

Veritas Enterprise Vault™ Classification using the Veritas Information Classifier

12.2

Veritas Enterprise Vault: Classification using the Veritas Information Classifier

Last updated: 2017-08-10.

Legal Notice

Copyright © 2017 Veritas Technologies LLC. All rights reserved.

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

This Veritas product may contain third party software for which Veritas is required to provide attribution to the third party ("Third Party Programs"). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Licensed Software does not alter any rights or obligations you may have under those open source or free software licenses. For more information on the Third Party Programs, please see the Third Party Notice document for this Veritas product that is available at <https://www.veritas.com/about/legal/license-agreements>.

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

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

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

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

<http://www.veritas.com>

Technical Support

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

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

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

<https://my.veritas.com>

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

Worldwide (except Japan)

CustomerCare@veritas.com

Japan

CustomerCare_Japan@veritas.com

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

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

Documentation

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

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

Documentation feedback

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

evdocs@veritas.com

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

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

Contents

Chapter 1	About this guide	7
	Introducing this guide	7
	Relationship between the Veritas Information Classifier and other classification methods	8
	What's in this guide	8
	Where to get more information about Enterprise Vault	9
	Enterprise Vault training modules	11
Chapter 2	Preparing Enterprise Vault for classification	12
	About the preparatory steps	12
	What you need	13
	Checking the cache location on the Enterprise Vault storage servers	13
	Setting up the Data Access account	15
	Enabling the Veritas Information Classifier on all Enterprise Vault servers	15
	Configuring the Veritas Information Classifier for secure client connections	16
Chapter 3	Setting up Veritas Information Classifier policies	19
	Introducing the Veritas Information Classifier	19
	Opening the Veritas Information Classifier	20
	Finding your way around	21
	About policies	22
	Creating or editing policies	23
	About policy conditions	24
	Enabling or disabling policies	30
	Resetting policies	30
	Deleting policies	30
	About patterns	31
	Creating or editing patterns	31
	Deleting patterns	32
	About tags	33

	Creating or editing tags	33
	About the Enterprise Vault index properties	34
	How classification property values and retention categories interact	36
	Points to note on setting retention categories	38
	Deleting tags	39
Chapter 4	Defining and applying Enterprise Vault classification policies	40
	About Enterprise Vault classification policies	40
	Defining classification policies	42
	Configuring classification policies to assign retention categories with the shortest duration	43
	About the PowerShell cmdlets for working with classification policies	44
	Associating classification policies with retention plans	45
	About the PowerShell cmdlets for working with retention plans	47
	Applying retention plans to your Enterprise Vault archives	48
Chapter 5	Running classification in test mode	51
	About classification test mode	51
	Implementing classification test mode	52
	About the PowerShell cmdlets for running classification in test mode	53
	Understanding the classification test mode reports	53
Appendix A	Enterprise Vault properties for use in custom field searches	55
	About the Enterprise Vault properties	55
	System properties	56
	Attachment properties	59
	Custom Enterprise Vault properties	59
	Custom Enterprise Vault properties for File System Archiving items	61
	Custom Enterprise Vault properties for SharePoint items	61
	Custom Enterprise Vault properties for Compliance Accelerator-processed items	62
	Custom properties for use by policy management software	63
	Custom properties for Enterprise Vault SMTP Archiving	64

Appendix B	PowerShell cmdlets for use with classification	
	65
	About the classification cmdlets	65
	Disable-EVClassification	66
	Get-EVClassificationPolicy	67
	Get-EVClassificationStatus	70
	Get-EVClassificationTestMode	71
	Get-EVClassificationVICTags	72
	Initialize-EVClassificationVIC	74
	New-EVClassificationPolicy	76
	Remove-EVClassificationPolicy	80
	Set-EVClassificationPolicy	81
	Set-EVClassificationTestMode	85
Appendix C	Classification cache folder	86
	How Enterprise Vault caches the items that it submits for classification	
	86
	Limits on the size of classification files	87
	Configuring Enterprise Vault to keep the classification files in the cache	
	folder	88
Appendix D	Migrating from FCI classification to the Veritas	
	Information Classifier	89
	Converting FCI classification rules for use with the Veritas Information	
	Classifier	89
Appendix E	Monitoring and troubleshooting	91
	Auditing	91
	Checking the classification performance counters	92
	Troubleshooting classification	93
	Searching archives for items that the Veritas Information Classifier has	
	classified	95
Index	97

About this guide

This chapter includes the following topics:

- [Introducing this guide](#)
- [What's in this guide](#)
- [Where to get more information about Enterprise Vault](#)

Introducing this guide

This guide is designed for Enterprise Vault administrators who want to use the Veritas Information Classifier to assign classification tags to all new and existing archived content. When the users of applications such as Enterprise Vault Search, Compliance Accelerator, and Discovery Accelerator conduct searches or reviews, they can filter items according to the tags that the Veritas Information Classifier has assigned to them.

The Veritas Information Classifier evaluates the items that you submit for classification against a set of policies. Each policy specifies the conditions that the items must meet to be assigned a specific classification tag. For example, a policy may look for items whose contents include a credit card number and assign the tag "Credit-Card" to any that do. The Veritas Information Classifier includes over 50 built-in classification policies, which cover many of the data protection regulations and corporate standards worldwide. For example, you can meet privacy regulations such as GDPR through policies to detect Personally Identifiable Information (PII). You can also create custom policies.

Besides assigning classification tags, the Veritas Information Classifier can also update the retention categories of items, mark items for deletion, and tag them for inclusion in (or exclusion from) Compliance Accelerator review sets.

Relationship between the Veritas Information Classifier and other classification methods

Enterprise Vault 12 provided the means to classify items using the File Classification Infrastructure, which is a classification engine that is built into recent Windows Server editions. This facility is still available in the current version of Enterprise Vault, and you can use it in addition to or as an alternative to the Veritas Information Classifier. However, not only are the classification options in the File Classification Infrastructure less sophisticated than those in the Veritas Information Classifier but they are more difficult to implement. For this reason, the Veritas Information Classifier is the recommended way to classify archived content.

See [“Converting FCI classification rules for use with the Veritas Information Classifier”](#) on page 89.

For more information on the File Classification Infrastructure, see the *Classification using the Microsoft File Classification Infrastructure* guide.

What's in this guide

[Table 1-1](#) summarizes the contents of this guide.

Table 1-1 Contents of this guide

Chapter	Function
1	Introduces this guide and describes how to obtain more information about Enterprise Vault.
2	Guides you through some steps to prepare Enterprise Vault for classification. See “About the preparatory steps” on page 12.
3	Explains how to set up the Information Classifier policies with which you can tag the items that you submit for classification. See “Introducing the Veritas Information Classifier” on page 19.
4	Describes how to select the classification features that you want to implement in your Enterprise Vault site and assign them to your users' archives. See “About Enterprise Vault classification policies” on page 40.
5	Outlines how to run classification in test mode before you put the feature into effect. See “About classification test mode” on page 51.

This guide assumes that you are familiar with a number of Enterprise Vault features, including the Administration Console and PowerShell Management Shell.

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	<p>Includes all the following documents in Windows Help (.chm) format so that you can search across them all. It also includes links to the guides in Acrobat (.pdf) format.</p> <p>You can access the library in several ways, including the following:</p> <ul style="list-style-type: none"> ■ In Windows Explorer, browse to the <code>Documentation\language</code> subfolder of the Enterprise Vault installation folder, and then open the <code>EV_Help.chm</code> file. ■ On the Help menu in the Administration Console, click Help on Enterprise Vault.
<i>Introduction and Planning</i>	Provides an overview of Enterprise Vault functionality.
<i>Deployment Scanner</i>	Describes how to check the required software and settings before you install Enterprise Vault.
<i>Installing and Configuring</i>	Provides detailed information on setting up Enterprise Vault.
<i>Upgrade Instructions</i>	Describes how to upgrade an existing Enterprise Vault installation to the latest version.
<i>Setting up Domino Server Archiving</i>	Describes how to archive items from Domino mail files and journal databases.
<i>Setting up Exchange Server Archiving</i>	Describes how to archive items from Microsoft Exchange user mailboxes, journal mailboxes, and public folders.
<i>Setting up File System Archiving</i>	Describes how to archive the files that are held on network file servers.
<i>Setting up IMAP</i>	Describes how to configure IMAP client access to Exchange archives and Internet mail archives.

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

Document	Comments
<i>Setting up Skype for Business Archiving</i>	Describes how to archive Skype for Business conversations.
<i>Setting up SMTP Archiving</i>	Describes how to archive SMTP messages from other messaging servers.
<i>Setting up SharePoint Server Archiving</i>	Describes how to archive content from Microsoft SharePoint servers.
<i>Administrator's Guide</i>	Describes how to perform day-to-day administration procedures.
<i>Backup and Recovery</i>	Describes how to implement an effective backup strategy to prevent data loss, and how to provide a means for recovery in the event of a system failure.
<i>Classification using the Microsoft File Classification Infrastructure</i>	Describes how to use the classification engine that is built into recent Windows Server editions to classify all new and existing archived content.
<i>Classification using the Veritas Information Classifier</i>	Describes how to use the Veritas Information Classifier to evaluate all new and archived content against a comprehensive set of industry-standard classification policies. If you are new to classification with Enterprise Vault, we recommend that you use the Veritas Information Classifier rather than the older and less intuitive File Classification Infrastructure engine.
<i>NSF Migration</i>	Describes how to migrate content from Domino and Notes NSF files into Enterprise Vault archives.
<i>PST Migration</i>	Describes how to migrate content from Outlook PST files into Enterprise Vault archives.
<i>Reporting</i>	Describes how to implement Enterprise Vault Reporting, which provides reports on the status of Enterprise Vault servers, archives, and archived items. If you configure FSA Reporting, additional reports are available for file servers and their volumes.
<i>Utilities</i>	Describes the Enterprise Vault tools and utilities.
<i>PowerShell Cmdlets</i>	Describes how to perform various administrative tasks by running the Enterprise Vault PowerShell cmdlets.

Table 1-2 Enterprise Vault documentation set (continued)

Document	Comments
<i>Registry Values</i>	A reference document that lists the registry values with which you can modify many aspects of Enterprise Vault behavior.
Help for Administration Console	The online Help for the Enterprise Vault Administration Console.
Help for Enterprise Vault Operations Manager	The online Help for Enterprise Vault Operations Manager.

For the latest information on supported devices and versions of software, see the *Enterprise Vault Compatibility Charts* book, which is available from this address:

<http://www.veritas.com/docs/000097605>

Enterprise Vault training modules

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>.

Preparing Enterprise Vault for classification

This chapter includes the following topics:

- [About the preparatory steps](#)
- [What you need](#)
- [Checking the cache location on the Enterprise Vault storage servers](#)
- [Setting up the Data Access account](#)
- [Enabling the Veritas Information Classifier on all Enterprise Vault servers](#)
- [Configuring the Veritas Information Classifier for secure client connections](#)

About the preparatory steps

After you have completed the preparatory steps in [Table 2-1](#), you can begin to set up your Veritas Information Classifier policies.

Table 2-1 Steps to prepare Enterprise Vault for classification

Step	Action	More information
Step 1	Ensure that you meet the requirements for implementing classification.	See “What you need” on page 13.
Step 2	Check that a suitable cache location exists in which Enterprise Vault can temporarily store the items that it submits for classification.	See “Checking the cache location on the Enterprise Vault storage servers” on page 13.

Table 2-1 Steps to prepare Enterprise Vault for classification (*continued*)

Step	Action	More information
Step 3	If you have not already done so, set up the Data Access account. Enterprise Vault uses this account to communicate with the Veritas Information Classifier.	See “Setting up the Data Access account” on page 15.
Step 4	Run a PowerShell cmdlet to enable the Veritas Information Classifier on all Enterprise Vault servers.	See “Enabling the Veritas Information Classifier on all Enterprise Vault servers” on page 15.
Step 5	For extra security, consider configuring the Veritas Information Classifier to require HTTPS with SSL for all connections to it.	See “Configuring the Veritas Information Classifier for secure client connections” on page 16.

What you need

All the components that you need for classification using the Veritas Information Classifier are installed when you install Enterprise Vault. However, you also need the following:

- A license for the Enterprise Vault retention feature.
Classification operates in test mode if you have yet to install a license for the retention feature, or the existing license has expired.
- One or more of the following RBA roles in the Vault Administration Console:
 - Domino Administrator
 - Exchange Administrator
 - Extension Content Provider Administrator
 - File Server Administrator
 - NSF Administrator
 - Power Administrator
 - PST Administrator
 - SharePoint Administrator
 - SMTP Administrator

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

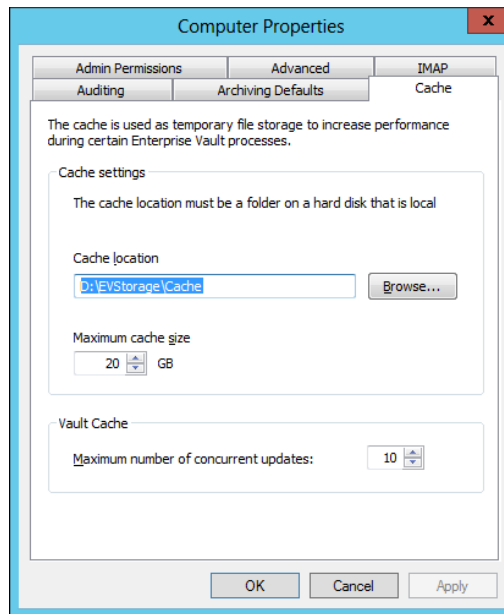
Checking the cache location on the Enterprise Vault storage servers

On each storage server that is to perform classification, Enterprise Vault stores a plain-text copy of each item that it is classifying in a subfolder of the nominated

cache location. You may want to check that you have correctly configured this location.

To check the cache location on an Enterprise Vault storage server

- 1 In the Administration Console, expand the Enterprise Vault site until the **Enterprise Vault Servers** container is visible.
- 2 Expand the **Enterprise Vault Servers** container.
- 3 Right-click the appropriate server and then, on the shortcut menu, click **Properties**.
- 4 In the **Computer Properties** dialog box, click the **Cache** tab.
- 5 Under **Cache Location**, ensure that a suitable local path is specified.



The classification feature stores the files that it is classifying in a `Classification` subfolder of the specified cache location; for example, `D:\EVStorage\Cache\Classification`.

To ensure optimum performance, it is important to create the cache folder on fast, locally-attached storage. We recommend creating the folder on a drive other than the operating system drive.

Setting up the Data Access account

Enterprise Vault accesses the Veritas Information Classifier through the Data Access account. If you have yet to set up this account, you can do so by following the steps below.

To set up the Data Access account

- 1 Create a Windows domain user account to use as the Data Access account. This should be a basic domain account that you have specifically created for the purpose; you cannot use a local machine account. The account must not belong to any administrative group.
- 2 Log on to the Enterprise Vault server using the Vault Service account.
- 3 Start the Enterprise Vault Administration Console.
- 4 In the left pane of the Administration Console, right-click the **Directory** container and then, on the shortcut menu, click **Properties**.
- 5 In the **Directory Properties** dialog box, click the **Data Access Account** tab.
- 6 In the **Account** box, select the Data Access account.
- 7 Enter and confirm the password for the account.

Enabling the Veritas Information Classifier on all Enterprise Vault servers

You enable the Veritas Information Classifier on all the servers in an Enterprise Vault site by running the supplied PowerShell cmdlet, `Initialize-EVClassificationVIC`. For each of these servers, the cmdlet also configures the Veritas Information Classifier website in Microsoft Internet Information Services (IIS).

This section provides an outline of how to run the cmdlet. A later section provides comprehensive information on the cmdlet.

See [“Initialize-EVClassificationVIC”](#) on page 74.

To enable the Veritas Information Classifier on all Enterprise Vault servers

- 1 On a shared network drive to which all the Enterprise Vault servers have access, create a folder in which the Veritas Information Classifier can keep policy information.

