNS names to connect to Service Control Manager. To do this, set the following registry string value to 1:

On a 32-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
  \SOFTWARE
    \KVS
      \Enterprise Vault
        \Admin
          \UseLanmanNameForSCM
```

On a 64-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
  \SOFTWARE
    \Wow6432Node
      \KVS
        \Enterprise Vault
          \Admin
            \UseLanmanNameForSCM
```

- Items never become eligible for archiving, or manual archives do not work, or an item cannot be restored.

All of these problems can happen if an Enterprise Vault server does not have the necessary Windows codepages installed. If you need to install extra languages, see the following article in the Microsoft Knowledge Base:

<http://support.microsoft.com/?kbid=177561>

- Microsoft Message Queue Server: MQIS Initialization Error.

There is a known MSMQ Server problem that results in the following error message:

```
Error: 0xc00e0013 No connection with the Site's
controller.
```

Alternatively, the following error may be logged in the Windows Application Event Log:

```
MQIS Database Initialization Error.
```

These errors may be caused by the lack of, or the misplacement of, the ODBC System Data Source Name (DSN) used to connect SQL Server to the MQIS database. For more information on how to solve this problem, see the following article in the Microsoft Knowledge Base:

<http://support.microsoft.com/?kbid=193510>

Restoring items for users

There may be occasions when you need to restore items on behalf of users. With suitable permissions, it is possible for you to restore items from any archive to any mailbox.

The account you use to retrieve the items must have the following features:

- Have Domain Admin permissions
- Have permissions to write to the user's mailbox
- Have read permissions on the archive
- Be a member of the local administrators' group on the Enterprise Vault computer that is running the appropriate Exchange Mailbox task.

To restore an item on behalf of a user

- 1 In the Vault Administration Console, display the properties of the archive that contains the item to restore.
- 2 Click the **Permissions** tab, and then click **Add**.
- 3 Add yourself to the list of users.
- 4 Start the Enterprise Vault web application, and log on to it as yourself.
- 5 Click the **Search Vault** icon.
- 6 On the Search Archive page, select the archive that contains the item you want to restore.
- 7 Restore the item to the appropriate mailbox.

Techniques to aid troubleshooting

This section provides information on the following topics:

- [Veritas Quick Assist](#)

- [Running on Demand: Run Now](#)
- [Use the Exchange mailbox archiving reports](#)
- [Moved Items report from the Exchange Mailbox task](#)
- [Running DTrace from the Administration Console](#)
- [Using the Deployment Scanner](#)
- [Creating a mail message that contains the Outlook Add-In log](#)
- [How to modify registry settings](#)

Veritas Quick Assist

Veritas Quick Assist (VQA) is a diagnostics tool that scans the system for common issues as well as installation requirements. It produces a report that shows the issues that it has diagnosed and provides actionable solutions where possible. VQA can also collect and upload data for use by Veritas Technical Support.

Run VQA to make sure that you have satisfied the system requirements for Enterprise Vault before you contact Technical Support.

You can run VQA from the Deployment Scanner, or download the latest version from the following article on the Veritas Support website:<http://www.veritas.com/docs/000095758>.

Running on Demand: Run Now

The archiving tasks normally run according to a schedule that you set up. However, you may sometimes want to run a task outside this schedule. On such occasions, you can use Run Now to run the task immediately. Run Now is often useful when you are piloting or demonstrating Enterprise Vault.

To run an Exchange Mailbox or Public Folder task immediately

- 1 In the left pane of the Administration Console, expand the Site hierarchy until the **Enterprise Vault Servers** container is visible.
- 2 Expand the **Enterprise Vault Servers** container.
- 3 Expand the computer that runs the task you want to start.
- 4 Click **Tasks**.
- 5 In the right pane, right-click the task that you want to run and then, on the shortcut menu, click **Run Now**.
- 6 Complete the **Run Now** dialog box, and then click **OK**.

Use the Exchange mailbox archiving reports

Every time the Exchange mailbox archiving task runs, it automatically produces an archiving report which you can examine to troubleshoot problems with Exchange mailbox archiving.

See “[About Exchange mailbox archiving reports](#)” on page 43.

For more information about using Exchange mailbox archiving reports for troubleshooting, see the following technical note on the Veritas Support website:

<http://www.veritas.com/docs/000068569>

Moved Items report from the Exchange Mailbox task

The Exchange Mailbox task Moved Items report shows information about the numbers of moved and copied shortcuts. The report shows this information for each folder of the mailboxes that Enterprise Vault processes in a run of an Exchange Mailbox task. The report also includes information about any moved or copied shortcuts whose retention category has been updated.

Enterprise Vault produces the report after the following types of Exchange Mailbox task run:

- A scheduled run
- A run that you start with the Run Now option, in **Archiving and shortcut processing** mode or **Shortcut processing** mode

Hidden mailboxes do not appear in the report.

The report file is in the `Reports\Exchange Mailbox Archiving` subfolder of the Enterprise Vault installation folder (for example `C:\Program Files (x86)\Enterprise Vault\Reports\Exchange Mailbox Archiving`).

The file name is as follows:

`MovedItemsUpdateSummary_exchangeserver_yyyymmdd.txt`

where *exchangeserver* is the Exchange Server that is associated with the task and *yyymmdd* is the date when the report was generated.

The fields within the file are tab-separated so that you can easily transfer them to a spreadsheet program for analysis.

For each mailbox folder, the report provides the details that are shown in [Table C-8](#).

Table C-8 Fields in an Exchange Mailbox task Moved Items report

Field	Description
Mailbox Name	The legacy distinguished name.
Associated Account	The primary Windows account for the mailbox.
Mailbox Folder	The mailbox folder to which the information applies.
Date	The date on which the task processed the mailbox.
Start Time	The time at which processing started.
End Time	The time at which processing finished.
No. of moved shortcuts	The number of shortcuts that have been moved into this folder from another folder in the mailbox.
No. of copied shortcuts	The number of shortcuts that have been copied into this mailbox folder from another folder in the mailbox.
No. of shortcuts with updated Retention Category	The number of shortcuts that have had their retention category updated.
No. of failed updates	The number of shortcuts for which an update failed.
Archiving policy applied	The Exchange Mailbox policy that applies to the mailbox.

Running DTrace from the Administration Console

In the Administration Console, you can choose from a number of supplied DTrace scripts that collect tracing information.

