Veritas Enterprise Vault™ Registry Values

12.1

VERITAS™

Veritas Enterprise Vault: Registry Values

Last updated: 2017-07-27.

Legal Notice

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

About this guide

This chapter includes the following topics:

- Introducing this guide

- Where to get more information about Enterprise Vault

Introducing this guide

This guide describes Windows registry values with which you can modify the behavior of Enterprise Vault.

Table 1-1 lists the main categories in which the Enterprise Vault registry values are grouped. Each of the following chapters describes the values in one category.

Table 1-1   Categories of Enterprise Vault registry values

Category	Function
Admin Service	Controls the behavior of the Admin service, which installs new Enterprise Vault license keys and provides a general monitoring service that runs automatically when any other Enterprise Vault task or service starts.
Administration Console	Customizes the features of the Administration Console, with which you can configure all the various entities in an Enterprise Vault implementation.
Agents	Controls the behavior of the Enterprise Vault archiving tasks.
Clustering	Stores the information that you submit when you configure Enterprise Vault for use in a Veritas Cluster Server or Windows Server Failover Clustering environment.
Code Page Detection	Controls how Enterprise Vault detects and sets the code pages of the items that it archives.

Table 1-1   Categories of Enterprise Vault registry values *(continued)*

Category	Function
Directory Service	Controls the behavior of the service with which the other Enterprise Vault services and tasks access the configuration information for their site.
Enterprise Vault	Provides miscellaneous settings with which you can control the archiving, indexing, and conversion of items, and optimize Enterprise Vault performance.
EVcloudExporter	Provides settings for use with Enterprise Vault.cloud Archive Migrator.
External filtering	Provides more granular control over how Enterprise Vault archiving tasks process items during an archiving run.
File System Archiving	Controls how Enterprise Vault archives files from network shares.
Indexing	Lets you manage how Enterprise Vault indexes archived data.
Installation	Stores the folder paths, version numbers, and other details of installed Enterprise Vault components.
Miscellaneous	Specifies whether to convert any hidden text in PDF files to HTML.
Outlook Add-In	Configures the add-in to Microsoft Outlook with which users access their mailbox archives.
Selective Journaling	Manages aspects of your selective journaling filter, if you have one.
Storage Service	Controls the behavior of the service that manages the vault stores and archives on the computer where it is running.

Where to get more information about Enterprise Vault

Table 1-2 lists the documentation that accompanies Enterprise Vault.

Table 1-2   Enterprise Vault documentation set

Document	Comments
Veritas Enterprise Vault Documentation Library	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.
	You can access the library in several ways, including the following:
	■ In Windows Explorer, browse to the `Documentation\`*language* subfolder of the Enterprise Vault installation folder, and then open the `EV_Help.chm` file.
	■ On the **Help** menu in the Administration Console, click **Help on Enterprise Vault**.
Introduction and Planning	Provides an overview of Enterprise Vault functionality.
Deployment Scanner	Describes how to check the required software and settings before you install Enterprise Vault.
Installing and Configuring	Provides detailed information on setting up Enterprise Vault.
Upgrade Instructions	Describes how to upgrade an existing Enterprise Vault installation to the latest version.
Setting up Domino Server Archiving	Describes how to archive items from Domino mail files and journal databases.
Setting up Exchange Server Archiving	Describes how to archive items from Microsoft Exchange user mailboxes, journal mailboxes, and public folders.
Setting up File System Archiving	Describes how to archive the files that are held on network file servers.
Setting up IMAP	Describes how to configure IMAP client access to Exchange archives and Internet mail archives.
Setting up SMTP Archiving	Describes how to archive SMTP messages from other messaging servers.
Setting up SharePoint Server Archiving	Describes how to archive content from Microsoft SharePoint servers.
Administrator's Guide	Describes how to perform day-to-day administration procedures.

Table 1-2   Enterprise Vault documentation set *(continued)*

Document	Comments
Backup and Recovery	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.
Classification	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.
NSF Migration	Describes how to migrate content from Domino and Notes NSF files into Enterprise Vault archives.
PST Migration	Describes how to migrate content from Outlook PST files into Enterprise Vault archives.
Reporting	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.
Utilities	Describes the Enterprise Vault tools and utilities.
PowerShell Cmdlets	Describes how to perform various administrative tasks by running the Enterprise Vault PowerShell cmdlets.
Registry Values	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

Veritas Education Services provides comprehensive training for Enterprise Vault, from basic administration to advanced topics and troubleshooting. Training is available in a variety of formats, including classroom-based and virtual training.

For more information on Enterprise Vault training, curriculum paths, and certification options, see https://www.veritas.com/services/education-services.

2

Admin Service

This chapter includes the following topics:

- ClientDiagnosticsEnabled

- Critical

- DelFilesOlderThanHours

- DelFileTypes

- EVConvertersEventLogFull

- EVEventLogFull

- MaxCFSAllowed

- MonitorDiskFreeMb

- NoMonitor

- PollingInterval

- SkipChecks

- SkipTempFolderCheck

- SPSOnly

- TempFolderExceptions

- UseMQCounterMethod

- Warning

ClientDiagnosticsEnabled

Location

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

Content

DWORD.

0 — The Vault Cache Diagnostics page is not enabled.

1 — The Vault Cache Diagnostics page is enabled.

The default is 0 for Enterprise Vault 10.0.2, 10.0.3 and 10.0.4, and 1 for Enterprise Vault 11.0 or later.

Description

In Enterprise Vault 10.0.2 or later, the Vault Cache Diagnostics page allows administrators to view the results of Vault Cache synchronization attempts by the Outlook Add-In.

You must restart the Admin service after you have changed the registry value for the change to take effect.

The following technical note on the Veritas Support website describes how to access the Vault Cache Diagnostics page and how to use the diagnostic information to troubleshoot synchronization issues:

http://www.veritas.com/docs/000068591

The same information is contained in the "Troubleshooting" appendix of the *Administrator's Guide*.

Note: Although the Enterprise Vault server must be version 10.0.2 or later, the Outlook Add-In can be version 9.0.4, or 10.0.2 or later.

Critical

Location

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \Wow6432Node
   \KVS
    \Enterprise Vault
     \AdminService
      \EventLog
```

Content	DWORD
	0 — The Admin Service does not monitor the Windows Application Log.
	An integer specifying a maximum percentage.
	Default value = 90 (percent)
Description	The Admin Service checks the Windows Application Log for errors every PollingInterval seconds.
	See "PollingInterval" on page 24.
	If the proportion of error log entries is larger than the percentage specified by Critical, the Admin Service shuts down Enterprise Vault.
	Critical specifies the threshold maximum percentage of all log entries (not just those from Enterprise Vault) that can be errors.

DelFilesOlderThanHours

Location	HKEY_LOCAL_MACHINE
	 \Software
	  \Wow6432Node
	   \KVS
	    \Enterprise Vault
	     \AdminService

Content	DWORD
Description	Specifies the number of hours since a temporary file was last accessed before it becomes eligible for deletion. The default is 1.
	Additionally, you can set DelFilesOlderThanHours to 0 to force immediate deletion of all files matching DelFileTypes except for folders, read-only files, and files that are currently in use.
	If you modify DelFilesOlderThanHours, the change is picked up automatically at the end of the existing period. So, for example, if the current period is 1 and you change it to 24, the change takes effect at the end of the 1 hour period. However, the change will be picked up immediately if you restart the Admin Service.

DelFileTypes

Location	HKEY_LOCAL_MACHINE
	 \Software
	  \Wow6432Node
	   \KVS
	    \Enterprise Vault
	     \AdminService

Content	String
Description	Specifies additional files that you want the Admin Service to delete. The files matching `~*.tmp` and `EV$*.*` are always deleted once their last access time is older than DelFilesOlderThanHours. Use semicolons (;) to separate file specifications.

EVConvertersEventLogFull

Location	HKEY_LOCAL_MACHINE
	 \Software
	  \Wow6432Node
	   \KVS
	    \Enterprise Vault
	     \AdminService

Content	String values (yyyyMMdd).
Description	Contains the last date when a message about Enterprise Vault Converters Event Log being full was written to the Application Event Log.

EVEventLogFull

Location	HKEY_LOCAL_MACHINE
	 \Software
	  \Wow6432Node
	   \KVS
	    \Enterprise Vault
	     \AdminService

Content	String values (yyyyMMdd)

Description   Contains the last date when a message about Enterprise Vault Event
                   Log being full was written to the Application Event Log.

MaxCFSAllowed

Location   `HKEY_LOCAL_MACHINE`
                   ` \Software`
                   `  \Wow6432Node`
                   `   \KVS`
                   `     \Enterprise Vault`
                   `      \AdminService`

Content   String indicating number of simultaneous download slots. Default 30;
                   maximum 99.

Description   When multiple users are updating the Vault Cache, you may see the
                   following warning in the Event log on the Storage service server:

```
Event Type: Warning
Event Source: ASP.NET n.n.n.n
Event Category: Web Event
Event ID: 1309
Event code: 3001
Event message: The request has been aborted.
```

The warning is an indication that there were insufficient simultaneous
download slots available to update the Vault Caches. If this event occurs
only occasionally, you can safely ignore it. The downloads are retried
automatically. If this event occurs frequently, do one of the following to
increase the number of download slots:

- Set the MaxCFSAllowed registry value, as follows:
  - Create MaxCFSAllowed and set it to an integer value that is the
    maximum number of downloads that you want to allow. The
    maximum value you can set is 99.

    Make sure that the value you specify is larger than is set for
    Maximum number of concurrent updates in the Administration
    Console properties of the Storage server.
- Increase the value of Maximum number of concurrent updates in
  the Administration Console, as follows:
  - In the Administration Console, open the properties of the Storage
    service server.

    Click the **Cache** tab. Increase the value of **Maximum number
    of concurrent updates**.

Restart the Enterprise Vault Admin service to enable the change.

MonitorDiskFreeMb

Location   HKEY_LOCAL_MACHINE
                   \Software
                    \Wow6432Node
                     \KVS
                       \Enterprise Vault
                        \AdminService

Content   DWORD

Description   Forces disk monitoring of free space in megabytes instead of percent used.

                   If this is set then the Warning and Critical registry values must contain a value in megabytes instead of percentages from 0 to 100.

NoMonitor

Location   HKEY_LOCAL_MACHINE
                    \SOFTWARE
                     \Wow6432Node
                      \KVS
                       \Enterprise Vault
                        \AdminService

Content   DWORD

                   0 — Monitor resources

                   1 — Do not monitor resources

Description   The Admin Service automatically monitors memory and disk space resources, logging warnings in the Application Log if necessary and, in extreme cases, shutting down Enterprise Vault services. You can use NoMonitor to force the Admin Service not to monitor resources.

                   You can also control the monitoring by editing the Admin Service's startup parameters.

                   See the information about monitoring disks in the *Administrator's Guide*.

PollingInterval

Location   HKEY_LOCAL_MACHINE
                    \SOFTWARE
                     \Wow6432Node
                      \KVS
                       \Enterprise Vault
                        \AdminService

Content   DWORD

                   The default value is 7200 (seconds).

Description   The Admin Service checks the Enterprise Vault Event log periodically
                     for errors. If too many errors have occurred since the last check, the
                     Admin Service shuts down Enterprise Vault.

                     PollingInterval specifies how often the Admin Service checks the
                     Enterprise Vault Event Log for errors.

SkipChecks

Location   HKEY_LOCAL_MACHINE
                      \SOFTWARE
                       \Wow6432Node
                        \KVS
                         \Enterprise Vault
                          \AdminService

Content   DWORD

                     0 — (Default) Perform memory and disk space checks

                     1 —Skip the checks

Description   Controls whether the Enterprise Vault Admin Service performs memory
                     and disk space checks when it starts. If any check fails the Admin
                     Service does not start and thus the other Enterprise Vault services do
                     not start.

SkipTempFolderCheck

Location   HKEY_LOCAL_MACHINE
                      \SOFTWARE
                       \Wow6432Node
                        \KVS

Content   DWORD32

                     0 — (Default) TEMP folder security checks enabled

                     1 — TEMP folder security checks disabled

Description   To protect against unauthorized access to the TEMP folder, which can
contain sensitive data, Enterprise Vault, and Compliance Accelerator
and Discovery Accelerator services check access to the folder on
startup, and periodically thereafter. If the services find unauthorized
access, they write an error to the event log and terminate immediately.

Use SkipTempFolderCheck to disable the TEMP folder security checks
made by the Enterprise Vault Admin service, the Accelerator Manager
service, and by the Compliance Accelerator client and the Discovery
Accelerator client.

For more information about TEMP folder security checks, see the
following technical note on the Veritas Support website:

http://www.veritas.com/docs/000023496

SPSOnly

Location   HKEY_LOCAL_MACHINE
 \SOFTWARE
  \Wow6432Node
   \KVS
    \Enterprise Vault
     \AdminService

Content   DWORD

1 — Force the Admin Service to start an Authserver process and
perform no monitoring.

Description   Set by the installation when the SharePoint Portal Server Web Parts
component is installed without any Enterprise Vault services.

Do not change this setting.

TempFolderExceptions

Location   HKEY_LOCAL_MACHINE
 \SOFTWARE
  \Wow6432Node
   \KVS

Content   String

Description   To protect against unauthorized access to the TEMP folder, which can contain sensitive data, Enterprise Vault, and Compliance Accelerator and Discovery Accelerator services check access to the folder on startup, and periodically thereafter. If the services find unauthorized access, they write an error to the event log and terminate immediately.

If you want to grant TEMP folder access to accounts other than those that the services expect, add these accounts to TempFolderExceptions as a semicolon-separated list. For example:

`MyDomain\JohnDoe;builtin\JohnDoe`

Note the use of `builtin` to identify local users and groups.

For more information, see the section called "TEMP folder security requirements" in the *Installing and Configuring* guide and the following technical note on the Veritas Support website:

http://www.veritas.com/docs/000023496

UseMQCounterMethod

Location
```
HKEY_LOCAL_MACHINE
 \Software
  \Wow6432Node
   \KVS
    \Enterprise Vault
     \AdminService
      \MSMQ Queue
```

Content   1 or 0.

Description   Reads the number of messages currently in the queue using the MSMQ API.

Set to zero to force use of default method, either WMI (Windows Management Instrumentation) or PDH (Performance Data Helper).

Warning

Location
```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \Wow6432Node
   \KVS
    \Enterprise Vault
     \AdminService
      \EventLog
```

Content
DWORD

Default value = 500.

0 — The Admin Service does not monitor the Enterprise Vault Event Log.

An integer specifying the number of Event Log entries that must occur within PollingInterval seconds before the Admin Service shuts down Enterprise Vault.

Description
The Admin Service checks the Enterprise Vault Event Log for errors every PollingInterval seconds. If the number of entries since the previous check is larger than that specified in Warning, the Admin Service calculates the percentage of errors that have come from Enterprise Vault. If this percentage is larger than that specified by Critical, the Admin Service shuts down Enterprise Vault.

Administration Console

This chapter includes the following topics:

- PSTMDirComputer

- PSTMDoDeletedFolder

- PSTMHideFile

- PSTMLastFolder

- PSTMMergeOption

- PSTMSetReadOnly

- ResetAuthorizationStore

- RunNowMailboxesMode

- RunNowReportingMode

- UseLanmanNameForSCM

- WarnCustomizeShortcut

- WarnScheduleConversion

- WarnSiteModified

AutoCreateMailboxPrefix

Location   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
```

Content   String value containing the prefix for the Exchange Server mailbox
                 created by Enterprise Vault.

Description   The mailbox name is constructed from:

Prefix-ExchangeServerName

E2KAutoCreateMailboxContainerADsPath

Location   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
```

Content   String.

User — The user is created in the default domain 'User' container.

ADsPath — the Active Directory fully-qualified path of the container to use.

Description   Enterprise Vault agents require an Exchange Server mailbox that they can use to log on. To facilitate this, a user is created in the Active Directory organization container where the currently-logged-on user is located.

Since organizations can set up Active Directory in many ways, this registry key can be used to override the default organization container.

FSARunNowReportingMode

Location   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
```

Content   String

Description   Used by File System Archiving to store the last Run Now mode used
                      for a file server.

                      Do not edit this value.

MaxArchivesToFind

Location   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
```

Content	String
	The default limit is 10000 (items).
Description	The maximum number of archives that the Export Archive wizard is to list.

MaxDominoMailboxes

Location	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
```

Content	String
Description	Controls the maximum number of items that are listed in the following dialog boxes:

- The mailbox listing when you are selecting mailboxes to add to a Domino Provisioning Group. The default maximum is 250.
- The list of users when you are adding users to the permissions of a Domino archive. The default maximum is 10000.

Set MaxDominoMailboxes on each computer that runs the Administration Console.

MaxFilterCount

Location	`HKEY_LOCAL_MACHINE`
	`  \SOFTWARE`
	`    \Wow6432Node`
	`      \KVS`
	`        \Enterprise Vault`
	`          \Admin`

Content	DWORD containing integer specifying the maximum number of filters. Default is 100.
Description	Specifies the maximum number of filters that users can create within each of the Personal Store Management nodes.
	We recommend that you limit the filter count to 100. Exceeding this value may affect the performance of Enterprise Vault.

NSFMCompact

Location	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`

Content	DWORD
	0 — Do not compress
	1 — Compress

Description   This value is created by the NSF migrator to remember the
                   corresponding setting chosen in the wizard.

                   Stores the last compression option selected by the user of the NSF
                   migrator.

NSFMDefaultRCId

Location   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
```

Content   String

Description   Stores settings chosen in the NSF migrator.

NSFMDeleteNSF

Location	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
```

Content	DWORD
	0 — Do not delete NSF files after migration
	1 — Delete NSF files after migration
Description	This value is created by the NSF migrator to remember the corresponding setting chosen in the wizard.
	Stores the last delete option selected by the user of the NSF migrator.

NSFMDirComputer

Location   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
```

Content   String value containing a computer name

Description   This value is created by the NSF migrator to remember the corresponding setting chosen in the wizard.

Stores the name of the directory computer that the NSF migrator connected to when it was last run.

NSFMDoDeletedFolder

Location   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
```

Content	DWORD
	0 — Trash items are not processed
	1 — Trash items are processed
Description	This value is created by the NSF migrator to remember the corresponding setting chosen in the wizard.
	Stores the last trash folder option selected by the user of the NSF migrator.

NSFMHideFile

Location	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
```

Content	DWORD
	0 — Do not hide NSF files
	1 — Hide NSF files
Description	This value is created by the NSF migrator to remember the corresponding setting chosen in the wizard.
	Stores the last hide option selected by the user of the NSF migrator.

NSFMLastFolder

Location   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
```

Content   String containing a folder name

Description   This value is created by the NSF migrator to remember the
                  corresponding setting chosen in the wizard.

                  The name of the last folder selected by the user of the NSF migrator.

NSFMMergeOption

Location   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
```

Content	DWORD
	0 — Merge
	1 — Separate
Description	This value is created by the NSF migrator to remember the corresponding setting chosen in the wizard.
	Stores the last merge option selected by the user of the NSF migrator.

NSFMSetReadOnly

Location	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
```

Content	DWORD
	0 — Set NSF files to read-only
	1 — Do not set NSF files to read-only
Description	This value is created by the NSF migrator to remember the corresponding setting chosen in the wizard.
	Stores the last read-only option selected by the user of the NSF migrator.

PSTMAutoCorrelate

Location   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
```

Content   String value:

0 — No automatic correlation.

1 — Automatic correlation.

Description   This value is created by the PST Migration wizard to remember the corresponding setting chosen in the wizard.

Specifies whether or not the PST Migration wizard does automatic correlation.

PSTMCompact

Location   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
```

Content   String value

0 — No compaction

1 — Compaction

Description   This value is created by the PST Migration wizard to remember the corresponding setting chosen in the wizard.

Specifies whether or not the PST Migration wizard compacts PST files after their migration.

PSTMDefaultRCId

Location   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
```

Content   String.

Description   Stores settings chosen in the PST Migration wizard.

PSTMDirComputer

Location   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
```

Content   String value containing a computer name.

Description   This value is created by the PST Migration wizard to remember the corresponding setting chosen in the wizard.

Stores the name of the Directory Computer that the PST Migration wizard connected to when it was last run.

PSTMDoDeletedFolder

Location   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
```

Content   String value:

0 — Deleted items are not processed.

1 — Deleted items are processed.

Description   This value is created by the PST Migration wizard to remember the corresponding setting chosen in the wizard.

Specifies whether the PST Migration wizard should process the Deleted Items folder.

PSTMHideFile

Location   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
```

Content   String:

0 — PST files are not hidden.

1 — PST files are hidden.

Description   This value is created by the PST Migration wizard to remember the corresponding setting chosen in the wizard.

Specifies whether the PST Migration wizard should hide PST files after migration.

PSTMLastFolder

Location   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
```

Content   String containing folder name.

Description   This value is created by the PST Migration wizard to remember the
                    corresponding setting chosen in the wizard.

                    Name of the last folder selected by the user of the PST Migration wizard.

PSTMMergeOption

Location   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
```

Content	String.
Description	This value is created by the PST Migration wizard to remember the corresponding setting chosen in the wizard.
	Name of the last folder selected by the user of the PST Migration wizard.

PSTMSetReadOnly

Location	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
```

Content	String:
	0 — PST files are not set to read only.
	1 — PST files are set to read only.
Description	This value is created by the PST Migration wizard to remember the corresponding setting chosen in the wizard.
	Specifies whether the PST Migration wizard should set PSTs to read only after migration or not.

ResetAuthorizationStore

Location	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
```

Content	String
Description	For use with roles-based administration. When set to 1, resets all the roles and role assignments so that they are the same as they were when installed.

RunNowMailboxesMode

Location	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
```

Content	String

Description   Used to store the **All Mailboxes**, **Select mailboxes** option of **Run Now**
                     in the Administration Console.

RunNowReportingMode

Location   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
```

Content   String

Description   Used to store the reporting mode last used for an Archiving Service
                     Run Now.

UseLanmanNameForSCM

Location

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
```

Content

String value:

0 — Use DNS name for SCM calls (default).

1 — Use the lanman name for SCM calls.

Description   May be needed to fix the "RPC server unavailable" error.

Each Enterprise Vault computer requires a registered IP address and the DNS properties for the TCP/IP protocol must be defined. Dynamic Host Configuration Protocol (DHCP) is not supported for Enterprise Vault services.

You may see this problem if the computer on which you are configuring the Enterprise Vault services does not have any WINS Servers defined and the check box for Enable DNS for Windows Resolution is not selected on the TCP/IP Protocol property page for WINS. You can either use DNS for service control management or enable DNS for Windows resolution.

To enable DNS for Windows resolution, perform the following steps in the order listed:

- In Windows Control Panel, double-click the **Network** applet.
- Click the **Protocols** tab.
- Select **TCP/IP Protocol**, and then click **Properties**.
- Click the **WINS Address** tab.
- Check **Enable DNS for Windows Resolution**, and then click **OK**.
- Restart your system.
- Create the services again.

If this does not solve the problem, set up the Administration Console computer to use the Lanman names instead of DNS names to connect to Service Control Manager.

WarnCustomizeShortcut

Location   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
```

Content	String
Description	Used to control whether, on the Shortcut Content tab of Site Properties, there is a warning when Customize is selected. WarnCustomizeShortcut is set when the message check box Always display this warning is changed.

WarnScheduleConversion

Location	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
```

Content	String value:
	0 — Do not warn when switching scales.
	1 — Warn when switching scale.
Description	When setting task schedules you can use either 1 hour or 15 minute scale. If you change the scale the Administration Console warns you that you are changing scale. WarnScheduleConversion controls whether this message is displayed.

WarnSiteModified

Location   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
```

Content   String value:

0 — Do not display the site warning message.

1 — Display the site warning message.

Description   When the **OK** button in Site Properties is clicked, the Administration Console displays, if necessary, a warning that some services need to be restarted. WarnSiteModified controls whether this message is displayed.

Agents

This chapter includes the following topics:

- ArchiveAppointmentOffset

- ClearDoNotArchive

- ClearDoNotJournal

- ClearUnreadNotification

- ClientRegInfoCacheReloadTimeOut

- ComplexMsgProcessing

- ComplexMsgs

- DeleteNonShortcutItems

- DisableProvisioningMbxSync

- DisableTransactionIDRecycling

- DominoArchiveMacBinHexOnNotes8

- DominoArchiveMissingFormMails

- DominoDeleteNonShortcutItems

- DominoHubServers

- DominoJournalingTemplates

- DominoMailTemplates

- DominoNewPersonDocAction

- DominoProvisioningACLSyncFilters

- DominoRepairMissingDefArchiveID

- DominoSynchMigratedMailFiles

- EnableLocalPartLookup (Domino)

- ExcludeDisabledADAccounts

- FixOrphanedShortcut

- FwdDateEligibility

- FwdDateEligibility_<server>

- FwdDateEligibilityEnd

- FwdDateEligibilityEnd_<server>

- HandleShortcutsWithMissingProps

- HardDeleteItems

- HideMovedItemUpdateFailure

- IgnoreEVDates (Domino)

- IgnoreEVDates (Exchange)

- IgnoreEVDatesEnd (Exchange)

- InternalSMTPDomains (Domino)

- InternalSMTPDomains (Exchange, SMTP, and File System Archiving)

- JournalTaskAccounts

- JournalWarningMsgCount

- ManualArchiveMessageClassCheck

- MaxNumOfRecipients

- MigratorApplyArchivePermOnNewFolders

- MigratorDisableShortcuts

- MigratorMoveEmptyFolders

- MoveFailedArchivalNotes

- MoveFailedItemsToInbox

- MoveNotEligibleForArchiveNotes

- MoveShortcutsToMailFile

- NetAppHomeMap

- NotesDomains

- NotesMoveRestrictDays

- OwaRestoredItemTimeout

- PopulateBillingAccount

- PreferQuotaNoSendLimit

- ProcessHiddenMailboxes

- ProfileExpire

- ProfileNamePoolSize

- RecoverTombstoneItems

- RestartAllMAPITaskIntervalMins

- RestartOnMAPIMutexError

- RetrievalKeepAliveMins

- RetryFailedDL

- ShortcutCalcAverageBodySize

- ShortcutCalcBannerSize

- ShortcutCalcBaseItemSize

- ShortcutCalcBodySizeMultiplier

- ShortcutCalcOverride

- ShortcutCalcRecipientSize

- ShortcutMoveRestrictDays

- SkipEnvelopeSMTPDomain

- SkipRecipCheckSize

- SynchInMigrationMode

- UseCharSetsInCustomisedBody

ArchiveAppointmentOffset

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

Content	DWORD
	The default (and minimum) value is 5 seconds.
Description	Enterprise Vault sets the archived time of an item by taking the item's last-modified time and adding a specified number of seconds to it. By default, Enterprise Vault adds five seconds to the last-modified time and then sets the archived time accordingly.
	In the case of calendar items only, you can increase the number of seconds that Enterprise Vault adds to the last-modified time. This may help to resolve a problem where Enterprise Vault archives multiple copies of large calendar items. Increase the value of ArchiveAppointmentOffset until there are no more duplicates in the archive.