Both the Vault Service account and the Data Access account must have read/write access to this folder.

- 2 Log on to an Enterprise Vault server as the Vault Service account.

3 Open the Enterprise Vault Management Shell.

4 At the command prompt, enter a command like the following:

```
Initialize-EVClassificationVIC [-PoliciesPath <String>] [-SiteId
<String>]
```

Where:

-PoliciesPath	Specifies the UNC path to the network folder in which the Veritas Information Classifier should keep policy information.
-SiteId	Specifies the ID of the Enterprise Vault site for which to configure the Veritas Information Classifier. You may find this parameter useful if you have multiple Enterprise Vault sites.

For example:

```
Initialize-EVClassificationVIC -PoliciesPath \\server1\VicPolicies
```

Note: The cmdlet displays a warning that you do not have any enabled policies. This is simply a reminder that you can only classify items after you have set up the required policies in the Veritas Information Classifier.

Configuring the Veritas Information Classifier for secure client connections

The Veritas Information Classifier engine is a Java application that is managed by Internet Information Services (IIS). By default, client users can access the Veritas Information Classifier using HTTP on the standard Enterprise Vault IIS port, which is typically TCP port 80. However, you can strengthen the security of your Veritas Information Classifier deployment by configuring it to use HTTPS with Secure Sockets Layer (SSL).

Note the following:

- The following procedure secures the connections between client computers and IIS, but it does not secure the connections between IIS and the Veritas Information Classifier engine. However, as both IIS and the Veritas Information Classifier engine reside on the same server, this is unlikely to be a problem; there is no network traffic for a malicious user to intercept.
- Implementing HTTPS with SSL for the Veritas Information Classifier also implements it for other Enterprise Vault features, such as Enterprise Vault Search.

To configure the Veritas Information Classifier for secure client connections

- 1 In the Vault Administration Console, in the properties for your Enterprise Vault site, ensure that you have selected the option **Use HTTPS on SSL Port**.

The default port for HTTPS is 443, but you can choose an alternative port, if necessary.

- 2 Create and submit an SSL certificate request.

We recommend that you obtain a certificate from a trusted certificate authority, but a self-signed certificate is also acceptable.

- 3 On the Enterprise Vault server, perform the following steps in IIS Manager:

- Use the **Server Certificates** feature to install the new certificate.
- In the site bindings for the Default Web Site, add a binding for the HTTPS protocol and link it to the new certificate.

See the IIS documentation for more information on how to perform these two steps.

- 4 If your certificate has not come from a trusted certificate authority, import it into the Java Runtime Environment (JRE) keystore that is in the Enterprise Vault installation folder on your Enterprise Vault server (typically, C:\Program Files (x86)\Enterprise Vault\Services\JRE\lib\security\cacerts).

You can use the Keytool utility to import the certificate. This utility is included in the JRE, and you can find instructions on how to run it on the Oracle website. For example:

<http://docs.oracle.com/javase/7/docs/technotes/tools/windows/keytool.html>

The Keytool command for importing certificates has the following form:

```
keytool -importcert -trustcacerts -alias alias_name -file
path_to\certificate_file -keystore path_to\keystore_file
-storepass keystore_password
```

For example:

```
keytool -importcert -trustcacerts -alias mydomain.cdb.local -file
C:\MyKey.cer -keystore C:\Program Files (x86)\Enterprise
Vault\Services\JRE\lib\security\cacerts -storepass changeit
```

Note: Each time you upgrade Enterprise Vault, it first makes a backup copy of the `cacerts` keystore file and then replaces it with a new version of the file. So, you must import your SSL certificate into the keystore file again. For this reason, it is advisable to keep a copy of the certificate. Alternatively, you can export the certificate from the backup copy of the keystore file by following the instructions in this article:

<http://www.veritas.com/docs/000126903>

- 5** Confirm that you have successfully imported the certificate into the keystore by running a Keytool command like the following one:

```
keytool -list -keystore C:\Program Files (x86)\Enterprise  
Vault\Services\JRE\lib\security\cacerts
```

Setting up Veritas Information Classifier policies

This chapter includes the following topics:

- [Introducing the Veritas Information Classifier](#)
- [Opening the Veritas Information Classifier](#)
- [Finding your way around](#)
- [About policies](#)
- [About patterns](#)
- [About tags](#)

Introducing the Veritas Information Classifier

The Veritas Information Classifier lets you automatically classify items based on their content and metadata. In applications like Data Insight and Enterprise Vault, you can search for and filter items according to the tags that the Veritas Information Classifier has assigned to them.

Use the Veritas Information Classifier to set up the following:



Policies. The Veritas Information Classifier evaluates the items that you submit for classification against a set of policies. Each policy specifies the conditions that an item must meet to be assigned a specific classification tag. The numerous built-in policies cover many of the regulations and corporate standards for which you may want to classify items, and you can create custom policies if you have additional requirements.

See [“About policies”](#) on page 22.



Patterns. Each of the built-in policies checks the items that you submit for classification for one or more patterns. These patterns use sophisticated algorithms to look for matches that meet the required confidence level. You can incorporate the built-in patterns in any custom policies that you create, and also create custom patterns of your own.

See [“About patterns”](#) on page 31.



Tags. When an item that you have submitted for classification meets the conditions of a policy, the Veritas Information Classifier assigns the associated tags to the item. You can create custom tags to add to the large number of built-in ones.

You associate each tag with an index property. This is the metadata property of an item in which you want to store the tag. You can also associate the tag with a retention category. By doing this, you can assign the retention category to items at the same time that the Veritas Information Classifier assigns the tag to them.

See [“About tags”](#) on page 33.

Opening the Veritas Information Classifier

You can open the Veritas Information Classifier from the Vault Administration Console by following the procedure below.

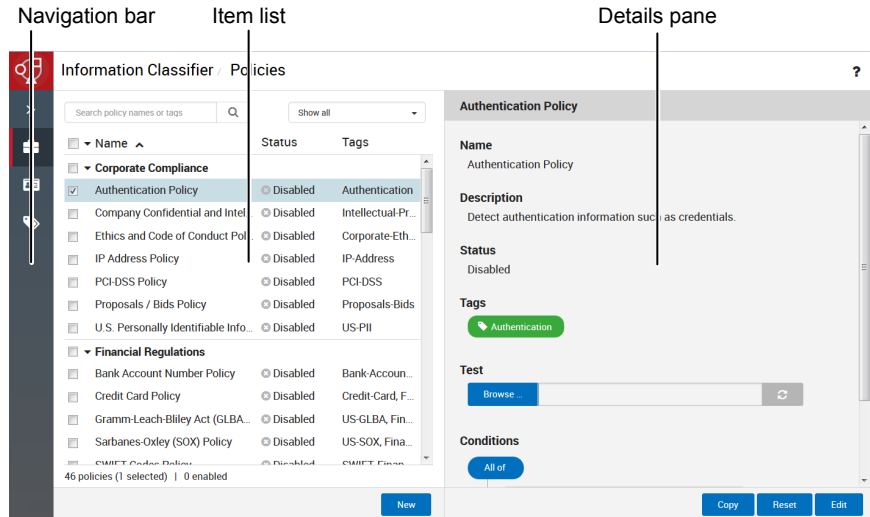
To open the Veritas Information Classifier

- 1 In the left pane of the Administration Console, expand your Enterprise Vault site.
- 2 Expand the **Policies** container, and then expand the **Retention & Classification** container.
- 3 Right-click the **Classification** container, and then click **Launch Information Classifier**.

The Veritas Information Classifier appears in your default web browser.

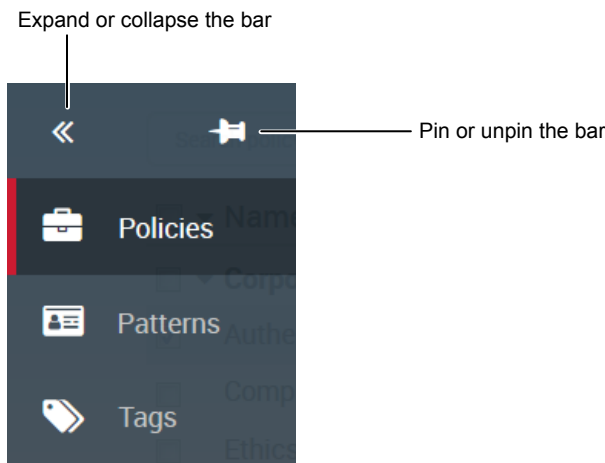
Finding your way around

The Veritas Information Classifier window is divided into three main areas: the navigation bar, item list, and details pane.



Navigation bar

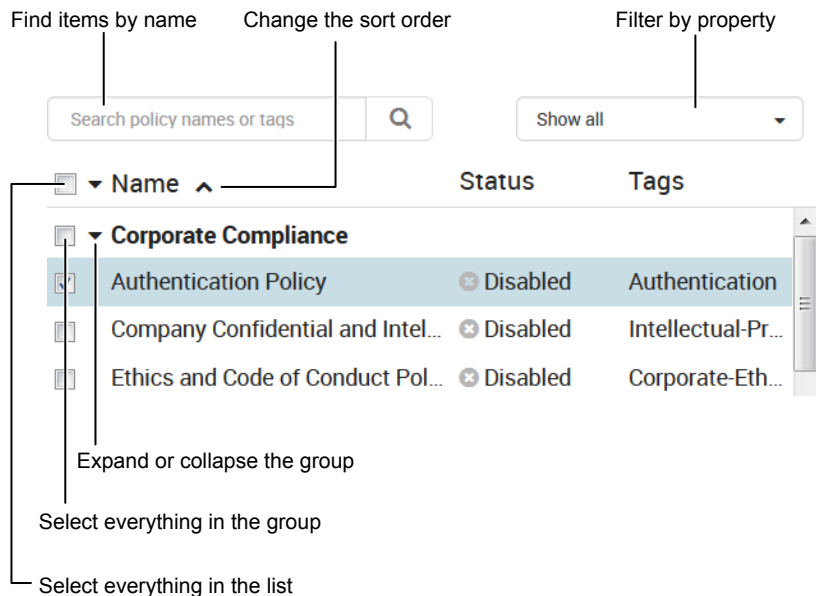
The navigation bar provides buttons with which you can open the Veritas Information Classifier pages. You can collapse the bar so that only the buttons show, or pin the bar so that it remains expanded while you work.



Item list

The item list provides a list of the available items, together with basic information about them. Click an item to view more information in the details pane.

The controls at the top of each list let you search for items by name, filter the items according to various criteria, expand and collapse the list, and change the sort order.



Details pane

The details pane provides extensive information on the selected item. You also use this pane to edit an item or create a new one to add to the list.

About policies

The Veritas Information Classifier evaluates the items that you submit for classification against a set of policies. Each policy specifies the conditions that the items must meet to be assigned a specific classification tag. For example, you can create a simple policy to assign the tag "Financial" to items that contain any of the terms *fraud*, *cover up*, and *write off*.

Description

Detects financial misconduct. ✓

Tags *

Financial ✕

Conditions

Any of ▾

Content ▾ contains text ▾

fraud
cover up
write off

The Veritas Information Classifier comes with a large number of built-in policies, but you can create custom policies if the built-in ones do not meet your needs.

Initially, all the policies are disabled. You must enable a policy if you want the Veritas Information Classifier to check for and tag the items that match the policy.

Creating or editing policies

The Veritas Information Classifier comes with a large number of built-in policies, but you can create custom policies if the built-in ones do not meet your needs.

You can also edit existing policies. However, in the case of the built-in policies, the changes that you can make are quite limited.

To create or edit a policy

- 1 At the left of the Veritas Information Classifier, click **Policies**.
- 2 Do one of the following:
 - To create a policy from the beginning, click **New**.
 - To create a policy by copying an existing one, select the policy and then click **Copy**.
 - To edit an existing policy, select the policy and then click **Edit**.

3 Set the fields as follows:

Name	Specifies the policy name. The name must be unique, and it can contain up to 100 alphanumeric, space, and special characters.
Status	Enables or disables the policy. You must enable the policy if you want the Veritas Information Classifier to check for and tag the items that match the policy.
Description	(Optional.) Provides a short description of the policy for display in the Veritas Information Classifier.
Tags	Nominates one or more tags that you want to apply to the items that match the policy conditions. Click the Tags field to choose from a list of the available tags.
Conditions	Specifies one or more conditions that an item must meet for the Veritas Information Classifier to consider it a match. See “About policy conditions” on page 24.

4 Test the policy by clicking **Browse** and then choosing an item that ought to match it.

After a few moments, the Veritas Information Classifier indicates whether it has found a match. When this is the case, you can click **Show details** to see the matching text and confidence levels.

Note: This test facility can help to confirm that the policy works as you expect. However, we recommend that you run the PowerShell cmdlet `Get-EVClassificationVICTags` against one or more test items to make certain that this is the case.

See [“Get-EVClassificationVICTags”](#) on page 72.

5 Click **Save**.

About policy conditions

A condition specifies the criteria that an item must meet for the Veritas Information Classifier to consider it a match. Your policies can contain any number of conditions.

This topic provides information on the following:

- [Basic components of a condition](#)
- [Custom fields](#)

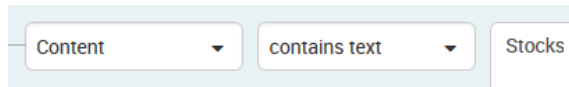
- [Text matches](#)
- [Regular expression matches](#)
- [Pattern matches](#)
- [Condition groups](#)

Basic components of a condition

All conditions have this basic form:

property operator value

For example, in the following condition, "Content" is the property, "contains text" is the operator, and "Stocks" is the value:



The property specifies the part or characteristic of an item that you want to evaluate: its content, title, modified date, file size, and so on. When you choose a property from the list, the options in the two other fields change to suit it. For example, if you choose the "Modified date" property, the other fields provide options with which you can set one or more dates. For properties such as "Content", "Title", and "Author", the available operators are as follows:

- **contains text**
- **matches regex**
- **matches pattern**

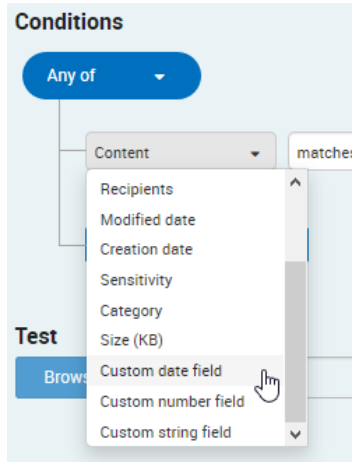
The following sections describe how to enter the required values to look for text, regular expression, and pattern matches.

At the right of each condition, you can specify the minimum number of times that an item must meet the criteria for the Veritas Information Classifier to consider it a match.

Custom fields

Various applications that you use in your organization may add custom property information to the items that you want to classify. For example, when Enterprise Vault processes an item, it populates a number of the item's metadata properties with information and stores this information with the archived item: the date on which Enterprise Vault archived the item, the number of attachments that it has, and so on.

If you know the name of a property that particularly interests you, you can enter it as a custom field in your policy conditions.



See [“About the Enterprise Vault properties”](#) on page 55.

Text matches

Observe the following guidelines when you set up a condition to look for specific words or phrases in the items that you submit for classification:

- The condition can look for multiple words or phrases, if you place each one on a line of its own. An item needs to contain just one word or phrase in the list to meet the condition.
- Select **Match Case** to find only exact matches for the uppercase and lowercase characters in the specified words or phrases.
- Select **String Match** to find instances where the specified words or phrases are contained within other ones. For example, if you select this option, the word **enter** matches *enters*, *entertainment* and *carpenter*. If you clear the option, **enter** matches only *enter*.
Similarly, if you select **String Match**, the phrase **call me** matches *call media* and *recall meeting*, but not *surgically mend*.
- You can place the proximity operators NEAR and BEFORE between two words in the same line. For example, **tax NEAR/10 reform** matches instances where there are no more than ten words between *tax* and *reform*. **sales BEFORE/5 report** matches instances where *sales* precedes *report* and there are no more than five words between them. The number is mandatory in both cases.