To run DTrace from the Administration Console

- 1** In the Administration Console, expand the Enterprise Vault site until the **Enterprise Vault Servers** container is visible.
- 2** Expand the **Enterprise Vault Servers** container.
- 3** Expand the Enterprise Vault server on which you want to run a trace.
- 4** On the **Tools** menu, check **Advanced Features**.

Note that this setting is not remembered; it applies to the current session of the Administration Console only.

- 5** Press F5 to refresh the view. A **Traces** container appears underneath the server.

- 6** Right-click the **Traces** container, and then click **New > Trace**.
- 7** In the New Trace wizard, enter the following information:
 - The trace category that is closest to the Enterprise Vault subsystem that you want to trace. For example, you might choose "Search and Indexing issues" or "Restoring and Retrieval issues (Exchange)".
 - A title and optional description for the trace. If you log a call with Veritas Support, you may want to include the call number in the trace title. The title appears in the trace list in the Administration Console and at the start of the trace log file.
 - The length of time that you want to run the trace. Trace files can quickly grow large, so a few minutes is usually appropriate.
 - A maximum size for the log file. The trace stops if the log file reaches this maximum size.
 - The folder in which to store the log file.

After you have started the trace, you can view its properties by double-clicking the trace title in the Administration Console. The Trace Properties dialog box provides options with which you can open and copy the log, but they are unavailable until the trace is complete.

Using the Deployment Scanner

If there is a problem you are trying to solve you may find it useful to run the Deployment Scanner to analyze a server's environment. Additionally, if you call Veritas support you may be asked to run the Deployment Scanner.

You can run Enterprise Vault Deployment Scanner from within the Administration Console, as described in this section. Alternatively, you can run the Deployment Scanner from the Enterprise Vault installation folder or from the folder `Veritas Enterprise Vault\Deployment Scanner` on the Enterprise Vault media. Double-click the file, `Deployment_Scanner.exe`, to start the Deployment Scanner wizard.

To enable the Deployment Scanner in the Administration Console

- 1** Start the Administration Console on the server on which you want to run the Deployment Scanner.
- 2** On the **Tools** menu, click **Advanced Features** to select it.

Note that this setting is not remembered: it applies only to the current session of the Administration Console.

You are now ready to run the Deployment Scanner.

To run the Deployment Scanner from the Administration Console

- 1 In the Administration Console, expand the Enterprise Vault site until the **Enterprise Vault Servers** container is visible.
- 2 Expand the **Enterprise Vault Servers** container.
- 3 Right-click the Enterprise Vault server on which you are running the Administration Console and, on the shortcut menu, click **Deployment Scanner**.
- 4 Work through the Deployment Scanner wizard.

Deployment Scanner saves a report in the Enterprise Vault **Deployment Scanner\Reports** folder.

If you choose the **Gather information through Veritas Quick Assist** option, Deployment Scanner launches the Veritas Quick Assist tool to gather support information, which you can send to Veritas Support.

Note: If Veritas Quick Assist has Internet access, it automatically checks for and downloads a newer version. For more information, see the following article on the Enterprise Vault Support website:

<http://www.veritas.com/docs/000023653>

Creating a mail message that contains the Outlook Add-In log

The **Send Log** button in the Outlook Add-In log viewer enables the user to create a mail message that contains the Outlook Add-In log.

You can use the `SendLogFileMaxSizeMB` and `SendLogFileRecipients` registry values on users' computers to control the behavior of Send Log. `SendLogFileMaxSizeMB` controls the maximum size of the message (default 5 MB), and `SendLogFileRecipients` specifies default recipients. For more information, see the *Registry Values* guide.

To mail the Outlook Add-In log

- 1 In Outlook, open the **Enterprise Vault Information** dialog box:

- Click the **File** tab, then **Enterprise Vault**, and then **Additional support information**.
- 2 In the **Enterprise Vault Information** dialog box, click **Send Log**.
 Outlook creates a mail message that contains the text of the log. The subject line is set to **Enterprise Vault Outlook Add-In log file** and the To field is left blank.
- 3 Add more information if required, and then send the message.

How to modify registry settings

For the most part you can configure Enterprise Vault with the Vault Administration Console, but there are occasions when you may need to use other tools. This section lists changes to the Windows registry that you can make to change the behavior of Enterprise Vault.

This section includes information on the following topics:

- [Changing the MSMQ timeout](#)
- [Optimizing offline storage by sharing items](#)
- [Controlling content conversions](#)
- [Setting the maximum number of message recipients](#)

Changing the MSMQ timeout

Enterprise Vault has a timeout value that limits the amount of time services wait for responses from MSMQ. Usually, if a timeout occurs then there is some problem. However, in a few cases a timeout can be expected to occur and so a reasonably short wait time is required in order for the component not to be idle for too long.

If you make the timeout too short, then systems that are heavily loaded can signal timeout errors simply due to the fact the system has not had time complete the request. If you make the timeout value too long, then this can slow the overall throughput of Enterprise Vault, because timeouts are expected in some circumstances.

The default timeout is 240 seconds. There is no maximum value. We recommend that you adjust the timeout value in small steps, such as five seconds, until you have a suitable value. If you need to increase the timeout by a significant amount, then you need to investigate your MSMQ and Enterprise Vault performance.

To change the timeout value

- 1 Edit the registry on the computer that is running the Enterprise Vault Storage service.
- 2 Edit, or if necessary add, the following DWORD value:

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

- 3 Set the value to the number of seconds to wait.
- 4 Stop and restart the Storage service and Exchange Mailbox task.

Optimizing offline storage by sharing items

Some HSM software products do not support the OFFLINE file attribute to indicate that a file has been moved to HSM secondary storage. In such cases, the Storage service assumes that a file is offline when a specific number of days have elapsed since the file was last modified.

To specify the number of days before the Storage service assumes that a file is offline, you use the OfflineDays registry value. The default value is 0, which means that the Storage service assumes that items are always online.

If several users share an item, the Storage service archives another copy of the item. All copies of a shared item are usually archived at the same time so that only one is archived.

To change the offline setting

- 1 Edit the registry on the computer that is running the Enterprise Vault Storage service.
- 2 Edit, or if necessary add, the following DWORD value:

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

- 3 Set the value to the number of days that items stay online. The default value is 0, which stops the Storage service using the secondary offline status checking. If you set OfflineDays to 0, then the offline status is determined by the OFFLINE file attribute setting.