ClearDoNotArchive

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

Content	DWORD
	0 — (Default) Do not archive items that are marked as "Do Not Archive".
	1 — Archive items even when they are marked "Do Not Archive".
Description	Clears the Do Not Archive property on items, thus allowing them to be archived. Only applies for the Exchange Mailbox and Exchange Public Folder tasks.
See also	See "ClearDoNotJournal" on page 58.

ClearDoNotJournal

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

Content	DWORD 0 — off 1 — on
Description	If set, an Exchange Journaling task resets any message with 'DoNotJournal' set to true back to false. This means the Exchange Journaling task will then attempt to archive the message. Applies only to Exchange Journaling tasks.

ClearUnreadNotification

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

Content	DWORD 0 — (Default) Send a notification to users who have deleted shortcuts to unread archived items. 1 — Do not send a notification to users who have deleted shortcuts to unread archived items.
Description	For manually deleted shortcuts to unread archived items: specifies whether to send notifications to users who have requested read receipts.

ClientRegInfoCacheReloadTimeOut

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

Content	DWORD. The default value is 1440 (minutes).
Description	This registry value sets a timeout value in minutes after which Enterprise Vault reloads the client registration information cache.

ComplexMsgProcessing

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

Content	DWORD 0 — (Default) Archive complex messages in PST format if archiving in MSG format fails. 1 — Do not archive complex messages in PST format if archiving in MSG format fails. Log an event. 2 — Do not archive complex messages in PST format if archiving in MSG format fails. Do not log an event.
Description	Controls the archiving behavior when a complex message cannot be archived in MSG format. The default in this case is to archive in PST format. However, if you do not want to allow PST files you can use ComplexMsgProcessing to change this behavior.

ComplexMsgs

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

Content   DWORD

Description   A counter used to store the number of messages that are successfully processed as complex. The counters are system-wide and are not reset on startup.

DeleteNonShortcutItems

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

Content   DWORD

The registry setting can have one of the following integer values, or a value which is the sum of two or more of the values:

- 0 (default) – Original items are not included in any shortcut deletion.
- 1– Original items are included in aged-based shortcut deletion.
- 2– Original items are included in storage expiry shortcut deletion.
- 4 – Original items are included in orphaned shortcut deletion.

Example cumulative values:

- 3 – Original items are included in aged-based shortcut deletion and storage expiry shortcut deletion.
- 7 – Original items are included in aged-based shortcut deletion, storage expiry shortcut deletion, and orphaned shortcut deletion.

If the value set is greater than or equal to 8, then task behavior is as for 0 (default); items are not included in any shortcut deletion.

Description   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 original items are not included in storage expiry shortcut
               deletion, age-based shortcut deletion, or orphaned shortcut deletion.
               Configure this registry setting to include such items in the required
               shortcut deletion runs.

               Storage expiry is configured in site properties.

               Aged-based shortcut deletion and orphaned shortcut deletion are
               configured in the Exchange Mailbox policy, on the **Shortcut Deletion**
               tab.

DisableProvisioningMbxSync

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

Content   DWORD

               0 — Synchronize user mailboxes after provisioning (Default).

               1 — Do not synchronize user mailboxes after provisioning.

Description   Specifies whether the Exchange provisioning task should issue mailbox
               synchronization requests for every user whose policy assignment has
               changed.

               In large installations, where it is undesirable to submit synchronization
               requests to all Exchange servers in the domain at the same time, you
               may want to disable this and defer synchronization to the scheduled
               nightly run.

DisableTransactionIDRecycling

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

Content	DWORD
	0 — Let Enterprise Vault recycle transaction IDs when making a repeat attempt to archive a message.
	1 — Do not recycle transaction IDs when retrying message archives.
Description	When Enterprise Vault makes a repeat attempt to archive a message, specifies whether to use the original transaction identifier or generate a new one each time.

DominoArchiveMacBinHexOnNotes8

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

Content	DWORD
	0 — (Default) Do not archive Domino MIME format messages with Mac BinHex attachments.
	1 — Archive Domino MIME format messages with Mac BinHex attachments.
Description	Due to a Notes 8.0 issue, Enterprise Vault servers that run any of the following Notes versions do not archive Domino MIME format messages with Mac BinHex attachments:

- 8.0
- 8.0.1
- 8.0.2

You can change this behavior as follows:

- Obtain and install the appropriate IBM hotfix. For details of the hotfix, see the Enterprise Vault *Compatibility Charts* at http://www.veritas.com/docs/000097605.
- Set DominoArchiveMacBinHexOnNotes8 to 1.

IBM have fixed the problem in Notes 8.0.3 and later. You can delete DominoArchiveMacBinHexOnNotes8 in Notes 8.0.3 and later but there is no requirement to do so because Enterprise Vault ignores DominoArchiveMacBinHexOnNotes8 in these versions of Notes.

DominoArchiveMissingFormMails

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

Content	DWORD 0 — (Default) Do not archive items that do not have a Form field. 1 — Archive items that do not have a Form field.
Description	Specifies whether Domino mailbox archiving and the NSF migrator should archive items that do not have a Form field. By default, these items are not archived.

DominoDeleteNonShortcutItems

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

Content	DWORD
	The registry setting can have one of the following integer values, or a value which is the sum of two or more of the values:

- 0 (default) – Original items are not included in any shortcut deletion.
- 1 – Original items are included in age-based shortcut deletion.
- 2 – Original items are included in storage expiry shortcut deletion.
- 4 – Original items are included in orphaned shortcut deletion.

Example cumulative values:

- 3 – Original items are included in age-based shortcut deletion and storage expiry shortcut deletion.
- 5 – Original items are included in age-based shortcut deletion and in orphaned shortcut deletion.
- 6 – Original items are included in storage expiry shortcut deletion and in orphaned shortcut deletion.
- 7 – Original items are included in age-based shortcut deletion, storage expiry shortcut deletion, and orphaned shortcut deletion.

If the value is 8 or greater, then the task behavior is as for 0; items are not included in any shortcut deletion.

Description	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 original items are not included in storage expiry shortcut deletion, age-based shortcut deletion, or orphaned shortcut deletion. Configure this registry setting to include such items in the required shortcut deletion runs.

Storage expiry is configured in site properties.

Aged-based shortcut deletion and orphaned shortcut deletion are configured in the Domino Mailbox policy, on the **Shortcut Deletion** tab.

DominoHubServers

Location	Define `DominoHubServers` on the Enterprise Vault server that runs the Domino provisioning task.

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

Define `DominoHubServers` on the Enterprise Vault server that runs the Domino provisioning task.

Content	Multi-String value listing Domino servers. Use a commas to separate server names.
	For example, `Hub1/Domain, Hub2/Domain`.
Description	If you use secondary Domino servers to keep replicas of users' mail files, it is possible to archive from those secondary servers instead of from the mail servers.
	If a user's mail server and secondary server are both defined as archiving targets, Enterprise Vault archives from the mail server. If the mail server is not defined, Enterprise Vault checks through the secondary servers in the sequence in which they are defined in `DominoHubServers` and archives from the first one that has a copy of the mail file.
	If a replica mail file moves from one secondary server to another, the archiving task automatically archives from the new server.

DominoJournalingTemplates

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

Content	String.
	Comma-separated list of mail journaling templates.

Description   Provides a list of the mail journaling templates for the Journaling task
to process on the Domino mail server. This list is in addition to the
normal journaling template (`StdMailJournaling`), for which the
Journaling task checks as a matter of course.

DominoMailTemplates

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

Content   String value containing comma separated Domino mail template names

Description   NSF migrator treats the templates in this registry value as standard
mail templates. For any NSF file that is based on any other Domino
template, NSF migrator warns that unexpected results can occur if you
continue to migrate the file. However, you can continue and migrate
the file if you are sure that it is a mail based file.

For a list of templates considered standard by default, see the *NSF
Migration* guide.

DominoNewPersonDocAction

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

Content   DWORD.

0 — (Default.) Locks the mail file of the former user to stop it from being
archived and prevent the new user from accessing the associated
archive.

1 — Gives the new user access to the archive of the former user.

2 — Create a new archive for the new user.

Description   Specifies whether, when the Domino Provisioning task configures mail
                     files that are new to Enterprise Vault and enables them for archiving,
                     it permits new users who have the same names as former users to
                     access those users' archives.

                     By default, new users cannot access the archives of their predecessors,
                     even when they share the same name, but there may be some
                     circumstances in which you want to allow this. For example, it may be
                     appropriate when a former employee rejoins the organization.

DominoProvisioningACLSyncFilters

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

Content   Multi-string (REG_MULTI_SZ).

                     One or more Domino user name, or group name — one string per line.

                     You can enter hierarchical names in either the Abbreviated or Canonical
                     format. You can enter non-hierarchical names as flat names.

                     If a Domino user or group name is hierarchical, it is displayed in
                     Abbreviated format in the ACL user interface, for example, John
                     Doe/Sales/Acme. However, the name is actually stored in Canonical
                     format, for example, CN=John Doe/OU=Sales/O=Acme.
                     Non-hierarchical names, such as group names, are displayed and
                     stored as flat names, for example, AdminGroup.

                     The following example value specifies two users and one group. The
                     first user is specified using the Abbreviated format, the second using
                     the Canonical format, and the group is specified as a flat name:

                     "Mike Smith/HCDomain"

                     "CN=Kevin Jones/O=HCDOMAIN"

                     "GroupOfSpecialAdmins"

Description   The Domino Provisioning task synchronizes ACL entries on a mail file
                   to the associated archive (except entries of type Anonymous, Server
                   or Server Group). Therefore, users with access to the mail file, also
                   have access to the associated archive. Access permissions are assigned
                   by means of a specific username ACL entry, or membership of a person,
                   or mixed group ACL entry.

                   This registry setting allows you to specify the names of Domino users
                   or groups, whose mail file ACL entry you do not want synchronized
                   automatically to the associated Enterprise Vault archives.

                   Note that the synchronization filter applies to all mail files in the Domino
                   domain. The ACL entry for each specified user and group will not be
                   synchronized automatically from any mail file in the Domino domain to
                   their associated archives.

                   Configure the setting on the Enterprise Vault server that is running the
                   Domino Provisioning task for your Domino domain.

DominoRepairMissingDefArchiveID

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

Content   DWORD

                 0 — (Default) Provisioning does not repair missing default archive IDs.

                 1 — Provisioning repairs missing default archive IDs.

Description   If Enterprise Vault finds that an archive ID in the Directory database does not match that in the corresponding mail file, Enterprise Vault can repair the database. Enterprise Vault copies the archive ID from the mail file to the database.

Enterprise Vault does not repair the database until you set the **DominoRepairMissingDefArchiveID** registry value.

If Enterprise Vault finds that an archive ID is incorrect it logs event 41300, as follows:

```
The default archive ID for mail file
'MailFileName'
has not been repaired as the
'DominoRepairMissingDefArchiveID'
registry key is not set.
```

If you see that event 41300 has been logged you can perform the repair as follows:

1   Set **DominoRepairMissingDefArchiveID** to 1.

2   Run the Domino Provisioning task to provision the mailbox that needs to be repaired.

The Domino Provisioning task repairs the ID entry and logs event 41299 as follows:

```
The default archive ID for mail file
MailFileName'
has been repaired as the
'DominoRepairMissingDefArchiveID'
registry key is set.
```

3   Set **DominoRepairMissingDefArchiveID** to 0.

Do not leave **DominoRepairMissingDefArchiveID** set to 1 permanently.

DominoSynchMigratedMailFiles

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

Content	DWORD
	0 — (Default) Provisioning does not synchronize migrated mail files.
	1 — Provisioning synchronizes migrated mail files.
Description	If Enterprise Vault finds that an archive ID in a mail file is incorrect, Enterprise Vault can copy the archive ID from the Directory database to the mail file.
	The archive ID may be incorrect if the user has changed name or has moved to a different domain, for example.
	If Enterprise Vault finds that an archive ID is incorrect it logs event 41302, as follows:

```
The migrated mail file 'MailFileName' has not been
synchronized as the 'DominoSynchMigratedMailFiles'
registry key is not set.
```

If you see that event 41302 has been logged you can perform the repair as follows:

1 Set **DominoSynchMigratedMailFiles** to 1.

2 Run the Domino Provisioning task to repair the mail file.

The Domino Provisioning task repairs the ID entry and logs event 41301 as follows:

```
The migrated mail file 'MailFileName'
has been synchronized.
```

3 Set **DominoSynchMigratedMailFiles** to 0.

Do not leave **DominoSynchMigratedMailFiles** set to 1 permanently.

EnableLocalPartLookup (Domino)

Location	HKEY_LOCAL_MACHINE
	 \Software
	  \Wow6432Node
	   \KVS
	    \Enterprise Vault
	     \Agents
	      \NotesDomains
	       \NotesDomainName

Content   DWORD.

                     0—Local part lookup is disabled (default).

                     1—Local part lookup is enabled.

Description   Controls whether Enterprise Vault performs a local address lookup for
                     specific Notes domains. The local lookup enables Enterprise Vault to
                     identify the Notes user name for those messages that are addressed
                     to alternative email addresses. The local lookup results can aid
                     searching in the web applications and in Compliance Accelerator and
                     Discovery Accelerator.

                     See "NotesDomains" on page 87.

ExcludeDisabledADAccounts

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

Content   DWORD.

                     0 — Enterprise Vault tries to synchronize all mailboxes, regardless of
                     whether they are associated with disabled Active Directory accounts.
                     If a synchronization attempt fails, Enterprise Vault records an error in
                     the event log.

                     1 — (Default) Enterprise Vault does not synchronize mailboxes that
                     are associated with disabled Active Directory accounts.

Description   Specifies whether Enterprise Vault tries to synchronize mailboxes that
                     are associated with disabled Active Directory accounts.

FixOrphanedShortcut

Location   HKEY_LOCAL_MACHINE
                      \Software
                       \Wow6432Node
                        \KVS
                         \Enterprise Vault
                          \Agents

Content   DWORD.

Description   When set to 1, forces the agent to use "fat" orphaned shortcut
                 processing. For each shortcut that is considered to be orphaned, a
                 further check is made to see if a duplicate of the original shortcut saveset
                 can be found. If it can, the shortcut is fixed to point to the remaining
                 duplicate saveset.

                 If you use FixOrphanedShortcut, remember to remove it as soon as
                 the shortcuts have been fixed. This registry value may have an adverse
                 effect on archiving performance.

FwdDateEligibility

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

Content   String value containing a date in ISO 8601 format.

Description   Set FwdDateEligibility to control the earliest date of items that Exchange
                 Journaling and Exchange Mailbox Tasks will archive. This is useful if
                 you want to restore multiple Exchange Server backups in sequence,
                 archiving each one and then restoring the next.

                 By setting FwdDateEligibility to be the date of the previous backup you
                 can archive just items that are newer than that date.

FwdDateEligibility_<server>

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

Content   String value containing a date in ISO 8601 format.

                 <server> is the name of the Exchange Server computer for which you
                 want to control the date.

Description	Set FwdDateEligibility_<server> to control the earliest date of items that the Exchange Mailbox Task will archive from server <server>. This is useful if you want to restore multiple Exchange Server backups in sequence, archiving each one and then restoring the next.
	By setting FwdDateEligibility_<server> to be the date of the previous backup you can archive just items that are newer than that date.

FwdDateEligibilityEnd

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

Content	String value containing a date in ISO 8601 format.
	<server> is the name of the Exchange Server computer for which you want to control the date.
Description	Set FwdDateEligibilityEnd to control the latest date of items that all Exchange Mailbox tasks and Exchange Journaling tasks will archive. This is useful if you want to restore multiple Exchange Server backups in sequence, archiving each one and then restoring the next.

FwdDateEligibilityEnd_<server>

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

Content	String value containing a date in ISO 8601 format.
	<server> is the name of the Exchange Server computer for which you want to control the date.

Description   Set FwdDateEligibilityEnd_<server> to control the latest date of items
                that the Exchange Mailbox task will archive from Exchange Server
                <server>. This is useful if you want to restore multiple Exchange Server
                backups in sequence, archiving each one and then restoring the next.

HandleShortcutsWithMissingProps

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

Content   0 - Warnings are logged for items with missing properties.

1 - Only DTrace output is produced for items with missing properties.

2 - (Default) If the retention category or archive ID (Enterprise Vault
custom MAPI properties) is missing, Enterprise Vault tries to fix these
properties.

3 - If the retention category or archive ID (Enterprise Vault custom MAPI
properties) is missing, Enterprise Vault tries to fix these properties. If it
fails, the item is deleted from the mailbox and an event is logged.

4 - If the shortcut is missing properties that are required for updating
moves, the item is deleted from the mailbox and an event is logged.

5 - If the shortcut is missing properties that are required for updating
moves, the item is deleted from the mailbox.

All other values are treated as 2 which forces default behavior.

Description   Controls what Enterprise Vault does with items that have Enterprise
                Vault custom MAPI properties missing.

HardDeleteItems

Location   HKEY_LOCAL_MACHINE
                                \SOFTWARE
                                 \Wow6432Node
                                  \KVS
                                    \Enterprise Vault
                                      \Agents
                                        \Common

Content   DWORD

0 — (Default) Deleted items are placed in the Deleted Items folder.

1 — Hard delete. Deleted items do not go into the Deleted Items folder.

Description   It is possible for you to configure the Exchange Journaling task so that it calls an external filter that makes the decision on whether to archive, move or delete an item.

By default, items are deleted to the journal mailbox Deleted Items folder. Use HardDeleteItems to force a hard delete so that items do not go into the Deleted Items folder.

See *Setting up SMTP Archiving* for details of setting up selective journaling.

HideMovedItemUpdateFailure

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

Content   DWORD

0 – (Default) Do not suppress event ID 3378.

1 – Suppress event ID 3378.

Description	When a user moves an archived item from one folder to another, certain item attributes such as location and retention category can be updated. If an error occurs during this update, or if the update is not allowed, event ID 3378 is written to the event log. For example, if an item is moved from a folder whose retention category prevents the deletion of items, the retention category from the target folder cannot be applied to this item unless it also prevents deletion.
	In some cases, event ID 3378 is logged in very large quantities. You can use HideMovedItemUpdateFailure to suppress the logging of these events. Set HideMovedItemUpdateFailure to 1 to suppress logging of event ID 3378. If HideMovedItemUpdateFailure is not present, or is set to its default value of 0, these events are logged.

IgnoreEVDates (Domino)

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

Content	DWORD
	0 or 1 — Off
	2 or 3 — Ignore RestoredDate
Description	Controls whether the RestoredDate property of items is ignored when archiving.
	After you set this value, run the Domino provisioning and Domino archiving tasks, and then set the value to 0 or remove it to resume normal archiving.

IgnoreEVDates (Exchange)

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

Content	DWORD
	0 — Off
	1 — Ignore Archived date
	2 — Ignore Restored date
	3 — Ignore both Archived and Restored date
Description	Controls whether the Archived date and Restored date properties of items are ignored when archiving.
	You must also set the IgnoreEVDatesEnd registry value to specify the latest date to be ignored. Items archived on or before that date will be treated as though they had never been archived or restored.
	After you set these values, use Run Now to run the archiving task, and then set the value of IgnoreEVDates to 0 or remove it to resume normal archiving.
See also	See "IgnoreEVDatesEnd (Exchange)" on page 77.

IgnoreEVDatesEnd (Exchange)

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

Content	String value containing a UTC date and time in the following ISO 8601 format: yyyyMMddThh:mm:ssZ
Description	Sets the date that the IgnoreEVDates registry value uses as the latest Archived or Restored date.
See also	See "IgnoreEVDates (Exchange)" on page 76.

InternalSMTPDomains (Domino)

Location
```
HKEY_LOCAL_MACHINE
 \Software
  \Wow6432Node
   \KVS
    \Enterprise Vault
     \Agents
      \NotesDomains
       \NotesDomainName
```

Content   String

A semi-colon separated list of domains for which you want to use local
lookup.

Description   You can specify that Enterprise Vault must perform a local address
lookup for specific Notes domains. The local lookup enables Enterprise
Vault to identify the Notes user name for messages that are addressed
to alternative email addresses. InternalSMTPDomains specifies the
SMTP domains for which you want to control local address lookup.

See "NotesDomains" on page 87.

InternalSMTPDomains (Exchange, SMTP, and File System Archiving)

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

Content   String.

A list of domains separated by semi-colons.

Description   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 Service account's email addresses.

Note: This registry value performs the same function as the advanced SMTP setting **List of internal SMTP domains**, which you can set when you edit the properties of your Enterprise Vault site with the Administration Console. Enterprise Vault automatically combines any domains that you specify through the registry value with those that you specify through the advanced setting. We recommend that you use the Administration Console setting to specify the domain list, as this saves you from having to set the registry value on every Enterprise Vault server.

For more information, see the *Administrator's Guide*.

JournalTaskAccounts

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

Content   String

Description   List of accounts used by Exchange Server Journaling tasks on this computer.

This registry value is generated automatically by the Task Controller Service. Do not edit this registry value.

JournalWarningMsgCount

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

Content	DWORD
	0 — Warning is disabled.
	Threshold — An integer specifying the maximum number of messages allowed in the Journal Inbox before a warning message is logged. The default is 150000.
Description	Controls whether Enterprise Vault logs a warning in the event log when the Journal Inbox contains JournalWarningMsgCount messages.
	The warning is logged when the Exchange Journal task starts and then every three hours.

ManualArchiveMessageClassCheck

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

Content	DWORD.
	0 — [Default] Archive all items when a user performs a manual archiving operation.
	1 — Archive only those items that belong to the message classes that are listed in the mailbox policy
Description	Specifies whether, when a user performs a manual archiving operation, Enterprise Vault archives only those items that belong to the message classes that are in the mailbox policy. By default, Enterprise Vault archives all items when manual archiving is performed. Enterprise Vault ignores the message class list that is in the mailbox policy.
	This registry value does not affect automatic, background archiving runs.

MaxNumOfRecipients

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

Content DWORD containing integer specifying the maximum number of recipients. Default is 5000.

Description Sets a maximum number of recipients. If a message has more recipients than this, it is not archived.

Opening the message to check the number of recipients results in a performance hit, so the number of recipients is ignored unless the message is bigger than the size set in SkipRecipCheckSize.

MigratorApplyArchivePermOnNewFolders

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

Content DWORD value.

0—PST import folders inherit their permissions from the parent folders.

1—PST import folders inherit the user's default archive permissions.

Description Specifies the permissions to assign to any archive folders that are created during the PST migration process.

MigratorDisableShortcuts

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

Content   DWORD

              0 — Create shortcuts when migrating PST contents with PST Migrator
              (Default)

              1 — Do not create shortcuts when migrating PST contents

Description   Works in combination with the PST Migrator policy setting Create
              Shortcuts in Mailboxes, which instructs Enterprise Vault to duplicate
              the folder structure of migrated PST files under a new, top-level folder
              in the mailboxes. This registry value lets you specify whether to create
              shortcuts.

See also   See "MigratorMoveEmptyFolders" on page 82.

MigratorMoveEmptyFolders

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

Content   DWORD.

              0 — Do not recreate empty folders in folder structure of migrated PSTs
              (default).

              1 — Recreate empty folders in folder structure of migrated PSTs.

Description   Works in combination with the PST Migrator policy setting Create
              Shortcuts in Mailboxes, which instructs Enterprise Vault to duplicate
              the folder structure of migrated PST files under a new, top-level folder
              in the mailboxes. This registry value lets you specify whether to recreate
              empty folders in the folder structure.

See also   See

MoveFailedArchivalNotes

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

Content   DWORD

             0 — Do not move failed notes to mail file

             1 — Move failed notes to mail file

Description Controls whether NSF migrator moves notes that fail archiving to the
             mail file.

MoveFailedItemsToInbox

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

Content   DWORD

             0 —Do not restore items from Failed to... folders when Journaling task
             starts (Default).

             1 — Restore items from Failed to... folders when Journaling task starts.

Description Specifies whether, when an Exchange Journaling task starts, it copies
             back to the Inbox any messages in the Failed to... folders under the
             Enterprise Vault Exchange Journaling Task folder.

MoveNotEligibleForArchiveNotes

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

Content	DWORD
	0 — Do not move ineligible notes to mail file
	1 — Move ineligible notes to mail file
Description	Controls whether NSF migrator moves ineligible notes to the mail file.

MoveShortcutsToMailFile

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

Content	DWORD
	0 — (Default) Do not move shortcuts to mail file
	1 — Move shortcuts to mail file
Description	Controls whether NSF migrator moves shortcuts to the mail file.
	Note: If this DWORD value is not set, Enterprise Vault's default action (do not move shortcuts to mail file) is applied. However, this default action is overridden by the setting of MoveNotEligibleForArchiveNotes.

NetAppHomeMap

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

Content   String

Description   The NetApp Filer autohome feature provides each Windows user with
                     a home directory that is accessible through a share in this format:

```
\\filer_name\user_name$
```

During PST migration, Enterprise Vault must find the complete UNC
paths to the NetApp Filer shares. You must host users' home directories
beneath designated directories on the NetApp Filer. Share these
directories and assign the Vault Service account permission to access
the shares. Finally, add the list of shared directories to the
NetAppHomeMap registry value on all the Enterprise Vault Directory
service computers.