- Word and phrases can include the asterisk (*) and question mark (?) wildcard characters. As part of a word, an asterisk matches zero or more characters. On its own, the asterisk matches exactly one word. A question mark matches exactly one character. For example:
 - **stock*** matches *stock*, *stocks*, and *stockings*.
 - ***ock** matches *stock* and *clock*.
 - ***ock*** matches *stock* and *clocks*.
 - **??ock** matches *stock* and *clock*, but not *dock*.
 - **sell * stock** matches *sell the stock* and *sell some stock*, but not *sell stock*.

You can use wildcards in combination with the NEAR and BEFORE operators. For example:

- **s?!? BEFORE/1 stock*** matches *sold the stock*, *sell stocks*, and *sale of stockings*.

Regular expression matches

A regular expression, or regex for short, is a pattern of text that consists of ordinary characters (for example, letters *a* through *z*) and special characters, called *metacharacters*. The pattern describes one or more strings to match when searching text. For example, the following regular expression matches the sequence of digits in all Visa card numbers:

```
\b4[0-9]{12}([0-9]{3})?\b
```

Your regular expressions must conform to the Perl regular expression syntax. For more information on this syntax, see the following article:

<http://perldoc.perl.org/perlre.html>

For the best results, we recommend that you use the basic features of this syntax only and avoid more advanced features, such as lookaheads and lookbehinds.

Pattern matches

A pattern match evaluates the selected item property against an existing Veritas Information Classifier pattern. If you choose a built-in pattern, you can set the confidence levels that you are willing to accept. A high confidence level is likely to produce fewer but more relevant matches. You cannot set the confidence levels for any custom patterns that you have created.

Note the following if you do not get the expected results when you test a policy that makes use of a built-in pattern:

- It is important to check that your test item meets the pattern confidence levels. For example, by default, the Credit Card Policy looks for content that matches

the pattern "Credit/Debit Card Number" with medium to very high confidence. To meet the requirements of the medium confidence level, an item must contain either of the following:

- A delimited credit card number (one that contains spaces or dashes between the numbers).
- Both a non-delimited credit card number and one or more credit card keywords, such as "AMEX" or "Visa".

So, an item does not meet these requirements if it contains a non-delimited credit card number but it does not also contain credit card keywords.

- After you click **Show details** to view the results of a test, the **Test classification results** window may fail to highlight some or all of the matches. This is a known issue with certain patterns only. A future version of the Veritas Information Classifier will correct the issue.

Condition groups

You can group a set of conditions and nest grouped conditions within other grouped conditions. The group operator that you choose determines whether an item must meet all, some, or none of the conditions in the group to be considered a match. The following group operators are available:

- **All of**. An item must meet all the specified conditions.
- **Any of**. An item must meet at least one of the specified conditions.
- **None of**. An item must not meet any of the specified conditions.

Note: You can nest a **None of** group within an **All of** group to look for certain condition matches while also excluding others. For example, to achieve the effect of "(condition X AND condition Y) BUT NOT condition Z", you would include the X and Y conditions in an **All of** group and the Z condition in a nested **None of** group.

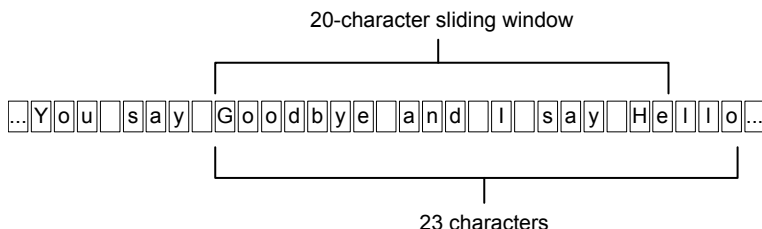
- **n or more of**. An item must meet the specified number of conditions.

For an **All of** group only, you can choose to look for instances where the conditions occur within a specified number of characters of each other. For example, the following condition group looks for instances where the word *Goodbye* appears within 20 characters of the word *Hello*:

The text string "You say Goodbye and I say Hello" matches these conditions because there are fewer than 20 characters between the first character of *Hello* and the first character of *Goodbye*. Similarly, the string "You say Hello and I say Goodbye" also matches because there are fewer than 20 characters between the ends of the two words. In each case, the spaces count as characters.

Note: When you conduct **within *nn* characters** proximity searches, take care not to duplicate the same search terms across multiple conditions. For example, suppose that you define one condition to look for the names *Fred*, *Sue*, and *Bob*, and a second to look for *Joe*, *Bob*, and *Sarah*. An item that contains a single instance of *Bob* would match these conditions.

Rather than choose the **from the first condition** option, you can choose **in a sliding window**. This option looks for instances where the conditions occur within any sequence of characters of the specified number. For example, a condition group that looks for instances where the word *Goodbye* appears within a 20-character sliding window of the word *Hello* does not match "You say Goodbye and I say Hello". There are 23 characters between the start of the word *Goodbye* and the end of the word *Hello*.



Enabling or disabling policies

Initially, all the policies are disabled. You must enable a policy if you want the Veritas Information Classifier to check for and tag the items that match the policy.

Note: Enabling a lot of policies can affect performance. In addition, policies with complex conditions take longer to process than those with simple conditions.

To enable or disable a policy

- 1 At the left of the Veritas Information Classifier, click **Policies**.
- 2 Select one or more policies that you want to enable or disable and then click **Edit**.

You can enable or disable multiple policies at once.

- 3 In the **Status** field, select **Enabled** or **Disabled**.
- 4 Click **Save**.

Resetting policies

If you make a mistake when you edit a built-in policy, you can reset it to its original settings. However, you cannot reset any custom policies that you have created.

To reset a policy

- 1 At the left of the Veritas Information Classifier, click **Policies**.
- 2 Select the policy that you want to reset and then click **Reset**.
- 3 Click **Yes** to confirm that you want to reset the policy.

Deleting policies

You cannot delete the built-in policies, but you can delete any custom policies that you have created.

To delete a policy

- 1 At the left of the Veritas Information Classifier, click **Policies**.
- 2 Select the policy that you want to delete and then click **Delete**.
- 3 Click **Yes** to confirm that you want to delete the policy.

About patterns

In the conditions of a policy, you can instruct the Veritas Information Classifier to look for one or more patterns in the items that it classifies. For example, here are the conditions for the built-in policy that is called "Ethics and Code of Conduct Policy":

The screenshot shows a configuration interface titled "Conditions". At the top, there is a blue button labeled "All of" with a downward arrow. Below this, there are two conditions listed vertically, connected by a vertical line. Each condition has a "Content" dropdown menu, followed by a "matches pattern" dropdown menu, and then a pattern name dropdown menu. The first condition's pattern name is "Individual Communication", and the second's is "Ethics & Code of Conduct". Below each pattern name, there is a "confidence:" label followed by two dropdown menus: "High" and "Very High", with a "to" label between them.

Each condition looks for a match between the content of an item and an existing pattern: either "Individual Communication" or "Ethics & Code of Conduct". When an item matches both patterns, it meets the conditions of the policy.

The built-in patterns that come with the Veritas Information Classifier use sophisticated algorithms to look for pattern matches and assign a confidence level. You can view the range of confidence levels for a pattern by selecting it in the item list. For example, the pattern "Credit/Debit Card Number" matches with low confidence if it finds a string of digits that conform to the format of a credit card number, but it matches with high confidence if these digits are accompanied by credit-related keywords like "AMEX" and "Visa". When you create or edit policies, you can set the required confidence level for these pattern matches.

Each built-in pattern is used by at least one of the built-in policies, and you can incorporate the patterns in any custom policies that you create. You can also create custom patterns if the built-in ones do not meet your needs. However, it is important to note that these custom patterns are not as sophisticated as the built-in ones. Custom patterns can look for matches with a keyword list or regular expression only, with no confidence levels.

You can edit and delete custom patterns, but you cannot edit and delete built-in patterns.

Creating or editing patterns

You cannot edit the built-in patterns, but you can edit any custom patterns that you have created.

To create or edit a pattern

- 1 At the left of the Veritas Information Classifier, click **Patterns**.
- 2 Do one of the following:
 - To create a pattern, click **New**.
 - To edit an existing pattern, select it and then click **Edit**.
- 3 Set the fields as follows:

Name	Specifies the pattern name. The name must be unique, and it can contain up to 100 alphanumeric, space, and special characters.
Description	(Optional.) Provides a short description of the pattern for display in the Veritas Information Classifier.
Type	Specifies whether the pattern consists of text (one or more words or phrases) or a regular expression. The option that you choose here determines what you can set in the Value field.
Value	Specifies the pattern's text or regular expression value. The same guidelines that you must observe when you enter these values in a policy condition apply when you enter them as a pattern value. See " About policy conditions " on page 24.

- 4 Test the pattern by clicking **Browse** and then choosing a document that ought to match it.

After a few moments, the Veritas Information Classifier indicates whether it has found a match. When this is the case, you can click **Show details** to see the matching text and confidence levels.
- 5 Click **Save**.

Deleting patterns

You can delete the custom patterns that you have created, provided that they are not in use in any policies. You cannot delete the built-in patterns.

To delete a pattern

- 1 At the left of the Veritas Information Classifier, click **Patterns**.
- 2 Select the pattern that you want to delete and then click **Delete**.
- 3 Click **Yes** to confirm that you want to delete the pattern.

About tags

Every Veritas Information Classifier policy is associated with one or more tags. When an item that you have submitted for classification matches the conditions of a policy, the Veritas Information Classifier assigns the associated tags to the item. For example, the Veritas Information Classifier assigns the tag "Corporate-Ethics" to items that match the built-in policy "Ethics and Code of Conduct Policy". In applications like Data Insight and Enterprise Vault, you can search for and filter items according to the tags that the Veritas Information Classifier has assigned to them.

When you create or edit a tag, you can choose the following:

- **Index Property.** This is the metadata property of items in which to store the tag. The property that you choose determines how Enterprise Vault processes the items to which the Veritas Information Classifier assigns the tag. For example, it can determine whether Enterprise Vault automatically discards the items, or whether the items are considered important enough to include in a Compliance Accelerator review.
- **Retention Category.** At the same time that the Veritas Information Classifier assigns the tag to items, it can also assign a retention category. The retention category specifies the minimum amount of time for which to retain the items. It also determines whether users can manually delete the items, and whether Enterprise Vault can automatically delete the items after their retention period has expired.

By default, none of the built-in tags has an associated retention category. You must edit the tags if you want to associate them with retention categories.

Creating or editing tags

The Veritas Information Classifier comes with a large number of built-in tags, but you can create custom tags if the built-in ones do not meet your needs.

To create or edit a tag

- 1 At the left of the Veritas Information Classifier, click **Tags**.
- 2 Do one of the following:
 - To create a tag, click **New**.
 - To edit an existing tag, select it and then click **Edit**.
- 3 Set the fields as follows:

Tag	<p>Specifies the tag name. The name must be unique, and it can contain up to 30 alphanumeric, space, and special characters. However, the name must not include the following characters:</p> <p>& : / \ % + < > ?</p> <p>If you are editing an existing tag, you cannot change its name.</p>
Description	<p>(Optional.) Provides a short description of the tag for display in the Veritas Information Classifier.</p>
Index Property	<p>Specifies the metadata property of the item in which you want to store the tag. There are four index properties from which to choose.</p> <ul style="list-style-type: none">■ evtag.category. Assigns one or more categories to an item.■ evtag.exclusion. Stops Enterprise Vault Compliance Accelerator from sampling an item that has this property■ evtag.inclusion. Requires Enterprise Vault Compliance Accelerator to sample an item that has this property.■ evaction.discard. Marks an item for deletion. <p>See “About the Enterprise Vault index properties” on page 34.</p> <p>You can search for the assigned property values in applications such as Enterprise Vault Search, Compliance Accelerator, and Discovery Accelerator.</p>
Retention Category	<p>Specifies the retention category that you want to assign to items to which you assign this tag. This is optional except in cases where you specify evaction.discard as the index property.</p> <p>See “How classification property values and retention categories interact” on page 36.</p> <p>See “Points to note on setting retention categories” on page 38.</p>

4 Click **Save**.

About the Enterprise Vault index properties

When an item matches a Veritas Information Classifier policy that you have defined, Enterprise Vault records the fact in the metadata properties of the item. The chosen property and the tag that Enterprise Vault assigns to it determine what Enterprise Vault does with the item. You can search for the assigned tags in applications such as Enterprise Vault Search, Compliance Accelerator, and Discovery Accelerator.

As [Table 3-1](#) explains, Enterprise Vault can process the tags that are stored in four predefined properties only.

Table 3-1 Enterprise Vault index properties for classification

Property	Description
evtag.category	<p>This property assigns one or more category values to an item when the item is added to Enterprise Vault. For example, you may want to assign the category value "US-PII" to items that contain U.S.-centric personally identifiable information, such as a North American telephone number or postal address.</p>
evtag.exclusion	<p>In environments where you use Enterprise Vault Compliance Accelerator, this property instructs the random sampling feature of that application to ignore any item that Enterprise Vault has classified with the property. (Where appropriate, however, Compliance Accelerator users can still add these items to their review sets by conducting searches for them.)</p> <p>For example, you may want to use this property to exclude auto-generated news feeds, charity solicitations, and other unimportant items from Compliance Accelerator review sets.</p>
evtag.inclusion	<p>In environments where you use Enterprise Vault Compliance Accelerator, this property instructs the random sampling feature of that application to capture any item that Enterprise Vault has classified with the property. For the best results, use this property selectively to prevent Compliance Accelerator from randomly sampling an excessive number of items.</p> <p>For example, you may want to use this property to include company-confidential items and items that contain financial or legal data in Compliance Accelerator review sets.</p>

Table 3-1 Enterprise Vault index properties for classification (*continued*)

Property	Description
evaction.discard	<p>By assigning the name of a retention category to this property of an item, you can mark the item for deletion.</p> <p>The way in which Enterprise Vault handles such items depends on the point at which it classifies them.</p> <ul style="list-style-type: none"> ■ During indexing. If an item is classified when Enterprise Vault indexes it, Enterprise Vault assigns to the item the retention category that you have chosen in the Veritas Information Classifier. You can no longer search for the item, but, for a limited number of days, you may be able to recover it. This is the case even if, in the archive settings for your Enterprise Vault site, you have chosen to disable the recovery of user-deleted items. ■ During automatic expiry. If an item is classified because its retention period has expired, Enterprise Vault immediately deletes the item. ■ During user deletion. If an item is classified because a user has tried to delete it then, depending on how you have configured the archive settings for your Enterprise Vault site, the item is either immediately deleted or temporarily recoverable. <p>This property overrides the other classification properties, such as evtag.inclusion. So, if one Veritas Information Classifier policy marks an item for deletion then it is deleted, even if a second policy tags the item for inclusion in a Compliance Accelerator review set.</p> <p>Some items may not be eligible for deletion because, for example, they are on legal hold. Where this is the case, the classification feature updates the item's retention category but does not delete the item.</p>

You can assign several tags to each of the four properties. For example, an email that the built-in Veritas Information Classifier policies have processed could have two values assigned to its evtag.category property, "Intellectual-Property" and "Corporate-Ethics", to indicate that it may contain both intellectual property source code and terms that deviate from your corporate code of conduct. The evaction.discard property differs slightly because, although you can assign several tags to it, Enterprise Vault uses the first assigned tag only.

How classification property values and retention categories interact

If both of the following conditions apply, Enterprise Vault updates the retention category of an item when the item matches a Veritas Information Classifier policy:

- You have configured the Enterprise Vault classification policy to set the retention category of items.

See [“About Enterprise Vault classification policies”](#) on page 40.

- You have associated a retention category with the tag that the Veritas Information Classifier policy assigns to the item.