The new setting is used immediately.

Controlling content conversions

By default, Enterprise Vault stores the compressed text or HTML versions of archived items. This lets users search for items and preview their contents before retrieving them. If you have no requirement for users to search on or preview the contents of items, you can improve performance by turning off content conversion.

To control content conversions

- 1 Edit the registry on the computer that is running the Enterprise Vault Storage service.
- 2 Edit, or if necessary add, the following DWORD value:

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

- 3 Give BypassConversions a value of 0 to perform content conversions or 1 to turn off content conversion.
- 4 Stop and restart the Storage service to make the change take effect.

Setting the maximum number of message recipients

By default, Enterprise Vault does not archive messages that have more than 5000 recipients but you can control this setting.

To set the maximum number of message recipients:

- ◆ Edit the MaxNumOfRecipients registry value on the Exchange Mailbox task computer. This value is under the following registry key:

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

You can also use the SkipRecipCheckSize registry value to set the minimum size of message that is checked for its number of recipients. The size includes the size of the recipient list itself. The default for SkipRecipCheckSize is 750 KB. Messages that are larger than this are checked for the number of recipients, whereas smaller messages are assumed to have fewer than the maximum number of recipients.

About moving an Indexing service

The instructions in this section let you do the following:

- Move an Indexing service and all its data to a different computer.
- Combine two or more Indexing services into one.
- Move some of an Indexing service's data to a different Indexing service.

Warning: We strongly recommend that you do not move an Indexing service because of the amount of work involved and because of the potential for introducing mistakes that take time to rectify.

You require a database tool for viewing and changing data stored in the Enterprise Vault Directory service. Some examples of such tools are VisData (a sample application provided with Microsoft Visual Basic) and Query Analyzer (part of Microsoft SQL Server). The following instructions do not include details of how to set up your database tool to access the Vault Directory database.

Notes on the Indexing data structure of the Vault Directory database

Each Indexing service has an entry in the Directory database, referred to as the `IndexingServiceEntry`. Each `IndexingServiceEntry` contains the ID of a `ComputerEntry` in the Directory database. The `ComputerEntry` contains the name of the computer on which the Indexing service is installed.

An Indexing service has one or more root path locations. These are the folders on the local computer in which the Indexing service stores index data, such as `D:\VaultData\Indexes`.

There is a Vault Directory database entry for each root path location. This is the `IndexRootPathEntry`. Each `IndexRootPathEntry` contains the folder name for the root path location in the `IndexRootPath` field, and the `IndexingServiceID` for the corresponding Indexing service in the `IndexServiceEntryID` field.

An `IndexingServiceEntry` does not contain a list of its `IndexRootPathEntry` records. The link is the other way round; an `IndexRootPathEntry` contains a pointer to its `IndexingServiceEntry`.

Each archive has a Vault Directory database entry. This is the `VaultEntry`. Each `VaultEntry` contains the ID of the `IndexRootPathEntry` where the archive's index data is stored.

Moving the Indexing service

We recommend that, when moving an Indexing service's data, you move whole root paths intact and do not change the `IndexRootPathEntry` used by individual archives. These instructions describe moving whole root paths.

In the instructions below, the computer from which you are moving the Indexing service is the source computer, whereas the computer to which you are moving the service is the target computer.

Note: For the Indexing service to function correctly, you must install it on a computer whose year format is equivalent to the Gregorian year (currently 2017). For example, setting the computer's regional format to Thai causes the Indexing service to fail, as the current year in the Thai solar calendar falls outside the date range that the service supports.

To move the Indexing service

- 1 Install the Enterprise Vault software on the target computer, as described in the *Installing and Configuring Enterprise Vault* manual.
- 2 Configure an Indexing service on the target computer.

You do not need to create root path locations using the Administration Console. Any locations that you create with the Administration Console are not used for the indexes moved to the target computer.

You can also move data to an existing Indexing service, using exactly the same steps below. The moved indexes are placed in new root path locations and do not share existing root path locations.
- 3 Perform the following steps to obtain the Vault Database Directory entry for the Indexing service on the target computer:
 - Search the ComputerEntry records in the directory until you find the entry for the target computer.
 - Note the ComputerEntryId for this entry.
 - Search the IndexingServiceEntry records in the directory for the one that contains this ComputerEntryId.
 - Note the IndexingServiceEntryId of this IndexingServiceEntry record.
 - You use this in [9](#).
- 4 Perform the following steps to find the Directory database entry for the Indexing service on the source computer:
 - Search the ComputerEntry records in the directory until you find the entry for the source computer.
 - Note the ComputerEntryId for this entry.
 - Search the IndexingServiceEntry records in the directory for the one that contains this ComputerEntryId.
 - Note the IndexingServiceEntryId of this IndexingServiceEntry record.
 - You use this in [5](#).
- 5 Perform the following steps to identify all the Indexing service root path locations on the source computer:
 - Search the IndexRootPathEntry records in the directory for those that contain the IndexingServiceEntryId for the source computer.
 - This is the value you obtained in [4](#).

- Decide which root path locations to move to the target computer. You can choose to move all of them, if you want to move the entire Indexing service to a new computer, or only some of them, if you want to spread the load between two Indexing services.
 - Make a list of all the root path locations that you want to move. This list should record the IndexRootPathEntryID for each root path and the IndexRootPath folder where the index data is stored.
- 6** Perform the following steps to create folders on the target computer corresponding to the root path locations:
- On the target computer, manually create one folder for each root path on the list that you made in [5](#).
 There is normally one root path for each disk used for storing index data. If the target computer has fewer disks than the source computer, this may not be possible. In this case, create multiple folders on the same disk. There is no harm in this: the important thing is to create as many folders as there are root paths to be moved.
 Do not try to combine multiple root paths into one, or to split the data within a root path and store it in multiple root paths.
 - Assign one of these folders to each root path on the list that you made in [5](#).
 - You must create each new folder on the target computer on a disk with enough free space to hold all the data stored within its corresponding root path on the source computer.
 - If using NTFS, modify the security permissions on each folder (and on each file created in the folder) so that it is fully accessible to the Administrators group but not accessible to anyone else.
- 7** Use the Service Control Manager to stop the Indexing services on both the source and target computers.
- 8** Wait until both services have stopped.
- 9** For each root path location on the list that you created in step [5](#), do the following:
- Recursively copy all the files and subfolders from the root path location on the source computer to the corresponding folder on the target computer (that is, the folder you created in [6](#)).
 There must be a one-to-one correspondence between the root path locations on the source computer and the new folders on the target computer. Do not use existing folders on the target computer, and do not copy more than one root path to the same folder.