In the following example, users' directories are stored below three
directories called `engineering`, `finance` and `marketing`:

```
+---engineering
|   +---UserA
|   +---UserB
|   \---UserC
|
+---finance
|   +---UserD
|   +---UserE
|   \---UserF
|
\---marketing
    +---UserG
    +---UserH
    \---UserI
```

You must share `engineering`, `finance`, and `marketing` and make
each accessible to the Vault Service account. Then add the three share
names in a semicolon-separated list to NetAppHomeMap:

```
engineering;finance;marketing
```

When Enterprise Vault processes a PST file that is on
`\\filer_name\UserG$`, it attempts to connect to a directory called
`UserG` under each of the shares listed in NetAppHomeMap:

```
\\filer_name\engineering\UserG
\\filer_name\finance\UserG
\\filer_name\marketing\UserG
```

In the first two cases, Enterprise Vault does not find the directory, but
in the third case it does. When Enterprise Vault has found
`\\filer_name\marketing\UserG`, it can then ascertain the
complete UNC path to the directory, and proceed with the migration of
the PST files that it contains.

NotesDomains

Location

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

Content

String.

Description

You can specify that Enterprise Vault must perform a local address lookup for specific Notes domains. The local lookup enables Enterprise Vault to identify the Notes user name for those messages that are addressed to alternative email addresses. The local lookup results can aid searching in the web applications and in Compliance Accelerator and Discovery Accelerator.

To specify local lookup domains

1   On an Enterprise Vault server that runs a Domino archiving or journaling task, create a new registry key called **NotesDomains**.

2   Under the new **NotesDomains** key, create a subkey for each Notes domain. For example, if you have Notes domains 'MyNotesDomain1' and 'MyNotesDomain2' you create subkeys 'MyNotesDomain1' and 'MyNotesDomain2'.

3   Under each of the Notes domain subkeys, create a new String value called InternalSMTPDomains.

4   Assign to each InternalSMTPDomains value a string that lists the domains for which you want to use local lookup. Use semi-colons (;) to separate domains. For example:

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

5   Under each of the Notes domain subkeys, create a new DWORD value called **EnableLocalPartLookup**.

6   Give EnableLocalPartLookup one of the following values:
   ■   0 to disable local part lookup
   ■   1 to enable local part lookup

7   Repeat all these steps for any other Enterprise Vault servers that run Domino archiving or journaling tasks.

The Enterprise Vault behavior is as follows:

- If the NotesDomains key is not present Enterprise Vault performs a full address lookup and places a warning in the event log.
- If the NotesDomain key is present but has no key for the current Notes domain, Enterprise Vault records the original address and performs a full address lookup.
- If the NotesDomain key is present and has a key for the current Notes domain, Enterprise Vault does the following:
    - If EnableLocalPartLookup is set to 0, performs a full address lookup.
    - If EnableLocalPartLookup is set to 1, performs a full address and local part lookup for those addresses that match the domain.

If the InternalSMTPDomains list is present and the SMTP domain matches a domain in the list, SMTP messages being archived from journals are checked with full address and local part lookup.

If the InternalSMTPDomains list is not present or there is no match, Enterprise Vault performs a full address lookup.

NotesMoveRestrictDays

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

Content	DWORD specifying a number of days
Description	When set to a non-zero value, notes are moved to mail files by NSF migrator only if they are within the number of days specified. Otherwise, they remain in the NSF files.

OwaRestoredItemTimeout

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

Content	DWORD
	An integer indicating a number of minutes.
	Default is 120 (minutes).
Description	When an OWA user chooses Open, Forward, Reply, or Reply To All, the selected item is temporarily restored to the deleted items folder. OwaRestoredItemTimeout specifies the minimum amount of time that must elapse before the temporarily restored item can be automatically deleted by the Mailbox Archiving Task.

PopulateBillingAccount

| Location | ```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \Wow6432Node
   \KVS
    \Enterprise Vault
     \Agents
``` |
Content	DWORD.
	0 — Do not repopulate the Billing Owner field on archives where it is blank. (Default.)
	1 — Repopulate the Billing Owner field on archives where it is blank.
Description	In archives for which no billing owner is specified, lets you specify one by synchronizing with the mailbox.

PreferQuotaNoSendLimit

| Location | ```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \Wow6432Node
   \KVS
    \Enterprise Vault
     \Agents
``` |
| Content | DWORD |

Description   A value greater than zero signifies a preference for the NO_SEND limit
over the NO_SEND_RECEIVE limit. If the value is zero or missing then
the behavior is as before and NO_SEND_RECEIVE takes preference.
However, if the NO_SEND_RECEIVE limit is set to a value smaller than
the NO_SEND limit then NO_SEND_RECEIVE will be used, even if
the registry value is set. This has to be the case otherwise the archive
attempt will fail.

ProcessHiddenMailboxes

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

Content   DWORD.

              0 — Ignore hidden mailboxes (default).

              1 — Process hidden mailboxes.

Description   Specifies whether the Exchange Mailbox archiving task should ignore
              or process hidden mailboxes. By default, the task ignores hidden
              mailboxes.

              Hidden mailboxes are mailboxes that are excluded from the Exchange
              Global Address List.

              If you set the value to 1, you may first need to run the Exchange
              Provisioning task to process any hidden mailboxes that have never
              been processed by Enterprise Vault. Restart the Exchange Mailbox
              task and synchronize the mailboxes.

ProfileExpire

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

Content	DWORD
	Default is 3 (days)
Description	The number of days to wait before deleting abandoned MAPI profiles.
	Do not specify 0, because profiles may be in use.

ProfileNamePoolSize

Location	HKEY_LOCAL_MACHINE
	 \SOFTWARE
	  \Wow6432Node
	   \KVS
	    \Enterprise Vault
	     \MAPI

Content	DWORD
	1500 — (Default)
Description	Sets the size of Enterprise Vault's profile name pool.
	Do not change ProfileNamePoolSize from its default value unless your technical support provider advises you to do so. If you do change this value, you must restart Enterprise Vault services for the change to take effect.

RecoverTombstoneItems

Location	HKEY_LOCAL_MACHINE
	 \Software
	  \Wow6432Node
	   \KVS
	    \Enterprise Vault
	     \Agents

Content	DWORD
	0 — (Default) Do not recover any "tombstone" (soft-deleted) items when processing a mailbox folder.
	1 — Recover tombstone items.

Description   As the Enterprise Vault archiving service processes each mailbox folder, controls whether the service recovers any items that have been soft-deleted from the folder. These are items that the user has deleted but for which a backup copy is kept on the Microsoft Exchange server for a certain period of time. If you set RecoverTombstoneItems to 1, all the items are recovered except for pending items and shortcuts. Enterprise Vault recovers the items to their original folders, which it recreates if they have been deleted.

Note: Depending on the mailbox policy settings, there can be an undesired effect on the mailbox if you choose to recover tombstone items. For example, the mailbox store will grow in size if you have chosen not to create shortcuts and not to delete the original items after archiving. An email that was archived by Enterprise Vault and then deleted by the user will be rearchived as a new item, resulting in duplicate items in the archive.

RestartAllMAPITaskIntervalMins

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

Content   DWORD

0 — (Default) Enterprise Vault does not restart MAPI tasks automatically.

An integer that specifies, in minutes, the MAPI task restart interval.

Description   When RestartAllMAPITaskIntervalMins is set to 0 or is not set, Enterprise Vault does not automatically restart MAPI tasks.

Set RestartAllMAPITaskIntervalMins to specify the interval in minutes, at which Enterprise Vault automatically restarts MAPI tasks.

RestartOnMAPIMutexError

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

Content   DWORD

                    0 — Do not restart MAPI tasks when a MAPI mutex error occurs.

                    1 — (Default) Restart MAPI tasks when a MAPI mutex error occurs.

Description   By default, Enterprise Vault restarts all MAPI tasks when a MAPI mutex
                    error occurs.

                    Change the value of RestartOnMAPIMutexError to 0 if you do not want
                    Enterprise Vault to restart MAPI tasks when a MAPI mutex error occurs.

RetrievalKeepAliveMins

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

Content   DWORD value set to a number of minutes. The default is 2.

                    If set to 0, the retrieval task keeps running indefinitely.

Description   Specifies the number of minutes for which the Enterprise Vault retrieval
                    task should continue to run when no work has arrived for it to do. After
                    the specified time has elapsed, the task stops running automatically.

RetryFailedDL

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

Content	DWORD
	0 — If the Journaling Service cannot open the distribution list for a message, move the message into the `Failed DL Expansions` folder.
	1 — If the Journaling Service cannot open the distribution list for a message, requeue the message for later archiving. By default, the message is moved to the `Failed DL Expansions` folder after three failed attempts.
Description	Specifies how the Journaling Service handles messages when it cannot open a distribution list in the **To**, **Cc** and **Bcc** fields.

ShortcutCalcAverageBodySize

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

Content	DWORD containing an integer specifying a number of Bytes. The default is 5120.
Description	Enterprise Vault uses this value when it calculates how many items to archive to keep a percentage of Exchange mailbox quota free. For information about archiving based on mailbox quota, see the *Enterprise Vault Administrator's Guide*.
	This value specifies the size that Enterprise Vault uses for the body of the item. The body size is included in the calculation when shortcuts include the original body of the item.

ShortcutCalcBannerSize

Location

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

Content

DWORD containing an integer specifying a number of Bytes. The default is 3072.

Description

Enterprise Vault uses this value when it calculates how many items to archive to keep a percentage of Exchange mailbox quota free. For information about archiving based on mailbox quota, see the *Enterprise Vault Administrator's Guide*.

This value specifies the size that Enterprise Vault uses for a shortcut banner. The banner size is included in the calculation when shortcuts include a banner that contains a link to the archived item.

See also

ShortcutCalcBaseItemSize

Location

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

Content

DWORD containing an integer specifying a number of Bytes. The default is 3072.

Description

Enterprise Vault uses this value when it calculates how many items to archive to keep a percentage of Exchange mailbox quota free. For information about archiving based on mailbox quota, see the *Enterprise Vault Administrator's Guide*.

This value specifies the size that Enterprise Vault uses as the base size for a shortcut. The base size is included in the calculation when shortcuts replace items. In addition to the base size, Enterprise Vault includes in the calculation other elements of a shortcut.

See also

See "ShortcutCalcAverageBodySize" on page 94.

See "ShortcutCalcBannerSize" on page 95.

See "ShortcutCalcBodySizeMultiplier" on page 96.

See "ShortcutCalcOverride" on page 97.

See "ShortcutCalcRecipientSize" on page 98.

ShortcutCalcBodySizeMultiplier

Location

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

Content

DWORD containing a value that represents a multiplier. The default is x1.

Description   Enterprise Vault uses this value when it calculates how many items to
                   archive to keep a percentage of Exchange mailbox quota free. For
                   information about archiving based on mailbox quota, see the *Enterprise
                   Vault Administrator's Guide*.

                   This value specifies the multiplier that Enterprise Vault applies to the
                   number of characters to include in a shortcut. This number is the value
                   specified in the **Message characters to include** box on the **Shortcut
                   Content** tab of the Exchange Mailbox Policy. The result is included in
                   the calculation when shortcuts replace items.

See also

ShortcutCalcOverride

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

Content   DWORD containing an integer specifying a number of Bytes. The default
                   is no value.

Description   Enterprise Vault uses this value when it calculates how many items to
                   archive to keep a percentage of Exchange mailbox quota free. For
                   information about archiving based on mailbox quota, see the *Enterprise
                   Vault Administrator's Guide*.

                   This value specifies a fixed average size for shortcuts. If you set this
                   value, it overrides the calculation of average shortcut size that Enterprise
                   Vault otherwise performs, based on separate elements of a shortcut.

See also   See "ShortcutCalcAverageBodySize" on page 94.

See "ShortcutCalcBannerSize" on page 95.

See "ShortcutCalcBaseItemSize" on page 96.

See "ShortcutCalcBodySizeMultiplier" on page 96.

See "ShortcutCalcRecipientSize" on page 98.

ShortcutCalcRecipientSize

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

Content   DWORD containing an integer specifying a number of Bytes. The default is 1024.

Description   Enterprise Vault uses this value when it calculates how many items to archive to keep a percentage of Exchange mailbox quota free. For information about archiving based on mailbox quota, see the *Enterprise Vault Administrator's Guide*.

This value specifies the size that Enterprise Vault uses for recipient information in a shortcut. The size of recipient information is included in the calculation when shortcuts replace items.

See also   See "ShortcutCalcAverageBodySize" on page 94.

See "ShortcutCalcBannerSize" on page 95.

See "ShortcutCalcBaseItemSize" on page 96.

See "ShortcutCalcBodySizeMultiplier" on page 96.

See "ShortcutCalcOverride" on page 97.

ShortcutMoveRestrictDays

Location

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

Content   DWORD specifying a number of days

Description   When set to a non-zero value, shortcuts are moved to mail files by NSF migrator only if they are within the number of days specified. Otherwise, they remain in the NSF files.

SkipEnvelopeSMTPDomain

Location

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

Content   String.

                   A list of domains separated by semi-colons.

Description   Causes Journaling to skip recipient addresses that include the specified domains when checking whether message envelope recipients are contained in distribution lists. For example, "example.com;example.net".

SkipRecipCheckSize

Location

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

Content	DWORD value specifying the message size in KB. Default is 750.
Description	Specifies the threshold size below which MaxNumOfRecipients does not check messages to see how many recipients there are.
See also	See "MaxNumOfRecipients" on page 81.

SynchInMigrationMode

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

Content	DWORD. 0 — (Default.) Enterprise Vault does not assign or update moved mailboxes to existing entries that have the same legacyMbxDN values. Instead, the server produces an event warning. 1 — Makes Enterprise Vault assign new or moved mailboxes to existing archives if the legacyMbxDN values match. 2 — Creates new entries for the new or moved mailboxes and renames any old entries that have matching legacyMbxDN values, by adding timestamps to the legacyMbxDN fields.
Description	Specifies whether, when migrating mailboxes from one Exchange Server to another, Enterprise Vault automatically assigns migrated mailboxes to existing archives. SynchInMigrationMode affects only the association between user mailboxes and archives; it does not affect the association between journal mailboxes and their archives.

UseCharSetsInCustomisedBody

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

Content	DWORD
	0 — Do not include character set information in custom shortcut body.
	1 — Include character set information in custom shortcut body.
Description	Specifies whether, when it successfully archives a message and leaves a custom shortcut in its place, Enterprise Vault includes character set information in the shortcut body. If this information is included, the shortcut content displays correctly even when stored in non-Unicode—aware mediums.

Backtrace

This chapter includes the following topics:

Enabled

Location	HKEY_LOCAL_MACHINE
	 \SOFTWARE
	  \Wow6432Node
	   \KVS
	    \Enterprise Vault
	     \Backtrace

Content	DWORD. 0 — (Default) Backtrace is disabled. 1 — Backtrace is enabled.

Description   Specifies whether Backtrace is enabled. By default, Backtrace is disabled. For best performance, disable Backtrace when it is not required.

Backtrace is disabled automatically while DTrace is running.

Changes to Backtrace registry values take effect automatically, within a minute or so. You do not need to restart any Enterprise Vault services or tasks.

See the "Backtrace" chapter in the *Utilities* guide.

Exclude

Location   ```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \Wow6432Node
   \KVS
     \Enterprise Vault
      \Backtrace
```

Content   String.

A semicolon-separated list of event IDs. For example:

3310;3230;2776

Description   A list of the events that Backtrace must ignore when RuleType is set to 'Exclude'.

See "RuleType" on page 107.

See the "Backtrace" chapter in the *Utilities* guide.

Include

Location   ```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \Wow6432Node
   \KVS
     \Enterprise Vault
      \Backtrace
```

Content          String.

                 A semicolon-separated list of event IDs. For example:

                 **3310;3230;2776**

Description      A list of the events that trigger Backtrace when RuleType is set to
                 'Include'.

                 See "RuleType" on page 107.

                 See the "Backtrace" chapter in the *Utilities* guide.

# LogFileKeepDays

Location         HKEY_LOCAL_MACHINE
                  \SOFTWARE
                   \Wow6432Node
                    \KVS
                      \Enterprise Vault
                       \Backtrace

Content          DWORD

                 An integer that specifies the number of days to keep log files. The
                 default is 7 (days). Specify 0 to make Backtrace keep logs forever.

Description      Enterprise Vault automatically deletes old BackTrace log files.
                 LogFileKeepDays specifies the number of days to keep log files before
                 Enterprise Vault deletes them.

                 See the "Backtrace" chapter in the *Utilities* guide.

# LogFolderPath

Location         HKEY_LOCAL_MACHINE
                  \SOFTWARE
                   \Wow6432Node
                    \KVS
                      \Enterprise Vault
                       \Backtrace

Content                 STRING

The path to the folder where Backtrace must save its log files. The
default folder is the `Backtrace` subfolder of the Enterprise Vault
`Reports` folder.

Description             Backtrace saves its log files in the folder that is specified by
LogFolderPath. Backtrace creates the folder automatically if it does not
already exist. If the folder path is invalid or cannot be accessed,
Backtrace uses the default folder.

If no value is specified for LogFolderPath, Backtrace stores its log files
in the default folder.

See the "Backtrace" chapter in the *Utilities* guide.

# MaxEventsOfEachTypePerDay

Location                HKEY_LOCAL_MACHINE
 \SOFTWARE
  \Wow6432Node
   \KVS
    \Enterprise Vault
     \Backtrace

Content                 DWORD

An integer that specifies the maximum number of log files to create
each day for each event. The default is 5. Specify '0' for no limit.

Description             By default Backtrace does not create more than five log files for each
event per process per day. This limit means that the space that
Backtrace log files take up is unlikely to cause a problem.

The MaxEventsOfEachTypePerDayAcrossAllProcesses registry value
controls the maximum number of log files from all Enterprise Vault
processes. If you set this value too low you be careful not to prevent
log file generation by MaxEventsOfEachTypePerDay.

See the "Backtrace" chapter in the *Utilities* guide.

# MaxEventsOfEachTypePerDayAcrossAllProcesses

| | |
|---|---|
| Location | HKEY_LOCAL_MACHINE<br> \SOFTWARE<br>  \Wow6432Node<br>   \KVS<br>    \Enterprise Vault<br>     \Backtrace |
| Content | DWORD |
| | An integer that specifies the maximum number of log files to create each day for each event for all processes. The default is 40. Specify '0' for no limit. |
| Description | By default Backtrace does not create more than 40 log files for each event per day for all processes. This limit means that the space that Backtrace log files take up is unlikely to cause a problem. |
| | The MaxEventsOfEachTypePerDayAcrossAllProcesses registry value controls the maximum number of log files from all Enterprise Vault processes in a day. |
| | If you set this value too low, be careful not to prevent log file generation by MaxEventsOfEachTypePerDay. |
| | See "MaxEventsOfEachTypePerDay" on page 105. |
| | Backtrace does not log any data if there is less than 100 MB free on the disk. You cannot change this value. |
| | See the "Backtrace" chapter in the *Utilities* guide. |

# MaxSizeOfAllLogsPerDayMB

| | |
|---|---|
| Location | HKEY_LOCAL_MACHINE<br> \SOFTWARE<br>  \Wow6432Node<br>   \KVS<br>    \Enterprise Vault<br>     \Backtrace |
| Content | DWORD |
| | An integer that specifies the maximum total size of all backtrace log files that can be generated in a single day. The default is 200 (megabytes). Specify '0' for no limit. |

Description   By default Backtrace does not create more than 200MB of log files per day. This limit means that the space that Backtrace log files take up is unlikely to cause a problem.

Backtrace does not log any data if there is less than 100MB free on the disk. You cannot change this value.

See the "Backtrace" chapter in the *Utilities* guide.

# RuleType

Location   HKEY_LOCAL_MACHINE
 \SOFTWARE
  \Wow6432Node
   \KVS
    \Enterprise Vault
     \Backtrace

Content   String

Exclude — (Default) The events that are specified in the Exclude registry value do not trigger Backtrace. All other error events and warning events trigger Backtrace.

Include — All the events that are specified in the Include registry value trigger Backtrace. Other events do not trigger Backtrace.

Description   The **Ruletype** value controls the manner in which Backtrace is triggered, as follows:

- When Ruletype is set to 'Exclude', all error events and warning events trigger Backtrace, except for those that are listed in the Exclude registry value.
- When Ruletype is set to 'Include', all the events that are specified in the Include registry value trigger Backtrace. Other events do not trigger Backtrace.

See the "Backtrace" chapter in the *Utilities* guide.

# Clustering

This chapter includes the following topics:

- Cluster

- ClusterNetworkDomain

- ClusterNetworkFQDN

- ClusterNetworkHostName

- ClusterNetworkName

- ComputerName

## Cluster

| Location | HKEY_LOCAL_MACHINE<br> \SOFTWARE<br>  \Wow6432Node<br>   \KVS<br>    \Enterprise Vault<br>     \Clustering |
|---|---|
| Content | DWORD |
| Description | Stores the information that you submitted when you configured Enterprise Vault for use in a Veritas Cluster Server or Windows Server Failover Clustering environment. Do not modify this value. |

# ClusterNetworkDomain

| | |
|---|---|
| Location | HKEY_LOCAL_MACHINE<br> \SOFTWARE<br>  \Wow6432Node<br>   \KVS<br>    \Enterprise Vault<br>     \Clustering |

Content          String

Description      Stores the information that you submitted when you configured
                 Enterprise Vault for use in a Veritas Cluster Server environment. Do
                 not modify this value.

# ClusterNetworkFQDN

| | |
|---|---|
| Location | HKEY_LOCAL_MACHINE<br> \SOFTWARE<br>  \Wow6432Node<br>   \KVS<br>    \Enterprise Vault<br>     \Clustering |

Content          String

Description      Stores the information that you submitted when you configured
                 Enterprise Vault for use in a Veritas Cluster Server or Windows Server
                 Failover Clustering environment. Do not modify this value.

# ClusterNetworkHostName

| | |
|---|---|
| Location | HKEY_LOCAL_MACHINE<br> \SOFTWARE<br>  \Wow6432Node<br>   \KVS<br>    \Enterprise Vault<br>     \Clustering |

Content          String

Description          Stores the information that you submitted when you configured
                     Enterprise Vault for use in a Veritas Cluster Server or Windows Server
                     Failover Clustering environment. Do not modify this value.

# ClusterNetworkName

Location             HKEY_LOCAL_MACHINE
                      \SOFTWARE
                       \Wow6432Node
                        \KVS
                          \Enterprise Vault
                            \Clustering

Content              String

Description          Stores the information that you submitted when you configured
                     Enterprise Vault for use in a Veritas Cluster Server or Windows Server
                     Failover Clustering environment. Do not modify this value.

# ComputerName

Location             HKEY_LOCAL_MACHINE
                      \SOFTWARE
                       \Wow6432Node
                        \KVS
                          \Enterprise Vault
                            \Clustering

Content              String

Description          Stores the information that you submitted when you configured
                     Enterprise Vault for use in a Veritas Cluster Server or Windows Server
                     Failover Clustering environment. Do not modify this value.

# Code Page Detection

This chapter includes the following topics:

- DecisionType

- FallbackCodepage

- LogConversions

- MinimumConfidenceLevel

- MinimumDocumentPercent

- PriorityCodepages

## DecisionType

| | |
|---|---|
| Location | HKEY_LOCAL_MACHINE<br> \SOFTWARE<br>  \Wow6432Node<br>   \KVS<br>    \Enterprise Vault<br>     \Storage<br>      \CodePageDetection |
| Content | DWORD.<br><br>0 — Use the code page to which Enterprise Vault attaches the highest confidence value (Default).<br><br>1 — Use the code page in which the highest percentage of the message is written.<br><br>2 — Use the code page with the highest (document percentage) x (confidence) value. |

| Description | Specifies the method with which Enterprise Vault detects the most appropriate code page for messages. |
|---|---|
| | For more information on this registry value, see the following article on the Veritas Enterprise Support site: |
| | http://www.veritas.com/docs/000030991 |

# FallbackCodepage

| Location | HKEY_LOCAL_MACHINE<br> \SOFTWARE<br>  \Wow6432Node<br>   \KVS<br>    \Enterprise Vault<br>     \Storage<br>      \CodePageDetection |
|---|---|
| Content | DWORD. |
| Description | Specifies the default code page to use if Enterprise Vault cannot guess at the code page. The default is 1252 - Western European. |
| | For more information on this registry value, see the following article on the Veritas Enterprise Support site: |
| | http://www.veritas.com/docs/000030991 |

# LogConversions

| Location | HKEY_LOCAL_MACHINE<br> \SOFTWARE<br>  \Wow6432Node<br>   \KVS<br>    \Enterprise Vault<br>     \Storage<br>      \CodePageDetection |
|---|---|
| Content | DWORD. |
| | 0 — Do not add an event log record when a code page decision is made (Default). |
| | 1 — Add an event log record when a code page decision is made. |

Description        Specifies whether to add a record to the event log for each message
                   for which Enterprise Vault has to make a decision about the code page.

                   For more information on this registry value, see the following article on
                   the Veritas Enterprise Support site:

                   http://www.veritas.com/docs/000030991

# MinimumConfidenceLevel

Location           HKEY_LOCAL_MACHINE
                    \SOFTWARE
                     \Wow6432Node
                      \KVS
                       \Enterprise Vault
                        \Storage
                         \CodePageDetection

Content            DWORD.

Description        Specifies a value indicating the degree to which the detected code page
                   is correct before that code page is used. Confidence is based on an
                   internal scoring method. It is a relative cumulative data item rather than
                   an absolute percentage. The default confidence level is 30.

                   For more information on this registry value, see the following article on
                   the Veritas Enterprise Support site:

                   http://www.veritas.com/docs/000030991

# MinimumDocumentPercent

Location           HKEY_LOCAL_MACHINE
                    \SOFTWARE
                     \Wow6432Node
                      \KVS
                       \Enterprise Vault
                        \Storage
                         \CodePageDetection

Content            DWORD.

Description          Specifies the minimum percentage of message text that is in a specific
                     language before Enterprise Vault will use the associated code page for
                     the message. The default is 10 percent.