For example, the Veritas Information Classifier comes with a built-in tag that is called "Authentication ". By default, this tag is assigned to any item that matches the Authentication policy. By editing the details of the Authentication tag in the Veritas Information Classifier, you can associate it with a retention category.

The result is that when an item matches the Authentication policy, both the Authentication tag and its associated retention category are assigned to the item.

For instructions on how to create retention categories, see the *Administrator's Guide*.

An item may sometimes match multiple several Veritas Information Classifier policies, all of which are competing to assign a retention category to it. Where this is the case, the classification feature selects the winning retention category as follows:

- If you use retention categories to mark items as *records*, for the purposes of implementing Capstone or an equivalent records management system, then those retention categories that mark items as records take precedence over those that do not. Retention categories that mark items as permanent records take precedence over those that mark them as temporary records, and these take precedence over retention categories that mark items as any other type of record.

For more information on using Enterprise Vault for records management, see the *Administrator's Guide*.

- If the competing retention categories want to retain the item for exactly the same duration, the winner is the retention category that you created first. For example, suppose that the retention categories "Customer Accounts" and "Legal" both have a retention period of five years. If you created the "Customer Accounts" category before you created the "Legal" category, a policy that assigns the "Customer Accounts" category overrides one that assigns the "Legal" category.
- If the durations vary, the default behavior is to assign the retention category that retains the item for the longest duration. For example, a retention category that retains items for 7 years normally overrides one that retains them for 5 years. However, you can change this behavior if you prefer to assign the retention category with the shortest duration.

See [“Configuring classification policies to assign retention categories with the shortest duration”](#) on page 43.

Points to note on setting retention categories

The following are some important points to note when you use the classification feature to set the retention categories of items:

- Suppose that you configure a retention category to prevent the automatic deletion or user deletion of items to which the category is assigned.

Retention Category Properties - Default Retention Cat...

General Details Records

Choose how long to keep items that have this retention category.

Retention

☒ Period 6 Years

Start date: Inherit from Site settings

☐ Fixed expiry date

☐ Retain items forever

Settings

☒ Prevent automatic deletion of expired items with this category

☒ Prevent user deletion of items with this category

OK Cancel Apply Help

If the classification feature assigns this retention category to an item when a user tries to delete it or Enterprise Vault tries to expire it, the action is blocked.

- By default, Enterprise Vault updates the retention categories of archived items when users perform actions that cause the retention categories to change. For example, users may move archived items between folders to which you have applied different retention categories, or they may change the retention categories of items in Enterprise Vault Search, if permitted. Both actions can cause the retention categories of the items to change, potentially overriding the retention categories that the classification feature has set. To stop this, select the option **Prevent user actions from updating retention categories** when you define an Enterprise Vault classification policy.

See [“About Enterprise Vault classification policies”](#) on page 40.

If you do not use the Enterprise Vault classification policy to prevent user actions from updating retention categories, the updates proceed subject to the options that you choose on the **Archive Settings** tab of the **Site Properties** dialog box.

- If an application such as Discovery Accelerator has placed an item on legal hold, Enterprise Vault does not submit the item for classification when a user tries to delete it or Enterprise Vault tries to expire it. In consequence, the classification feature cannot update the retention categories of such items. However, the classification feature can update the retention categories of such items when it indexes and archives them.
- When the classification feature classifies an item that Enterprise Vault has archived to a WORM storage device, it may apply a new retention category that changes the item's expiry date. In this case, Enterprise Vault expires the item on the later of the two dates.
For example, if the classification feature applies a retention category that sets a later expiry date, it is this new, later date that Enterprise Vault honors. On the other hand, if the new retention category sets an earlier expiry date, it is the original, later date that Enterprise Vault honors.

Deleting tags

You cannot delete the built-in tags, but you can delete any custom tags that you have created. However, you must first ensure that no policies use these tags.

To delete a tag

- 1 At the left of the Veritas Information Classifier, click **Tags**.
- 2 Select the tag that you want to delete and then click **Delete**.
- 3 Click **Yes** to confirm that you want to delete the tag.

Defining and applying Enterprise Vault classification policies

This chapter includes the following topics:

- [About Enterprise Vault classification policies](#)
- [Defining classification policies](#)
- [About the PowerShell cmdlets for working with classification policies](#)
- [Associating classification policies with retention plans](#)
- [About the PowerShell cmdlets for working with retention plans](#)
- [Applying retention plans to your Enterprise Vault archives](#)

About Enterprise Vault classification policies

An Enterprise Vault classification policy specifies the range of classification features that you want to implement in your Enterprise Vault site. With a classification policy, you can choose to do the following:

- **Classify items during indexing.** If you choose to do this, Enterprise Vault sends items for classification and tags them with the results at the same time that it indexes and archives them. This is also the case if you perform an index rebuild of an archive or index volume, which causes Enterprise Vault to reclassify the associated items. (This process does not affect users, as the old index volumes continue to be searchable during the rebuild.)

Enterprise Vault tags the items with `evtag.category`, `evtag.exclusion`, and `evtag.inclusion` values according to the Veritas Information Classifier policies. Users of applications like Compliance Accelerator and Discovery Accelerator can then use the classification values to filter the items when they conduct searches and reviews.

If you perform an index rebuild that causes Enterprise Vault to reclassify items, Enterprise Vault discards the classification tags that it previously applied and applies new ones in their place.

- **Set the retention category of items.** If you choose to do this then, when an item matches a Veritas Information Classifier policy, Enterprise Vault assigns the retention category that you have associated with the policy to the item. See [“How classification property values and retention categories interact”](#) on page 36.
- **Prevent user actions from updating retention categories.** By default, Enterprise Vault updates the retention categories of archived items when users perform actions that cause the retention categories to change. For example, users may move archived items between folders to which you applied different retention categories, or change the retention categories of items in Enterprise Vault Search, if permitted. Both actions can cause the retention categories of the items to change, potentially overriding the retention categories that the classification feature has set. With an Enterprise Vault classification policy, however, you can prevent such retention category updates in the archives to which you apply the policy.

You can choose to prevent retention category updates in all instances or, if you use the Enterprise Vault records management feature, you can allow them in instances where this also causes the record types of the items to change.
- If you choose to classify items during indexing, the classification feature assigns retention categories to the items when it indexes and archives them. In these circumstances, the classification feature's retention category overrides that of the retention plan. The following additional options provide finer control over how the classification feature sets the retention category of items:
 - **During user deletion.** If you choose to implement this option, the classification feature classifies an item when a user tries to delete it. In some instances this may prevent the item from being discarded, because the classification feature assigns a retention category that blocks the action.
 - **During automatic expiry.** If you choose to implement this option, the classification feature classifies an item when its retention period has elapsed. As with user deletion, this may prevent the item from being discarded, because the classification feature assigns a retention category that either blocks deletion or extends the item's retention period.

Defining classification policies

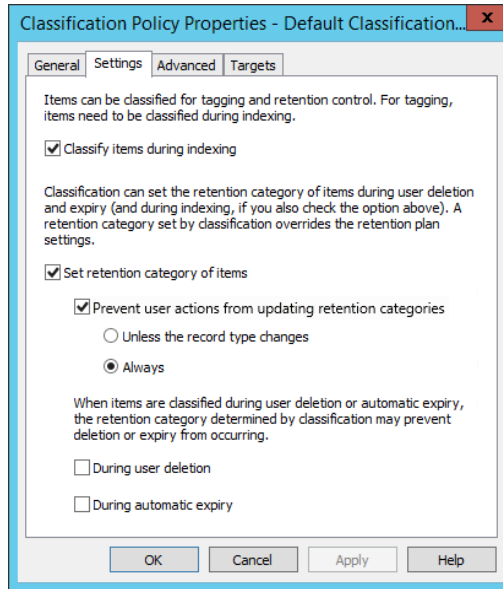
Enterprise Vault comes with a default classification policy, which you can modify as necessary, but you can also define one or more custom policies. This may be a requirement if you want to implement different classification policies for different content sources. For example, your classification requirements for File System items may be different from those for Exchange mailbox items. Where this is the case, you can define a classification policy for each content source and then associate the two policies with different retention plans: one targeted at File System archives and the other targeted at Exchange mailbox archives.

The following procedure describes how to use the Administration Console to define a classification policy. However, you can also perform the same activity with PowerShell cmdlets.

See [“About the PowerShell cmdlets for working with classification policies”](#) on page 44.

To view and modify the properties of the default classification policy

- 1 In the left pane of the Administration Console, expand your Enterprise Vault site.
- 2 Expand the **Policies** container, and then expand the **Retention & Classification** container.
- 3 Click the **Classification** container.
- 4 In the right pane, right-click **Default Classification Policy** and then click **Properties**.
- 5 Modify the settings, if necessary.



- 6 Click **OK** to save any changes that you have made.

To define a custom classification policy

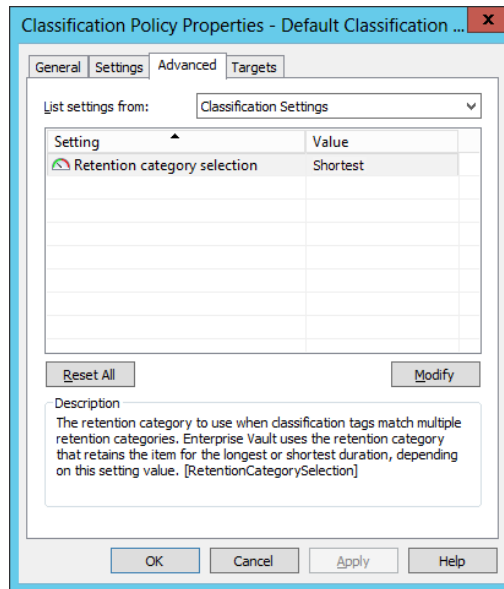
- 1 In the left pane of the Administration Console, expand your Enterprise Vault site.
- 2 Expand the **Policies** container, and then expand the **Retention & Classification** container.
- 3 Right-click the **Classification** container, and then point to **New** and click **Policy**. The **New Classification Policy** wizard appears.
- 4 Follow the on-screen instructions.

Configuring classification policies to assign retention categories with the shortest duration

One of the settings that you can choose for a classification policy is to set the retention categories of items. An item may sometimes match multiple Veritas Information Classifier policies, all of which are competing to assign a retention category to it. By default, Enterprise Vault assigns the retention category that retains the item for the longest duration. If this is not what you want, you can configure your classification policies to assign the retention category with the shortest duration.

To configure a classification policy to assign the retention category with the shortest duration

- 1 In the left pane of the Administration Console, expand your Enterprise Vault site.
- 2 Expand the **Policies** container, and then expand the **Retention & Classification** container.
- 3 Click the **Classification** container.
- 4 In the right pane, right-click the classification policy that you want to modify, and then click **Properties**.
- 5 On the **Advanced** tab, set the **Retention category selection** option to **Shortest**.



About the PowerShell cmdlets for working with classification policies

Enterprise Vault comes with a number of PowerShell cmdlets with which you can create or modify classification policies. These cmdlets perform the same functions as the equivalent facilities in the Administration Console.

Table 4-1 PowerShell cmdlets for creating or modifying classification policies

Cmdlet	Description
<code>Get-EVClassificationPolicy</code>	Returns a list of all the classification policies that you have configured in an Enterprise Vault site. See “Get-EVClassificationPolicy” on page 67.
<code>New-EVClassificationPolicy</code>	Creates a classification policy. See “New-EVClassificationPolicy” on page 76.
<code>Remove-EVClassificationPolicy</code>	Removes the specified classification policy, if it is not in use. See “Remove-EVClassificationPolicy” on page 80.
<code>Set-EVClassificationPolicy</code>	Sets or updates the properties of an existing classification policy. See “Set-EVClassificationPolicy” on page 81.

Associating classification policies with retention plans

A retention plan provides the means to assign a classification policy to your Enterprise Vault archives. You associate each classification policy with one or more retention plans and apply each plan to one or more archives. Enterprise Vault then processes the items in the archives according to the associated classification policy. For instructions on how to set up retention plans, see the *Administrator's Guide*.

The following procedure describes how to use the Administration Console to associate a classification policy with a retention plan. However, you can also perform the same activity with PowerShell cmdlets.

See [“About the PowerShell cmdlets for working with retention plans”](#) on page 47.

To associate a classification policy with a retention plan

- 1 In the left pane of the Enterprise Vault Administration Console, expand the tree view until the **Policies** container is visible.
- 2 Expand the **Policies** container and then expand the **Retention & Classification** container.
- 3 Do one of the following:
 - If you have yet to create any retention plans, right-click the **Plans** container, and then point to **New** and click **Plan**.

The **New Retention Plan** wizard appears. As part of the procedure for creating the plan, you must select the **Classify items** option and then select the required classification policy.

New Retention Plan

Choose whether to assign a classification policy with this Retention Plan

☒ **Classify items**

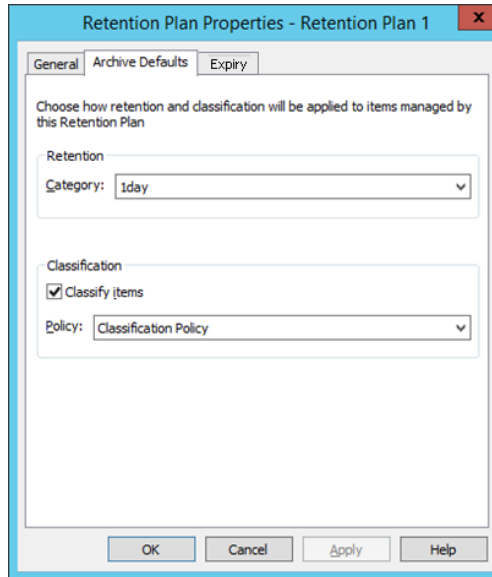
Classification Policy: New...

To view the Classification Policy, click View: View

[Tell me more about this page](#)

Next Cancel

- To associate a classification policy with an existing retention plan, click the **Plans** container and then double-click the required plan at the right. The **Retention Plan Properties** dialog box appears. The options to classify items and select the required classification policy are on the **Archive Defaults** tab of this dialog box.



In both cases, the classification feature overrides the retention plan when it comes to assigning retention categories to items.

About the PowerShell cmdlets for working with retention plans

Enterprise Vault comes with a number of PowerShell cmdlets with which you can create or modify retention plans—and at the same time change the classification options that are associated with those plans. These cmdlets perform the same function as the equivalent facilities in the Administration Console.

Table 4-2 PowerShell cmdlets for creating or modifying retention plans

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

Table 4-2 PowerShell cmdlets for creating or modifying retention plans
(continued)

Cmdlet	Description
<code>Set-EVRetentionPlan</code>	Sets or updates the properties of an existing retention plan, including its associated classification policy.

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

Applying retention plans to your Enterprise Vault archives

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

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

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

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

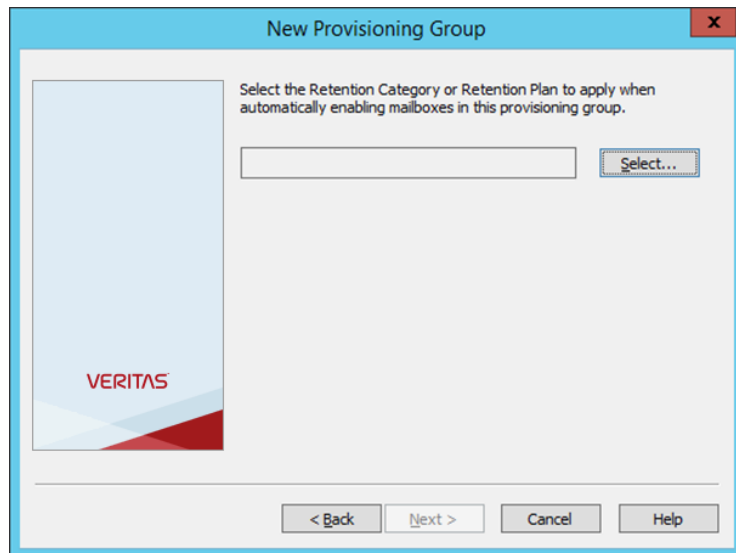
As an example, the following procedure describes how to choose a retention plan when you set up a new Exchange provisioning group.