- When the data has been safely copied, use your database tool to select the root path's IndexRootPathEntry in the directory, using its ID recorded on the list made in 5.
- Change the value in the IndexingServiceEntryID field to the ID that you obtained in 3.
- This associates this IndexRootPathEntry with the Indexing service on the target computer.
- Change the value in the IndexRootPath field to the name of the folder on the target computer into which the data for this root path has just been copied. Use the full, correct path name for the folder, including the drive letter.
- Ensure that the modified IndexRootPathEntry is written back to the directory.

Do not delete any data from the source computer at this stage.

10 Perform the following steps to start the Indexing services:

- Start the Indexing service on the target computer.
- Identify all the archives whose data has been moved by searching the directory for all VaultEntry records that contain one of the IndexRootPathEntry IDs on the list created in 5.
- Search each archive to verify that the data has been copied and that the Vault Directory database has been updated correctly.
- When you are sure that the target computer is working correctly, restart the Indexing service on the source computer if it still contains other root paths that were not moved.
- Do not delete the index data from the source computer until you have safely backed it up on the target computer.

Enterprise Vault accounts and permissions

This appendix includes the following topics:

- [About accounts and permissions](#)

About accounts and permissions

See the following technical note for a summary of the various accounts and permissions that are required by Enterprise Vault:

<http://www.veritas.com/docs/000040861>

Index

Symbols

- 'Reply To All' mode [Reply To All] 211
- 'Search Vaults' on Basic toolbar [Search Vaults] 212
- 'Search Vaults' on Premium toolbar [Search Vaults] 212

A

- Action for failed items 170
- Add server to Intranet Zone 188
- Additional StorageOnlineOpns instances
 - Advanced site setting 261
- AddServerToIntranetZone 188
- AddToDoNotDisableAddinList 200
- Admin permissions 19, 38
- Admin service
 - modifying 53
- Administration Console 37, 47–48
- Administrator security 19
- Age and quota-based archiving 328–330, 332
- Age-based archiving 328–329
- Agent Proxy
 - SCOM 302
- Agents advanced settings 264
- AllInfosSuppressible
 - registry value 146
- Allow script in public folders 189
- Allow script in shared folders 189
- Allow shortcut copy 189
- AllowCopyShortcut 190
- Allowed index location characters 255
- AllowScriptSharedFolders 189
- Alternative Web Application URL 190
- AlwaysOn settings 243
- Application logs
 - monitoring 42
- Applying settings 174
- Archive confirmation 207
- Archive deleted items 175
- Archive draft items 170, 176
- Archive Exchange Managed Folders 176
- Archive naming convention 177

- Archive queue 345
- Archive subfolders 207
- Archive unexpired Calendar Events 178, 236
- ArchiveDeletedItems 176
- ArchiveDraftItems 170
- ArchiveManagedFolders2 176
- ArchiveNameFormat 178
- ArchiveNonExpiredCalEvents 178, 236
- Archives
 - deleting 116
 - exporting 309
 - moving 94, 97, 99, 101
- Archiving
 - disabling 341
- Archiving General 169, 230
- Archiving General advanced settings 174
- Archiving only items with attachments 339
- Archiving strategies 328
- Archiving task 317
- Assigning permissions 38
- Audit categories
 - configuring 350
- Auditing 347
 - connection pool size 355
 - converting permissions to text 354
 - creating database 349
 - tuning 355
 - viewing audit log 353
- Auditing database
 - moving 120
- Automatic Monitoring 292
- Automatic monitoring
 - introduction 292
- Automatically delete IE file cache 190
- Automatically re-enable Outlook add-in 191
- AutoReEnable 191
- Availability (Exchange Office Mail App setting) 185

B

- Backup
 - checking 70

- Basic archive function 207
- Basic restore function 207
- Behavior of Mail App Bar (Exchange Office Mail App setting) 186
- Building Blocks
 - failover 357, 359
 - Services 357
 - Update Service Locations 359

C

- Caching duration 253
- Caching duration when disk space is low 253
- Capstone records management
 - common configuration scenarios 135
 - configuring with EVPm 131
 - creating retention categories for 127
 - creating retention plans for 128–129
 - exporting records 143
 - how Enterprise Vault marks items as records 124
 - introduction to 122
 - searching for records 139
 - setting default record types 126
 - types of records 123
 - using classification for 133
 - viewing archive settings 142
- Change Location wizard 149, 154
- Change vault store group 66
- Checking disk space for vault stores 52
- Checking logs 49
- Classification
 - and conflicts with EVPm 134
 - and records management 125, 133, 136
- classification
 - and roles-based administration 30
- ClearText copies of RMS Protected items 230
 - Advanced SMTP policy setting 240
- ClearTextPrimary 231, 240
- Code pages for right-to-left custom shortcuts 179, 236
- Codepage
 - adding 51
 - adding default 51
 - deleting 51
- Compliance Accelerator
 - and records management 139
- Computer properties
 - Advanced settings 263–264, 266
- Content Conversion advanced settings 243
- Content Conversion settings 243
- Content conversion settings 242

- Conversion timeout 247
- Conversion timeout for archive file types 247
- Create multiple Index Locations 268
- Creating a new retention category 78
- CryptoModule event log 42
- Customizations and best practice 328

D

- Delete messages without recipients or a matching target
 - SMTP setting 260
- Delete shortcut after restore 208
- Deleting a vault store 116
- Deleting a vault store group 67
- Deleting an archive 116
- Deleting moved archives 113
- Deletion 75
 - shortcut 77
- Deploy forms locally 191
- Deployment Scanner 415
- Desktop policies
 - Domino mailbox archiving 171
 - Exchange mailbox archiving 185
- Directory Database
 - maintaining 56
 - moving 119
- Discovery Accelerator
 - and records management 139
- Disk space for indexes 55
- Disk space for vault stores
 - checking 52
- Disks
 - monitoring 52
- Display notifications 192
- Display Office Apps on original items 192
- DisplayOfficeAppsOnOriginalItems 193
- Do not archive pending reminders 179, 237
- Domino Administrator role 21
- Domino desktop policy
 - Advanced settings 171
 - Pause interval 172
 - Preemptive archiving threshold 172
 - Vault Cache 171
- Domino journal archives
 - associating retention plans with 129
- Domino mailbox and desktop Advanced settings
 - editing 169
- Domino mailbox policy
 - Action for failed items 170