                     For more information on this registry value, see the following article on
                     the Veritas Enterprise Support site:

                     http://www.veritas.com/docs/000030991

# PriorityCodepages

Location             HKEY_LOCAL_MACHINE
                      \SOFTWARE
                       \Wow6432Node
                        \KVS
                         \Enterprise Vault
                          \Storage
                           \CodePageDetection

Content              String.

Description          Provides a comma-separated list of up to 20 code pages that should
                     be given priority. The earlier a code page appears in the list, the higher
                     its priority. If one of the possible code pages detected is in this list, the
                     code page is used regardless of confidence level or document
                     percentage.

                     If you do not set this registry value then, by default, there are no priority
                     code pages.

                     For more information on this registry value, see the following article on
                     the Veritas Enterprise Support site:

                     http://www.veritas.com/docs/000030991

# Directory Service

This chapter includes the following topics:

- ArchiveListChunkThreshold

- Database Name

- Database Username

- Network Type

## ArchiveListChunkThreshold

| | |
|---|---|
| Location | HKEY_LOCAL_MACHINE<br> \SOFTWARE<br>  \Wow6432Node<br>   \KVS<br>    \Enterprise Vault<br>     \Directory<br>      \DirectoryService |
| Content | Default is 5000. |
| Description | Controls the maximum number of archives that the Administration Console displays. If there are more archives than this limit the Administration Console displays them in A-Z subcontainers. |

# Database Name

| | |
|---|---|
| Location | HKEY_LOCAL_MACHINE<br> \SOFTWARE<br>  \Wow6432Node<br>   \KVS<br>    \Enterprise Vault<br>     \Directory<br>      \DirectoryService |
| Content | String value containing database name. |
| Description | The name of the SQL database used by the Directory Service.<br><br>Do not change this setting. |

# Database Username

| | |
|---|---|
| Location | HKEY_LOCAL_MACHINE<br> \SOFTWARE<br>  \Wow6432Node<br>   \KVS<br>    \Enterprise Vault<br>     \Directory<br>      \DirectoryService |
| Content | DWORD |
| Description | Reserved for Veritas use. |

# Network Type

| | |
|---|---|
| Location | HKEY_LOCAL_MACHINE<br> \SOFTWARE<br>  \Wow6432Node<br>   \KVS<br>    \Enterprise Vault<br>     \Directory<br>      \DirectoryService |
| Content | DWORD value. |

Description          Always 1 for DNS-based network.

                     Do not change this setting.

# Enterprise Vault

This chapter includes the following topics:

- AnonymousUser

- ApplyRtnPolicyOnlyOnExistingFolders

- AuditAccessFailureEvent

- BypassConversions

- ConversionIncludeHiddenSpreadsheetData

- ConversionIncludeHiddenText

- ConversionSpreadsheetBorder

- ConversionTimeout

- ConversionTimeoutArchiveFiles

- ConvertExcelToText

- ConvertRTFCoverToText

- ConvertWordToText

- Driver

- DriverVersion

- EnableLinkedAccountPermissionChecks

- ExceptionHandlingMode

- ExcludedFileTypesFromConversion

- IndexServerTimeout

- LastExportPSTUnicode

- MaxIndexDataHTMLContentKB

- MemLimitForTextConversionFallback

- OfflineDays

- ServiceSyncWait

- SiteID

- SortByDateTime

- TextConversionFileTypes

# AnonymousUser

| | |
|---|---|
| Location | HKEY_CURRENT_USER<br> \SOFTWARE<br>  \Wow6432Node<br>   \KVS<br>    \Enterprise Vault |
| Content | String |
| Description | Specifies, in the form *domain\username*, the Enterprise Vault Data Access account. This is an account that Enterprise Vault uses to request items on behalf of a user. This account is used by the following: |

- The Domino Mailbox Archiving web application
- The Enterprise Vault OWA extensions

Do not edit the AnonymousUser value. Always use the appropriate Enterprise Vault configuration procedure to change the Data Access account.

# ApplyRtnPolicyOnlyOnExistingFolders

| | |
|---|---|
| Location | HKEY_LOCAL_MACHINE<br> \SOFTWARE<br>  \Wow6432Node<br>   \KVS<br>    \Enterprise Vault |

| | |
|---|---|
| Content | DWORD |
| | 0 — (Default) Recreate deleted or moved folders in the folder hierarchy that the Retention Folder policy defines. |
| | 1 — Do not recreate deleted or moved folders in the folder hierarchy that the Retention Folder policy defines. |
| Description | Lets you control whether the File System Archiving task recreates deleted or moved folders in the folder hierarchy that the Retention Folder policy defines. |
| | Enterprise Vault does not create ApplyRtnPolicyOnlyOnExistingFolders. To use this registry value you must add it to the registry key on the Enterprise Vault server on which the File System Archiving task runs. |
| | If ApplyRtnPolicyOnlyOnExistingFolders is not present, Enterprise Vault recreates the folders. |
| | Note that when ApplyRtnPolicyOnlyOnExistingFolders is set to 1, the report that the File System Archiving task generates may include the following entry: |

```
Root folder:\\folder_name is not synchronized as its
associated file system folder path does not exist
```

Where *folder_name* is a folder that is not present. This entry is for information only.

AuditAccessFailureEvent

Location	`HKEY_CURRENT_USER`
	` \SOFTWARE`
	`  \Wow6432Node`
	`   \KVS`
	`     \Enterprise Vault`

Content	DWORD

Description   By default, Enterprise Vault does not generate log or audit entries when either of the following occurs:

- A user attempts to search an archive but does not have permission to do so. (Event 6940.)
- A user attempts to search an archive but does not have permission to search any folder in that archive. (Event 7263.)

You can use this registry value to enable logging of these events as necessary. Note that on some Enterprise Vault installations the events may incorrectly be logged frequently for no apparent reason. If the events are logged incorrectly, disable this registry value.

To enable event 6940, create AuditAccessFailureEvent on each Storage server and set the value to 1.

To enable event 7263, create AuditAccessFailureEvent on each Index server and set the value to 1.

BypassConversions

Location   HKEY_LOCAL_MACHINE
 \SOFTWARE
  \Wow6432Node
   \KVS
    \Enterprise Vault

Content   DWORD

0 — Content conversions are performed (Default)

1 — Content conversions are not performed

Description   Controls whether or not the local Storage service performs content conversions when archiving items. Turning off content conversions speeds up archiving, but means that users cannot view, or search the content of items using Enterprise Vault Search.

If the value is not 0 (zero), then the all file types wildcard, "*", is added to the value of the registry setting, ExcludedFileTypesFromConversion, on the local Enterprise Vault server.

Restart the Storage service to apply changes.

This value is supported as a local server override of the site setting, **File types excluded from conversion**. The site setting should be used to ensure a consistent content conversion configuration for all Enterprise Vault Storage servers in the site.

See also   See "ExcludedFileTypesFromConversion" on page 129.

ConversionIncludeHiddenSpreadsheetData

Location   HKEY_LOCAL_MACHINE
             \SOFTWARE
              \Wow6432Node
               \KVS
                \Enterprise Vault

Content   DWORD

            0 — Enterprise Vault does not convert or index hidden text.

            1 — (Default) Enterprise Vault converts and indexes hidden text.

Description Controls whether Enterprise Vault converts and indexes the contents
            of hidden cells, columns, and sheets in spreadsheets.

            Restart the Storage service to apply changes.

            This value is supported as a local server override of the site setting,
            Include hidden spreadsheet data. The site setting should be used to
            ensure a consistent content conversion configuration for all Enterprise
            Vault Storage servers in the site.

See also   See "ConversionIncludeHiddenText" on page 122.

            See "ConversionSpreadsheetBorder" on page 123.

ConversionIncludeHiddenText

Location   HKEY_LOCAL_MACHINE
             \SOFTWARE
              \Wow6432Node
               \KVS
                \Enterprise Vault

Content   DWORD

            0 — Enterprise Vault does not convert or index hidden text.

            1 — (Default) Enterprise Vault converts and indexes hidden text.

Description	Controls whether Enterprise Vault includes hidden text when converting documents to HTML. If you include hidden text then it is also indexed and so can be searched.
	PDF files that are created by OCR software often include hidden text versions of the scanned images. If you enable this registry value Enterprise Vault converts and indexes this hidden text.
	Restart the Storage service to apply changes.
	This value is supported as a local server override of the site setting, **Include hidden text**. The site setting should be used to ensure a consistent content conversion configuration for all Enterprise Vault Storage servers in the site.
See also	See "ConversionSpreadsheetBorder" on page 123.
	See "ConversionIncludeHiddenSpreadsheetData" on page 122.

ConversionSpreadsheetBorder

Location	HKEY_LOCAL_MACHINE
	 \SOFTWARE
	  \Wow6432Node
	   \KVS
	    \Enterprise Vault

Content	DWORD
	0 — (Default) Do not create borders around spreadsheet and database cells in HTML previews.
	1 — Create borders around spreadsheet and database cells in HTML previews.
Description	Controls whether Enterprise Vault creates borders around spreadsheet and database cells in HTML previews. The borders make the previews easier to read but do increase the file size and it takes longer to generate files with borders.
	Restart the Storage service to apply changes.
	This value is supported as a local server override of the site setting, **Show spreadsheet border**. The site setting should be used to ensure a consistent content conversion configuration for all Enterprise Vault Storage servers in the site.
See also	See "ConversionIncludeHiddenText" on page 122.
	See "ConversionIncludeHiddenSpreadsheetData" on page 122.

ConversionTimeout

Location	HKEY_LOCAL_MACHINE
	 \SOFTWARE
	  \Wow6432Node
	   \KVS
	    \Enterprise Vault

Content	String value that specifies a positive number greater than zero. Default: 10 (minutes).
Description	Maximum conversion time allowed for converting the content of an item. By default, ConversionTimeout has the same value as ConversionTimeoutArchiveFiles. You can use ConversionTimeoutArchiveFiles to set a different conversion timeout value for archive files. Restart the Storage service to apply changes. This value is supported as a local server override of the site setting, **Conversion timeout**. The site setting should be used to ensure a consistent content conversion configuration for all Enterprise Vault Storage servers in the site.
See also	See "ConversionTimeoutArchiveFiles" on page 124.

ConversionTimeoutArchiveFiles

Location	HKEY_LOCAL_MACHINE
	 \SOFTWARE
	  \Wow6432Node
	   \KVS
	    \Enterprise Vault

Content	String value that specifies a positive number greater than zero. Default: 10 (minutes).

Description	Maximum conversion time allowed for converting the content of archive files, for example ZIP files.
	By default, ConversionTimeoutArchiveFiles has the same value as ConversionTimeout. You can use ConversionTimeoutArchiveFiles to set a different conversion timeout value for archive files.
	Restart the Storage service to apply changes.
	This value is supported as a local server override of the site setting, **Conversion timeout for archive file types**. The site setting should be used to ensure a consistent content conversion configuration for all Enterprise Vault Storage servers in the site.
See also	See "ConversionTimeout" on page 124.

ConvertExcelToText

Location	HKEY_LOCAL_MACHINE
	  \SOFTWARE
	   \Wow6432Node
	    \KVS
	     \Enterprise Vault

Content	DWORD.
	0 — (Default) Convert to HTML.
	1 — Convert to text.
Description	Specifies the format in which to convert Microsoft Excel spreadsheets: HTML or text. By default, Enterprise Vault converts Excel spreadsheets to HTML, which is more readable but less compact than text.
	If the value is not 0 (zero), then ".xls" is logically added to the value of the registry setting, TextConversionFileTypes, on the local Enterprise Vault server.
	Restart the Storage service to apply changes to the registry value.
	This value is supported as a local server override of the site setting, **File types converted to text**. The site setting should be used to ensure a consistent content conversion configuration for all Enterprise Vault Storage servers in the site.
See also	See "ConversionIncludeHiddenSpreadsheetData" on page 122.
	See "ConversionSpreadsheetBorder" on page 123.
	See "TextConversionFileTypes" on page 135.

ConvertRTFCoverToText

Location	HKEY_LOCAL_MACHINE
	 \SOFTWARE
	  \Wow6432Node
	   \KVS
	    \Enterprise Vault

Content	DWORD. 0 — (Default) Convert to HTML. 1 — Convert to text.
Description	Enterprise Vault converts RTF message bodies to HTML. If Enterprise Vault performs many such conversions, or if the documents are complex, then 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. Use ConvertRTFCoverToText to specify whether to convert messages whose body is RTF text or HTML. If the value is not 0 (zero), then ".rtf" is logically added to the value of the registry setting, TextConversionFileTypes, on the local Enterprise Vault server. Restart the Storage service to apply changes to the registry value. This value is supported as a local server override of the site setting, **File types converted to text**. The site setting should be used to ensure a consistent content conversion configuration for all Enterprise Vault Storage servers in the site.
See also	See "TextConversionFileTypes" on page 135.

ConvertWordToText

Location	HKEY_LOCAL_MACHINE
	 \SOFTWARE
	  \Wow6432Node
	   \KVS
	    \Enterprise Vault

Content	String.
	0 — (Default) Convert to HTML.
	1 — Convert to text.
Description	Enterprise Vault converts Microsoft Word documents to HTML. If Enterprise Vault performs many such conversions, or if the documents are complex, then 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.
	Use ConvertWordToText to specify whether to convert Microsoft Word documents to text or HTML.
	If the value is not 0 (zero), then ".doc" is logically added to the value of the registry setting, TextConversionFileTypes, on the local Enterprise Vault server.
	Restart the Storage service to apply changes to the registry value.
	This value is supported as a local server override of the site setting, **File types converted to text**. The site setting should be used to ensure a consistent content conversion configuration for all Enterprise Vault Storage servers in the site.
See also	See "TextConversionFileTypes" on page 135.

Driver

Location	HKEY_LOCAL_MACHINE
	 \SOFTWARE
	  \Wow6432Node
	   \KVS
	    \Enterprise Vault

Content	String.
Description	Do not change this setting.
	Storage databases use this value to determine which type of database to create for a vault store.

DriverVersion

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

Content	String.
Description	Do not change this setting. Storage databases use this value.

EnableLinkedAccountPermissionChecks

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

Content	DWORD 0 — Access to archived items is disabled. 1 — Enable access to archived items.
Description	This setting enables access to archived items in public folders in a cross domain environment with the following configuration: ■ User accounts in one domain are linked to mailboxes in a different domain. ■ A one-way cross domain trust exists, such that the mailbox domain trusts the user domain. ■ Public folder access is managed using group membership, where the groups are created in the mailbox domain, not in the user account domain. To enable cross-forest permission checking, configure this setting with a value of '1' on the Enterprise Vault server. The Enterprise Vault Auth Server then generates a list of SIDs for the mailbox and user forests, and uses this combined list to complete permission checks.

ExceptionHandlingMode

Location   `HKEY_CURRENT_USER`
                              `\SOFTWARE`
                               `\Wow6432Node`
                                `\KVS`
                                  `\Enterprise Vault`

Content   Value (DWORD):

2 = Enable Logging (only).

4 = Enable Throw on Exception (only).

6 = Enable Logging and Thowing (default).

Description   By default, debug builds run in mode 6 (Log & Throw), release builds run in mode 2 (Log).

When set to Throw (Modes 4 or 6) exceptions from the Exchange Agents bubble to the outer edges of the process giving the system debugger the opportunity of catching and acting on them.

ExcludedFileTypesFromConversion

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

Content   String value containing list of file types. The list format is:

`.filetype[.filetype].`

Prefix each file type with a period and end the list with a period. For example:

`.GIF.JPG.`

Description   If you find that some types of item cause conversion problems, you can
                prevent 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. Users cannot preview items that have not been
                converted to HTML.

                ExcludedFileTypesFromConversion lists all the file types that are not
                currently converted on the local Enterprise Vault server. This value is
                supported as a local server override of the site setting, **File types
                excluded from conversion**. The site setting should be used to ensure
                a consistent content conversion configuration for all Enterprise Vault
                Storage servers in the site.

                Restart the Storage service to apply changes to the value of this setting.

IndexServerTimeout

Location   HKEY_LOCAL_MACHINE
                 \SOFTWARE
                  \Wow6432Node
                   \KVS
                     \Enterprise Vault

Content   String value containing an integer value that specifies a number of
                minutes.

                Default: 5 (minutes). The permitted range of values is limited to 1 to
                720 inclusive. Any value outside the range is ignored and the default
                value is used instead.

Description   When working with indexes, an Enterprise Vault Indexing Service will
                launch one or more IndexServer processes.

                IndexServerTimeout enables you to specify the time, in minutes, after
                which an idle IndexServer process will terminate.

LastExportPSTUnicode

Location   HKEY_LOCAL_MACHINE
                 \SOFTWARE
                  \Wow6432Node
                   \KVS
                     \Enterprise Vault

Content	DWORD
Description	Stores the last used PST type setting made by the Administrator in the Export Archive Wizard. For example, Unicode or ANSI.

MaxIndexDataHTMLContentKB

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

Content	DWORD
	Integer value.
	Default 5120 (KB).
Description	This setting applies to client applications that use the Enterprise Vault Content Management API, including Veritas Discovery Accelerator.
	When calls are made to Item.Get that request index data (DETAIL_LEVEL__SYSTEM_INDEXDATA), the "cont" property is included in the properties returned. This property contains the HTML representation (converted content) of the item or attachment. If the size of the item's converted content is larger than 5 MB, then the converted content is not returned. You can override this limit using the MaxIndexDataHTMLContentKB registry setting. Configure the registry setting on the Content Management API client system.
	Discovery Accelerator uses calls to Item.Get with requests for index data when retrieving the HTML versions of items to preview. For this reason, changes to the value of this setting will affect the size of items or attachments that can be previewed in Discovery Accelerator.
	Displaying the HTML version of large items may have previously failed because there was insufficient process memory available. Before changing the value of this setting, check that the system has sufficient memory resources available. If there are insufficient memory resources available, then no system index properties are returned.
	Note that this setting relates to the converted content of an item. There is no limit when retrieving the actual content of an item.

MemLimitForTextConversionFallback

Location	HKEY_LOCAL_MACHINE
	 \SOFTWARE
	  \Wow6432Node
	   \KVS
	    \Enterprise Vault

Content	DWORD Integer value — The maximum size in megabytes of content conversion output. Default — 30 (MB).
Description	The maximum size (MB) of the content conversion output that can be indexed for an item. If an item's content conversion output (HTML or text) exceeds this value, then attributes such as subject, recipients, and so on are indexed, but the content is not indexed. Instead, a content missing reason ("comr") property is indexed. We recommend that you do not increase this value. If you do increase the value, and an item's conversion output exceeds the value set, then even attributes of the item may not be indexed. Restart the Storage service to apply changes to the setting value. This value is supported as a local server override of the site setting, **Maximum conversion size**. The site setting should be used to ensure a consistent content conversion configuration for all Enterprise Vault Storage servers in the site.

OfflineDays

Location	HKEY_CURRENT_USER
	 \SOFTWARE
	  \Wow6432Node
	   \KVS
	    \Enterprise Vault

Content	DWORD. Default: 0 (days). You can set a value of zero to stop the Storage Service using the secondary offline status checking, in which case the offline status is determined by the OFFLINE file attribute setting.

Description   Some HSM software products do not support the OFFLINE file attribute that indicates 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 has elapsed since the file was last modified.

If an item is older than the OfflineDays number of days, the Storage Service assumes that the file is offline. A value of 0 means that items are assumed to be always online.

If there are more than OfflineDays days between one instance of a message being archived and the next instance, the Storage Service archives another copy of the item. Usually all the copies of a shared item are archived at the same time so only one copy is archived.

If items stay online for longer than seven days, you may want to change the default offline setting.

ServiceSyncWait

Location   HKEY_CURRENT_USER
                   \SOFTWARE
                    \Wow6432Node
                     \KVS
                      \Enterprise Vault

Content   DWORD

Default: 30 (minutes)

If set to 0 (zero) the synchronization checks are disabled.

Description   This is the amount of time a service will wait for other services that it depends on to become available.

A warning is logged in the Windows Application Log if a service is forced to wait for another service to start. A further log event is added when either the synchronization is complete or the synchronization wait period expires. If the period expires, the waiting service stops.

SiteID

Location	HKEY_LOCAL_MACHINE
	 \SOFTWARE
	  \Wow6432Node
	   \KVS
	    \Enterprise Vault

Content	String value containing SiteID in GUID format.
Description	This setting must not be changed.
	The DNS name of the Enterprise Vault site.

SortByDateTime

Location	HKEY_LOCAL_MACHINE
	 \SOFTWARE
	  \Wow6432Node
	   \KVS
	    \Enterprise Vault

Content	DWORD.
	0 — (Default) do not sort results by time.
	1 — Sort results by time.
Description	When sorting search results by date, the results are normally returned sorted by date, but not sorted by time. Thus, within the results for a particular day, the results can be in a seemingly random order.
	SortByDateTime, which you can create on the Index Server computer, forces results that are sorted by date to be also sorted by time.
	There will be a performance impact associated with sorting by time, which will become significant when a large number of results is returned.

TextConversionFileTypes

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

Content	String value containing list of file types.
	
	The list format is:
	
	`.filetype[.filetype].`
	
	Each file type must be prefixed by a period and the list ending with a period. For example:
	
	`.DOC.XLS.`
	
	From Enterprise Vault 6.0, all file types can be converted to text by using the * wildcard character. For example, value of .*. converts all file types to text.

Description	By default, when an item is archived, Enterprise Vault attempts to convert the item to HTML. If this fails, Enterprise Vault then attempts to convert the item to text. This setting overrides the default behavior and always converts items of the configured file types to text without attempting conversion to HTML. This setting may be useful for some file types which cause the following conversion issues: ■ Conversion to HTML takes too long, causing frequent conversion timeouts and fallback conversion to text. ■ HTML output generated is very large, causing indexing failure because the output size exceeds the value set in the site setting, **Maximum conversion size**. This value is supported as a local server override of the site setting, **File types converted to text**. The site setting should be used to ensure a consistent content conversion configuration for all Enterprise Vault Storage servers in the site. Restart the local Storage service to apply changes to the registry value.
See also	See "ConvertWordToText" on page 126. See "ConvertExcelToText" on page 125. See "ConvertRTFCoverToText" on page 126.

EVcloudExporter

This chapter includes the following topics:

- ExcludeForm

- ExcludeMessageClass

- IncludeForm

- IncludeMessageClass

ExcludeForm

Location   On a 32-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \KVS
   \Enterprise Vault
    \EVcloudExporter
```

On a 64-bit installation of Windows:

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

Content   DWORD.

A comma-separated or semicolon-separated list of message types.

Description	Specifies the Domino forms to exclude from the output when you export Domino archives from Enterprise Vault with Enterprise Vault.cloud Archive Migrator.
	For example, to exclude the `Appointment` and `Nondelivery Report` Domino forms, you can use ExcludeForm with the following value:
	Appointment;Nondelivery Report
	Create this registry value on the Enterprise Vault storage server whose archives you want to migrate.
	Note: If you include the same form in both the IncludeForm registry value and the ExcludeForm registry value, exclusion takes precedence.
	For more information on migrating archives from Enterprise Vault to Enterprise Vault.cloud with Archive Migrator, see the Enterprise Vault.cloud *Archive Migrator Guide*.
See also	See "IncludeForm" on page 138.

ExcludeMessageClass

Location	On a 32-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \KVS
   \Enterprise Vault
    \EVcloudExporter
```

On a 64-bit installation of Windows:

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

Content	DWORD.
	A comma-separated or semicolon-separated list of message types.

Description   Specifies the Exchange message classes to exclude from the output
                       when you export Exchange archives from Enterprise Vault with
                       Enterprise Vault.cloud Archive Migrator.

                       For example, to exclude the Exchange message classes
                       `IPM.Calendar`, `IPM.Appointment`, and `IPM.Contact`, you can
                       use ExcludeMesssageClass with the following value:

                       IPM.Calendar, IPM.Appointment, IPM.Contact

                       Create this registry value on the Enterprise Vault storage server whose
                       archives you want to migrate.

                       Note: If you include the same message class in both the
                       IncludeMessageClass registry value and the ExcludeMessageClass
                       registry value, exclusion takes precedence.

                       For more information on migrating archives from Enterprise Vault to
                       Enterprise Vault.cloud with Archive Migrator, see the Enterprise
                       Vault.cloud *Archive Migrator Guide*.

See also   See "IncludeMessageClass" on page 139.

IncludeForm

Location   On a 32-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \KVS
   \Enterprise Vault
    \EVcloudExporter
```

                       On a 64-bit installation of Windows:

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

Content   DWORD.

                       A comma-separated or semicolon-separated list of message types.

Description
Specifies the Domino forms to include in the output when you export Domino archives from Enterprise Vault with Enterprise Vault.cloud Archive Migrator.

For example, to include only the `Memo` and `Reply` Domino forms, you can use IncludeForm with the following value:

Memo;Reply

Create this registry value on the Enterprise Vault storage server whose archives you want to migrate.

Note: If you include the same form in both the IncludeForm registry value and the ExcludeForm registry value, exclusion takes precedence.

For more information on migrating archives from Enterprise Vault to Enterprise Vault.cloud with Archive Migrator, see the Enterprise Vault.cloud *Archive Migrator Guide*.

See also
See "ExcludeForm" on page 136.

IncludeMessageClass

Location
On a 32-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \KVS
   \Enterprise Vault
    \EVcloudExporter
```

On a 64-bit installation of Windows:

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

Content
DWORD.

A comma-separated or semicolon-separated list of message types.

Description   Specifies the Exchange message classes to include in the output when you export Exchange archives from Enterprise Vault with Enterprise Vault.cloud Archive Migrator.

For example, to include only `IPM.Note` in the output, you can use IncludeMessageClass with the following value:

IPM.Note

Create this registry value on the Enterprise Vault storage server whose archives you want to migrate.

Note: If you include the same message class in both the IncludeMessageClass registry value and the ExcludeMessageClass registry value, exclusion takes precedence.

For more information on migrating archives from Enterprise Vault to Enterprise Vault.cloud with Archive Migrator, see the Enterprise Vault.cloud *Archive Migrator Guide*.