To associate a retention plan with an Exchange provisioning group

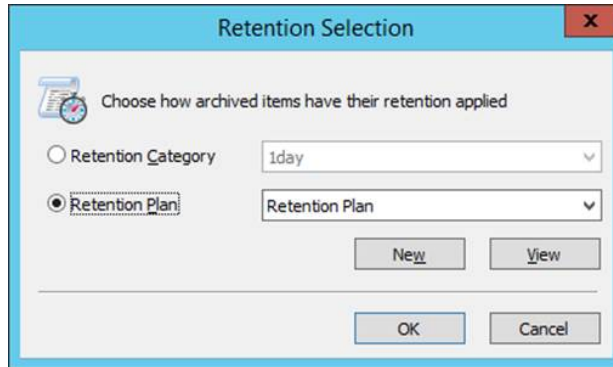
- 1 In the left pane of the Administration Console, expand the hierarchy until the **Targets** container is visible.
- 2 Expand the Exchange domain.
- 3 Right-click the **Provisioning Groups** container, and then point to **New** and click **Provisioning Group**.

The **New Provisioning Group** wizard appears.

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



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



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

Running classification in test mode

This chapter includes the following topics:

- [About classification test mode](#)
- [Implementing classification test mode](#)
- [About the PowerShell cmdlets for running classification in test mode](#)
- [Understanding the classification test mode reports](#)

About classification test mode

By running classification in test mode, you can identify and resolve any issues with your Veritas Information Classifier policies before you put them into effect. Classification does still occur in test mode, but in the following ways:

- When Enterprise Vault indexes items, it does so without applying the classification properties, their values, and any resulting retention changes to the archived items. However, the classification information is stored, and you can review it in a test mode report.
- When a user manually deletes an archived item, or Enterprise Vault automatically deletes an item whose retention period has expired, the item is deleted as normal. However, the test mode report indicates whether the action would have been blocked as the result of classification. For example, this might be the case if classification were to apply a retention category that extends the item's retention period or blocks manual deletion or automatic expiry.

The test mode report may help you to identify any Veritas Information Classifier policies that do not work as you expect. Where this is the case, you can amend the policies and rerun the tests until you are satisfied with the outcome.

Implementing classification test mode

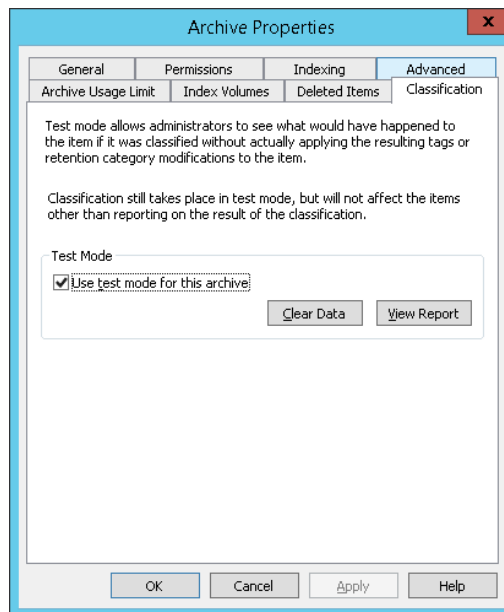
You implement classification test mode on individual archives. Only archives to which you have assigned a retention plan that has an associated classification policy are eligible for test mode.

The following procedure describes how to use the Administration Console to implement classification test mode on an archive. However, you can also perform the same activity with PowerShell cmdlets.

See [“About the PowerShell cmdlets for running classification in test mode”](#) on page 53.

To implement classification test mode

- 1 In the left pane of the Administration Console, expand the hierarchy until the **Archives** container is visible.
- 2 Locate and then right-click an archive in which you want to implement classification test mode.
- 3 In the properties dialog box for the archive, click the **Classification** tab.
- 4 Select **Use test mode for this archive**.



- 5 Click **OK** to save the change that you have made.

- 6
- Go back to the **Classification** tab and click **View Report** to open the report in your default web browser. You can use the facilities in your browser to save the report, if necessary.
- 7
- If you turn off test mode for an archive and want to reclassify the archived items, use the Rebuild wizard to rebuild the index volume. (This process does not affect users, as the old index volumes remain searchable during the rebuild.) So long as you have configured the classification policy to classify items during indexing, Enterprise Vault reclassifies the items as part of the index rebuild. For more information on the Rebuild wizard, see the *Administrator's Guide*.
- The report data persists in the vault store database after you turn off test mode or dissociate the archive from a classification policy. To remove it, click **Clear Data** in the **Classification** tab.

About the PowerShell cmdlets for running classification in test mode

Enterprise Vault comes with two PowerShell cmdlets for running classification in test mode. These cmdlets perform the same functions as the equivalent facilities in the Administration Console.

Table 5-1 PowerShell cmdlets for running classification in test mode

Cmdlet	Description
Get-EVClassificationTestMode	Reports on whether the classification feature is operating in test mode in the nominated archive. See “Get-EVClassificationTestMode” on page 71.
Set-EVClassificationTestMode	Enables or disables classification test mode in the nominated archive. See “Set-EVClassificationTestMode” on page 85.

Understanding the classification test mode reports

As [Table 5-2](#) indicates, a classification test mode report contains several sections.

Table 5-2 Contents of a classification test mode report

This section	Shows
Rule Matches	The Veritas Information Classifier policies that the items match, and the number of items in each case.

Table 5-2 Contents of a classification test mode report (*continued*)

This section	Shows
Proposed Tag Application on Indexing	The classification property values that Enterprise Vault would assign to the items when it indexes them, and the number of items in each case.
Retention Category	The number of items whose retention category would change because they match a Veritas Information Classifier policy that assigns a different one.
Proposed Changes to Retention	<p>The number of items whose retention period Enterprise Vault would modify, extend, or reduce. Note that the number of modified items may not be the same as the sum of items with an extended or reduced retention period. For example, some items may acquire a new retention category that sets the same retention period as the original retention category.</p> <p>This section also shows the number of items that would be eligible for expiry if Enterprise Vault were to classify them now.</p>
Blocked Deletions	The number of items that Enterprise Vault would block from automatic expiry or user deletion because it would reevaluate their retention categories during classification. The report omits this section if there are no blocked deletions.

Enterprise Vault properties for use in custom field searches

This appendix includes the following topics:

- [About the Enterprise Vault properties](#)
- [System properties](#)
- [Attachment properties](#)
- [Custom Enterprise Vault properties](#)
- [Custom Enterprise Vault properties for File System Archiving items](#)
- [Custom Enterprise Vault properties for SharePoint items](#)
- [Custom Enterprise Vault properties for Compliance Accelerator-processed items](#)
- [Custom properties for use by policy management software](#)
- [Custom properties for Enterprise Vault SMTP Archiving](#)

About the Enterprise Vault properties

When Enterprise Vault indexes an item, it populates a number of the item's metadata properties with information about the item. Some examples of such information include the display name and email address of the message author, the number of attachments, and the file size of the item.

Indexed items can have a large number of properties, but only a subset is of interest for classification purposes. These are the properties and associated values that

Enterprise Vault passes to the Veritas Information Classifier for classification. When you create a Veritas Information Classifier policy, you can enter the names of these properties as custom fields in the policy conditions.

See [“About policy conditions”](#) on page 24.

System properties

[Table A-1](#) lists the system properties defined in Enterprise Vault.

Table A-1 Enterprise Vault system properties

Property	Type	Description
adat	Date	The date on which the item was archived.
archiveid	String	The ID of the archive in which the item is stored. You can use the PowerShell cmdlet <code>Get-EVArchive</code> to obtain the required ID.
audn	String	The display names of the author and, if appropriate, of the person on whose behalf the item has been sent.
aua	String	The email addresses of the author and, if appropriate, of the person on whose behalf the item has been sent.
cend	Date	The end date of an event, such as a calendar meeting.
clcn	String	The current location of the item. A sequence of folders.
cllf	String	The last or leaf folder of the current location.
clon	String	The location of an event, such as a calendar meeting.
cntp	String	The conversation tracking topic. This is currently populated for MAPI and SMTP items only.

Table A-1 Enterprise Vault system properties (*continued*)

Property	Type	Description
comr	String	The reason for missing content. The options are as follows: <ul style="list-style-type: none">■ 0. No reason available.■ 1. Content does not exist.■ 2. Content could not be obtained.■ 3. Content is (or appears to be) corrupt.■ 4. Not possible to convert content to suitable format.■ 5. Conversion of content failed (converter error).■ 6. Conversion of content timed out.■ 7. Content requires conversion but its data format is excluded from conversion.■ 8. Content requires conversion but conversion bypass has been set.■ 9. Content is encrypted.■ 10. Content requires conversion but converters are not available, or have not been initialized.■ 11. Unable to add content to index.■ 12. Converters did not recognize the file type.■ 13. Conversion excluded for large files.■ 14. Conversion excluded for codepages we cannot detect.
cpnm	String	The name of the extension content provider.
crcn	String	The current retention category name. May reflect the value that various Enterprise Vault features, such as classification, retention plans, and retention folders, have applied to the item.
cre	Integer	Calendar recurrence exception.
crp	String	Calendar recurrence pattern.
crt	Integer	Calendar recurrence type.
csrt	Date	The start date of an event, such as a calendar meeting.
date	Date	The created, sent, received, or archived date.
dtype	String	The data type of the item. For example, DOCX, XLSX, or MSG.
flag	String	The message flag status.

Table A-1 Enterprise Vault system properties (*continued*)

Property	Type	Description
impo	String	The message importance, expressed as a numeric value. 0 = Low, 1 = Normal, and 2 = High.
keys	String	Categories/keywords.
locn	String	The original location of the item. A sequence of folders.
mdat	Date	The last-modified date of the item.
msgc	String	The item's original MAPI message class (for example, IPM.Note).
natc	Number	The number of attachments.
nrcp	Number	The number of recipients.
prio	String	The message priority, expressed as a numeric value. -1 = Low, 0 = Normal, and 1 = High.
rbdn	String	The display names of the BCC recipients.
rbea	String	The email addresses of the BCC recipients.
rcdn	String	The display names of the CC recipients.
rcea	String	The email addresses of the CC recipients.
rsdt	Date	The retention start date/time Not supported by queries that target 32-bit volumes.
rtdn	String	The display names of the TO recipients.
rtea	String	The email addresses of the TO recipients.
sens	String	The message sensitivity, expressed as a numeric value. 0 = Normal, 1 = Personal, 2 = Private, and 3 = Confidential.
size	Number	The size of the item in KB.
subj	String	The subject/title.
tcdt	Date	The completion date of a task.
tddt	Date	The due date of a task.
tsts	Number	The status of a task. 0 = Not started, 1 = In progress, 2 = Completed, 3 = Paused, and 4 = Deferred.

Attachment properties

When an item that Enterprise Vault has passed for classification has one or more attachments, multiple properties of those attachments are also available for classification. You can distinguish these attachment properties by their *a_* prefixes: *a_comr*, *a_date*, and so on. [Table A-2](#) lists a typical set of attachment properties that Enterprise Vault passes for classification.

Table A-2 Enterprise Vault attachment properties

Property	Type	Description
<i>a_comr</i>	String	The reason for missing content (encrypted content, converter error, and so on). See the description of the <i>comr</i> property for more details. See “System properties” on page 56.
<i>a_date</i>	Date	The created, sent, received, or archived date of the attachment.
<i>a_dtyp</i>	String	The data type of the attachment. For example, DOCX, XLSX, or MSG.
<i>a_mdat</i>	Date	The last-modified date of the attachment.
<i>a_size</i>	Number	The size of the attachment in KB.
<i>a_subj</i>	String	The file name of the attachment or, if it is a message, the subject.

The classification feature always treats attachments as files. So, even if an attachment is an email message, its sender information and recipient information are not available for classification.

Custom Enterprise Vault properties

[Table A-3](#) lists the custom properties that are defined in Enterprise Vault.

Table A-3 Custom Enterprise Vault properties

Property	Type	Description
Vault.CopiedFrom	String	<p>Provides the following details for an item that Enterprise Vault's Move Archive feature has copied:</p> <ul style="list-style-type: none">■ The date and time at which the item was copied.■ The identifier of the source archive.■ The saveset identifier of the source item. <p>The format is as follows:</p> <p><i>UTC_datetime_of_copy,source_archive_ID,source_item_Saveset_ID</i></p> <p>If an archive has been moved several times, there is a value for each move.</p>
Vault.JournalType	String	<p>For journal messages, the journal type. The options are as follows:</p> <ul style="list-style-type: none">■ E2003■ E2007■ E2007ClearText■ E2007RMS
Vault.MsgDirection	String	<p>The message direction. The options are as follows:</p> <ul style="list-style-type: none">■ 0 - undefined■ 1 - internal (sender and all recipients are internal)■ 2 - external-in (sender is external, one or more recipients are internal)■ 3 - external-out (sender is external, one or more recipients are external)
Vault.MsgType	String	<p>The message type. The options are as follows:</p> <ul style="list-style-type: none">■ Bloomberg■ DXL■ EXCH■ FAX.vendor■ IM.vendor■ SMTP

Custom Enterprise Vault properties for File System Archiving items

Table A-4 lists the custom properties that are defined in Enterprise Vault for File System Archiving items.

Table A-4 Custom Enterprise Vault properties for File System Archiving items

Property	Type	Description
EVFSADLMImport.DLM	String	An indicator that the item was imported from the legacy archiving application, Veritas Data Lifecycle Management (DLM). This is currently only populated with the string "Imported".
EVFSA.OriginalFileName	String	The original name of the file at the point that Enterprise Vault archived it.

Custom Enterprise Vault properties for SharePoint items

Table A-5 lists the custom properties that are defined in Enterprise Vault for SharePoint items.

Some of these properties are similar to certain Enterprise Vault system properties. For example, the SharePoint property, "EVSP.Title", is similar to the Enterprise Vault system property, "subj". However, the Enterprise Vault system property may not hold the expected information for some SharePoint items, such as social content items. For this reason, you should use the custom SharePoint index properties instead of the equivalent Enterprise Vault system properties when searching SharePoint archives.

Table A-5 Custom Enterprise Vault properties for SharePoint items

Property	Type	Description
EVSP.AttachmentName	String	A list of names of all the attachments to this item. This property applies to social content only, except for Wikis.
EVSP.Comment	String	The check-in comment.

Table A-5 Custom Enterprise Vault properties for SharePoint items
(continued)

Property	Type	Description
EVSP.Created	String	The date of creation of the item. This property applies to social content only.
EVSP.CreatedBy	String	The domain name (Windows account name) of the document author.
EVSP.DocId	String	The identifier of the SharePoint document.
EVSP.Editor	String	The display name of the document editor.
EVSP.Modified	String	The date on which the item was last modified. This property applies to social content only.
EVSP.ModifiedBy	String	The domain name (Windows account name) of the document editor.
EVSP.ProgId	String	The program identifier for the item.
EVSP.Site	String	The name of the SharePoint site.
EVSP.SiteId	String	The identifier of the SharePoint site.
EVSP.SiteUrl	String	The URL of the SharePoint site.
EVSP.Title	String	The title of the SharePoint document.
EVSP.UniqueId	String	The GUID that uniquely identifies the item.
EVSP.Version	String	The version of the SharePoint document.
EVSP.Attachments	String	Whether the item has attachments: true or false. This property applies to social content only, except for Wikis.
EVSP.display_name	String	The display name of the archived item.
EVSP.SharePoint_property_name	String	Customer configurable properties. Any SharePoint property.

Custom Enterprise Vault properties for Compliance Accelerator-processed items

Table A-6 lists the custom properties that are defined in Enterprise Vault for the items that Compliance Accelerator has randomly sampled.