- Domino mailbox policy *(continued)*
 - Advanced settings 169
 - Archive draft items 170
 - Archiving General 169
 - Lookup e-mail addresses 170
 - Reset archive names 171
 - Strip attachments to non-shortcut items 171
 - Domino provisioning groups
 - associating retention plans with 129
 - DontArchiveItemsPendingReminder 179, 237
 - Download item age limit 213
 - DownloadShortcutHideProgress 204
- E**
- Editing settings 169, 174, 242, 263, 281
 - Empty index volume deletion limit 269
 - Enabled
 - event filter registry value 147
 - Enabling archiving for new mailboxes 84
 - Encode custom body using appropriate code pages 179
 - Enterprise Vault Event Log 49
 - Enterprise Vault Operations Manager
 - Roles-based administration 30
 - troubleshooting 407
 - Enterprise Vault Reporting
 - Roles-based administration 31
 - Enterprise Vault Search
 - and records management 139
 - Enterprise Vault services
 - monitoring 42
 - EVArchive cmdlets
 - Get-EVArchive 88
 - Event filtering 145
 - configuring 146
 - EvMoveArchiveTask.exe.config 102
 - EVPM
 - and conflicts with classification 134
 - and records management 125, 131, 138
 - EVservice 48
 - evtag.category
 - and records management 133
 - EvTaskGuardian.exe.config 103
 - Exchange Administrator role 21
 - Exchange desktop policy
 - advanced settings 185
 - Office Mail App 185
 - Outlook 186
 - OWA 206
 - Exchange desktop policy *(continued)*
 - Vault Cache 213
 - Virtual Vault 218
 - Exchange journal archives
 - associating retention plans with 129
 - Exchange journal policy
 - Archiving General 230
 - Exchange Journaling task queues 320
 - notes 321
 - Exchange mailbox archiving reports 43
 - configuring 43
 - using 44
 - Exchange mailbox policy
 - Advanced settings 174
 - Archiving General 174
 - Synchronize folder permissions 183
 - Text direction indicator for custom shortcuts 183
 - Valid Enterprise Vault site aliases 183
 - Exchange Mailbox Task
 - Moved Items report 413
 - Exchange Mailbox task queues 317
 - notes 319
 - Exchange managed content settings 176, 334
 - Exchange managed folder
 - preventing synchronization 338
 - synchronization 336
 - system default filter 336
 - Exchange managed folders 176, 334
 - Exchange provisioning groups
 - associating retention plans with 129
 - Exchange Public Folder policy
 - Archiving General settings 236
 - Exchange Public Folder task queues 322
 - notes 323
 - Expand distribution lists 231
 - ExpandDistributionLists 231
 - Expiry 75
 - storage 76
 - Export-EVArchive 143
 - Export-EVNARAArchive 144
 - Exported files
 - importing 310
 - Exporting archives 309
 - starting the export 312
 - wizard 309
 - Extension content provider 305
 - enabling 307
 - properties 306
 - reports 307

- Extension Content Provider Administrator 21
- Extension Content Provider Administrator role 306
- Extension Content Provider Application role 24, 306
- External Web Application URL 208
- ExternalWebAppURL 209

F

- Failed DL expansion behavior 232
- FailedDLExpansion 232
- Failover in a Building Blocks configuration 357
- File Server Administrator role 22
- File System Archiving advanced settings 252
- File types converted to text 245
- File types excluded from conversion 244
- File types for IFilter conversion 246
- File types for OCR conversion 246
- File types for Postscript conversion 246
- Filtering events 145
- Fingerprint database
 - monitoring 68
 - moving 120
- Fingerprint databases
 - maintaining 57
- Firewall settings 366
- Folder limit 253
- Folder properties visible 193
- FolderPropertiesVisible 193
- Force form reload on error 193
- Force Indexing Engine Shutdown 269
- Forward mode 209
- Forward original item 193
- ForwardOriginalItem 194
- Frequency
 - on Monitoring tab of Site Properties 293
- Frequency of checks for failed volumes 269
- Frequency of checks for index volumes to process 270
- Frequency of full checks for index volumes to process 270
- FSA databases
 - maintaining 58
- FSA folder policies
 - associating retention plans with 129
- FSA Reporting
 - troubleshooting 408
- FSA volume policies
 - associating retention plans with 129
- Future item retention category 180
- FutureItemsRetCat 180

G

- Get-EVArchive 88
- Get-EVArchive cmdlet 87
- Get-EVRecordSettings 142
- Get-EVRetentionPlan 82
- Get-IndexServerForIndexLocation 165–166

H

- Hidden mailboxes 87

I

- IFilter settings 243
- IMAP access advanced settings 243, 253, 264
- IMAP Administrator 22
- IMAP provisioning groups
 - associating retention plans with 129
- Importing exported files 310
- Include default and anonymous permissions 180
- Include hidden spreadsheet data 248
- Include hidden text 247
- IncludeDefOrAnonPerms 180
- IncludeInheritedRights 181, 232, 237
- Index Group server preference for mailboxes 255
- Index locations 55
- Index volumes 118
- Index Volumes Browser 165
- Indexing Administrator role 22
- Indexing advanced settings 243, 254, 264, 266
- Indexing Engine Query Service Port 270
- Indexing Execution Timeout 270
- Indexing Max Request Length 271
- Indexing memory throttling threshold 271
- Indexing tasks
 - managing 156
- Indexing tasks and subtasks 150
 - deleting 151
 - managing 162–163
- IndexingServiceEntry 421
- Inherited permissions 181, 232, 237
- Internal SMTP Domains
 - SMTP setting 260
- Internet Explorer
 - security settings 393
- InternetOpenTypeDirect 205
- Item Ready
 - Retrieval 325

J

- Journal archives
 - moving 101
- Journal delay 232
- Journal mailbox
 - customizing settings 340
- Journal mailboxes
 - checking 50
- Journal report processing
 - Advanced SMTP policy setting 241
- JournalDelay 232
- Journaling task 320