See also   See "ExcludeMessageClass" on page 137.

Event filtering

This chapter includes the following topics:

- About event filtering
- AllInfosSuppressible
- Enabled
- MaxEventsInSequence
- MaxSecsBetweenEventsInSequence
- NeverSuppressEventIDs
- ReportConfigPeriodMinutes
- SuppressibleInfoEventIDs

About event filtering

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 events that are repeats of events that have already been logged recently.

See the "Automatically filtering events" chapter in the *Administrator's Guide*.

AllInfosSuppressible

Location	HKEY_LOCAL_MACHINE
	 \SOFTWARE
	  \Wow6432Node
	   \KVS
	    \Enterprise Vault
	     \Event Filter

Content	DWORD. 0 (Default) – Do not suppress informational events unless explicitly named in SuppressibleInfoEventIDs. 1 – All informational events can be suppressed.
Description	Controls whether all informational events can be suppressed. See "SuppressibleInfoEventIDs" on page 145. See the "Automatically filtering events" chapter in the *Administrator's Guide*.

Enabled

Location	HKEY_LOCAL_MACHINE
	 \SOFTWARE
	  \Wow6432Node
	   \KVS
	    \Enterprise Vault
	     \Event Filter

Content	DWORD. 0 – Event filtering is disabled. 1 – (Default) Event filtering is enabled.
Description	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. See the "Automatically filtering events" chapter in the *Administrator's Guide*.

MaxEventsInSequence

Location	HKEY_LOCAL_MACHINE
	 \SOFTWARE
	  \Wow6432Node
	   \KVS
	    \Enterprise Vault
	     \Event Filter

Content	DWORD. Integer in the range 2 to 100. Default is 12.
Description	The maximum number of events that a process can generate in successsion before events are suppressed. See the "Automatically filtering events" chapter in the *Administrator's Guide*.

MaxSecsBetweenEventsInSequence

Location	HKEY_LOCAL_MACHINE
	 \SOFTWARE
	  \Wow6432Node
	   \KVS
	    \Enterprise Vault
	     \Event Filter

Content	DWORD. Integer in the range 1 to 86400 (1 day). Default is 180
Description	The maximum time difference between events for them to be treated as part of the same sequence. Events that occur more frequently than this can be suppressed. See the "Automatically filtering events" chapter in the *Administrator's Guide*.

NeverSuppressEventIDs

Location
```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \Wow6432Node
   \KVS
    \Enterprise Vault
     \Event Filter
```

Content   String.

Default: None.

Description   A semi-colon delimited list of the IDs of events that must never be suppressed.

See the "Automatically filtering events" chapter in the *Administrator's Guide*.

ReportConfigPeriodMinutes

Location
```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \Wow6432Node
   \KVS
    \Enterprise Vault
     \Event Filter
```

Content   DWORD.

Default: 15 (minutes)

Range: 1 to 1440 (1 day).

Description   A time interval in minutes that determines the following:

- How frequently to check for configuration changes.
- How frequently to generate an event that summarizes the event filtering activity.

See the "Automatically filtering events" chapter in the *Administrator's Guide*.

SuppressibleInfoEventIDs

Location	HKEY_LOCAL_MACHINE
	 \SOFTWARE
	  \Wow6432Node
	   \KVS
	    \Enterprise Vault
	     \Event Filter

Content	String.
	Default: None.
Description	A semi-colon delimited list of the IDs of the informational events that can be suppressed when AllInfosSuppressible is set to 0.
	See "AllInfosSuppressible" on page 142.
	See the "Automatically filtering events" chapter in the *Administrator's Guide*.

Chapter **12**

External filtering

This chapter includes the following topics:

- About external filtering

- ActionForInvalidDL

- EnableTestModeLog

- File System

- IgnoreNoDefault

- Journaling

- Lotus Archiving

- Lotus Journaling

- Mailbox

- MessageTimeoutSeconds

- MoveOnFilterFailure

- Override (Domino custom filtering)

- Override (Exchange custom filtering)

- PublicFolder

- ShutdownThresholdMinutes

- WarningThresholdSeconds

About external filtering

Enterprise Vault provides the following filtering features:

- Selective journaling.
  This feature provides simple filtering of Exchange Server journaled messages. You set up a filter for the Exchange Journaling task that selects, by address, the messages to archive. Other messages are deleted.

- Group journaling.
  This feature enables the Exchange Journaling task to mark selected messages, in order to reduce the scope of subsequent searches. This can be particularly useful where there is a high volume of journaled email and you want to be able to identify messages sent between particular groups of users.

- Custom filtering.

  This feature provides more sophisticated filtering for the following:

  - Exchange mailbox, journal, and public folder archiving

  - Domino mailbox and journal archiving

  - File System archiving

  In each case, a filter controls the behavior of the archiving task during an archiving run.

  For Exchange and Domino server archiving, generic filters are shipped with Enterprise Vault. You create rules to control which messages are selected and what action the task takes. The rules can select messages by matching one or more attributes, such as email addresses, subject text, message direction, or the value of certain message properties. The rules also define how selected messages are processed. This can include assigning a particular retention category, storing in a specified archive, deleting attachments of a specified type or size, and deleting or marking the message.

  Filtering for File System Archiving lets you select files by matching certain file attributes, and apply a given filtering action to selected files. For example, the file can be archived with or without creating a shortcut, a different retention category can be applied, or the file can be deleted. No generic filter is shipped for File System Archiving. You can create a filter using the Enterprise Vault APIs.

ActionForInvalidDL

Location

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

Content

DWORD:

0 — (Default) If a distribution list is invalid, continue to process the remainder of the recipient list.

1 — If a distribution list is invalid, stop processing the recipient list.

2 — If a distribution list is invalid, treat this as a match and archive message.

3 — If a distribution list is invalid, leave the message in the journaling mailbox and log an error event in the Windows Application Log.

Description

Used with selective journaling only: controls what an Exchange Journaling Task does if a distribution list is invalid.

See the *Setting up Exchange Server Archiving* guide for information on setting up selective journaling.

EnableTestModeLog

Location

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \Wow6432Node
   \KVS
    \Enterprise Vault
     \External Filtering
      \DCS
```

Content

DWORD.

0 — Disable test mode logging for Enterprise Vault Data Classification Services.

1 — Enable test mode logging for Enterprise Vault Data Classification Services.

Description   Applies to the Enterprise Vault Data Classification Services component only. The value does not apply to the classification feature that was introduced in Enterprise Vault 12.

You can configure a Classification Server so that, instead of affecting the archiving process, policies show what would take place if they were used. Then you can check that you have configured the policies correctly.

On the Classification Server, policies that match in test mode generate some incidents that you can view in the incident report. On the Enterprise Vault server, setting EnableTestModeLog to 1 creates a log file for each agent. The log files are under the `Enterprise Vault\Reports\DataClassificationServices` folder. Each log file contains the details of any messages that at least one policy in test mode has classified and matched. All policies that match for the message are listed, and not just the ones that are in test mode.

File System

Location
```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \Wow6432Node
   \KVS
    \Enterprise Vault
     \External Filtering
      \File System
```

Content   The File System sub-key can contain a string value that specifies the name of a filter. Filter names must be an unbroken numbered sequence that starts at 1.

For the value of a custom filter setting, enter a string value that contains the name of the .NET assembly and the fully-qualified filter class name of the new external filter, as follows:

PathToFilterAssembly!*FilterClassName*

A fully-qualified class name includes the namespace. For example, if the class name is CustomFilter, the namespace is Veritas.EnterpriseVault.FileSystem, and the filter is implemented in the assembly Veritas.EnterpriseVault.FileSystemCustomFilter.dll, the value of the registry entry should be as follows:

Veritas.EnterpriseVault.FileSystemCustomFilter.dll!Enterprise Vault.EnterpriseVault.FileSystem.CustomFilter

Description   Enables custom filtering for all File System Archiving tasks on the
                        computer. For instructions on how to configure file system filtering, see
                        the *Setting up File System Archiving* guide.

IgnoreNoDefault

Location   HKEY_LOCAL_MACHINE
                         \SOFTWARE
                          \Wow6432Node
                          \KVS
                           \Enterprise Vault
                            \External Filtering
                             \{agenttype}
                              \{filtername}

Content   DWORD

                        {agenttype} can be Mailbox/Journaling/PublicFolder/Lotus
                        Archiving/Lotus Journaling.

                        {filtername} is EnterpriseVault.CustomFilter for Exchange Server filtering
                        and KVS.EnterpriseVault.LotusDomino.CustomFilter for Domino Server
                        filtering.

Description   Custom Filter specific setting.

                        If Enterprise Vault archiving tasks are enabled for filtering, the action
                        they take when archiving is determined by the existence of the various
                        configuration entities:

                        ■ XML ruleset files in the folder, Enterprise Vault\Custom
                           Filter Rules.
                        ■ The XML ruleset file, Default Filter Rules.xml.
                        ■ The XML custom properties file, custom properties.xml.
                        ■ Content category entries in custom properties.xml.

                        The registry entry, IGNORENODEFAULT, can be used to alter the
                        archiving task behavior, if some of the configuration entities are not
                        defined. How to set the IGNORENODEFAULT registry entry is described
                        in the *Setting up Exchange Server Archiving* and *Setting up Domino
                        Server Archiving* guides.

Journaling

Location

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \Wow6432Node
   \KVS
    \Enterprise Vault
     \External Filtering
      \Journaling
```

Content

The Journaling sub-key can contain the following values:

- A String value named `1` whose value data is set to one of the following: `SelectiveJournal.SJFilter` (to enable selective journaling), `SelectiveJournal.SJGroupFilter` (to enable group journaling), or `EnterpriseVault.CustomFilter` (to enable custom filtering).
- A DWORD value named `MoveOnFilterFailure` that is set to 1.
- A DWORD value named `Override` that is set to 1 or 0 (zero).

For example:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KVS\Enterprise
Vault\External Filtering\Journaling]
"1"="EnterpriseVault.CustomFilter"
```

Description

Enables filtering for all Exchange Journaling tasks on the computer. Each type of journal filtering (selective, group and custom) uses rule files to control message selection and processing. For details of the various rule files, see the *Setting up Exchange Server Archiving* guide.

With selective journaling, items that are not archived are sent to the Deleted Items folder in the journal mailbox. If you want items to be deleted immediately, without going to the Deleted Items folder, add the DWORD HardDeleteItems to the following location and give it a value of 1:

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

Lotus Archiving

Location
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \Wow6432Node
   \KVS
    \Enterprise Vault
     \External Filtering
      \Lotus Archiving

Content
The Lotus Archiving sub-key can contain the following values:

- A String value named 1 that has a data value in the following format:
  dll_name!*class_name*
  Where:
  dll_name is KVS.EnterpriseVault.LotusDominoCustomFilter
  class_name is KVS.EnterpriseVault.LotusDomino.CustomFilter
- A DWORD value named Override that is set to 1 or 0 (zero).

For example:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KVS\Enterprise
Vault\External Filtering\Lotus Archiving]
"Override"=dword:00000001
```

Description
Enables custom filtering for all Domino mailbox archiving tasks on the computer. For instructions on how to configure custom filtering, see the *Setting up Domino Server Archiving* guide.

Lotus Journaling

Location
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \Wow6432Node
   \KVS
    \Enterprise Vault
     \External Filtering
      \Lotus Journaling

Content	The Lotus Journaling sub-key can contain the following values:

- A String value named `1` that has the following value data:

  ```
  KVS.EnterpriseVault.LotusDominoCustomFilter
  !KVS.EnterpriseVault.LotusDomino.CustomFilter
  ```
- A DWORD value named `Override` that is set to 1 or 0 (zero).

For example:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KVS\Enterprise
Vault\External Filtering\Lotus Journaling]
"Override"=dword:00000001
```

Description	Enables custom filtering for all Domino Journaling tasks on the computer. For instructions on how to configure custom filtering, see the *Setting up Domino Server Archiving* guide.

Mailbox

Location	HKEY_LOCAL_MACHINE
	 \SOFTWARE
	  \Wow6432Node
	  \KVS
	   \Enterprise Vault
	    \External Filtering

Content	Key containing following values:

- STRING name "1" with value "EnterpriseVault.CustomFilter".
- DWORD called MoveOnFilterFailure and value 1.
- DWORD called Override and value of 1 or 0 (zero).

Description	Enables custom filtering for all Exchange Mailbox tasks on the computer. For instructions on how to configure custom filtering, see the *Setting up Exchange Server Archiving* guide.

MessageTimeoutSeconds

Location	HKEY_LOCAL_MACHINE
	 \SOFTWARE
	  \Wow6432Node
	   \KVS
	    \Enterprise Vault
	     \External Filtering
	      \DCS

Content	DWORD. Hexadecimal value that specifies the timeout in seconds.
Description	Applies to the Enterprise Vault Data Classification Services component only. The value does not apply to the classification feature that was introduced in Enterprise Vault 12. MessageTimeoutSeconds specifies the number of seconds before the Data Classification Filter gives up waiting for Data Classification Services to classify a message. The default is 300 seconds. **Note:** If you set too low a value for this option, Data Classification Services may never classify some messages. Make sure that you specify a higher value for the ShutdownThresholdMinutes option than for MessageTimeoutSeconds.

MoveOnFilterFailure

Location	HKEY_LOCAL_MACHINE
	 \SOFTWARE
	  \Wow6432Node
	   \KVS
	    \Enterprise Vault
	     \External Filtering
	      \{agentname}

Content	DWORD with value 1 or 0.
Description	Valid for Exchange Journaling and Mailbox custom filtering only. When MoveOnFilterFailure is enabled (1), the archiving task moves messages that the external filter cannot handle to the Failed External Filter folder in the associated mailbox. See the *Setting up Exchange Server Archiving* guide.

Override (Domino custom filtering)

Location HKEY_LOCAL_MACHINE
 \SOFTWARE
  \Wow6432Node
   \KVS
    \Enterprise Vault
     \External Filtering

Or

HKEY_LOCAL_MACHINE
 \SOFTWARE
  \Wow6432Node
   \KVS
    \Enterprise Vault
     \External Filtering
      \{agenttype}

{agenttype} can be Lotus Archiving or Lotus Journaling.

Content DWORD with value "1" or "0".

Description Set Override to 1 to force custom filtering to reprocess items marked MARK_DO_NOT_ARCHIVE. You can set Override directly under External Filtering to configure both mailbox custom filtering and journal custom filtering. You can also set it under Lotus Archiving or Lotus Journaling to configure them individually. If Override is set under Lotus Archiving or Lotus Journaling, this takes priority if Override is also set under External filtering.

For more information, see the *Setting up Domino Server Archiving* guide.

Override (Exchange custom filtering)

Location HKEY_LOCAL_MACHINE
 \SOFTWARE
  \Wow6432Node
   \KVS
    \Enterprise Vault
     \External Filtering
      \{agentname}

Content DWORD with value "1" or "0".

Description   If custom filtering is implemented, and Override is set to 0 (zero), then the Exchange archiving task processes the archiving rules for all messages as normal for user mailbox and public folder archiving before it processes filters. You can prevent the Exchange archiving task from processing archiving rules by setting Override to 1.

For more information, see the *Setting up Exchange Server Archiving* guide.

PublicFolder

Location

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \Wow6432Node
   \KVS
    \Enterprise Vault
     \External Filtering
```

Content   Key containing the following values:

- STRING name "1" with value "EnterpriseVault.CustomFilter".
- DWORD called Override and value of 1 or 0 (zero).

Description   Enables custom filtering for all Exchange Public Folder tasks on the computer. For instructions on how to configure custom filtering, see the *Setting up Exchange Server Archiving* guide.

ShutdownThresholdMinutes

Location

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \Wow6432Node
   \KVS
    \Enterprise Vault
     \External Filtering
      \DCS
```

Content   DWORD.

Hexadecimal value that specifies the shutdown threshold in minutes.

Description   Applies to the Enterprise Vault Data Classification Services component only. The value does not apply to the classification feature that was introduced in Enterprise Vault 12.

If Data Classification Services cannot classify a message for a period longer than this setting, the Data Classification Filter instructs the Enterprise Vault Exchange Agent to shut down. (The task controller restarts the agent a number of times before finally failing the archiving task. This lets you remedy the situation without having to restart all the Enterprise Vault agents.)

The default shutdown threshold is 15 minutes.

WarningThresholdSeconds

Location
```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \Wow6432Node
   \KVS
    \Enterprise Vault
     \External Filtering
      \DCS
```

Content   DWORD.

Hexadecimal value that specifies the warning threshold in seconds.

Description   Applies to the Enterprise Vault Data Classification Services component only. The value does not apply to the classification feature that was introduced in Enterprise Vault 12.

If Data Classification Services cannot classify a message for a period longer than this setting, it logs a warning in the event log to show the status of the Classification Servers.

The default is 60 seconds.

File System Archiving

This chapter includes the following topics:

- LogLevel

- PassThruRecallLimitMaxRecalls

- PassThruRecallLimitTimeInterval

- RecallLimitMaxRecalls

- RecallLimitTimeInterval

- ResetFolderModifiedTimeStamp

- ResetFolderModifiedTimeStamp (PlaceholderService)

- ScanThreads

- SetNetappPHOriginalSize

- SingleNodeFSA

- SynchroniseFSASharePermissions

- TempFilePath

- WebServiceTimeout

- WSTempFilePath

BulkUploadThreads

Location

On a 32-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \KVS
   \Enterprise Vault
    \FSA
       \Reporting
```

On a 64-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \Wow6432Node
   \KVS
    \Enterprise Vault
     \FSA
        \Reporting
```

Content	DWORD.
	An integer in the range 1 to 10.
Description	BulkUploadThreads specifies the maximum number of FSAReporting data upload threads per file server. The data upload threads collect data from the scan threads, and then upload the data to the FSA Reporting database.
	The BulkUploadThreads registry value does not exist by default. If BulkUploadThreads is not specified, FSAReporting uses up to three data upload threads per file server.
	If the scan threads queue large amounts of data for upload simultaneously, you can use BulkUploadThreads to increase the number of available data upload threads.
	For Windows file servers, set this registry value on the file server. For NetApp and Celerra/VNX file servers, set this registry value on the FSA Reporting proxy server.
See also	See "ScanThreads" on page 184.

BypassPassThruRecallLimitsForAdmins

Location	On a 32-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \KVS
   \Enterprise Vault
    \FSA
      \PlaceholderService
       \PassThrough
```

On a 64-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \Wow6432Node
   \KVS
    \Enterprise Vault
     \FSA
       \PlaceholderService
        \PassThrough
```

Content	DWORD
	0 — (Default) The pass-through recall limit applies to local administrators
	1 — The pass-through recall limit does not apply to local administrators
Description	For Windows file servers you can specify a maximum rate of pass-through recall on each computer that runs an Enterprise Vault Placeholder service. The registry values PassThruRecallLimitMaxRecalls and PassThruRecallLimitTimeInterval set the maximum rate.

See "PassThruRecallLimitMaxRecalls" on page 177.

See "PassThruRecallLimitTimeInterval" on page 179.

By default the maximum recall rate applies to all users. BypassPassThruRecallLimitsForAdmins enables you to exempt members of the local Administrators group on the file server from this limit.

Note: BypassPassThruRecallLimitsForAdmins applies only when EnableRecallLimitForPassThrough is set to 1. Otherwise this registry value is ignored.

See "EnableRecallLimitForPassThrough" on page 167.

BypassRecallLimitsForAdmins

Location	On a 32-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \KVS
   \Enterprise Vault
    \FSA
      \PlaceholderService
```

On a 64-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \Wow6432Node
   \KVS
    \Enterprise Vault
     \FSA
       \PlaceholderService
```

Content	DWORD.
	0 — (Default) Recall limits apply to local administrators.
	1 — There are no recall limits for local administrators.
Description	For Windows file servers, you can specify a maximum rate of placeholder recall on each computer that runs an Enterprise Vault Placeholder service. The registry values RecallLimitMaxRecalls and RecallLimitTimeInterval together set the maximum recall rate.
	See "RecallLimitMaxRecalls" on page 180.
	See "RecallLimitTimeInterval" on page 181.
	By default the maximum recall rate applies to all users. BypassRecallLimitsForAdmins enables you to exempt members of the local Administrators group on the file server from this limit.

CheckEVPHOnCelerra

Location	On a 32-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \KVS
   \Enterprise Vault
    \FSA
      \Reporting
```

On a 64-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \Wow6432Node
   \KVS
    \Enterprise Vault
     \FSA
       \Reporting
```

Content	DWORD
	0 — (Default if the value does not exist.) FSA Reporting assumes that a file on a Celerra/VNX device with the offline attribute set is a placeholder shortcut.
	1 — FSA Reporting performs an enhanced scan for Celerra/VNX to verify whether a file with the offline attribute set is a placeholder.
	This registry value does not exist by default.
Description	By default, FSA Reporting uses the offline attribute to identify placeholders on Celerra/VNX devices. If programs other than Enterprise Vault set the offline attribute on Celerra/VNX files, some FSA Reporting reports can show incorrect space saving information for Celerra/VNX.
	To avoid this issue you can force FSA Reporting to perform an enhanced scan that verifies whether a file with the offline attribute set is a placeholder.
	Note: Placeholder verification can lengthen the time of an FSA Reporting scan on a Celerra/VNX device significantly.
	To configure FSA Reporting to perform enhanced scans for Celerra/VNX, create this registry value on the FSA Reporting proxy server for the Celerra/VNX device, and set the value to 1.
	After you set or change this value, do as follows:
	■ If the FSA Reporting proxy server is an Enterprise Vault server, restart the Enterprise Vault Admin service.
	■ Otherwise, restart the Enterprise Vault File Collector service on the FSA Reporting proxy server.

CheckpointSort

Location	HKEY_LOCAL_MACHINE
	\SOFTWARE
	\Wow6432Node
	\KVS
	\Enterprise Vault
	\FSA

Content	DWORD.
	0 — Do not perform alphabetical sorting of the list of folders that the FSA checkpoint mechanism is to process.
	1 — Perform alphabetical sorting of the list of folders before the FSA checkpoint mechanism inspects it.
	This registry value is not created automatically.
Description	The FSA checkpoint mechanism is designed to process the subfolders of a partially processed target volume in alphabetical order to determine whether the previous checkpoint has been reached. Some file server systems do not present the list of folders in alphabetical order. A non-alphabetical list can cause FSA to reprocess some folders repeatedly during multiple archiving runs.
	To fix this issue, you can use the CheckpointSort registry value to make the checkpoint mechanism sort the list of folders into alphabetical order before inspection.
	To enable alphabetical sorting, create this registry value on the Enterprise Vault server, and set its value to 1.
	The change takes effect from the next run of the File System Archiving task.

CModeIgnoreServerCertVerification

Location	HKEY_LOCAL_MACHINE
	 \SOFTWARE
	  \Wow6432Node
	   \KVS
	    \Enterprise Vault
	      \FSA

Content	DWORD
	0 — Verify certificate.
	1 — Verify certificate, but ignore any host name mismatches.
	2 — (Default) Do not verify certificate.
	This registry value is not created automatically. It is applicable only when the registry value CModeServerTransportStyle is set to use HTTPS.

Description   Specifies whether the ONTAPI Management API should ignore
                     certificate validation.

                     To verify the server certificate that is issued to the NetApp C-Mode
                     server, make sure that the certificate of the certificate issuing authority
                     is in the cacert.pem file in the Enterprise Vault installation folder.

                     Set the value to 1 to verify the certificate, but ignore any mismatch that
                     is found between the host name specified in the certificate and the host
                     name of the management LIF.

See also   See "CModeServerTransportStyle" on page 165.

CModeServerTransportStyle

Location   HKEY_LOCAL_MACHINE
                      \SOFTWARE
                       \Wow6432Node
                        \KVS
                         \Enterprise Vault
                          \FSA

Content   DWORD

                     0 — HTTP

                     1 — (Default) HTTPS

                     This registry value is not created automatically.

Description   Specifies the transport type used by the ONTAPI Management API.
                     The default value is HTTPS.

See also   See "CModeIgnoreServerCertVerification" on page 164.

                     See "CModeServerPort" on page 165.

CModeServerPort

Location   HKEY_LOCAL_MACHINE
                      \SOFTWARE
                       \Wow6432Node
                        \KVS
                         \Enterprise Vault
                          \FSA

Content	DWORD
	Any valid port number.
	This registry value is not created automatically.
Description	Specifies the port number that the ONTAPI Management API should use to communicate with the NetApp C-Mode server. The port number should be same as the one that is configured on the NetApp C-Mode server. By default, port 443 is used for HTTPS connections and port 80 is used for HTTP connections.
See also	See "CModeServerTransportStyle" on page 165.

DeleteOnDelete

Location	HKEY_LOCAL_MACHINE
	 \SOFTWARE
	  \Wow6432Node
	   \KVS
	    \Enterprise Vault
	     \FSA
	      \ArchivedFilesFlags

Content	DWORD
	0 — Do not delete archived file when the corresponding placeholder is deleted.
	1 — Delete archived file when the corresponding placeholder is deleted.
	Not automatically created.

Description   For Dell EMC Celerra/VNX devices, this registry value lets you control whether Enterprise Vault deletes an item from the archive when the corresponding placeholder is deleted.

You must also perform the other steps that are required to configure the deletion of archived files on placeholder deletion from the Celerra/VNX.

See "Configuring the deletion of files on placeholder deletion for Dell EMC Celerra/VNX devices" in *Setting up File System Archiving*.

Set this value on the Enterprise Vault server whose File System Archiving task processes the Celerra/VNX device's root volume.

If required, create the ArchivedFilesFlags key and then create the DeleteOnDelete registry value.

If you set or change this registry value, restart the Enterprise Vault Admin service to activate the change.

EnableRecallLimitForPassThrough

Location   On a 32-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \KVS
   \Enterprise Vault
    \FSA
      \PlaceholderService
       \PassThrough
```

