Veritas Enterprise Vault™ Classification

12.1

VERITAS™

Veritas Enterprise Vault: Classification

Last updated: 2017-07-28.

Legal Notice

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

This chapter includes the following topics:

Introducing this guide

This guide is designed for Enterprise Vault administrators who want to use its classification feature to assign classification values to all new and existing archived content. After the classification feature has assigned the required values to items, users of applications such as Enterprise Vault Search, Compliance Accelerator, and Discovery Accelerator can use them to filter the items when they conduct searches and reviews.

The classification feature can also control the retention of items by applying specific retention categories to them. When users manually delete items or Enterprise Vault automatically expires them, the items can be reclassified to ensure that they are still safe to delete.

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	Gives an overview of the classification feature and the procedure for setting it up. See "About classification" on page 12.

Table 1-1 Contents of this guide *(continued)*

Chapter	Function
3	Leads you through the process of setting up the classification properties in which Enterprise Vault stores a classification value for each item. See "About the Enterprise Vault classification properties" on page 20.
4	Explains how to configure rules for defining the criteria that an item must match to be awarded a specific classification value. See "About classification rules" on page 33.
5	Describes how to define policies that specify the range of classification features that you want to implement. The chapter also describes how to associate these policies with one or more retention plans, which you can apply to the Enterprise Vault archives in which classification is to occur. See "About classification policies" on page 46.
6	Outlines how to test the classification feature before you put it into effect. See "About classification test mode" on page 56.
7	Shows you how to publish the required classification settings throughout your Enterprise Vault site. See "How to publish the classification properties and rules" on page 60.

This guide assumes that you are familiar with a number of Enterprise Vault features, including the Administration Console and PowerShell Management Shell, and with Microsoft technologies such as the File Server Resource Manager.

Where to get more information about Enterprise Vault

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

Table 1-2 Enterprise Vault documentation set

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

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

Document	Comments
Backup and Recovery	Describes how to implement an effective backup strategy to prevent data loss, and how to provide a means for recovery in the event of a system failure.
Classification	Describes how to assign classification values to the metadata properties of all new and existing archived items. Users of applications such as Enterprise Vault Search and Compliance Accelerator can then use the classification values to filter the items when they conduct searches or reviews.
NSF Migration	Describes how to migrate content from Domino and Notes NSF files into Enterprise Vault archives.
PST Migration	Describes how to migrate content from Outlook PST files into Enterprise Vault archives.
Reporting	Describes how to implement Enterprise Vault Reporting, which provides reports on the status of Enterprise Vault servers, archives, and archived items. If you configure FSA Reporting, additional reports are available for file servers and their volumes.
Utilities	Describes the Enterprise Vault tools and utilities.
PowerShell Cmdlets	Describes how to perform various administrative tasks by running the Enterprise Vault PowerShell cmdlets.
Registry Values	A reference document that lists the registry values with which you can modify many aspects of Enterprise Vault behavior.
Help for Administration Console	The online Help for the Enterprise Vault Administration Console.
Help for Enterprise Vault Operations Manager	The online Help for Enterprise Vault Operations Manager.

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

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

Enterprise Vault training modules

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

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

Chapter 2

Getting started

This chapter includes the following topics:

About classification

The Enterprise Vault classification feature works in combination with Microsoft's File Classification Infrastructure to assign classification values to the metadata properties of all new and existing archived content. The File Classification Infrastructure is a classification framework that is built into recent Windows Server editions. You control the File Classification Infrastructure through the File Server Resource Manager interface.

Rules

The File Server Resource Manager provides the means to define the *classification rules* that specify what you want to search for, and the property values that you want to assign to any matching items. For example, a rule may search for items whose contents include a credit card number and assign a property value of "PII" (for "personally identifiable information") to any that do.

After the classification feature has applied the classification property values to items, users of applications like Enterprise Vault Search, Compliance Accelerator, and Discovery Accelerator can use the values to filter items when they conduct searches and reviews.

Enterprise Vault comes with a set of example classification rules, which you can use as a starting point to create your own set of rules. Most of the example rules search for strings and regular expression patterns in items. For more advanced functionality, you can integrate third-party classification providers into the File Classification Infrastructure.

Note: The example rules are for test purposes only and may not deliver the required results in a production environment.