L

- Limit automatic re-enabling of add-in 194
- Location for restored items 209
- Lock for download item age limit 214
- Log action when a message does not contain any archiving-enabled target
 - SMTP setting 261
- Log conversion failure events 250
- Log conversion timeout events 251
- Log fallback to text events 250
- Log file type not recognized events 251
- Log maximum conversion size exceeded events 252
- Logs
 - checking 49
- Lookup e-mail addresses 170
- LookupNames 171

M

- Mailbox archives
 - moving 99
- mailbox archives
 - moving 97
- Mailbox archiving
 - best practice 328
- Mailbox policy
 - Domino 169
 - Exchange 174
- Mailbox properties visible 194
- Mailboxes
 - enabling archiving 84
 - hidden 87
- MailboxPropertiesVisible 194
- Maintaining SQL databases 55
- Manage Indexes Wizard 149
 - Change Location wizard 149

- Manage Indexes Wizard *(continued)*
 - Rebuild wizard 149
 - Synchronize wizard 149
 - Upgrade wizard 149
 - using 155
 - Verify wizard 149
- Manual archive inserts 214
- Mark PST files 195
- MarkPSTs 195
- Max archive requests per synchronization 219
- Max attempts to archive an item 220
- Max data archived per synchronization 220
- Max delete requests per synchronization 221
- Max item size to archive 221
- Max item updates per synchronization 222
- Max total size of contentless operations 222
- Max total size of items to archive 223
- MaxEventsInSequence
 - registry value 147
- Maximum child process shutdown time 271
- Maximum child process startup time 271
- Maximum concurrent indexing capacity 272
- Maximum concurrent indexing tasks 256
- Maximum consecutive failed items 256
- Maximum conversion size 249
- Maximum expiry errors per archive 262
- Maximum indexing application pool start time 272
- Maximum indexing engine shutdown time 272
- Maximum indexing engine startup time 273
- Maximum item wait time 273
- Maximum items in a file system index volume 273
- Maximum items in a journal index volume 273
- Maximum items in a mailbox index volume 274
- Maximum items in a public folder index volume 274
- Maximum items in a shared index volume 274
- Maximum items in a SharePoint index volume 275
- Maximum items in an index volume 275
- Maximum items in an internet mail index volume 275
- Maximum message size to archive in MB 181, 233, 237
- Maximum update errors 256
- MaxMessageSizeToArchiveMB 233
- MaxSecsBetweenEventsInSequence
 - registry value 147
- Message properties visible 195
- Message queues 314
 - access 314
- MessagePropertiesVisible 195
- Messaging Administrator role 22

- Microsoft Operations Manager (MOM) 292
- Migrating exported files 310
- Mode (Exchange Office Mail App setting) 186
- Modifying Admin service 53
- MOM 292
 - configuring 296
 - installing 296
 - monitoring 295
 - optional configuration 296
- Monitor Indexing Tasks page
 - subtask view 158
 - task view 156
- Monitoring 292
 - fingerprint database 68
 - MOM 295
 - SCOM 298
 - site properties 293
- Monitoring Application logs 42
- Monitoring Application role 24
- Monitoring database
 - maintaining 58
 - moving 120
 - troubleshooting 408
- Monitoring disks 52
- Monitoring Enterprise Vault services 42
- Monitoring journal mailboxes 49
- Monitoring MSMQ queues 46
- Monitoring system status 42
- Move Archive 94
 - Accelerator restrictions 96
 - change performance 104
 - configuring 102
 - deleting moved archives 113
 - how it works 95
 - indexing levels 96
 - monitoring 110, 115
 - move statuses 111
 - reporting 115
 - retrying 114
 - starting, stopping and restarting 111
 - user-deleted items 96
 - using 104
- Move Archive task 102
 - configuring 102
- Move Archive wizard 105
- MoveFailedItemsToInbox 234
- Moving a fingerprint database 120
- Moving a vault store 66
- Moving a vault store database 119

- Moving active archive
 - to inactive archive 99
 - to new archive 97
- Moving active archives 100
- Moving inactive archive
 - to active archive 98
- Moving journal archives 101
- Moving mailbox archives 99
 - between sites 99
- Moving Monitoring database 120
- Moving other mailbox archives 101
- Moving the auditing database 120
- Moving the Directory Database 119
- MSMQ queue summary 315
- MSMQ queues
 - monitoring 46
- MSMQ timeout 417

N

- Name of the folder shortcut file 252
- NeverSuppressEventIDs
 - registry value 147
- New-EVRetentionPlan 82
- non-records
 - introduction to 124
- NoSoftDeletes 204
- NotificationsEnabled 192
- NSF Administrator role 22

O

- OAAvailability 186
- OAMailBarBehavior 186
- OAMode 186
- OCR
 - conversion settings 243
- OCR language 249
- OCR optimization 250
- Office Mail App 185
- Offline store required 214
- Open mode 210
- Operation Failed
 - Archiving Task 318
 - Journaling task 321
 - Public Folder Task 323
 - Retrieval 325
- Operations Manager
 - accessing 294
 - introduction 294