On a 64-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \Wow6432Node
   \KVS
    \Enterprise Vault
     \FSA
      \PlaceholderService
       \PassThrough
```

Content   DWORD

0 — (Default) The pass-through recall limit does not apply

1 — The pass-through recall limit applies

Description   For Windows file servers you can specify a maximum rate of pass-through recall on each computer that runs a Placeholder Service. The registry values PassThruRecallLimitMaxRecalls and PassThruRecallLimitTimeInterval set the maximum rate.

See "PassThruRecallLimitMaxRecalls" on page 177.

See "PassThruRecallLimitTimeInterval" on page 179.

EnableRecallLimitForPassThrough enables or disables the maximum rate.

You can bypass the limit for administrators by using BypassPassThruRecallLimitsForAdmins.

See "BypassPassThruRecallLimitsForAdmins" on page 160.

ExcludedExes

Location   On a 32-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \KVS
   \Enterprise Vault
    \FSA
      \PlaceholderService
```

On a 64-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \Wow6432Node
   \KVS
    \Enterprise Vault
     \FSA
      \PlaceholderService
```

Content   String

Description   For Windows file servers you can specify a list of programs that are
               prohibited from recalling archived items. This mechanism can be useful
               if you use an antivirus or backup program that does not honor the file
               system offline attribute.

               To specify a list of prohibited programs, edit ExcludedExes on the file
               server to specify the names of the program executable files, separated
               by semicolons (;).

               For example, to exclude Windows Explorer, MyBackupProg.exe, and
               Antivirus.exe, specify:

               `Explorer.exe;MyBackupProg.exe;Antivirus.exe`

               If you change the list of prohibited programs you must restart the
               Placeholder Service on the file server in order to make the change take
               effect.

ExcludedExes (PassThrough)

Location   On a 32-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \KVS
   \Enterprise Vault
    \FSA
      \PlaceholderService
       \PassThrough
```

On a 64-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \Wow6432Node
   \KVS
    \Enterprise Vault
     \FSA
      \PlaceholderService
       \PassThrough
```

Content   String

Description   For Windows file servers you can specify a list of programs that are prohibited from receiving archived items from the pass-through recall mechanism. This is most likely to be useful if you use an antivirus or backup program that does not honor the file system offline attribute.

To specify a list of prohibited programs, edit ExcludedExes to specify the names of the program executable files, separated by semicolons (;).

For example, to exclude Windows Explorer, MyBackupProg.exe, and Antivirus.exe, specify:

```
Explorer.exe;MyBackupProg.exe;Antivirus.exe
```

If you change the list of prohibited programs you must restart the Placeholder Service to make the change take effect.

ExcludeSnapshotFolder

Location   On a 32-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \KVS
   \Enterprise Vault
    \FSA
      \Reporting
```

On a 64-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \Wow6432Node
   \KVS
    \Enterprise Vault
     \FSA
       \Reporting
```

Content   DWORD.

0 — Exclude NetApp filer `~snapshot` folders from FSA Reporting scans.

Any value other than 0 — Include the `~snapshot` folders in FSA Reporting scans.

This registry value does not exist by default.

Description You can use ExcludeSnapshotFolder to control whether FSA Reporting includes NetApp filer `~snapshot` folders in its scans.

If the registry value does not exist, FSA Reporting excludes the content of the `~snapshot` folders. To override this behavior and allow FSA Reporting to scan `~snapshot` folders, create this registry value and set it to 0.

Note: ExcludeSnapshotFolder has no effect on the scans of `~snapshot` folders for file server types other than NetApp filers.

You must create the registry value on the FSA Reporting proxy server for the NetApp filer.

After you set or change the value, do as follows:

■ If the FSA Reporting proxy server is an Enterprise Vault server, restart the Enterprise Vault Admin service.

■ Otherwise, restart the Enterprise Vault File Collector service on the FSA Reporting proxy server.

ExpandLocalGroups

Location
```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \Wow6432Node
   \KVS
    \Enterprise Vault
     \FSA
```

Content DWORD

0 — (Default) Local groups are not expanded

1 — Local groups are expanded

Description Controls whether File System Archiving expands local groups when synchronizing permissions. If local groups are used but not expanded, the Enterprise Vault Search facilities cannot find items that a user accesses using local group permissions.

Set this registry value on the Enterprise Vault server that runs the File System Archiving tasks.

FileDownloadTimeOut

Location   On a 32-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \KVS
   \Enterprise Vault
    \FSARestore
```

On a 64-bit installation of Windows:

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

Content   DWORD.

Description   FileDownloadTimeOut lets you change the placeholder recall
                  mechanism of the FSAUtility -t and -b options from asynchronous to
                  synchronous, and to specify a timeout, in seconds, for the synchronous
                  recall of each file.

                  If FileDownloadTimeOut is set to 0, recall is asynchronous.

                  If set to any value greater than 0, file recalls happen synchronously
                  with a timeout of the specified seconds. If the recall operation does not
                  complete within the specified timeout, FSAUtility moves on to recall the
                  next file.

                  For example, if you set the value to 30, FSAUtility adds a file to the
                  queue for file recall and waits for 30 seconds for the file recall to
                  complete. If the file is not recalled in 30 seconds, the recall operation
                  runs in the background, and FSAUtility puts the next file in the queue.

                  Set this registry value on the computer on which you run FSAUtility.
                  This registry value does not exist by default. If FileDownloadTimeOut
                  does not exist, FSAUtility -t and -b options recall files asynchronously.

FilePartSize

Location

On a 32-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \KVS
   \Enterprise Vault
    \FSA
      \Reporting
```

On a 64-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \Wow6432Node
   \KVS
    \Enterprise Vault
     \FSA
      \Reporting
```

Content

DWORD.

The default value is 2048 (kilobytes), which is also the maximum size.

Description

Specifies the maximum chunk size for the XML data that FSA Reporting sends from the file server to the FSA Reporting web service.

Set this value on the Windows file server or on the FSA Reporting proxy server for a non-Windows file server.

FileSizeEmulation

Location	On a 32-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \KVS
   \Enterprise Vault
    \FSA
      \PlaceholderService
```

On a 64-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \Wow6432Node
   \KVS
    \Enterprise Vault
     \FSA
      \PlaceholderService
```

Content	DWORD

0 — Placeholder files show a size of zero.

1 — (Default) Placeholder files show the size of the original files.

Description	FileSizeEmulation controls the apparent size of placeholders that were created by a version of Enterprise Vault before 6.0 SP2.

In older versions of Enterprise Vault, placeholders show one of the following sizes:

- Zero
- The size of the corresponding archived items.

Placeholders created by Enterprise Vault 6.0 SP2 and later always show the original file size.

Because placeholders may exist for a long time, both types of placeholder can be present on a system. If both types of placeholder are present, use the default value of FileSizeEmulation so that old placeholders behave in the same manner as new placeholders.

IgnoreSSLCertificateError

Location   HKEY_LOCAL_MACHINE
                 \SOFTWARE
                  \Wow6432Node
                   \KVS
                    \Enterprise Vault
                     \FSA
                      \EMCC

Content   DWORD

                0 — Do not suppress any SSL errors. (Default behavior if the registry value does not exist.)

                1 — Suppress errors that are associated with a certificate that is unavailable.

                2 — Suppress errors that are associated with a certificate name mismatch.

                4 — Suppress errors that are associated with the certificate chain.

Description   IgnoreSSLCertificateError enables SSL certificate errors to be ignored when a Celerra/VNX device is configured to use SSL.

                Set this registry value on the Enterprise Vault server that archives from the Celerra/VNX. Create the **EMCC** key if it does not already exist.

                Note: Do not suppress SSL errors except to avoid temporary configuration issues.

LogLevel

Location   On a 32-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \KVS
   \Enterprise Vault
    \FSA
```

On a 64-bit installation of Windows:

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

Content   DWORD.

Description   Specifies the level of logging to employ for the FSA Cluster Configuration wizard, or for the FSA Agent services on a clustered file server node.

You can set the value on the following computers:

- On the computer on which you run the FSA Cluster Configuration wizard, to set the log level for the wizard.
- On a clustered file server node, to set the log level for the FSA Agent services on that node.

LogLevel can have a value in the range 0 through 5, where 0 or 1 records critical messages only, whereas 5 records debug and diagnostic messages.

PassThruRecallLimitMaxRecalls

Location   On a 32-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \KVS
   \Enterprise Vault
    \FSA
      \PlaceholderService
       \PassThrough
```

On a 64-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \Wow6432Node
   \KVS
    \Enterprise Vault
     \FSA
       \PlaceholderService
        \PassThrough
```

Content   DWORD

Initial value 20

Description

For Windows file servers you can specify a maximum rate of pass-through recall on each computer that runs a Placeholder service. This value controls the maximum rate at which an individual user can retrieve files. The limit also prevents any applications that do not honor the file system offline attribute from retrieving all the files that have been archived from a volume.

If the maximum rate is exceeded, the application receives an Access Denied status. How the status is displayed to the user depends on the individual application.

PassThruRecallLimitMaxRecalls specifies the maximum number of items that you can retrieve for pass-through recall in PassThruRecallLimitTimeInterval seconds.

The default maximum rate is 20 recalls in 10 seconds.

When the maximum retrieval rate is reached, there is an additional wait of PassThruRecallLimitTimeInterval seconds before Enterprise Vault resets the count.

The limit only takes effect if you enable it by using EnableRecallLimitForPassThrough.

See also

PassThruRecallLimitTimeInterval

Location   On a 32-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \KVS
   \Enterprise Vault
    \FSA
       \PlaceholderService
        \PassThrough
```

On a 64-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \Wow6432Node
   \KVS
    \Enterprise Vault
     \FSA
      \PlaceholderService
        \PassThrough
```

Content   DWORD

Initial value 10 (seconds)

Description   Specifies the number of seconds in which you can retrieve a specified
number of items for pass-through recall on a Windows file server.

The value PassThruRecallLimitMaxRecalls sets the maximum number
of items that you can retrieve in this time.

See "PassThruRecallLimitMaxRecalls" on page 177.

RecallLimitMaxRecalls

Location

On a 32-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \KVS
   \Enterprise Vault
    \FSA
      \PlaceholderService
```

On a 64-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \Wow6432Node
   \KVS
    \Enterprise Vault
     \FSA
      \PlaceholderService
```

Content

DWORD

Initial value 20

Description

For Windows file servers you can specify a maximum rate of placeholder recall on each computer that runs an Enterprise Vault Placeholder service. This limit controls the maximum rate at which an individual user can recall files. It also prevents any applications that do not honor the file system offline attribute from recalling all files that had been archived from a volume. If the recall limit is exceeded, the application receives an Access Denied status. How the status is displayed to the user depends on each individual application.

RecallLimitMaxRecalls specifies the maximum number of items that a user is allowed to recall in RecallLimitTimeInterval seconds.

See "RecallLimitTimeInterval" on page 181.

The default maximum rate is 20 recalls in 10 seconds.

You can use another registry value to waive the maximum recall rate for members of the local Administrators group on the file server, if required.

See "BypassRecallLimitsForAdmins" on page 161.

RecallLimitTimeInterval

Location	On a 32-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \KVS
   \Enterprise Vault
    \FSA
      \PlaceholderService
```

On a 64-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \Wow6432Node
   \KVS
    \Enterprise Vault
     \FSA
      \PlaceholderService
```

Content	DWORD
	Initial value 10 (seconds)
Description	This registry value in combination with RecallLimitMaxRecalls sets the maximum placeholder recall rate for a Windows file server that runs the Enterprise Vault Placeholder service.
	RecallLimitTimeInterval specifies the number of seconds in which a maximum of RecallLimitMaxRecalls recalls is allowed.
	See "RecallLimitMaxRecalls" on page 180.
	When the recall limit is reached, Enterprise Vault applies an additional wait of RecallLimitTimeInterval seconds before the count is reset.
See also	See "BypassRecallLimitsForAdmins" on page 161.

ResetFolderModifiedTimeStamp

Location	HKEY_LOCAL_MACHINE

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

Content   DWORD.

0 — After an action is performed, FSA does not reset the last modified
time to the previous value on the parent folder and volume of the folder
hierarchy.

1 — (Default) After an action is performed, FSA resets the last modified
time to the previous value on the parent folder and volume of the folder
hierarchy.

Description   Before Enterprise Vault 10.0.1, the last modified time for the parent
folder and volume of a folder hierarchy changed when any of the
following occurred:

- A File System Archiving task processed a folder in the folder
  hierarchy.
- You added or deleted a target volume or folder in the folder hierarchy
  using the Enterprise Vault Administration Console.
- You created or deleted archive points in the folder hierarchy using
  the ArchivePoints utility, or the Enterprise Vault Administration
  Console.
- You recalled archived files from placeholders.

This change meant that searches for changes using the last modified
time on the parent folder or volume could return unexpected results.

From Enterprise Vault 10.0.1, FSA's default behavior is to reset the last
modified time to the previous value when it has finished processing a
folder.

ResetFolderModifiedTimeStamp lets you revert to the previous behavior
if required.

Set this registry value on the Enterprise Vault server.

Note: You must restart the Enterprise Vault Admin service if you
change the value of this setting, or delete the setting.

See also   Another registry value set under the **FSA\PlaceholderService** subkey
on Windows file servers controls whether FSA resets the last modified
time after placeholder recall on the file server.

ResetFolderModifiedTimeStamp (PlaceholderService)

Location
On a 32-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \KVS
   \Enterprise Vault
    \FSA
     \PlaceholderService
```

On a 64-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \Wow6432Node
   \KVS
    \Enterprise Vault
     \FSA
      \PlaceholderService
```

Content
DWORD.

0 — After placeholder recall, FSA does not reset the last modified time to the previous value on the placeholder folder and volume.

1 — (Default) After placeholder recall, FSA resets the last modified time to the previous value on the placeholder folder and volume.

Description
Before Enterprise Vault 10.0.1, if you recalled a placeholder on a Windows file server the last modified time changed on the placeholder folder and volume. This change meant that searches for changes using the last modified time on the folder or volume could return unexpected results.

From Enterprise Vault 10.0.1, FSA's default behavior is to reset the last modified time to the previous value after the placeholder is recalled.

ResetFolderModifiedTimeStamp lets you revert to the previous behavior if required.

Set this registry value on the Windows file servers on which you use placeholders.

Note: You must restart the Enterprise Vault File Placeholder service on the file server if you change the value of this setting, or delete the setting.

See also   Another registry value set under the **FSA** subkey on the Enterprise
              Vault server controls whether FSA resets the last modified time after
              other FSA actions are performed.

              See "ResetFolderModifiedTimeStamp" on page 181.

ScanThreads

Location   On a 32-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \KVS
   \Enterprise Vault
    \FSA
      \Reporting
```

              On a 64-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \Wow6432Node
   \KVS
    \Enterprise Vault
     \FSA
      \Reporting
```

Content   DWORD.

              The default value is 5, and the maximum value is 10.

Description   ScanThreads specifies the maximum number of volumes that FSA
                Reporting can scan simultaneously on a target file server. For example,
                if you set ScanThreads to 3, and more than three volumes are enabled
                for FSA Reporting, only three volumes are scanned initially. FSA
                Reporting does not start to scan another volume until the scan
                completes on at least one of the three initial volumes.

                By reducing this value you reduce the resource demand, although you
                lengthen the time for multiple FSA Reporting scans to complete.

                For Windows file servers, set this registry value on the file server. For
                NetApp and Celerra/VNX file servers, set this registry value on the FSA
                Reporting proxy server.

                After you set or change this value, do as follows:

                ■ If you changed the value on an Enterprise Vault server, restart the
                  Enterprise Vault Admin service on the Enterprise Vault server.
                ■ Otherwise, restart the Enterprise Vault File Collector service on the
                  computer on which you changed the value.

See also   See "BulkUploadThreads" on page 159.

SetNetappPHOriginalSize

Location   HKEY_LOCAL_MACHINE
                 \SOFTWARE
                  \Wow6432Node
                   \KVS
                    \Enterprise Vault
                      \NetAPPPlaceholderService

Content   DWORD

                0 — Show the size of NetApp placeholders as 0 KB.

                1 — Show the size of NetApp placeholders as the original file size (the
                default behavior if the registry value does not exist).

                This registry value is not created automatically.

Description   Determines whether to show the file size of placeholders on NetApp
                     devices as the original file size or as 0 KB. By default, the placeholders
                     are shown with the original file size. However, to determine the original
                     file size requires a performance overhead. For performance reasons
                     you may want to disable this functionality and show the size of the
                     placeholders as 0 KB.

                     To show the size of placeholders as 0 KB, create the registry value and
                     set a value of 0 on the Enterprise Vault server whose File System
                     Archiving task processes the NetApp filer volume.

                     Setting or changing this registry value does not affect existing
                     placeholders.

SingleNodeFSA

Location   On a 32-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \KVS
   \Enterprise Vault
    \FSA
```

                     On a 64-bit installation of Windows:

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

Content   DWORD value.

                     1 — lets you configure a single-node FSA file server cluster.

                     This registry value is not created automatically.

Description   SingleNodeFSA permits the configuration of a single-node FSA file server cluster.

SingleNodeFSA must be present on the computer or computers on which the Enterprise Vault Administration Console is installed and on the clustered file server node.

You must create SingleNodeFSA before you do either of the following:

- Install the FSA Agent on the file server, if you perform this task from the Administration Console.
- Run the FSA Cluster Configuration wizard.

Set SingleNodeFSA to 1 to allow a single-node FSA cluster.

You do not need to change or remove this registry value if you subsequently configure a multiple-node FSA cluster.

SynchroniseFSASharePermissions

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

Content   DWORD

0 — Do not synchronize archive permissions to the file server share permissions. On synchronization, assign to an archive the NTFS permissions of the corresponding archive point folder.

1 or greater, or registry key not present — (Default) Synchronize archive permissions to the file server share permissions. On synchronization, assign to an archive the permissions of the corresponding archive point folder, if it is a share. Otherwise, assign the permissions of the target volume share.

Description   By default, when a File System Archiving task synchronizes archive permissions it uses the file server share permissions:

- If the archive point folder (the file server folder with the archive point) is a share, the archive is assigned the permissions of the archive point folder.
- If the archive point folder is not a share, the archive is assigned the permissions of the target volume share.

SynchroniseFSASharePermissions enables you to change this behavior. If you set the value to 0, the task always assigns to an archive and its folders the permissions of the archive point folder, regardless of whether that folder is a share.

This registry value has no effect on archive folder permissions. Folders within an archive are always synchronized with the NTFS permissions of the corresponding file system folder's NTFS permissions.

Note that users must have both archive folder and archive permissions to access items.

TempFilePath

Location   On a 32-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \KVS
   \Enterprise Vault
    \FSA
      \Reporting
```

On a 64-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \Wow6432Node
   \KVS
    \Enterprise Vault
     \FSA
       \Reporting
```

Content   String value.

Initial value is the Enterprise Vault installation folder, for example
`C:\Program Files (x86)\Enterprise Vault`.

Description   Specifies a folder path on the file server under which FSA Reporting
stores its temporary data files. FSA Reporting creates a subfolder named
FSAReports under the specified path, in which to hold the temporary
files.

If there is likely to be insufficient space for the temporary files on the
installation drive, relocate the storage location to an existing path on a
drive that has sufficient free space.

Note: The value of TempFilePath must not exceed 100 characters,
including spaces.

For Windows file servers TempFilePath is located on the file server.
For NetApp and Celerra/VNX file servers, TempFilePath is located on
the Enterprise Vault server that performs the FSA Reporting file
collection.

If you change this value on a Windows file server, restart the Enterprise
Vault File Collector service on the file server. If you change this value
on an Enterprise Vault server, restart the Enterprise Vault server's
Admin service.

WebServiceTimeout

Location   On a 32-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \KVS
   \Enterprise Vault
    \FSA
      \Reporting
```

On a 64-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \Wow6432Node
   \KVS
    \Enterprise Vault
     \FSA
       \Reporting
```

Content   DWORD.

The default value is 9999, which is also the maximum value.

Description	Specifies the maximum number of minutes that the FSA Agents wait for their requests to the FSA Reporting web service to be serviced.
	For Windows file servers, set this registry value on the file server. For NetApp and Celerra/VNX file servers, set this registry value on the FSA Reporting proxy server.

WSTempFilePath

Location	`HKEY_LOCAL_MACHINE`
	` \SOFTWARE`
	`  \Wow6432Node`
	`   \KVS`
	`    \Enterprise Vault`
	`     \FSA`
	`      \Reporting`

Content	String value.
	This value does not exist by default.
Description	Specifies a folder path on the Enterprise Vault server where the FSA Reporting web service stores the temporary scan data and metadata XML files.
	If this registry value does not exist on the Enterprise Vault server or has no string value, FSA Reporting stores the temporary files in the `FRAReports\ReportingTempDir` folder of the Enterprise Vault installation folder.
	In configurations where a large number of FSA Reporting scans occur, the scans can take longer to complete if there is limited disk space where FSA Reporting stores the temporary files.
	Use this registry value to change the temporary file storage location if required.
	The path must be a local path. On a clustered Enterprise Vault server the path must be on a shared disk.
	Note: The path must not exceed 60 characters, including spaces.
	Set this value on the Enterprise Vault server. After you set or change this registry value, restart the IIS Admin Service on the Enterprise Vault server for the change to take effect.

Indexing

This chapter includes the following topics:

- AVSMaxLoc

- CheckWidthNormalization

- GetIndexServerWaitSecs

- LogMissingItems

- RetryAbandonedFailedItems

- RetryFailedIndexVolumesIntervalHours

- SearchChunkSize

AVSMaxLoc

Location	`HKEY_LOCAL_MACHINE`
	`\SOFTWARE`
	`\Wow6432Node`
	`\KVS`
	`\Enterprise Vault`
	`\Indexing`

Content	DWORD. Default value is 1,000,000,000.

Description   Maximum location value allowed in an index. Used to prevent indexes exceeding their maximum size. Can be specified per index by creating the values below a key with value equal to the Index entry-id.

This setting can also be used to create multiple index volume sets to use when testing archive search applications.

Note: For Enterprise Vault 10.0 and later, AVSMaxLoc affects 32-bit indexing only. For 64-bit indexing, use the appropriate **Maximum items in…** computer properties advanced setting.

For more information, see "Computer properties advanced settings" in the *Administrator's Guide*.

CheckWidthNormalization

Location
```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \Wow6432Node
   \KVS
    \Enterprise Vault
     \Indexing
```

Content   DWORD

0 — When an index is accessed for the first time, do not search for and flag unnormalized Katakana characters in its list of words. (Default.)

1 — When an index is accessed for the first time, search for and flag unnormalized Katakana characters in its list of words.

Description   Determines whether Enterprise Vault searches for and flags unnormalized Katakana characters in indexes when it accesses those indexes for the first time. Katakana is a Japanese writing system that is most often used for transcription of words from foreign languages. When unnormalized, these characters have not been converted to lowercase during the indexing process. Flagging these characters lets applications such as Compliance Accelerator and Discovery Accelerator make a judgment as to whether their search results are 100% reliable.

As Katakana width normalization affects Japanese content, it is important that Japanese customers turn on this setting. Similarly, Compliance Accelerator and Discovery Accelerator customers who may be worried about unnormalized content going undiscovered should also turn on this setting.

For Enterprise Vault 10.0 and later, CheckWidthNormalization affects 32-bit indexing only. For 64-bit indexing, there is no equivalent setting.

GetIndexServerWaitSecs

Location
```
HKEY_LOCAL_MACHINE
 \Software
  \Wow6432Node
   \KVS
    \EnterpriseVault
     \Indexing
```

Content   DWORD

Description   Specifies the number of seconds for which Enterprise Vault waits for a
free Indexing Service slot before giving up and returning the message
Indexing Service is busy.

The minimum value is 10 seconds, and the maximum is 15 minutes.
The default value is 120 seconds.

For Enterprise Vault 10.0 and later, GetIndexServerWaitSecs affects
32-bit indexing only. For 64-bit indexing, there is no equivalent setting.

LogMissingItems

Location
```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \Wow6432Node
   \KVS
    \Enterprise Vault
     \Indexing
```

Content   DWORD.

0 — Do not flag missing savesets and content in search results.

1 — (Default) In search results, flag savesets missing from the index.

2 — In search results, flag both savesets missing from the index, and
savesets that have some content missing from the index.

Description LogMissingItems controls whether search results flag only savesets that are missing from the index, or both missing savesets and savesets that have some content missing from the index.

Note that in versions of Enterprise Vault before version 10.0, the value you assigned to LogMissingItems also determined the level of information that Enterprise Vault recorded for missing items and content:

- 0 — The Indexing service did not log savesets and content missing from the index.
- 1 — The Indexing service logged only savesets that were missing from the index.
- 2 — The Indexing service logged both savesets missing from the index, and savesets that had some content missing from the index.

For any remaining 32-bit indexes in your environment, missing item information may be unavailable or limited due to the setting of LogMissingItems at the time the indexes were created.

RetryAbandonedFailedItems

Location
```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \Wow6432Node
   \KVS
    \Enterprise Vault
     \Indexing
```

Content DWORD.

0 — The Indexing service will not try to index consecutive failed items when you next update an index volume. You can set this value if you know that the items are missing or corrupted and cannot be recovered.

1 (default) — The Indexing service will try to index consecutive failed items when you next update an index volume. Items that will be retried in the next index volume update are not listed in the missing items log.

Description Specifies whether, during an update of a failed index volume, the Indexing service tries to index any consecutive failed items.

Note that you cannot use this feature to index every item that the Indexing service has ever failed to index. Only items that became consecutive failed items while RetryAbandonedFailedItems was set are eligible for retrying.

For Enterprise Vault 10.0 and later, RetryAbandonedFailedItems affects 32-bit indexing only. For 64-bit indexing, there is no equivalent setting.

RetryFailedIndexVolumesIntervalHours

Location	HKEY_LOCAL_MACHINE
	 \SOFTWARE
	  \Wow6432Node
	   \KVS
	    \Enterprise Vault
	     \Indexing

Content	DWORD
Description	Specifies the frequency in hours with which the Indexing service should check for and reset any index volumes that are marked as failed. The default is 6.
	Set this registry value to 0 to stop the Indexing service from trying to reset the index volumes.
	Note: For Enterprise Vault 10.0 and later, RetryFailedIndexVolumesIntervalHours affects 32-bit indexing only. For 64-bit indexing, use the computer properties advanced setting, **Frequency of checks for failed volumes**.
	For more information, see "Computer properties advanced settings" in the *Administrator's Guide*.