Table A-6 Custom Enterprise Vault properties for Compliance Accelerator-processed items

Property	Type	Description
KVSCA.Department	String	Combines the values of properties KVSCA.DeptAuthor and KVSCA.DeptRecips.
KVSCA.DeptAuthor	String	The set of Compliance Accelerator Department IDs of which the item's author is a member.
KVSCA.DeptRecips	String	The set of Compliance Accelerator Department IDs of which the item's recipients are members.
Vault.PolicyAction	String	The overall action that should be taken on an item; the sum result of all the applied policies. The defined values are as follows: <ul style="list-style-type: none">■ NOACTION■ EXCLUDE■ INCLUDE

Custom properties for use by policy management software

[Table A-7](#) lists the custom properties that certain policy management applications, such as Enterprise Vault Data Classification Services, may use.

(Data Classification Services is an older, add-on classification technology that combines various components of Veritas Enterprise Vault and Symantec Data Loss Prevention. It is different from the classification feature that is described here.)

Table A-7 Custom properties for use by policy management software

Property	Type	Description
evtag.category	String	Policies that do not affect capture either way; they only categorize items.
evtag.exclusion	String	Policies that either preclude capture or advocate non-capture in the review set.
evtag.inclusion	String	Policies that either demand or suggest capture.

Custom properties for Enterprise Vault SMTP Archiving

[Table A-8](#) lists the custom properties that third-party applications can add to SMTP messages to override the policy and target settings in Enterprise Vault SMTP Archiving. For more information on these properties, see the *Setting up SMTP Archiving* guide.

Table A-8 Custom properties for Enterprise Vault SMTP Archiving

Property	Type	Description
EVXHDR.X-Kvs-ArchiveId	String	The identifier of the archive in which to store the message.
EVXHDR.X-Kvs-IndexData	String	One or more properties for Enterprise Vault to index.
EVXHDR.X-Kvs-MessageType	String	The message type. This overrides the value of the Vault.MsgType property, which Enterprise Vault SMTP Archiving sets to SMTP.mail by default.
EVXHDR.X-Kvs-OriginalLocation	String	The folder in the content source where the message resides.
EVXHDR.X-Kvs-RetentionCategory	String	The ID of the retention category to assign to the message.

PowerShell cmdlets for use with classification

This appendix includes the following topics:

- [About the classification cmdlets](#)
- [Disable-EVClassification](#)
- [Get-EVClassificationPolicy](#)
- [Get-EVClassificationStatus](#)
- [Get-EVClassificationTestMode](#)
- [Get-EVClassificationVICTags](#)
- [Initialize-EVClassificationVIC](#)
- [New-EVClassificationPolicy](#)
- [Remove-EVClassificationPolicy](#)
- [Set-EVClassificationPolicy](#)
- [Set-EVClassificationTestMode](#)

About the classification cmdlets

This chapter describes the PowerShell cmdlets with which you can manage various features of Enterprise Vault classification. For the most part, these cmdlets duplicate facilities that are available in the Administration Console.

The *PowerShell Cmdlets* guide provides more information on using PowerShell to manage Enterprise Vault and describes many other cmdlets.

Disable-EVClassification

`Disable-EVClassification` lets you disable the File Classification Infrastructure engine or Veritas Information Classifier engine. This cmdlet does not let you disable both engines. Run the cmdlet on an Enterprise Vault server.

If you disable a classification engine and later want to reenable it, you can do so using one of the following cmdlets:

- For the File Classification Infrastructure engine, use `Import-EVClassificationFCIRules` **or** `Publish-EVClassificationFCIRules`.
- For the Veritas Information Classifier engine, use `Initialize-EVClassificationVIC`.

`Disable-EVClassification` is provided by `Symantec.EnterpriseVault.PowerShell.AdminAPI.dll`, which is loaded by the Enterprise Vault Management Shell.

Syntax

```
Disable-EVClassification [-FCI <SwitchParameter>] [-VIC <SwitchParameter>] [-SiteId <String>] [<CommonParameters>]
```

Parameters

Table B-1 Disable-EVClassification parameters

Parameter	Description
-FCI	If specified, disables classification using the File Classification Infrastructure engine.
-VIC	If specified, disables classification using the Veritas Information Classifier engine.
-SiteId	The ID of the Enterprise Vault site in which to disable the specified classification engine. If you omit this parameter, <code>Disable-EVClassification</code> checks the registry to determine the ID of the current site. You can use <code>Get-EVSite</code> to obtain the site ID.

Examples

- `Disable-EVClassification -FCI`
Disables classification using the File Classification Infrastructure engine. As no site ID is specified, the cmdlet checks the registry to determine the ID of the current site.

- `Disable-EVClassification -VIC -SiteId 198...example.com`
Disables classification using the Veritas Information Classifier engine in the specified Enterprise Vault site.

Output

This cmdlet returns an object of type

`Symantec.EnterpriseVault.PowerShell.Commands.ClassificationEngine`, which has the following properties.

Table B-2 Disable-EVClassification properties

Name	Type	Description
SiteName	String	The name of the Enterprise Vault site in which you have disabled the classification engine.
FCIEnabled	Boolean	Whether classification using the File Classification Infrastructure engine is enabled.
VICEnabled	Boolean	Whether classification using the Veritas Information Classifier engine is enabled.
VICPoliciesPath	String	The path to the folder in which Veritas Information Classifier engine keeps policy information. This path is blank if you have disabled the engine.

Get-EVClassificationPolicy

`Get-EVClassificationPolicy` returns a list of all the Enterprise Vault classification policies that are configured in a site. You can also return the properties of a specific classification policy using the `-Name` parameter.

`Get-EVClassificationPolicy` is provided by

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

Syntax

```
Get-EVClassificationPolicy [[-SiteId] <String>] [[-Name] <String>]  
[<CommonParameters>]
```

Parameters

Table B-3 Get-EVClassificationPolicy parameters

Parameter	Description
-SiteId	The ID of the site for which to return the Enterprise Vault classification policy details. If you omit this parameter, and the cmdlet cannot determine the ID by looking in the registry, then <code>Get-EVClassificationPolicy</code> prompts you to enter the required ID. You can use <code>Get-EVSite</code> to obtain the site ID.
-Name	The name of a specific Enterprise Vault classification policy whose properties you want to return.

Examples

- `Get-EVClassificationPolicy`
Returns a list of all the Enterprise Vault classification policies that are configured in the Enterprise Vault site. As no site ID is specified, the cmdlet first looks for it in the registry and then, if it cannot find the ID there, prompts you for it.
- `Get-EVClassificationPolicy -SiteId 13E...EV.example.com`
Returns a list of all the Enterprise Vault classification policies that are configured in the specified Enterprise Vault site.
- `Get-EVClassificationPolicy -SiteId 13E...EV.example.com -Name "Classification policy"`
Returns the properties of the Enterprise Vault classification policy that is named "Classification policy". For example:

```
Name                : Classification policy
EntryId             : 125...EV.example.com
IsADefaultPolicy    : True
DuringIndexing      : True
DetermineRC         : True
RCDuringDeletion    : True
RCDuringExpiry      : True
PreventRCDuringMove : True
AllowRCONRecTypeChange : True
Description          : Classification policy
SiteId              : 13E...EV.example.com
```

Output

This cmdlet returns an object of type

`Symantec.EnterpriseVault.Admin.ClassificationPolicy`, which has the following properties.

Table B-4 Get-EVClassificationPolicy properties

Name	Type	Description
Name	String	The name of the Enterprise Vault classification policy.
EntryId	String	The directory entry ID of the Enterprise Vault classification policy.
IsADefaultPolicy	Boolean	Whether the Enterprise Vault classification policy is a default policy.
DuringIndexing	Boolean	Whether to classify items during indexing, and reclassify them during an index rebuild.
DetermineRC	Boolean	Whether classification is used to determine the retention category.
RCDuringDeletion	Boolean	Whether items are classified during user deletion.
RCDuringExpiry	Boolean	Whether items are classified during automatic expiry.
PreventRCDuringMove	Boolean	Whether to prevent Enterprise Vault from updating the retention categories of archived items when users perform actions that could potentially update these retention categories. For example, users may move archived items between folders to which you have applied different retention categories, or change the retention categories of items in Enterprise Vault Search, if permitted. Both actions can cause the retention categories of the items to change.
AllowRCOnRecTypeChange	Boolean	Whether to allow user actions to update retention categories in instances where this also causes the record types of the items to change (for example, from Temporary to Permanent).
Description	String	The description of the Enterprise Vault classification policy.

Table B-4 Get-EVClassificationPolicy properties (*continued*)

Name	Type	Description
SiteId	String	The site ID to which the Enterprise Vault classification policy belongs.
Identity	Number	The identity number of the Enterprise Vault classification policy.

Related cmdlets

- See [“New-EVClassificationPolicy”](#) on page 76.
- See [“Remove-EVClassificationPolicy”](#) on page 80.
- See [“Set-EVClassificationPolicy”](#) on page 81.

Get-EVClassificationStatus

`Get-EVClassificationStatus` shows the current status of the File Classification Infrastructure and Veritas Information Classifier engines in all sites. You can also show the status of these engines in a specific site using the `-SiteId` parameter.

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

Syntax

```
Get-EVClassificationStatus [-SiteId <String>] [<CommonParameters>]
```

Parameters

Table B-5 Get-EVClassificationStatus parameters

Parameter	Description
<code>-SiteId</code>	The ID of the Enterprise Vault site for which to show the current status of both classification engines. You can use <code>Get-EVSite</code> to obtain the site ID.

Examples

- `Get-EVClassificationStatus`
Shows the current status of both classification engines in all Enterprise Vault sites.

- `Get-EVClassificationStatus -SiteId 13E...EV.example.com`
Shows the current status of both classification engines in the specified site.

Output

This cmdlet returns an array of objects of type

`Symantec.EnterpriseVault.PowerShell.Commands.ClassificationEngine`, which have the following properties.

Table B-6 Get-EVClassificationStatus properties

Name	Type	Description
SiteName	String	The name of the Enterprise Vault site for which to show the status of the classification engines.
FCIEnabled	Boolean	Whether classification using the File Classification Infrastructure engine is enabled.
VICEnabled	Boolean	Whether classification using the Veritas Information Classifier engine is enabled.
VICPoliciesPath	String	The path to the folder in which Veritas Information Classifier engine keeps policy information. This path is blank if you have disabled the engine.

Get-EVClassificationTestMode

`Get-EVClassificationTestMode` reports on whether the Enterprise Vault classification feature is operating in test mode in the nominated archive. In test mode, the classification feature generates a report that lists the planned changes instead of applying classification tags and other changes to the items in the archive.

`Get-EVClassificationTestMode` is provided by

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

Syntax

`Get-EVClassificationTestMode [-ArchiveID] <String>`

Parameters

Table B-7 Get-EVClassificationTestMode parameters

Parameter	Description
-ArchiveID (required)	Specifies the ID of the archive for which to get the status of classification test mode.

Examples

- `Get-EVClassificationTestMode -ArchiveID 19D...EVServer1`
Gets the current status of classification test mode for the specified archive.

Output

[Table B-8](#) lists the properties that are available.

Table B-8 Get-EVClassificationTestMode properties

Name	Type	Description
ArchiveID	String	The ID of the archive for which to get the test mode status.
ArchiveName	String	The name of the archive for which to get the test mode status.
TestMode	Boolean	The current status of classification test mode for the archive: enabled (<code>\$true</code>) or disabled (<code>\$false</code>).

Related cmdlets

- See [“Set-EVClassificationTestMode”](#) on page 85.

Get-EVClassificationVICTags

Note: This cmdlet is only for use with the Veritas Information Classifier in Enterprise Vault 12.2 and later. It is not designed for use with the classification features in earlier versions of Enterprise Vault, such as classification using the Microsoft File Classification Infrastructure (FCI).

For the specified pair of plain-text (.txt) files in the classification cache folder, `Get-EVClassificationVICTags` returns details of the matching Veritas Information Classifier policies and the associated classification properties. Run the cmdlet on an Enterprise Vault server.

By default, Enterprise Vault empties the cache folder at the first opportunity. However, you can configure it to retain the cache contents by choosing a setting in the Administration Console.

See [“Configuring Enterprise Vault to keep the classification files in the cache folder”](#) on page 88.

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

Syntax

Get-EVClassificationVICTags [-ContentFile] <String> [-MetadataFile] <String> []

Parameters

Table B-9 Get-EVClassificationVICTags parameters

Parameter	Description
-ContentFile (required)	The path to the plain-text content file for which to return the classification details (usually the text file whose name ends VC.txt). Enclose file names that contain a dollar sign (\$) in single quotation marks (').
-MetadataFile (required)	The path to the plain-text metadata file for which to return the classification details (usually the text file whose name ends VMD.txt). Enclose file names that contain a dollar sign (\$) in single quotation marks (').

Examples

- Get-EVClassificationFCITags -ContentFile 'E:\EVCache\Classification\EV\$9...B8VC.txt' -MetadataFile 'E:\EVCache\Classification\EV\$9...8VMD.txt'
Returns the classification details for the specified plain-text files.

Output

This cmdlet returns an array of objects of type Symantec.EnterpriseVault.PowerShell.Commands.ClassificationProperty, which have the following properties.

Table B-10 Get-EVClassificationVICTags properties

Name	Type	Description
PolicyName	String	The Veritas Information Classifier policy that matched.
Category	String	The evtag.category values that matched.
Inclusion	String	The evtag.inclusion values that matched.
Exclusion	String	The evtag.exclusion values that matched.
Discard	Boolean	Whether the item would be discarded.
RetentionCategories	String	The retention categories that matched.

Initialize-EVClassificationVIC

Note: This cmdlet is only for use with the Veritas Information Classifier in Enterprise Vault 12.2 and later. It is not designed for use with the classification features in earlier versions of Enterprise Vault, such as classification using the Microsoft File Classification Infrastructure (FCI).

`Initialize-EVClassificationVIC` enables the Veritas Information Classifier on all the Enterprise Vault servers in the specified site. For each of these servers, the cmdlet also configures the Veritas Information Classifier website in Microsoft Internet Information Services (IIS).

Permission to run `Initialize-EVClassificationVIC` is restricted to the Vault Service account. Run this cmdlet on an Enterprise Vault server rather than, for example, a separate computer on which you have installed a standalone Vault Administration Console.

Before you run the cmdlet for the first time, do the following:

- In the Vault Administration Console, in the properties of the Enterprise Vault Directory, set up the Data Access account. Enterprise Vault uses this account to access the Veritas Information Classifier system.
See [“Setting up the Data Access account”](#) on page 15.
- On a shared network drive to which all the Enterprise Vault servers have access, create a folder in which the Veritas Information Classifier can keep policy information. Both the Vault Service account and the Data Access account must have read/write access to the folder.

After you have run the cmdlet, we recommend that you do the following:

- Enable at least one Veritas Information Classifier policy.
See [“Enabling or disabling policies”](#) on page 30.
- Take regular backups of the policy information folder. In the event of a system failure, you can then recover any custom policies that you have created and any changes that you have made to the built-in policies, such as enabling or disabling those policies.

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

Syntax

```
Initialize-EVClassificationVIC [-PoliciesPath <String>] [-SiteId  
<String>] [<CommonParameters>]
```

Parameters

Table B-11 Initialize-EVClassificationVIC parameters

Parameter	Description
<code>-PoliciesPath</code>	<p>Specifies the UNC path to the folder in which the Veritas Information Classifier should keep policy information. The folder must already exist; the cmdlet does not create it.</p> <p>It is mandatory to specify this parameter when you run <code>Initialize-EVClassificationVIC</code> for the first time. For subsequent runs, you can omit the parameter if you want the cmdlet to use the folder path that you previously specified.</p> <p>Alternatively, you can specify the parameter again to nominate a different folder path. If you do nominate a different path, move the contents of the old policy folder to the new one before you use the Veritas Information Classifier again.</p>
<code>-SiteId</code>	<p>Specifies the ID of the Enterprise Vault site for which to configure the Veritas Information Classifier. If you omit this parameter, <code>Initialize-EVClassificationVIC</code> checks the registry to determine the ID of the current site. The cmdlet displays an error message if this check fails for any reason.</p> <p>You can use <code>Get-EVSite</code> to obtain the site ID.</p>

Examples

- `Initialize-EVClassificationVIC -PoliciesPath \\server1\VicPolicies`

Runs the cmdlet with the specified policy folder path on the current Enterprise Vault server. As no site ID is specified, the cmdlet checks the registry to determine the ID of the current site.