- Operations Manager *(continued)*
 - troubleshooting 407
 - Outlook Add-In behavior 196
 - Outlook advanced settings 186
 - OVItemArchiveAttempts 220
 - OVMaXItemArchivesPerSync 219
 - OVMaXItemDeletesPerSync 221
 - OVMaXItemUpdatesPerSync 222
 - OVMaXMessageSizeToArchiveMB 221
 - OVMaXToArchivePerSyncMB 220
 - OVMaXTotalToArchiveMB 223
 - OVPauseInterval 215
 - OVPerItemSleep 215
 - OVRequireOfflineStore 215
 - OVRootDirectory 217
 - OVRootDirectorySearchPath 217
 - OVSetupWizard 217
 - OVSyncArchiveTypes 218
 - OWA 'Archive Policy' context menu option 210
 - OWA Advanced settings 206
 - OWA2003ArchiveConfirmation 207
 - OWA2003ArchiveSubFolders 207
 - OWA2003BasicArchiveFunction 207
 - OWA2003BasicRestoreFunction 208
 - OWA2003ForwardMode 209
 - OWA2003OpenMode 210
 - OWA2003PremiumArchiveFunction 210
 - OWA2003PremiumRestoreFunction 211
 - OWA2003ReplyMode 211
 - OWA2003ReplyToAllMode 211
 - OWA2003RestoreConfirmation 212
 - OWA2003RestoreDeleteShortcut 208
 - OWA2003RestoreToRestoredItems 209
 - OWA2003SearchFromBasicNavbar 212
 - OWA2003ViewMode 212
 - OWA2010HideOWAArchivePolicy 210
 - OWAWebAppAlias 213
- P**
- Partition rollover
 - configuring 71
 - forcing 74
 - order 73
 - partition states 71
 - PowerShell cmdlet 74
 - password
 - changing Vault Service account 121
 - Pause interval 215
 - Pending shortcut timeout 181, 233, 237
 - PendingShortcutTimeout 181, 233, 238
 - Per item sleep 215
 - Performance tuning 343
 - Archive Queue 345
 - content conversion 344
 - excluding items 346
 - Storage service computers 344
 - Windows Temp folder 344
 - permanent records
 - creating retention categories for 127
 - exporting from archives 143
 - introduction to 123
 - Permissions
 - assigning 38
 - controlling access 37
 - link to technical note 425
 - Vault Service account 375
 - Placeholder Application role 24
 - Policy lookup locations 197
 - Policy Manager
 - and conflicts with classification 134
 - and records management 125, 131, 138
 - initialization file example 131
 - Ports 362
 - inbound ports 366
 - Post Process Archived Item
 - Journaling task 321
 - Power Administrator role 22
 - PowerShell cmdlets
 - indexing 165
 - partition rollover 74
 - remove custom settings 337
 - roles-based administration 31–36
 - Preemptive archiving in advance 216
 - Preemptive archiving threshold 172
 - Premium archive function 210
 - Premium restore function 211
 - Preserve message class 199
 - Preserve message class (for content class) 199
 - Prevent disabling of Outlook Add-In 200
 - Printing behavior 200
 - PrintOriginalItem 200
 - Process Folders
 - Public Folder Task 323
 - Process Item
 - Archiving Task 318
 - Process Mailbox
 - Archiving Task 318
 - Journaling task 321

- Process Moved Items in Folder
 - Archiving Task 318
 - Process System
 - Archiving Task 318
 - Provisioning groups
 - maintaining 84
 - PST Administrator role 23
 - PST configuration files 311
 - PST Import pause interval 200
 - PST Import work check interval 201
 - PST search interval 201
 - PSTImportNoWorkPauseInterval 201
 - PSTImportPauseInterval 200
 - PSTSearchInterval 201
 - Public folder archiving
 - best practice 342
 - Public Folder operations 201
 - public folder targets
 - associating retention plans with 129
 - Public Folder task 322
- Q**
- Queue Journal items 233
 - QueueJournalItems 233
 - Quota-based archiving 328–330, 332
- R**
- RBA 30
 - Rebuild wizard 149, 153
 - recordid property 139
 - records management
 - common configuration scenarios 135
 - configuring with EVPM 131
 - creating retention categories for 127
 - creating retention plans for 128–129
 - exporting records 143
 - how Enterprise Vault marks items as records 124
 - introduction to 122
 - searching for records 139
 - setting default record types 126
 - types of records 123
 - using classification for 133
 - viewing archive settings 142
 - Records tab
 - in Retention Category Properties 128
 - recordtype property 139
 - Remove PST entries 202
 - Remove server from Intranet Zone 202
 - Remove-EVRetentionPlan 82
 - RemovePSTEntries 202
 - RemoveServerFromIntranetZone 203
 - Reply behavior 203
 - Reply mode 211
 - ReplyToOriginalItem 203
 - Report
 - viewing extension content provider 307
 - ReportConfigPeriodMinutes
 - registry value 147
 - Reporting
 - Exchange mailbox archiving 43
 - troubleshooting 408
 - Reset archive names 171, 182, 233
 - ResetArchiveNames 182, 234
 - Restore an Item
 - Storage service 326
 - Restore confirmation 211
 - Restore Item
 - Retrieval 325
 - Restoring items for users 411
 - RestrictPolicyLookup 198
 - retention categories
 - applying with classification 133
 - applying with EVPM 131
 - associating with retention plans 128
 - creating for records management purposes 127
 - use in records management 124
 - Retention Category
 - creating 78
 - Retention Category Properties
 - Records tab 128
 - retention plans
 - applying to target users 129
 - creating 128
 - Retrieval queues 324
 - notes 325
 - RetryTimeInMinutes 103
 - Return failed items to inbox 234
 - role
 - Monitoring Application 300
 - Roles-based administration 19–20
 - Administration Console 24
 - customizing roles 34
 - determining current role 36
 - downloading the RBA store 35
 - editing the RBA store 36
 - Enterprise Vault Operations Manager 30
 - Enterprise Vault Reporting 31

Roles-based administration (*continued*)

- listing role members 32
- listing roles 32
- managing role membership 33
- PowerShell cmdlets 31–36
- predefined roles 21, 31–36
- resetting roles and assignments 37
- uploading the RBA store 36

roles-based administration 30

Root folder 216

Root folder search path 217

RPC over HTTP restrictions 203

RPCOverHTTPRestrictions 203

S

Safety copies

- configuring removal 69
- managing 69

SCOM 293

- Agent Proxy 302
- configuration 303
- creating Run As account 299
- monitoring 298
- Monitoring Application role 300
- Run As account credentials 300
- Run As profile 302

SCOM management pack

- importing 301

Search Administrator 23

Search behavior 204

Search Cache Permissions 257

Search HTTP Service Path 275

Search HTTP Service Port 276

Search HTTP Service Requires SSL 276

Search Log Queries 276

Search Log Results 277

Search Logs Folder 277

Search Max Attempts When Engine Busy 257

Search Max Folders For Specific Folder

- Optimization 257

Search Maximum Threads 277

Search Minimum Threads 278

Search Performance Counters Enabled 278

Search Specific Folder Optimization 258

Search VSA Can Search All Archives 258

Selective Journal Archiving

- SMTP setting 261

Send Email Timeout 254

Services

- starting 46
- stopping 46

Set failed messages 'Do Not Archive' 182, 238

Set-EVArchive cmdlet 87, 130

Set-EVRetentionPlan 82

Set-IndexMetadataSyncLevel 165–166

SetFailedMsgsDoNotArchive 170, 182, 238

SetForceFormReload 193

Setting a system message 118

Settings

- applying Advanced tab 174
- editing Advanced journal policy 229
- editing advanced public folder settings 235
- editing advanced SMTP Archiving settings 239
- editing Advanced tab 169, 174