SearchChunkSize

Location	HKEY_LOCAL_MACHINE
	 \SOFTWARE
	  \Wow6432Node
	   \KVS
	    \Enterprise Vault
	     \Indexing

Content	DWORD
Description	The maximum size of each search chunk. Default is 5000 words.
	For Enterprise Vault 10.0 and later, SearchChunkSize affects 32-bit indexing only. For 64-bit indexing, there is no equivalent setting.

Installation

This chapter includes the following topics:

■ About the installation registry values

About the installation registry values

The installation registry values are used by the Enterprise Vault installation program and may be required by support personnel.

The installation registry values are under the following registry keys:

On a 32-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \KVS
   \Enterprise Vault
    \Install
```

On a 64-bit installation of Windows:

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

Do not change any of the installation registry values.

Chapter **16**

Outlook Add-In

This chapter includes the following topics:

- Location of Outlook Add-In registry values

- ContentClassesPreventingMsgClassChangeOnView

- DCOMOverrideRPCHTTP

- DCOMPollInterval

- DeleteHiddenMsgBtnVisible

- DeployFormsLocally

- InternetOpenTypeDirect

- LastPSTSearch

- LoggingLevel

- MessageClassesPreventingMsgClassChangeOnView

- NoSoftDeletes

- NotificationsEnabled

- OVAllowMissedMDCSyncOnStartup

- OVContentDownload

- OVDownloadItemAgeLimit

- OVEnabled

- OVItemArchiveAttempts

- OVMaxItemArchivesPerSync

- OVMaxItemDeletesPerSync

- OVMaxItemUpdatesPerSync

- OVMaxMessageSizeToArchiveMB

- OVMaxToArchivePerSyncMB

- OVMaxTotalToArchiveMB

- OVMDCSyncFrequencyInSecs

- OVPauseInterval

- OVPerItemSleep

- OVPreemptAdvance

- OVRequireOfflineStore

- OVRootDirectory

- OVRootDirectorySearchPath

- OVStoreSize

- OVStoreSizePercent

- OVSyncArchiveTypes

- OVSyncSlotTimeOutInSecs

- RemoveOfflineVault

- RemovePSTEntries

- SendLogFileMaxSizeMB

- SendLogFileRecipients

- UpdateWDSIndexForVV

- VVAllowArchive

- VVAllowHardDelete

- VVAllowInterStoreCopyAndMove

- VVAllowIntraStoreCopy

- VVAllowReOrg

- VVAutoSyncItemsSizeThresholdMB

- VVAutoSyncItemThreshold

- VVDenyMultiContentlessOpsAboveMB

- VVEnabled

- VVReadingPaneContent

- VVStubOnlyModuleList

Location of Outlook Add-In registry values

You can set some of the Outlook Add-In registry values in more than one location. Choose the location that is appropriate for your configuration and your group policy requirements.

The Outlook Add-In processes policy values within the registry in a specific order. The first policy value that is identified is the policy that is used.

The Outlook advanced setting **Policy lookup locations** lets you control the use of registry values to override the Exchange desktop policy. For details of this advanced setting, see the *Administrator's Guide*.

Location of Vault Cache and Virtual Vault registry values

The Outlook Add-In looks for the Vault Cache and Virtual Vault registry values listed here in the following registry keys, in this order:

```
1      HKEY_LOCAL_MACHINE
         \SOFTWARE
          \(Wow6432Node)
           \KVS
             \Enterprise Vault
              \Client


2      HKEY_CURRENT_USER
         \SOFTWARE
          \(Wow6432Node)
           \KVS
             \Enterprise Vault
              \Client
                \VaultCacheStoreID
```

```
3      HKEY_CURRENT_USER
        \SOFTWARE
         \(Wow6432Node)
          \KVS
            \Enterprise Vault
              \Client
```

If the Outlook Add-In does not find the policy value in these registry keys, it uses the policy value that is set 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.

The registry values to which this information applies are as follows:

- NotificationsEnabled
- OVAllowMissedMDCSyncOnStartup
- OVContentDownload
- OVDownloadItemAgeLimit
- OVEnabled
- OVItemArchiveAttempts
- OVMaxItemArchivesPerSync
- OVMaxItemDeletesPerSync
- OVMaxItemUpdatesPerSync
- OVMaxMessageSizeToArchiveMB
- OVMaxToArchivePerSyncMB
- OVMaxTotalToArchiveMB
- OVMDCSyncFrequencyInSecs
- OVPauseInterval
- OVPerItemSleep
- OVPreemptAdvance

- OVRequireOfflineStore
- OVRootDirectory
- OVRootDirectorySearchPath
- OVStoreSize
- OVStoreSizePercent
- OVSyncArchiveTypes
- OVSyncSlotTimeOutInSecs
- VVAllowArchive
- VVAllowHardDelete
- VVAllowInterStoreCopyAndMove
- VVAllowIntraStoreCopy
- VVAllowReOrg
- VVAutoSyncItemsSizeThresholdMB
- VVAutoSyncItemThreshold
- VVDenyMultiContentlessOpsAboveMB
- VVEnabled
- VVReadingPaneContent
- VVStubOnlyModuleList

Location of other Outlook Add-In registry values

The Outlook Add-In looks for the registry values listed here in the following registry keys, in this order:

```
1    HKEY_LOCAL_MACHINE
      \SOFTWARE
       \KVS
        \Enterprise Vault
         \Client


2    HKEY_CURRENT_USER
      \SOFTWARE
       \KVS
        \Enterprise Vault
         \Client
```

If the Outlook Add-In does not find the policy value in these registry keys, it uses the policy value that is set in the Exchange desktop policy.

The registry values to which this information applies are as follows:

- DCOMOverrideRPCHTTP

- DCOMPollInterval

- DeleteHiddenMsgBtnVisible

- DeployFormsLocally

- NoSoftDeletes

- RemoveOfflineVault

- RemovePSTEntries

- SendLogFileMaxSizeMB

- SendLogFileRecipients

ContentClassesPreventingMsgClassChangeOnView

```
Location         HKEY_CURRENT_USER
                  \SOFTWARE
                   \KVS
                    \Enterprise Vault
                     \Client
```

Content   String.

               Specifies the content classes of items whose message classes are
               unchangeable when the items are opened in Outlook. The default value
               is as follows:

               rpmsg.message

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. This registry value stops Enterprise Vault from
               changing the message class of any item with the specified content
               class.

               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 class names are case-insensitive.

               Note: This registry value performs the same function as the advanced
               Exchange desktop policy setting "Preserve message class (for content
               class)", which you can set through the Administration Console. For
               more information on the policy setting, see the *Administrator's Guide*.

See also   See "MessageClassesPreventingMsgClassChangeOnView" on page 206.

DCOMOverrideRPCHTTP

Note: In Enterprise Vault 10.0.1 and later, DCOMOverrideRPCHTTP and
DCOMPollInterval only have an effect if the Outlook Add-In version is earlier than
Enterprise Vault 10.0.1.

Location   See "Location of other Outlook Add-In registry values" on page 200.

Content   DWORD

                0 — (Default) Do not test for the availability of full Enterprise Vault
                Outlook Add-In connectivity for Outlook clients that are configured to
                use RPC over HTTP.

                Non-zero — Test for the availability of full Enterprise Vault Outlook
                Add-In connectivity for Outlook clients that are configured to use RPC
                over HTTP.

Description   If the Outlook client is configured to use RPC over HTTP, Enterprise
                   Vault provides HTTP-Only Outlook Add-In functionality.

                   When DCOMOverrideRPCHTTP is enabled, Enterprise Vault tests
                   regularly for the availability of full Enterprise Vault Outlook Add-In
                   connectivity. If a full Outlook Add-In connection is available, the following
                   manual actions operate in full Outlook Add-In mode: Archive, Restore,
                   Delete, and changing folder settings.

                   The test for full Outlook Add-In connectivity is performed on startup.
                   The test is repeated at the intervals that the registry value
                   DCOMPollInterval defines.

See also   See "DCOMPollInterval" on page 203.

DCOMPollInterval

Note: In Enterprise Vault 10.0.1 and later, DCOMOverrideRPCHTTP and
DCOMPollInterval only have an effect if the Outlook Add-In version is earlier than
Enterprise Vault 10.0.1.

Location   See "Location of other Outlook Add-In registry values" on page 200.

Content   DWORD

                   Default: 15 (minutes)

Description   Sets the interval in minutes at which Enterprise Vault tests for the
                   availability of full Enterprise Vault Outlook Add-In connectivity when the
                   registry value DCOMOverrideRPCHTTP is enabled.

See also   See "DCOMOverrideRPCHTTP" on page 202.

DeleteHiddenMsgBtnVisible

Location   See "Location of other Outlook Add-In registry values" on page 200.

Content   DWORD.

                   0 – Not visible (default if the key does not exist).

                   1 – Visible.

Description   Controls whether the **Delete Hidden Message** button is visible in the
                   Vault Information dialog box.

DeployFormsLocally

Location	See "Location of other Outlook Add-In registry values" on page 200.
Content	DWORD
	0 — Never deploy forms locally.
	1 — Only deploy forms when there is no Organizational Forms Library available (default).
	2 — Always deploy forms locally.
	3 — Always delete Enterprise Vault forms from the user's Personal Forms Library.
Description	Specifies whether, when the user starts Outlook, the Enterprise Vault add-in determines whether the Enterprise Vault forms are installed or need updating and then adds or replaces them as necessary.
	This enhancement is required to enable Enterprise Vault to store forms in each user's Personal Forms Library in an Exchange Server environment when there is no Organizational Forms Library.

InternetOpenTypeDirect

Location	`HKEY_CURRENT_USER`
	`  \SOFTWARE`
	`    \KVS`
	`      \Enterprise Vault`
	`        \Client`

Content	DWORD
	0 - Use proxy settings (default).
	1 - Ignore proxy settings.
Description	Controls whether the Outlook Add-In uses the proxy settings on the client computer.
	This registry value performs the same function as the advanced Exchange desktop policy setting "Use proxy settings", which you can set through the Administration Console. For more information on the policy setting, see the *Administrator's Guide*.

LastPSTSearch

Location	`HKEY_CURRENT_USER`
	` \SOFTWARE`
	`  \KVS`
	`   \Enterprise Vault`
	`    \Client`

Content	String
Description	Used by Enterprise Vault to record the date on which a search for new `.pst` files was last conducted.

LoggingLevel

Location	`HKEY_CURRENT_USER`
	` \SOFTWARE`
	`  \KVS`
	`   \Enterprise Vault`
	`    \Client`

Content	The following levels of information can be logged: ■ 0 – Errors only. ■ 1 – Information (default). ■ 2 – Minimum tracing. ■ 3 – Maximum tracing. This includes function calls. ■ 9 – Verbose support logging. As this option is currently only available for Virtual Vault, you must specify the value as 0x80000009. ■ 0x80000000 – Include Virtual Vault logging. Combine this value with one of the above values to specify the level of logging, including Virtual Vault logging. For example, a value of 0x80000001 would provide informational logging for the client and Virtual Vault.
Description	Specifies the required level of logging from the Desktop environment to a log file. The log file is created in the user's temp directory, with a filename of `ev_client_log_`*`timestamp`*`.txt`. A maximum of 20 log files is available (the oldest is automatically deleted).

MessageClassesPreventingMsgClassChangeOnView

Location	HKEY_CURRENT_USER
	 \SOFTWARE
	  \KVS
	   \Enterprise Vault
	    \Client

Content

String.

Specifies the message classes that are unchangeable when items of the specified type are opened in Outlook. The default value is as follows:

IPM.Note.SMime*;IPM.Report.*;REPORT.IPM*

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. This registry value lets you preserve the original message class of these items so that they open without error.

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 class names are case-insensitive.

Note: This registry value performs the same function as the advanced Exchange desktop policy setting "Preserve message class", which you can set through the Administration Console. For more information on the policy setting, see the *Administrator's Guide*.

See also

See "ContentClassesPreventingMsgClassChangeOnView" on page 201.

NoSoftDeletes

Location	See "Location of other Outlook Add-In registry values" on page 200.
Content	DWORD

Description

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.

When NoSoftDeletes is set to a non-zero value, the client does not attempt a recoverable deletion and instead displays an error message.

NotificationsEnabled

Location	See "Location of Vault Cache and Virtual Vault registry values" on page 199.
Content	DWORD
	0 — (Default) Disable Enterprise Vault Outlook Add-In user notifications
	1 — Enable Enterprise Vault Outlook Add-In user notifications
Description	Set NotificationsEnabled to 1 to enable Enterprise Vault Outlook Add-In user notifications. For example, when NotificationsEnabled is set to 1, the Enterprise Vault Outlook Add-In notifies users of Vault Cache synchronization errors.
	If NotificationsEnabled is not set or is set to 0, Enterprise Vault Outlook Add-In user notifications are disabled.

OVAllowMissedMDCSyncOnStartup

Location	You can set this registry value in more than one location.
	See "Location of Vault Cache and Virtual Vault registry values" on page 199.
Content	DWORD
	0 — (Default) Disabled.
	1 — Enabled.
Description	When a user starts Outlook, a Vault Cache synchronization is initiated if a scheduled synchronization has been missed. Synchronization slot and SQL Server contention issues can occur if a large number of users, who have missed a scheduled synchronization, all start Outlook within a short timeframe.
	OVAllowMissedMDCSyncOnStartup allows you to configure clients so that missed scheduled Vault Cache synchronizations are ignored. A Vault Cache sychronization occurs at the next scheduled sychronization time .
	If the default value (0) is specified, or the setting does not exist, then a Vault Cache synchronization is initiated when a user starts Outlook, if a scheduled synchronization has been missed.

OVContentDownload

Location	See "Location of Vault Cache and Virtual Vault registry values" on page 199.
Content	DWORD

- 0 – Item headers are synchronized to Vault Cache, but the content of archived items is not stored in Vault Cache.

  If a user opens an item in Virtual Vault, Enterprise Vault immediately retrieves the content. With this option, the item's content is not stored in Vault Cache even after the content is retrieved.
- 1 (default) – Item headers are synchronized to Vault Cache and the content of archived items is stored in Vault Cache.
- 2 – Item headers are synchronized to Vault Cache, but the content of archived items is not automatically stored in Vault Cache; only the content of each item that a user opens in Virtual Vault is stored in Vault Cache.

Description	Specifies the strategy for storage of the content of archived items in Vault Cache.

This registry value performs the same function as the **Content strategy** setting on the **Vault Cache** tab of the Exchange desktop policy. You can set the value using the Administration Console.

OVDownloadItemAgeLimit

Location	See "Location of Vault Cache and Virtual Vault registry values" on page 199.
Content	DWORD

Description	Specifies the maximum age of an item that is downloaded automatically to the Vault Cache.
	For example, 365 (days) means that items up to one year old will be downloaded. Items older than 365 days are downloaded only if the user requests them.
	If OVDownloadItemAgeLimit is set to 0 (zero) then there is no age limit.
	If OVDownloadItemAgeLimit is set to 1 then items up to one day old are downloaded, and so on.
	Note: This registry value performs the same function as the advanced Exchange mailbox policy setting "Download item age limit", which you can set through the Administration Console. For more information on the policy setting, see the *Administrator's Guide*.

OVEnabled

Location	See "Location of Vault Cache and Virtual Vault registry values" on page 199.
Content	DWORD
	0 — Turns off Vault Cache for this user. No new Vault Cache is created. The user has access to an existing Vault Cache, but no new items are added to an existing Vault Cache.
	1 — (Default) The user can enable Vault Cache.
Description	Controls whether the user can enable Vault Cache.
	Note: This registry value performs a similar function to the Exchange desktop policy setting "Make Vault Cache available for users", which you can set through the Administration Console. However, the policy setting determines the availability of Vault Cache to all the users in an Enterprise Vault site. If the policy setting disables Vault Cache for all users, you cannot enable it for a particular user with the OVEnabled registry value. On the other hand, if the policy setting enables Vault Cache for all users, you can disable it for a particular user by setting the registry value to 0.

OVItemArchiveAttempts

Location	See "Location of Vault Cache and Virtual Vault registry values" on page 199.

Content   DWORD

                 An integer value. The default is 3.

Description   Specifies how many times Enterprise Vault tries to archive an item. The
                 archive operation is tried this number of times before the item is listed
                 in the Virtual Vault search folder named **Could not archive**.

                 Note: This registry value performs the same function as the advanced
                 Exchange desktop policy setting "Max attempts to archive an item".
                 You can configure the policy setting using the Administration Console.
                 For more information on the policy setting, see the *Administrator's
                 Guide*.

OVMaxItemArchivesPerSync

Location   See "Location of Vault Cache and Virtual Vault registry values"
                 on page 199.

Content   DWORD

                 An integer value. The default is 0 (no limit).

Description   Controls the maximum number of archive requests during a Vault Cache
                 synchronization. Any remaining requests are made at the next
                 synchronization.

                 When a user stores unarchived items in Virtual Vault, the archive
                 operation does not take place until after the next Vault Cache header
                 synchronization.

                 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.

                 Also, until the items that a user has stored in Virtual Vault are archived
                 in the online archive, there are no backup items.

                 Note: This registry value performs the same function as the advanced
                 Exchange desktop policy setting "Max archive requests per
                 synchronization". You can configure the policy setting using the
                 Administration Console. For more information on the policy setting, see
                 the *Administrator's Guide*.

OVMaxItemDeletesPerSync

Location	See "Location of Vault Cache and Virtual Vault registry values" on page 199.
Content	DWORD
	An integer value. The default is 0 (no limit).
Description	Controls the maximum number of delete requests during a Vault Cache synchronization. Any remaining requests are made at the next synchronization.
	Deletion requests use relatively few resources on the Enterprise Vault server.
	Note: This registry value performs the same function as the advanced Exchange desktop policy setting **Max delete requests per synchronization**. You can configure the policy setting using the Administration Console. For more information on the policy setting, see the *Administrator's Guide*.

OVMaxItemUpdatesPerSync

Location	See "Location of Vault Cache and Virtual Vault registry values" on page 199.
Content	DWORD
	An integer value. The default is 0 (no limit).
Description	Controls the maximum number of property change requests during a Vault Cache synchronization. Any remaining requests are made at the next synchronization.
	Update requests use relatively few resources on the Enterprise Vault server.
	Note: This registry value performs the same function as the advanced Exchange desktop policy setting **Max item updates per synchronization**. You can set the value using the Administration Console. For more information on the policy setting, see the *Administrator's Guide*.

OVMaxMessageSizeToArchiveMB

Location	See "Location of Vault Cache and Virtual Vault registry values" on page 199.
Content	DWORD
	An integer value. The default is 256 (MB). The value 0 specifies no limit.
Description	Controls the maximum size in megabytes of an item that can be moved or copied into Virtual Vault.
	If this value is similar to the value of **Max total size of items to archive** (**OVMaxTotalToArchiveMB**), a full synchronization can consist of one item.
	The value of **OVMaxMessageSizeToArchiveMB** may be used automatically for **Max data archived per synchronization** (**OVMaxToArchivePerSyncMB**) or **Max total size of items to archive** (**OVMaxTotalToArchiveMB**). It is used if the value of those settings is less than the **OVMaxMessageSizeToArchiveMB** value.
	Note: This registry value performs the same function as the advanced Exchange desktop policy setting **Max item size to archive**. You can set the value using the Administration Console. For more information on the policy setting, see the *Administrator's Guide*.

OVMaxToArchivePerSyncMB

Location	See "Location of Vault Cache and Virtual Vault registry values" on page 199.
Content	DWORD
	An integer value. The default is 512 (MB). The value 0 specifies no limit.

Description   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.

                     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.

                     Also, until Enterprise Vault archives the items that the user stores in
                     Virtual Vault in the online archive, there are no backup items.

                     The value of this setting must be greater than or equal to the value of
                     Max item size to archive (**OVMaxMessageSizeToArchiveMB**). If not,
                     the value of **Max item size to archive**
                     (**OVMaxMessageSizeToArchiveMB**) is used.

                     Note: This registry value performs the same function as the advanced
                     Exchange desktop policy setting "Max data archived per
                     synchronization". You can configure the policy setting using the
                     Administration Console. For more information on the policy setting, see
                     the *Administrator's Guide*.

OVMaxTotalToArchiveMB

Location   See "Location of Vault Cache and Virtual Vault registry values"
                     on page 199.

Content   DWORD

                     An integer value. The default is 512 (MB). The value 0 specifies no
                     limit.

Description   Controls the maximum total size in megabytes of pending archive data
                     in Vault Cache.

                     Pending archive data consists of the 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.

                     The value of this setting must be greater than or equal to the value of
                     OVMaxMessageSizeToArchiveMB. If not, the value of
                     OVMaxMessageSizeToArchiveMB is used.

                     Note: This registry value performs the same function as the advanced
                     Exchange desktop policy setting **Max total size of items to archive**.
                     You can set the value using the Administration Console. For more
                     information on the policy setting, see the *Administrator's Guide*.

OVMDCSyncFrequencyInSecs

Location	See "Location of Vault Cache and Virtual Vault registry values" on page 199.
Content	DWORD
	Number of seconds between scheduled synchronizations. The default value is 86400, which is 24 hours.
Description	Enables you to set the frequency of scheduled Vault Cache synchronizations. The default value (86400 seconds) means that a synchronization is initiated every 24 hours.
	The new value only takes effect after the next scheduled synchronization.

OVPauseInterval

Location	See "Location of Vault Cache and Virtual Vault registry values" on page 199.
Content	DWORD
	Default is 3.
Description	The number of minutes to wait before Enterprise Vault starts searching for items that need to be added to the Vault Cache.
	Note: This registry value performs the same function as the advanced Exchange mailbox policy setting "Pause interval", which you can set through the Administration Console. For more information on the policy setting, see the *Administrator's Guide*.

OVPerItemSleep

Location	See "Location of Vault Cache and Virtual Vault registry values" on page 199.
Content	DWORD

Description	Specifies the number of milliseconds sleep that will be used per item during various Vault Cache operations.

Note: This registry value performs the same function as the advanced Exchange mailbox policy setting "Per item sleep", which you can set through the Administration Console. For more information on the policy setting, see the *Administrator's Guide*.

OVPreemptAdvance

Location	See "Location of Vault Cache and Virtual Vault registry values" on page 199.
Content	DWORD
	An integer indicating a number of days. The default vault is 7.
Description	Enterprise Vault uses this setting when it calculates the age of items to preemptively copy from the .OST file to the Vault Cache. The process is known as preemptive caching. Preemptive caching reduces the number of items that need to be downloaded from the mailbox archive when the Vault Cache is synchronized with the mailbox archive.

Note: This registry value performs the same function as the advanced Exchange desktop policy setting "Preemptive archiving in advance", which you can set through the Administration Console. For more information on the policy setting, see the *Administrator's Guide*.

OVRequireOfflineStore

Location	See "Location of Vault Cache and Virtual Vault registry values" on page 199.
Content	DWORD

- 0 – An offline store is not required for Vault Cache to be enabled.
- 1 (default) – An offline store is required for Vault Cache to be enabled.

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** (**OVContentDownload**) is to store all items.

Note: This registry value performs the same function as the advanced Exchange desktop policy setting **Offline store required**. You can set the value using the Administration Console. For more information on the policy setting, see the *Administrator's Guide*.

OVRootDirectory

Location   See "Location of Vault Cache and Virtual Vault registry values" on page 199.

Content   String.

A path to a folder that Enterprise Vault can create on the user's local computer. If you do not specify OVRootDirectory, Enterprise Vault uses an `Enterprise Vault` subfolder in the user's `Application Data` folder.

Description   The location in which to place Vault Cache. This value is used when a user enables Vault Cache.

Changing this value has no effect on existing Vault Caches.

Note: This registry value performs the same function as the advanced Exchange mailbox policy setting "Root folder", which you can set through the Administration Console. For more information on the policy setting, see the *Administrator's Guide*.

OVRootDirectorySearchPath

Location   See "Location of Vault Cache and Virtual Vault registry values" on page 199.

Content   String containing a semi-colon separated list of folder paths.

Description	Controls the location of the Vault Cache.
	OVRootDirectorySearchPath 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 specify a list that is likely to be suitable for computers with different configurations.
	For example, if you specify `E:\vault;C:\vault` then the Vault Cache would be created in `E:\vault` if that was valid on the user's computer, and if it was not valid, then in `C:\vault`.
	If none of the locations in OVRootDirectorySearchPath is valid, the one specified by OVRootDirectory is used, if possible.
	Note: This registry value performs the same function as the advanced Exchange mailbox policy setting "Root folder search path", which you can set through the Administration Console. For more information on the policy setting, see the *Administrator's Guide*.

OVStoreSize

Location	See "Location of Vault Cache and Virtual Vault registry values" on page 199.
Content	DWORD
	The minimum value is 1 (GB), and the maximum value is 999 (GB).
Description	The maximum size, in gigabytes, that Vault Cache is allowed to occupy. If the Vault Cache reaches this size, the oldest items are automatically deleted in order to make room for new items.
	If neither OVStoreSize nor OVStoreSizePercent is specified a default value of 10% of disk capacity is used.
	See "OVStoreSizePercent" on page 217.
	The space is not allocated until it is needed.

OVStoreSizePercent

Location	See "Location of Vault Cache and Virtual Vault registry values" on page 199.
Content	DWORD

Description   Percentage of disk capacity to use.

                   If neither OVStoreSize nor OVStoreSizePercent is specified a default
                   value of 10% of disk capacity is used.

                   See "OVStoreSize" on page 217.

OVSyncArchiveTypes

Location   See "Location of Vault Cache and Virtual Vault registry values"
                   on page 199.

Content   DWORD

                   1 — (Default) Default mailbox archive only

                   2 — All mailbox archives and delegate mailbox archives

                   4 — All mailbox, delegate and shared archives

Description   Enables you to control what is synchronized with the Vault Cache.

                   If the synchronization scope is too great it can take a long time to
                   perform a synchronization. The default setting, which synchronizes just
                   the user's primary mailbox archive, minimizes the time needed for
                   synchronization.

                   Note: This registry value performs the same function as the advanced
                   Exchange desktop policy setting "Synchronize archive types", which
                   you can set through the Administration Console. For more information
                   on the policy setting, see the *Administrator's Guide*.

OVSyncSlotTimeOutInSecs

Location   See "Location of Vault Cache and Virtual Vault registry values"
                   on page 199.

Content   DWORD

                   Number of seconds. Default value is 0.

Description   Enables you to set the timeout value used in Vault Cache
                     synchronization download requests to Enterprise Vault.

                     If Outlook cannot connect to Enterprise Vault in order to perform a Vault
                     Cache synchronization download, then Outlook will wait the number of
                     seconds set before contacting the server again. Three connection
                     attempts are made before a synchronization failure is reported.

                     The default value, 0, means that the value set on the server is used;
                     this is 300 seconds (5 minutes).

RemoveOfflineVault

Location   See "Location of other Outlook Add-In registry values" on page 200.

Content   DWORD

                     0 — Takes no action (default).

                     1 — Removes the Vault Cache stores files and registry keys.

Description   Specifies whether to delete any Vault Caches and their related items
                     (current working directory, registry keys, and hidden messages). The
                     Vault Cache facility does not become available again until this registry
                     value is deleted.

RemovePSTEntries

Location   See "Location of other Outlook Add-In registry values" on page 200.

Content   DWORD

                     1 — Remove entry if PST has been deleted.

                     2 — Remove entry if PST is set to read-only.

                     4 — Remove entry if PST is hidden.

Description   Removes PST entries from a user's profile.

                     After a PST migration, you can make Enterprise Vault remove PST
                     entries from a user's profile, depending on the PST file's attributes. You
                     can delete the PST files or set the attributes automatically as part of
                     the PST migration.

                     The values can be combined. For example, a value of 6 makes
                     Enterprise Vault remove PST files from the profile that are read-only
                     or hidden.

SendLogFileMaxSizeMB

Location	See "Location of other Outlook Add-In registry values" on page 200.
Content	DWORD
	Default: 5
Description	Controls the maximum size, in megabytes, of the message that the **Send Log** button in the Outlook Add-In log viewer creates. If the log file is larger than this size, Send Log uses the most recent section of the file.
See also	See "SendLogFileRecipients" on page 220.

SendLogFileRecipients

Location	See "Location of other Outlook Add-In registry values" on page 200.
Content	String value containing a semicolon-separated list of recipients.
Description	Specifies the default recipients for the **To** field in the mail message that the **Send Log** button in the Outlook Add-In log viewer creates.
See also	See "SendLogFileMaxSizeMB" on page 220.

UpdateWDSIndexForVV

Location	`HKEY_CURRENT_USER`
	`  \SOFTWARE`
	`   \KVS`
	`    \Enterprise Vault`
	`     \Client`

Content	DWORD
	1 (default) – Windows Search reindexes Virtual Vault items when Outlook starts.
	0 – Windows Search does not reindex Virtual Vault items when Outlook starts.

Description   Controls whether Windows Search reindexes Virtual Vault items when Outlook starts. You can use UpdateWDSIndexForVV to repair a Windows Search index if necessary, so that Virtual Vault items appear in Outlook Instant Search results.

UpdateWDSIndexForVV is effective in all supported versions of Outlook.

VVAllowArchive

Location   See "Location of Vault Cache and Virtual Vault registry values" on page 199.

Content   DWORD

- 1 (default) – Users can archive items manually in Virtual Vault.
- 0 – Users cannot archive items manually in Virtual Vault.

Description   Controls whether users can archive items manually using Virtual Vault.

This registry value performs the same function as the advanced Exchange desktop policy setting **Users can archive items**. You can set the value using the Administration Console. For more information on the policy setting, see the *Administrator's Guide*.

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.

VVAllowHardDelete

Location   See "Location of Vault Cache and Virtual Vault registry values" on page 199.

Content   DWORD

- 1 (default) – Users can hard delete items from Virtual Vault.
- 0 – Users cannot hard delete items from Virtual Vault.

Description   Controls whether users can hard delete items from Virtual Vault.

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.

If you disable this setting, users can still move items to the **Deleted Items** folder if **Users can reorganize items** (**VVAllowReOrg**) is enabled.

Note: This registry value performs the same function as the advanced Exchange desktop policy setting **Users can hard delete items**. You can set the value using the Administration Console. For more information on the policy setting, see the *Administrator's Guide*.

VVAllowInterStoreCopyAndMove

Location   See "Location of Vault Cache and Virtual Vault registry values" on page 199.

Content   DWORD

- 1 (default) – Users can copy and move items to another message store.
- 0 – Users cannot copy and move items to another message store.

Description   Controls whether users can copy and move items from a Virtual Vault to another message store.

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.

If the value of Vault Cache **Content strategy** (**OVContentDownload**) is 0 (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** (**VVDenyMultiContentlessOpsAboveMB**) to control the maximum total size of view, copy, and move operations.

Note: This registry value performs the same function as the advanced Exchange desktop policy setting **Users can copy items to another store**. You can set the value using the Administration Console. For more information on the policy setting, see the *Administrator's Guide*.

VVAllowIntraStoreCopy

Location	See "Location of Vault Cache and Virtual Vault registry values" on page 199.
Content	DWORD

- 1 – Users can copy items within their archive.
- 0 (default) – Users cannot copy items within their archive.

Description	Controls whether users can copy items within their archive.

If users can copy items within their archive and the content is available in Vault Cache, the items are retrieved from Vault Cache.

If the value of Vault Cache **Content strategy** (**OVContentDownload**) is 0 (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** (**VVDenyMultiContentlessOpsAboveMB**) to control the maximum total size of view, copy, and move operations.

Note: This registry value performs the same function as the advanced Exchange desktop policy setting **Users can copy items within their archive**. You can set the value using the Administration Console. For more information on the policy setting, see the *Administrator's Guide*.

VVAllowReOrg

Location	See "Location of Vault Cache and Virtual Vault registry values" on page 199.
Content	DWORD

- 0 – Users cannot reorganize items in Virtual Vault.
- 1 (default) – Users can reorganize items in Virtual Vault.

Description	Controls whether users can reorganize items in Virtual Vault.
	This setting can enable users to move items between folders and to create, move, rename, or delete folders. Users can hard delete only empty folders, unless **Users can hard delete items** (**VVAllowHardDelete**) is enabled.
	If folders still exist in the mailbox, users cannot move, rename, or delete them.
	Note: This registry value performs the same function as the advanced Exchange desktop policy setting **Users can reorganize items**. You can set the value using the Administration Console. For more information on the policy setting, see the *Administrator's Guide*.

VVAutoSyncItemsSizeThresholdMB

Location	See "Location of Vault Cache and Virtual Vault registry values" on page 199.
Content	DWORD
	An integer value. The value 0 (default) specifies that there is no automatic Vault Cache synchronization based on the total size of pending archive items in Virtual Vault.
Description	Specifies the total size in megabytes of pending archive items in Virtual Vault that triggers automatic Vault Cache synchronization.
	Note: This registry value performs the same function as the advanced Exchange desktop policy setting **Threshold total size of items to trigger synchronization**. You can set the value using the Administration Console. For more information on the policy setting, see the *Administrator's Guide*.

VVAutoSyncItemThreshold

Location	See "Location of Vault Cache and Virtual Vault registry values" on page 199.
Content	DWORD
	An integer value. The value 0 (default) specifies there is no automatic Vault Cache synchronization based on the total number of pending archive items in Virtual Vault.

Description   Specifies the total number of pending archive items in Virtual Vault that
                            triggers automatic Vault Cache synchronization.

                            Note: This registry value performs the same function as the advanced
                            Exchange desktop policy setting **Threshold number of items to trigger
                            synchronization**. You can set the value using the Administration
                            Console. For more information on the policy setting, see the
                            Administrator's Guide.

VVDenyMultiContentlessOpsAboveMB

Location   See "Location of Vault Cache and Virtual Vault registry values"
                            on page 199.