- `Initialize-EVClassificationVIC -Verbose -PoliciesPath \\server1\VicPolicies -SiteId 198...example.com`

Runs the cmdlet in verbose mode with the specified policy folder path and Enterprise Vault site.

- `Initialize-EVClassificationVIC -Verbose`

Runs the cmdlet in verbose mode with the existing policy folder path on the current Enterprise Vault server. If you have not previously specified the folder path, the cmdlet displays an error message.

Output

None.

New-EVClassificationPolicy

`New-EVClassificationPolicy` creates an Enterprise Vault classification policy for a site.

`New-EVClassificationPolicy` is provided by

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

Syntax

```
New-EVClassificationPolicy [[-SiteId] <String>] [-Name] <String>
[-Description <String>] [-DuringIndexing <Boolean>] [-DetermineRC
<Boolean>] [-RCDuringDeletion <Boolean>] [-RCDuringExpiry <Boolean>]
[-PreventRCDuringMove <Boolean>] [-AllowRConRecTypeChange <Boolean>]
[<CommonParameters>]
```

Parameters

Table B-12 New-EVClassificationPolicy parameters

Parameter	Description
-SiteId	<p>The ID of the site for which to create the Enterprise Vault classification policy. If you omit this parameter, and the cmdlet cannot determine the ID by looking in the registry, then <code>New-EVClassificationPolicy</code> prompts you to enter the required ID.</p> <p>You can use <code>Get-EVSite</code> to obtain the site ID.</p>
-Name (required)	<p>The name of the Enterprise Vault classification policy. The name must be unique, and it can contain up to 40 alphanumeric or space characters.</p>
-Description	<p>The description to set for the Enterprise Vault classification policy. The description can contain up to 127 alphanumeric, space, or special characters.</p>
-DuringIndexing	<p>Specifies whether Enterprise Vault should classify items at the point that it indexes them (<code>\$true</code>) or not (<code>\$false</code>). The default is <code>\$true</code>.</p> <p>This setting also determines whether Enterprise Vault reclassifies items when you rebuild the indexes.</p>
-DetermineRC	<p>Specifies whether to allow the classification feature to update the retention categories of items (<code>\$true</code>) or not (<code>\$false</code>). The default is <code>\$true</code>.</p>
-RCDuringDeletion	<p>When <code>DetermineRC</code> is <code>\$true</code>, specifies whether to enable classification on user deletion (<code>\$true</code>) or not (<code>\$false</code>). The default is <code>\$false</code>.</p> <p>You cannot set <code>RCDuringDeletion</code> to <code>\$true</code> when <code>DetermineRC</code> is set to <code>\$false</code>.</p>
-RCDuringExpiry	<p>When <code>DetermineRC</code> is <code>\$true</code>, specifies whether to enable classification on automatic expiry (<code>\$true</code>) or not (<code>\$false</code>). The default is <code>\$false</code>.</p> <p>Note the following:</p> <ul style="list-style-type: none">■ You cannot set <code>RCDuringExpiry</code> to <code>\$true</code> when <code>DetermineRC</code> is set to <code>\$false</code>.■ You must set <code>RCDuringExpiry</code> to <code>\$true</code> when <code>DuringIndexing</code> is <code>\$false</code> and <code>DetermineRC</code> is <code>\$true</code>.

Table B-12 New-EVClassificationPolicy parameters (*continued*)

Parameter	Description
<code>-PreventRCDuringMove</code>	<p>When <code>DetermineRC</code> is <code>\$true</code>, specifies whether to prevent Enterprise Vault from updating the retention categories of archived items when users perform actions that could potentially update these retention categories. For example, users may move archived items between folders to which you have applied different retention categories, or change the retention categories of items in Enterprise Vault Search, if permitted. Both actions can cause the retention categories of the items to change, potentially overriding the retention categories that the classification feature has set.</p> <p>The default for <code>PreventRCDuringMove</code> is <code>\$false</code>. Enterprise Vault allows user actions to update the retention categories of items, subject to site archive settings.</p>
<code>-AllowRCONRecTypeChange</code>	<p>For use in environments where you use the Enterprise Vault records management feature to mark selected items as records.</p> <p>When <code>PreventRCDuringMove</code> is <code>\$true</code> (prevent user actions from updating retention categories), <code>AllowRCONRecTypeChange</code> specifies whether to allow these updates in instances where this also causes the record types of the items to change. The default for <code>AllowRCONRecTypeChange</code> is <code>\$true</code>.</p> <p>When <code>PreventRCDuringMove</code> is <code>\$false</code>, <code>AllowRCONRecTypeChange</code> has no effect.</p>

Examples

- `New-EVClassificationPolicy -SiteId 13E...EV.example.com -Name "Classification policy" -Description "Classification policy created using PowerShell"`
Creates an Enterprise Vault classification policy that is named "Classification policy" in the specified Enterprise Vault site. The new policy has the description "Classification policy created using PowerShell".
- `New-EVClassificationPolicy -Name "Classification policy" -DuringIndexing $true -DetermineRC $false`

Creates an Enterprise Vault classification policy that is named "Classification policy". This policy does classify items during indexing but does not use classification to determine their retention categories.

- `New-EVClassificationPolicy -Name "Classification policy" -PreventRCDuringMove $true`

Creates an Enterprise Vault classification policy to classify items during indexing and allow the classification feature to update the retention categories of items. The policy prevents Enterprise Vault from updating the retention categories of items when users perform actions that could potentially update these retention categories, except when this will change the record type of the items.

Output

This cmdlet returns an object of type

`Symantec.EnterpriseVault.Admin.ClassificationPolicy`, which has the following properties.

Table B-13 **New-EVClassificationPolicy** properties

Name	Type	Description
Name	String	The name of the Enterprise Vault classification policy.
EntryId	String	The directory entry ID of the Enterprise Vault classification policy.
IsADefaultPolicy	Boolean	Whether the Enterprise Vault classification policy is a default policy.
DuringIndexing	Boolean	Whether to classify items during indexing, and reclassify them during an index rebuild.
DetermineRC	Boolean	Whether classification is used to determine the retention category.
RCDuringDeletion	Boolean	Whether items are classified during user deletion.
RCDuringExpiry	Boolean	Whether items are classified during automatic expiry.

Table B-13 New-EVClassificationPolicy properties (*continued*)

Name	Type	Description
PreventRCDuringMove	Boolean	Whether to prevent Enterprise Vault from updating the retention categories of archived items when users perform actions that could potentially update these retention categories. For example, users may move archived items between folders to which you have applied different retention categories, or change the retention categories of items in Enterprise Vault Search, if permitted. Both actions can cause the retention categories of the items to change.
AllowRConRecTypeChange	Boolean	Whether to allow user actions to update retention categories in instances where this also causes the record types of the items to change (for example, from Temporary to Permanent).
Description	String	The description of the Enterprise Vault classification policy.
SiteId	String	The site ID to which the Enterprise Vault classification policy belongs.
Identity	Number	The identity number of the Enterprise Vault classification policy.

Related cmdlets

- See [“Get-EVClassificationPolicy”](#) on page 67.
- See [“Remove-EVClassificationPolicy”](#) on page 80.
- See [“Set-EVClassificationPolicy”](#) on page 81.

Remove-EVClassificationPolicy

`Remove-EVClassificationPolicy` removes the specified Enterprise Vault classification policy, if it is not in use. The cmdlet prompts you to confirm the removal of the classification policy.

`Remove-EVClassificationPolicy` is provided by `Symantec.EnterpriseVault.PowerShell.AdminAPI.dll`, which is loaded by the Enterprise Vault Management Shell.

Syntax

```
Remove-EVClassificationPolicy [[-SiteId] <String>] [-Name] <String>
[<CommonParameters>]
```

Parameters

Table B-14 Remove-EVClassificationPolicy parameters

Parameter	Description
-SiteId	The ID of the site to which the Enterprise Vault classification policy belongs. If you omit this parameter, and the cmdlet cannot determine the ID by looking in the registry, then <code>Remove-EVClassificationPolicy</code> prompts you to enter the required ID. You can use <code>Get-EVSite</code> to obtain the site ID.
-Name (required)	The name of the Enterprise Vault classification policy to remove.

Examples

- `Remove-EVClassificationPolicy -SiteId 13E...EV.example.com -Name "Classification policy"`
Removes the Enterprise Vault classification policy that is named "Classification policy" from the specified Enterprise Vault site.

Output

None.

Related cmdlets

- See [“Get-EVClassificationPolicy”](#) on page 67.
- See [“New-EVClassificationPolicy”](#) on page 76.
- See [“Set-EVClassificationPolicy”](#) on page 81.

Set-EVClassificationPolicy

`Set-EVClassificationPolicy` sets or updates the properties of an existing Enterprise Vault classification policy.

`Set-EVClassificationPolicy` is provided by `Symantec.EnterpriseVault.PowerShell.AdminAPI.dll`, which is loaded by the Enterprise Vault Management Shell.

Syntax

```
Set-EVClassificationPolicy [[-SiteId] <String>] [-Name] <String>  
[-Description <String>] [-DuringIndexing <Boolean>] [-DetermineRC  
<Boolean>] [-RCDuringDeletion <Boolean>] [-RCDuringExpiry <Boolean>]  
[-PreventRCDuringMove <Boolean>] [-AllowRConRecTypeChange <Boolean>]  
[<CommonParameters>]
```

Parameters

Table B-15 Set-EVClassificationPolicy parameters

Parameter	Description
-SiteId	The ID of the site for which to set or update the Enterprise Vault classification policy details. If you omit this parameter, and the cmdlet cannot determine the ID by looking in the registry, then <code>Set-EVClassificationPolicy</code> prompts you to enter the required ID. You can use <code>Get-EVSite</code> to obtain the site ID.
-Name (required)	The name of a specific Enterprise Vault classification policy whose properties you want to set or update. If you want to rename the policy then the new name must be unique, and it can contain up to 40 alphanumeric or space characters.
-Description	The description to set for the Enterprise Vault classification policy. The description can contain up to 127 alphanumeric, space, or special characters.
-DuringIndexing	Specifies whether Enterprise Vault should classify items at the point that it indexes them (<code>\$true</code>) or not (<code>\$false</code>). The default is <code>\$true</code> . This setting also determines whether Enterprise Vault reclassifies items when you rebuild the indexes.
-DetermineRC	Specifies whether to allow the classification feature to update the retention categories of items (<code>\$true</code>) or not (<code>\$false</code>). The default is <code>\$true</code> .

Table B-15 Set-EVClassificationPolicy parameters (*continued*)

Parameter	Description
-RCDuringDeletion	<p>When <code>DetermineRC</code> is <code>\$true</code>, specifies whether to enable classification on user deletion (<code>\$true</code>) or not (<code>\$false</code>). The default is <code>\$false</code>.</p> <p>You cannot set <code>RCDuringDeletion</code> to <code>\$true</code> when <code>DetermineRC</code> is set to <code>\$false</code>.</p>
-RCDuringExpiry	<p>When <code>DetermineRC</code> is <code>\$true</code>, specifies whether to enable classification on automatic expiry (<code>\$true</code>) or not (<code>\$false</code>). The default is <code>\$false</code>.</p> <p>Note the following:</p> <ul style="list-style-type: none">■ You cannot set <code>RCDuringExpiry</code> to <code>\$true</code> when <code>DetermineRC</code> is set to <code>\$false</code>.■ You must set <code>RCDuringExpiry</code> to <code>\$true</code> when <code>DuringIndexing</code> is <code>\$false</code> and <code>DetermineRC</code> is <code>\$true</code>.
-PreventRCDuringMove	<p>When <code>DetermineRC</code> is <code>\$true</code>, specifies whether to prevent Enterprise Vault from updating the retention categories of archived items when users perform actions that could potentially update these retention categories. For example, users may move archived items between folders to which you have applied different retention categories, or change the retention categories of items in Enterprise Vault Search, if permitted. Both actions can cause the retention categories of the items to change, potentially overriding the retention categories that the classification feature has set.</p> <p>The default for <code>PreventRCDuringMove</code> is <code>\$false</code>. Enterprise Vault allows user actions to update the retention categories of items, subject to site archive settings.</p>

Table B-15 Set-EVClassificationPolicy parameters (*continued*)

Parameter	Description
<code>-AllowRConRecTypeChange</code>	<p>For use in environments where you use the Enterprise Vault records management feature to mark selected items as records.</p> <p>When <code>PreventRCDuringMove</code> is <code>\$true</code> (prevent user actions from updating retention categories), <code>AllowRConRecTypeChange</code> specifies whether to allow these updates in instances where this also causes the record types of the items to change. The default for <code>AllowRConRecTypeChange</code> is <code>\$true</code>.</p> <p>When <code>PreventRCDuringMove</code> is <code>\$false</code>, <code>AllowRConRecTypeChange</code> has no effect.</p>

Examples

- ```
Set-EVClassificationPolicy -SiteId 13E...EV.example.com -Name "Classification policy" -Description "Classification example policy"
```

Updates the description of an existing Enterprise Vault classification policy that is named "Classification policy" in the specified Enterprise Vault site.
- ```
Set-EVClassificationPolicy -SiteId 13E...EV.example.com -Name "Classification policy" -PreventRCDuringMove $true -AllowRConRecTypeChange $false
```

Configures the specified Enterprise Vault classification policy to prevent user actions from updating the retention categories of items, including when this will change their record type, in those archives to which you apply the policy.

Output

There is a confirmation message on completion.

Related cmdlets

- See [“Get-EVClassificationPolicy”](#) on page 67.
- See [“New-EVClassificationPolicy”](#) on page 76.
- See [“Remove-EVClassificationPolicy”](#) on page 80.

Set-EVClassificationTestMode

`Set-EVClassificationTestMode` specifies whether the Enterprise Vault classification feature should operate in test mode in the nominated archive. In test mode, the classification feature generates a report that lists the planned changes instead of applying classification tags and other changes to the items in the archive. You can then run `Get-EVClassificationTestMode` on the same archive to check that the outcome is satisfactory.

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

Syntax

```
Set-EVClassificationTestMode [-ArchiveID] <String> [-Enabled  
<Boolean>]
```

Parameters

Table B-16 Set-EVClassificationTestMode parameters

Parameter	Description
<code>-ArchiveID</code> (required)	Specifies the ID of the archive for which to set the test mode status.
<code>-Enabled</code> (required)	Specifies whether to enable classification test mode for the archive (<code>\$true</code>) or disable it (<code>\$false</code>).

Examples

- `Set-EVClassificationTestMode -ArchiveID 1E...EVServer1 -Enabled $true`
Specifies that the classification feature should operate in test mode in the nominated archive.

Output

Returns an exception in the event of failure but otherwise provides no output.

Related cmdlets

- See [“Get-EVClassificationTestMode”](#) on page 71.

Classification cache folder

This appendix includes the following topics:

- [How Enterprise Vault caches the items that it submits for classification](#)
- [Limits on the size of classification files](#)
- [Configuring Enterprise Vault to keep the classification files in the cache folder](#)

How Enterprise Vault caches the items that it submits for classification

Note: Enterprise Vault restricts access to the cache location to the Local System account and members of the built-in Administrators group.

Before Enterprise Vault invokes the Veritas Information Classifier to process the items that it has submitted for classification, it stores plain-text versions of these items in a nominated cache location on the storage server. Each item is represented by a set of two or more plain-text files, which are as follows:

- One or more files contain the text content and subject line of the item. For very large items, Enterprise Vault splits this content into multiple plain-text files.