SharePoint Administrator role 23

SharePoint site collections

- associating retention plans with 129

SharePoint targets

- associating retention plans with 129

Shortcut deletion 77

Shortcut download progress 204

Show content in Reading Pane 223

Show metadata properties 248

Show Setup Wizard 217

Show spreadsheet border 248

Single instance storage

- monitoring 68

Site properties

- Advanced settings 242–243, 252–254, 259, 264

SMTP Administrator role 23

SMTP archives

- associating retention plans with 129

Soft deletes 204

SQL AlwaysOn checks 259

SQL databases

- maintaining 55

SQL queries 367

SQL Server advanced settings 259

SQL server connection timeout 259

Start At

- on Monitoring tab of Site Properties 293

Starting a service 48

Starting services 48

Starting tasks 47

Starting tasks or services 46

Stopping a service 48

Stopping services 48

- Stopping tasks 47
 - Stopping tasks or services 46
 - Storage Administrator role 23
 - Storage advanced settings 243, 264
 - Storage expiry 76
 - Storage service computers
 - performance 344
 - Storage service queues 326
 - notes 327
 - Store Item
 - Storage service 326
 - Strip attachments to non-shortcut items 171, 182, 238
 - StripAttachmentsToNonShortcutItems 171, 182, 238
 - SuppressibleInfoEventIDs
 - registry value 147
 - Synchronize archive types 218
 - Synchronize folder permissions 183
 - Synchronize System
 - Archiving task 319
 - Journaling task 321
 - Synchronize wizard 149, 153
 - SynchronizeFolderPermissions 183
 - System Center Operations Manager 2007 293
 - System mailbox
 - troubleshooting 376
 - System message
 - setting 118
 - System status
 - monitoring 42
- T**
- Task Applications role 24
 - Task guardian service 103
 - configuring 103
 - Tasks
 - starting 46
 - stopping 46
 - temporary records
 - creating retention categories for 127
 - introduction to 124
 - Text direction indicator for custom shortcuts 183
 - Text limit for custom properties 259
 - Threshold
 - on Monitoring tab of Site Properties 293
 - Threshold number of items to trigger
 - synchronization 224
 - Threshold total size of items to trigger
 - synchronization 225
 - Transaction history 262
- Troubleshooting 368
 - Archive pending problems 402
 - archive problems 402
 - archiving fails 397
 - client problems 372, 394
 - components 390
 - content conversion 419
 - cross-domain archiving 398
 - Deployment scanner 415
 - desktop clients 369
 - Directory service 394
 - Directory service problems 395
 - Directory service security problems 395
 - Enterprise Vault mailbox 376
 - Exchange Journaling Tasks 396
 - Exchange Mailbox Tasks 396
 - File System Archiving 393
 - index data problems 374
 - Indexing data structure 421
 - Indexing service moving 420–421
 - installation 368
 - installation procedure 369
 - low resources 393
 - mailbox problems 375
 - MAPI session not created 392
 - MAPISVC.INF 373
 - maximum message recipients 420
 - message restore problems 402
 - Moved Items report 413
 - moving shopping data 405
 - MSMQ dead letter queue 372
 - MSMQ message 392
 - MSMQ timeout 417
 - MSSQLServer 370
 - offline storage settings 418
 - online operation problems 402
 - Operations Manager 407
 - Outlook Add-In log 416
 - PowerPoint 375
 - queue access problems 401
 - queue creation problems 401
 - recovering lost disk space 405
 - registry settings 417
 - Reporting 408
 - resetting passwords 371
 - restoring items 411
 - Retrieval service 399
 - RPC server 374
 - Run Now 412

Troubleshooting (*continued*)

- server problems 371
- servers 368
- service not starting 391
- Shopping service 403
- Shopping service log messages 403
- Shopping service performance 405
- shortcut problems 374
- specific problems 408
- SQL problems 395
- SQL Server licenses 370
- SQL Server problems 369
- Storage service 400
- Storage service not starting 400
- techniques 411
- timeouts with large baskets 375
- tracing 414
- tracing levels 396
- user archive access problem 393
- user problems 374
- various problems 408
- Vault Cache Diagnostics web page 377
- Vault Cache synchronization 377
- vault store creation 401
- vault store creation errors 402
- Web Access application 373, 406
- Web Access general problems 407
- Web Access not working 406
- Web Access page not seen 406
- troubleshooting 64-bit indexing 399

U

- Update Basket
 - Retrieval 325
- Update Shortcut
 - Archiving Task 319
 - Public Folder Task 323
- Upgrade wizard 149, 151
- Use proxy settings 205
- UseNewStyleSearch 204
- UsePRIInternetCPIDForRTLdetermination 183
- Users can archive items 226
- Users can copy items to another store 226
- Users can copy items within their archive 227
- Users can hard delete items 227
- Users can reorganize items 228
- UseSelfInstallFunc 196

V

- Valid Enterprise Vault site aliases 183
- Vault Cache 171, 213
 - troubleshooting synchronization 377
- Vault Cache Diagnostics web page 377
- Vault Service Account
 - link to technical note 425
- Vault Service account
 - changing password 121
 - permissions 375
- vault service account
 - changing 38
- Vault store
 - change sharing level 65
 - moving to a different group 66
- Vault store databases
 - maintaining 56
 - moving 119
- Vault store group
 - configure sharing 65
 - deleting 67
 - managing 63
 - status 64
- Vault stores
 - deleting 116
- Verify wizard 149, 152
- View mode 212
- Virtual Vault 218
- VVAllowArchive 226
- VVAllowHardDelete 227
- VVAllowInterStoreCopyAndMove 226
- VVAllowIntraStoreCopy 227
- VVAllowReOrg 228
- VVAutoSyncItemsSizeThresholdMB 225
- VVAutoSyncItemThreshold 225
- VVDenyMultiContentlessOpsAboveMB 222
- VVReadingPaneContent 224

W

- Warn if default or anonymous permissions exist 184
- Warn when mailbox not under quota after archiving
 - run 184
- WarnWhenDefOrAnonPerms 184
- WDS search auto-enable 218
- Web Application alias 213
- Web Application URL 205
- WebAppURL 205
- WhitelistOfGoodEVConnectionPoints 184

Windows Event Viewer 49
 running 49
Windows Service Control manager 48
Windows Temp folder
 performance 344