```
HKEY_CURRENT_USER
 \SOFTWARE
  \KVS
   \Enterprise Vault
    \Client
     \VaultCacheStoreID
```

Content   DWORD

                            An integer value. The default is 64 (MB). The value 0 specifies no limit.

Description   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.

                            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.

                            Note: This registry value performs the same function as the advanced
                            Exchange desktop policy setting **Max total size of contentless
                            operations**. You can set the value using the Administration Console.
                            For more information on the policy setting, see the *Administrator's
                            Guide*.

VVEnabled

Location	See "Location of Vault Cache and Virtual Vault registry values" on page 199.
Content	DWORD

- 1 – Virtual Vault is enabled for Outlook users.
- 0 – Virtual Vault is not enabled.

Description	Controls whether Virtual Vault is available to Outlook users. To use Virtual Vault, users must also have Vault Cache enabled.

This registry value performs the same function as the **Make Virtual Vault available to users** option on the **Vault Cache** tab of the Exchange desktop policy. You can set the value using the Administration Console.

VVReadingPaneContent

Location	See "Location of Vault Cache and Virtual Vault registry values" on page 199.
Content	DWORD

- 0 – The reading pane never shows the content. It shows only the selected item's header. A banner provides a link to open the original item.
- 1 – 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.
- 2 – The reading pane always shows the header and content of the item that is selected in Virtual Vault.

  Note: In Enterprise Vault 9.0.3 and later service packs and 10.0/10.0.*n*, in the advanced Exchange desktop policy setting **Show content in Reading Pane**, you cannot specify that the reading pane always shows the item's header and content. The option is not available because it can result in excessive downloading of the content of items. For the same reason, we recommend that you do not set VVReadingPaneContent to the value 2.

Description   Controls whether content is shown in the Outlook reading pane.

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.

Note: This registry value performs the same function as the advanced Exchange desktop policy setting **Show content in Reading Pane**. You can set the value using the Administration Console. For more information on the policy setting, see the *Administrator's Guide*.

VVStubOnlyModuleList

Location   See "Location of Vault Cache and Virtual Vault registry values" on page 199.

Content   A string value containing a semicolon-separated list of DLL file names.

The default value is "googledesktopoffice.dll;mssphtb.dll".

The file googledesktopoffice.dll is the Google Desktop Search Outlook Add-In. The file mssphtb.dll is the Outlook Microsoft Search (MSSearch) Connector, which provides Windows Search email indexing.

Note: If you set this registry value, include the two default DLL file names. These file names are not automatically added to the list.

Description   Controls the behavior of Virtual Vault when an item is opened.

If the request to open the item comes from one of the named DLLs, then the opened item contains only header information. The Enterprise Vault Outlook Add-In does not retrieve the content from Vault Cache or download it from the Enterprise Vault server.

Selective Journaling

This chapter includes the following topics:

■ HardDeleteItems (Selective Journaling)

HardDeleteItems (Selective Journaling)

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

Content	DWORD
Description	Forces any item that does not match the selective journaling filter to be deleted immediately. It is not placed in the Deleted Items folder and is not marked with a tombstone date.

Storage Service

This chapter includes the following topics:

- BypassAddressLookups

- ConversionTimeoutEvents

- DeleteEmptyFolders

- EMCCenteraFileTypesExcludedFromSharing

- EnableArchive

- EnableCrawler

- EnableExpiry

- EnableFileWatch

- EnableNSFMigrations

- EnablePSTMigrations

- EnableReplayIndex

- EnableRestore

- FailedConversionEvents

- FallbackConversionEvents

- LogThrottling

- LogVerifyOfCollectionFiles

- MinimumFilesInCollection

- MinimumFileSizeForCollectionKB

- OCRUseLocalServerSettings

- OfflineItemRetryPeriod

- QueueTimeout

- RequestedAllocationSizeTooLargeEvents

- UnrecognisedFileTypeEvents

- VerifyCollectedFiles

- VerifyFilesInNewCollection

- VerifyFilesPreCollection

- WarnForMissingOutlook

BypassAddressLookups

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

Content	DWORD. 0 – (Default) Look up sender and recipient attributes. 1 – Bypass the lookup of sender and recipient attributes.
Description	During PST migration, it can be necessary for Enterprise Vault to connect to the relevant Exchange server's domain controller to retrieve sender and recipient data. This requires that at least one Exchange server is targeted in your environment. If a suitable Exchange server does not exist, PST migration performance is degraded. For example, this can happen when you migrate data from PST files that were created in an old Exchange environment whose servers no longer exist. Set BypassAddressLookups to 1 to bypass Active Directory lookups during PST migration.

ConversionTimeoutEvents

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

Content	DWORD
	0 — Do not log failures caused by timeouts
	1 — (Default) Log failures caused by timeouts
Description	Controls whether to report when an item failed conversion to HTML as a result of a timeout. Conversion timeout errors on the local Enterprise Vault server are reported in the Enterprise Vault Converters event log.
	Note that this setting is only applicable when Storage\FailedConversionEvents, and Storage\FallbackConversionEvents are "on", that is, have a non-zero value.
	Restart the Storage service to apply changes to the registry value.
	This value is supported as a local server override of the site setting, **Log conversion timeout events**. The site setting should be used to ensure a consistent content conversion configuration for all Enterprise Vault Storage servers in the site.
See also	See "FailedConversionEvents" on page 238.
	See "FallbackConversionEvents" on page 239.

DeleteEmptyFolders

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

Content	DWORD. Set to non-zero to enable.

Description When enabled and the storage service restarted, a new thread examines all vaults in all stores owned by that Storage Service. Empty folders in structured archives are deleted.

Special folders such as the following are never deleted: "Inbox", "Drafts", "Sent Items", "Outbox", "Deleted Items".

Note: Resets to zero (disabled) when all stores and archives have been processed.

EMCCenteraFileTypesExcludedFromSharing

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

Content String

Description Enterprise Vault does not split .MHT files into their constituent parts when they are stored with device-level sharing on a Dell EMC Centera device. The constituent parts are not eligible for sharing. `EMCCenteraFileTypesExcludedFromSharing` specifies a list of other file types that must not be split into constituent parts when stored with device-level sharing on a Centera device.

The list format is as follows:

`.filetype[.filetype].`

Prefix each file type with a period and end the list with a period. For example:

`.GIF.JPG.`

EnableArchive

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

Content	DWORD value: 0 — Component disabled 1 — Component enabled (Default)
Description	Allows the StorageArchive component of Storage to be disabled so that, when an Enterprise Vault Storage Service is started, the StorageArchive processes are started but do not process pending items from Microsoft Message Queue (MSMQ). **Note:** The use of EnableArchive is deprecated from Enterprise Vault version 8.0. The storage service logs an event at start-up if it finds that EnableArchive is set to 0. Vaults and indexes can now be placed in backup mode using the Enterprise Vault Administration Console or a PowerShell cmdlet. For more information, see the *Backup and Recovery* guide.

EnableCrawler

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

Content	DWORD 0 — Disable StorageCrawler process 1 — (Default) Enable StorageCrawler process

Description   Enables or disables the StorageCrawler process. Disabling the StorageCrawler process prevents index updates.

Set EnableCrawler to 0 when placing Enterprise Vault in read-only mode in preparation for backing up. Set EnableCrawler to 1 when backups are complete.

Note: The use of EnableCrawler is deprecated from Enterprise Vault version 8.0. The storage service logs an event at start-up if it finds that EnableCrawler is set to 0. Vaults and indexes can now be placed in backup mode using the Enterprise Vault Administration Console or a PowerShell cmdlet.

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

EnableExpiry

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

Content   DWORD

0 — Component disabled

1 — Component enabled (Default)

Description   Enables the StorageDelete component of Storage to be disabled so no StorageDelete processes are started when an Enterprise Vault Storage Service is started.

Note: The use of EnableExpiry is deprecated from Enterprise Vault version 8.0. The storage service logs an event at start-up if it finds that EnableExpiry is set to 0. Vaults and indexes can now be placed in backup mode using the Enterprise Vault Administration Console or a PowerShell cmdlet.

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

EnableFileWatch

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

Content	DWORD 0 — Component disabled 1 — Component enabled (Default)
Description	Enables the StorageFileWatch component of Storage to be disabled so that no StorageFileWatch processes are started when an Enterprise Vault Storage Service is started. **Note:** The use of EnableFileWatch is deprecated from Enterprise Vault version 8.0. The storage service logs an event at start-up if it finds that EnableFileWatch is set to 0. Vaults and indexes can now be placed in backup mode using the Enterprise Vault Administration Console or a PowerShell cmdlet. For more information, see the *Backup and Recovery* guide.

EnableNSFMigrations

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

Content	DWORD 0 — NSF migrations are blocked 1 — NSF migrations are allowed

Description   Controls whether NSF migrations are allowed.

EnableNSFMigrations is useful when you want to prevent data being written to archives, such as when performing backups.

Note: The use of EnableNSFMigrations is deprecated from Enterprise Vault version 8.0. The storage service logs an event at start-up if it finds that EnableNSFMigrations is set to 0. Vaults and indexes can now be placed in backup mode using the Enterprise Vault Administration Console or a PowerShell cmdlet.

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

EnablePSTMigrations

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

Content   DWORD

0 — PST migrations are blocked

1 — PST migrations are allowed

Description   Controls whether PST migrations are allowed.

EnablePSTMigrations is useful when you want to prevent data being written to archives, such as when performing backups.

Note: The use of EnablePSTMigrations is deprecated from Enterprise Vault version 8.0. The storage service logs an event at start-up if it finds that EnablePSTMigrations is set to 0. Vaults and indexes can now be placed in backup mode using the Enterprise Vault Administration Console or a PowerShell cmdlet.

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

EnableReplayIndex

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

Content	DWORD value 0 — Component disabled 1 — Component enabled (Default)
Description	Enables the StorageReplayIndex component of Storage to be disabled so that no StorageReplayIndex processes are started when an Enterprise Vault Storage Service is started. **Note:** The use of EnableReplayIndex is deprecated from Enterprise Vault version 8.0. The storage service logs an event at start-up if it finds that EnableReplayIndex is set to 0. Vaults and indexes can now be placed in backup mode using the Enterprise Vault Administration Console or a PowerShell cmdlet. For more information, see the *Backup and Recovery* guide.

EnableRestore

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

Content	DWORD value: 0 — Component disabled 1 — Component enabled (Default)

Description   Enables or disables the StorageRestore component of the Enterprise
                     Vault Storage Service. By disabling the component, you can prevent
                     any StorageRestore processes from starting when an Enterprise Vault
                     Storage Service starts.

                     Note: The use of EnableRestore is deprecated from Enterprise Vault
                     version 8.0. The storage service logs an event at start-up if it finds that
                     EnableRestore is set to 0. Vaults and indexes can now be placed in
                     backup mode using the Enterprise Vault Administration Console or a
                     PowerShell cmdlet.

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

FailedConversionEvents

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

Content   DWORD

                     0 — Errors are not logged

                     1 — Errors are logged (Default)

Description   Controls whether content conversion errors on the local Enterprise Vault
                     server are reported in the Enterprise Vault Converters event log. Setting
                     this value to "0" (zero) effectively disables all of the following conversion
                     log event settings: FallbackConversionEvents,
                     ConversionTimeoutEvents, RequestedAllocationSizeTooLargeEvents,
                     UnrecognisedFileTypeEvents.

                     Restart the Storage service to apply changes to the registry value.

                     This value is supported as a local server override of the site setting,
                     Log conversion failure events. The site setting should be used to
                     ensure a consistent content conversion configuration for all Enterprise
                     Vault Storage servers in the site.

See also   See "ConversionTimeoutEvents" on page 231.

                     See "FallbackConversionEvents" on page 239.

                     See "RequestedAllocationSizeTooLargeEvents" on page 243.

                     See "UnrecognisedFileTypeEvents" on page 244.

FallbackConversionEvents

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

Content	DWORD
	0 — Errors are not logged
	1 — Errors are logged (Default)
Description	Controls whether an Application Log entry is made when an item failed conversion to HTML and, as a fallback, the item was converted to text.
	Controls whether to report when an item failed conversion to HTML and, as a fallback, was converted to text. Fallback to text errors on the local Enterprise Vault server are reported in the Enterprise Vault Converters event log.
	Note that this setting does not override the registry setting, Storage\FailedConversionEvents
	Restart the Storage service to apply changes to the registry value.
	This value is supported as a local server override of the site setting, **Log fallback to text events**. The site setting should be used to ensure a consistent content conversion configuration for all Enterprise Vault Storage servers in the site.
See also	See "FailedConversionEvents" on page 238.

LogThrottling

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

Content	DWORD
	0 — (default) Disable logging
	1 — Enable logging
Description	Controls whether Enterprise Vault writes event log entries when throttling starts and stops.
	If you change the setting of LogThrottling you must restart the task in order to apply the new setting.

LogVerifyOfCollectionFiles

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

Content	DWORD
	0 — Disable logging when verifying collection files (Default)
	1 — Enable logging when verifying collection files
Description	As part of the optional verification process that can occur when adding savesets to collection (.CAB) files, specifies whether to add an Event Log entry if a corrupt file is found.
See also	See "VerifyCollectedFiles" on page 245.

MinimumFilesInCollection

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

Content	DWORD
	Maximum value: 200.
	Minimum value: 1
	Setting a value of 0 forces the default (1) to be used.
Description	When creating collections, MinimumFilesInCollection controls the minimum number of saveset files in a collection. The collection is not created unless there are at least this number of savesets to be added.

MinimumFileSizeForCollectionKB

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

Content	DWORD
	An integer value, that specifies the minimum file size in KB.
	When the key does not exist a default value of 1 is used.
Description	Enables you to control the minimum size of a collection file. A collection file is created only when its file size is equal to or greater than the value that MinimumFileSizeForCollectionKB specifies.

OCRUseLocalServerSettings

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

Content	DWORD
	0 — (Default) Use the advanced site settings: Content Conversion/OCR language, and Content Conversion/OCR optimization.
	1 — Do not apply the Content Conversion OCR site settings. Instead, use whatever settings are currently in force on the local server.
Description	This value is supported as a local server override of the site settings, **OCR language** and **OCR optimization**. The site settings should be used to ensure a consistent content conversion configuration for all Enterprise Vault Storage servers in the site.
	When the value of OCRUseLocalServerSettings is non-zero, the OCR language and OCR optimization site settings are not applied to the Windows TIFF IFilter configuration when the Storage service starts. The current local server settings are used instead.
	This setting could be used on Windows Server 2012 to enable multiple languages from a code page set, or to use the system default language.
	Restart the Storage service to apply changes to the setting value.

OfflineItemRetryPeriod

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

Content	DWORD
Description	Specifies the total retry period in minutes when retrieving offline items. If this is not set, the retry period is infinite.

QueueTimeout

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

Content	DWORD value set to a number of seconds.
Description	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.

RequestedAllocationSizeTooLargeEvents

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

Content	DWORD
	0 — Events are not logged
	1 — Events are logged (Default)

Description   Controls whether maximum conversion size exceeded events are
                     reported in the Enterprise Vault Converters event log on the local
                     Enterprise Vault server.

                     Setting FailedConversionEvents to "0" (zero) effectively disables this
                     conversion log event setting.

                     Restart the Storage service to apply changes to the registry value.

                     This value is supported as a local server override of the site setting,
                     Log maximum conversion size exceeded events. The site setting
                     should be used to ensure a consistent content conversion configuration
                     for all Enterprise Vault Storage servers in the site.

See also   See "FailedConversionEvents" on page 238.

UnrecognisedFileTypeEvents

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

Content   DWORD

                     0 — Errors are not logged

                     1 — Errors are logged (Default)

Description   Controls whether to report when an item failed conversion to HTML as
                     a result of an unrecognized file type. Unrecognized file type conversion
                     errors on the local Enterprise Vault server are reported in the Enterprise
                     Vault Converters event log.

                     Note that this setting is only applicable when
                     Storage\FailedConversionEvents, and
                     Storage\FallbackConversionEvents are "on", that is, have a non-zero
                     value.

                     Restart the Storage service to apply changes to the registry value.

                     This value is supported as a local server override of the site setting,
                     Log file type not recognized events. The site setting should be used
                     to ensure a consistent content conversion configuration for all Enterprise
                     Vault Storage servers in the site.

See also	See "FailedConversionEvents" on page 238.
	See "FallbackConversionEvents" on page 239.
ICO	404-0040
Introduced	4.0 CP4
Availability	Customer

VerifyCollectedFiles

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

Content	DWORD
	0 — Do not verify collection files.
	1 — Verify collection files (Default).
Description	Specifies whether to verify collection (`.CAB`) files after Enterprise Vault has added saveset files to them. You can turn off this feature to improve performance.
See also	See "LogVerifyOfCollectionFiles" on page 240.

VerifyFilesInNewCollection

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

Content	DWORD
	Default is 0

Description   Controls decompression of ARCHDVS files extracted from the newly
                     created CAB file. If VerifyCollectedFiles (set through the
                     VerifyCollectedFiles registry key) is set to 0, and
                     VerifyFilesInNewCollection is also set to 0, this fact is output via a trace
                     message as well as an event log warning. VerifyFilesInNewCollection
                     therefore relies on VerifyCollectedFiles being set to 1.

VerifyFilesPreCollection

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

Content   DWORD

                     0 — Do not verify files before collecting them in a new CAB file (Default)

                     1 — Verify files before collecting them

Description   Specifies whether to verify saveset files before collecting them in a new
                     CAB file. Enterprise Vault does not collect corrupt saveset files.

WarnForMissingOutlook

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

Content   DWORD

                     0 — Do not issue event log messages when FSA archives .MSG files
                     and Outlook is not installed on the Enterprise Vault server.

                     1 — (Default if not present.) Issue the event log messages.

                     This registry value does not exist by default.

Description   Specifies whether to generate warning messages in the Enterprise
                   Vault event log when both of the following are true:

                   ■ Enterprise Vault archives Outlook .MSG files from a File System
                      Archiving target.
                   ■ Outlook is not present on the Enterprise Vault server that runs the
                      File System Archiving task.

                   By default, Enterprise Vault generates warning messages to alert you
                   that the .MSG files are not fully indexed unless Outlook is installed on
                   the Enterprise Vault server.

                   Use the WarnForMissingOutlook registry value to prevent Enterprise
                   Vault from issuing these warning messages.

Index

W