Typically, these content files have names like the following:

`EV$704348C690A05389A4292971F3C6E691~0D84E700VC.txt`

Where the `vc` suffix that precedes the period indicates that this is a content file. If Enterprise Vault has created multiple content files to store the text of a large item, the rollover files have the suffixes `vc_1`, `vc_2`, and so on.

In any set of rollover files, the last 5000 characters of each file appear at the start of the next file in the sequence. This feature allows Veritas Information Classifier policies that look for proximity matches to work correctly.

- One file contains only the metadata properties and associated values with which Enterprise Vault has indexed the item. The file provides this information in the form *property:value*, as in the following example:

```
rtdn:Mike Smith  
rtea:mike_smith@yourcompany.com  
audn:Sean Gallagher  
auea:sean_gallagher@yourcompany.com  
msgc:IPM.Document.outlook.File.eml.15  
impo:1  
sens:0  
prio:0  
size:19  
dtyp:EML  
natc:0
```

Indexed items can have a large number of properties, but only a subset is of interest for classification purposes. These are the properties and associated values that Enterprise Vault stores in this metadata file and that you can configure your Veritas Information Classifier policies to search for.

See [“About the Enterprise Vault properties”](#) on page 55.

A metadata file has the same name as its equivalent content file, except that it has an `VMD` suffix before the period rather than `VC`. For example:

```
EV$704348C690A05389A4292971F3C6E691~0D84E700VMD.txt
```

By default, Enterprise Vault deletes the plain-text files from the cache folder as soon as it has finished classification, but this behavior is configurable.

See [“Configuring Enterprise Vault to keep the classification files in the cache folder”](#) on page 88.

Limits on the size of classification files

By default, the Veritas Information Classifier can classify files that are up to 32 MB in size. When a file exceeds this limit, Enterprise Vault automatically splits it into files of this size, and classification then proceeds across the set of files.

You can change the 32-MB limit by adjusting the option **Maximum classification content size** in the Vault Administration Console. You may want to increase the limit if you have a complex Veritas Information Classifier policy that fails to match items because different parts of it match different files in the set. For example, this issue can arise if you have a policy that searches for both of the words *fraud* and *corruption*, when the first word is in one file and the second word is in another.

To set the maximum classification content size

- 1 In the left pane of the Administration Console, right-click your Enterprise Vault site and then click **Properties**.
- 2 In the **Site Properties** dialog box, click the **Advanced** tab.

- 3 In the **List settings from** box, select **Storage**.
- 4 Click **Maximum classification content size**, and then click **Modify**.
- 5 Set the maximum content size, and then click **OK**.

Configuring Enterprise Vault to keep the classification files in the cache folder

The plain-text files that Enterprise Vault stores in the cache folder may contain sensitive data, so by default Enterprise Vault deletes them at the first opportunity. If you want to examine the contents of these files because, for example, Enterprise Vault does not classify them as you expect, you can configure it to stop them from being automatically deleted.

To configure Enterprise Vault to keep the classification files in the cache folder

- 1 In the left pane of the Administration Console, expand the vault site.
- 2 Expand the **Enterprise Vault Servers** container.
- 3 Right-click the server whose settings you want to modify and then click **Properties**.
- 4 In the **Computer Properties** dialog box, click the **Advanced** tab.
- 5 In the **List settings from** list, select **Storage**.
- 6 Double-click **Keep classification files** and then set it to **On**.
- 7 Click **OK** to save the change that you have made.

If you later turn off this setting, the files that Enterprise Vault has previously placed in the cache folder remain there until you restart the Storage service on the server. However, you can manually delete them if you want to get rid of them immediately.

Migrating from FCI classification to the Veritas Information Classifier

This appendix includes the following topics:

- [Converting FCI classification rules for use with the Veritas Information Classifier](#)

Converting FCI classification rules for use with the Veritas Information Classifier

Enterprise Vault 12 provided the means to classify items using the File Classification Infrastructure, which is a classification engine that is built into recent Windows Server editions. This facility is still available in the current version of Enterprise Vault, and you can use it in addition to or instead of the Veritas Information Classifier. However, the greater sophistication of the Veritas Information Classifier, and the effect on performance that can result from running both classification engines simultaneously, are good reasons to transfer your existing classification rules to the Veritas Information Classifier. After you have transferred the rules, you can disable the File Classification Infrastructure engine.

To convert FCI classification rules for use with the Veritas Information Classifier

- 1 Prepare a test server for classification using the Veritas Information Classifier. Most importantly, you must run the PowerShell cmdlet `Initialize-EVClassificationVIC` to enable the Veritas Information Classifier.

See [“About the preparatory steps”](#) on page 12.

See [“Initialize-EVClassificationVIC”](#) on page 74.

- 2 In the Veritas Information Classifier, create policies that perform the same function as the FCI classification rules.

See [“Creating or editing policies”](#) on page 23.

- 3 Use the test facilities in the Veritas Information Classifier to confirm that each policy works as you expect.

- 4 In the Enterprise Vault Administration Console, implement classification test mode on individual archives. This lets you identify any issues with your policies that the test facilities in the Veritas Information Classifier may have missed.

See [“About classification test mode”](#) on page 51.

Alternatively, you can configure Enterprise Vault to keep the classification files in the cache folder, and then use the PowerShell cmdlet

`Get-EVClassificationVICTags` to see how the Veritas Information Classifier has tagged them.

See [“Configuring Enterprise Vault to keep the classification files in the cache folder”](#) on page 88.

See [“Get-EVClassificationVICTags”](#) on page 72.

- 5 Prepare your production servers for classification using the Veritas Information Classifier. As before, you must run the PowerShell cmdlet `Initialize-EVClassificationVIC` to enable the Veritas Information Classifier.

See [“About the preparatory steps”](#) on page 12.

See [“Initialize-EVClassificationVIC”](#) on page 74.

If the folder in which the Veritas Information Classifier keeps policy information for your production servers is different from the folder that you set for the test server, you must move the contents of the latter folder to the new one.

- 6 Disable the File Classification Infrastructure engine on the production servers by running the PowerShell cmdlet `Disable-EVClassification` as follows:

```
Disable-EVClassification -FCI
```

See [“Disable-EVClassification”](#) on page 66.

Monitoring and troubleshooting

This appendix includes the following topics:

- [Auditing](#)
- [Checking the classification performance counters](#)
- [Troubleshooting classification](#)
- [Searching archives for items that the Veritas Information Classifier has classified](#)

Auditing

[Table E-1](#) describes the classification activities for which Enterprise Vault can store audit log entries in its auditing database. Auditing is disabled by default, but you can enable it by following the instructions in the *Administrator's Guide*.

Table E-1 Audited classification activities

Category	Logged classification activities
Admin Activity	<ul style="list-style-type: none">■ Create, update, or delete an Enterprise Vault classification policy.■ Enable or disable classification test mode for an archive.■ View or clear the classification test mode data for an archive.

Table E-1 Audited classification activities (*continued*)

Category	Logged classification activities
Classification	<ul style="list-style-type: none">■ Create, update, or delete a Veritas Information Classifier policy, pattern, or tag.■ Classify an item during indexing (CLASSIFIED).■ Classify and discard an item during indexing (DISCARDED).■ Classify and try to discard an item during indexing, but the item or archive is on hold (DISCARDONHOLD).■ Classify an item and allow it to be discarded during automatic expiry (EXPIRY_ALLOWED).■ Classify an item but do not allow it to be discarded during automatic expiry (EXPIRY_BLOCKED).■ Classify an item and allow it to be discarded during user deletion (USERDELETION_ALLOWED).■ Classify an item but do not allow it to be discarded during user deletion (USERDELETION_BLOCKED).

Enterprise Vault provides the Audit Viewer utility with which you can view and filter the data in the auditing database. For more information on Audit Viewer, see the *Utilities* guide.

Checking the classification performance counters

Enterprise Vault provides a number of counters with which you can get live, real-time performance data for the classification feature. You can view this data using the Windows Performance Monitor or any other program that you use to monitor performance counters.

[Table E-2](#) describes the counters.

Table E-2 Enterprise Vault Classification performance counters

Counter	Description
Items allowed for automatic expiry	The number of items that Enterprise Vault has allowed to be automatically expired as a result of classification.
Items allowed for user deletion	The number of items that Enterprise Vault has allowed users to delete as a result of classification.
Items blocked from automatic expiry	The number of items that Enterprise Vault has blocked from automatic expiry as a result of classification.

Table E-2 Enterprise Vault Classification performance counters (*continued*)

Counter	Description
Items blocked from discard on classification	The number of items that classification has marked for deletion but that Enterprise Vault cannot delete because they are on legal hold.
Items blocked from user deletion	The number of items that Enterprise Vault has blocked users from deleting as a result of classification.
Items discarded on classification	The number of items that Enterprise Vault has discarded because classification has marked them for deletion.
Items failed classification	The number of items that Enterprise Vault has failed to classify.
Items successfully classified	<p>The number of items that Enterprise Vault has passed for classification with a success result. The count includes any items that classification has marked for deletion, whether or not Enterprise Vault was able to discard them.</p> <p>Any items that are successfully classified but that Enterprise Vault later fails to index may be counted multiple times, as Enterprise Vault automatically retries the whole operation.</p>

Troubleshooting classification

The following issues may arise when you use the classification feature.

Table E-3 Potential classification issues

Issue	Explanation/solution
The Launch Information Classifier command is not available in the Administration Console.	<p>Ensure that you have run the PowerShell cmdlet <code>Initialize-EVClassificationVIC</code> to enable the Veritas Information Classifier.</p> <p>See “Initialize-EVClassificationVIC” on page 74.</p>

Table E-3 Potential classification issues (*continued*)

Issue	Explanation/solution
Enterprise Vault fails to classify items.	<p>Ensure all of the following:</p> <ul style="list-style-type: none">■ You have a valid license for the Enterprise Vault retention feature.■ You can open the Veritas Information Classifier. See “Opening the Veritas Information Classifier” on page 20.■ The correct Veritas Information Classifier policies are in place and enabled.■ You have correctly configured the cache location. See “Checking the cache location on the Enterprise Vault storage servers” on page 13.■ You have correctly configured the retention plan and Enterprise Vault classification policy for the target archives. Each archive must have an associated retention plan that has an Enterprise Vault classification policy.■ You are running classification in normal mode rather than test mode. See “About classification test mode” on page 51. <p>You may also want to examine the files in the classification cache folder.</p> <p>See “Configuring Enterprise Vault to keep the classification files in the cache folder” on page 88.</p>

Table E-3 Potential classification issues (continued)

Issue	Explanation/solution
Items are not classified as you expect.	<p>Try the following:</p> <ul style="list-style-type: none">■ Ensure that Enterprise Vault is classifying items (see above).■ If Enterprise Vault does classify items but the resulting tags do not persist, check whether classification is running in test mode. See “About classification test mode” on page 51.■ Configure Enterprise Vault to keep the classification files instead of automatically deleting them. See “Configuring Enterprise Vault to keep the classification files in the cache folder” on page 88. Then you can review the file contents for any anomalies that you did not anticipate.■ Run the PowerShell cmdlet <code>Get-EVClassificationVICTags</code> to identify the policies that each item matches. See “Get-EVClassificationVICTags” on page 72.■ Use Enterprise Vault Search to verify that the items have been classified using the current set of policies. See “Searching archives for items that the Veritas Information Classifier has classified” on page 95.
Classification operates in test mode only.	Enterprise Vault cannot detect a valid license for the retention feature.

Searching archives for items that the Veritas Information Classifier has classified

Enterprise Vault marks every item that it classifies during indexing with information about the version of the Veritas Information Classifier policies that it has used. Each item has a metadata property, `vpcv` (for "Veritas Information Classifier policy current version"), which records whether the Veritas Information Classifier has classified the item. This property also records whether the policies used are the latest set of policies.

When you conduct a search with Enterprise Vault Search, Compliance Accelerator, or Discovery Accelerator, you can use the `vpcv` property to filter the results that you obtain. For example, here are some queries that you can type in the simple search box of Enterprise Vault Search:

Searching archives for items that the Veritas Information Classifier has classified

<code>vpcv:**</code>	Finds all the items that the Veritas Information Classifier has classified.
<code>NOT vpcv:**</code>	Finds all the items that the Veritas Information Classifier has not classified.
<code>vpcv:True</code>	Finds the items that the Veritas Information Classifier has classified using the latest set of policies.
<code>vpcv:False</code>	Finds the items that the Veritas Information Classifier has classified using an older set of policies.

Index

A

- archives
 - applying retention plans to 48
 - implementing classification test mode in 52
- attachments, Enterprise Vault properties for 59

C

- cache folder
 - configuring Enterprise Vault to keep files in 88
 - configuring the location of 14
 - introduction to 87
- classification
 - and roles-based administration 13
 - introduction to 7
 - license for 13, 94
 - overview of setup procedure 12
 - PowerShell cmdlets for 65
 - prerequisites for 13
 - use of cache 87
- classification patterns
 - about 31
 - configuring 31
- Classification policy
 - configuring 23
- classification tags
 - about 33
 - configuring 33
- Compliance Accelerator
 - and evtag.exclusion property 35
 - and evtag.inclusion property 35
 - Custom Enterprise Vault properties for 62

D

- Data Classification Services, custom properties for 63
- default classification policy 42
- Disable-EVClassification 66

E

- Enterprise Vault Data Classification Services, custom properties for 63

- Enterprise Vault properties for Compliance
 - Accelerator-processed items 62
- Enterprise Vault properties for File System Archiving items 61
- Enterprise Vault properties for SharePoint items 61
- Enterprise Vault search properties 56, 59
- evaction.discard
 - introduction to 36
 - performance counters for 93
- EVClassification cmdlets
 - Disable-EVClassification 66
 - Initialize-EVClassificationVIC 74
- EVClassificationPolicy cmdlets
 - Get-EVClassificationPolicy 67
 - New-EVClassificationPolicy 76
 - Remove-EVClassificationPolicy 80
 - Set-EVClassificationPolicy 81
- EVClassificationStatus cmdlets
 - Get-EVClassificationStatus 70
- EVClassificationTestMode cmdlets
 - Get-EVClassificationTestMode 71
 - Set-EVClassificationTestMode 85
- EVClassificationVICTags cmdlets
 - Get-EVClassificationVICTags 72
- evtag.category
 - introduction to 35
- evtag.exclusion
 - introduction to 35
- evtag.inclusion
 - introduction to 35

F

- File System Archiving items, Enterprise Vault properties for 61

G

- Get-EVClassificationPolicy 45, 67
- Get-EVClassificationStatus 70
- Get-EVClassificationTestMode 53, 71
- Get-EVClassificationVICTags 72
- Get-EVRetentionPlan 47

I

index rebuilds, and classification 40
 Information Classifier. *See* policies
 Initialize-EVClassificationVIC 74

K

Keep classification files setting 88

N

New-EVClassificationPolicy 45, 76
 New-EVRetentionPlan 47

P

performance counters 92
 policies
 associating retention plans with 45
 default policy 42
 defining 42
 introduction to 7, 40
 PowerShell cmdlets for 44
 Policy management software, custom properties for 63
 prerequisites for classification 13
 properties
 and classification policies 41
 and retention categories 36
 introduction to 34

R

RBA 13
 Remove-EVClassificationPolicy 45, 80
 Remove-EVRetentionPlan 47
 report mode. *See* test mode
 retention categories
 and classification policies 41
 and classification properties 36
 Retention category selection option 44
 retention plans
 applying to archives 48
 associating policies with 45
 PowerShell cmdlets for 47
 roles-based administration 13

S

Set-EVArchive 48
 Set-EVClassificationPolicy 45, 81
 Set-EVClassificationTestMode 53, 85
 Set-EVRetentionPlan 48

SharePoint items, Enterprise Vault properties for 61

T

test mode
 contents of report 53
 enabling or disabling 52
 introduction to 51
 PowerShell cmdlets for 53
 troubleshooting 93

V

Veritas Information Classifier
 managing 23