Policies

You choose the classification options that you want to implement in your Enterprise Vault site by defining one or more *classification policies*. The policy options let you choose to do the following:

- Send items for classification and tag them with the results at the same time that Enterprise Vault 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 remain searchable during the rebuild.)
- Update the retention category of items when users manually delete them or Enterprise Vault automatically expires them—or optionally when Enterprise Vault indexes and archives the items.

After you have chosen the required policy options, you associate the classification policy with a *retention plan* and then apply the plan to one or more Enterprise Vault archives.

Test mode

Before you put your classification infrastructure into effect, you can identify and resolve any issues with it by running it in test mode. Classification does still occur in test mode, but Enterprise Vault writes the classification properties, their values, and any resulting retention changes to a report rather applying the changes to the archived items.

Overview of the procedure for setting up classification

Table 2-1 lists a series of steps with which you can set up classification with Enterprise Vault.

Table 2-1 Steps in the setup procedure

Step	Action	Description
Step 1	Ensure that the Enterprise Vault storage servers in your site meet the requirements for classification.	See "Prerequisites for classification" on page 14.
Step 2	Check that a suitable cache location exists on each Enterprise Vault storage server.	See "How Enterprise Vault caches the items that it submits for classification" on page 15.
Step 3	Familiarize yourself with the metadata properties of items in which Enterprise Vault stores classification values.	See "About the Enterprise Vault classification properties" on page 20.
Step 4	Set up the required classification property values.	See "Setting up new values for the Enterprise Vault classification properties" on page 28.
Step 5	Define the required classification rules.	See "About classification rules" on page 33.
Step 6	Configure one or more classification policies.	See "About classification policies" on page 46.
Step 7	Assign the classification policies to your archives by associating the policies with retention plans.	See "Associating classification policies with retention plans" on page 50.
Step 8	Verify the classification rules by running them in test mode.	See "About classification test mode" on page 56.
Step 9	Publish the classification properties and rules to other Enterprise Vault storage servers.	See "How to publish the classification properties and rules" on page 60.

Prerequisites for classification

To implement classification, you require all the following on all the Enterprise Vault storage servers in your site:

- Windows Server 2012 Original Release or R2.
  For performance reasons, we strongly recommend that you run Windows Server 2012 R2 on all Enterprise Vault servers, and not Windows Server 2012 Original Release.

- The File Server Resource Manager service and the associated tools feature (`fsrm.msc`).
  These components let you administer the Windows File Classification Infrastructure, so that you can create and edit classification rules and properties. In the Enterprise Vault Install Launcher, the **Prepare my system** option automatically enables the File Server Resource Manager service and tools.
- The Microsoft Data Classification Toolkit.
  To deploy the classification properties and rules across your Enterprise Vault site, you use Enterprise Vault PowerShell cmdlets, which work in combination with this toolkit. You can download it from the following page of the Microsoft website:
  https://msdn.microsoft.com/library/hh204743.aspx

You also require a license for the Enterprise Vault retention feature to manage classification. Classification operates in test mode if you have yet to install a license for the retention feature, or the existing license has expired.

Roles-based administration (RBA) and the classification feature

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

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

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

How Enterprise Vault caches the items that it submits for classification

At the start of the classification process, Enterprise Vault stores a plain-text version of each item that it is classifying in a nominated cache location on the storage server. Enterprise Vault then invokes the File Classification Infrastructure to perform immediate classification and retrieve the classification properties and their values. 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 18.

The name of each plain-text file has the following form:

```
EV$ + transaction_id + ~ + random_number + .txt
```

For example:

```
EV$60C32915D60F4FDFD748EE048DDAFCF1~01462D48.txt
```

The contents of each file comprise a number of the properties and associated values with which Enterprise Vault has indexed the item, in the form *name*:*value*. For instance, the following is a typical example of a classification file:

```
rtdn:Mike Smith
rtea:mike_smith@yourcompany.com
subj:The San Francisco event
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
cont:Are you going to be able to make it to the Metreon in San Francisco?
The event is at 11:30am on Monday.
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 the plain-text files and that you can configure your classification rules to search for.

See "About the Enterprise Vault properties" on page 62.

Limits on the size of classification files

By default, the File Classification Infrastructure can classify files that are up to 25 MB in size. When a text file exceeds this limit, Enterprise Vault automatically splits it into files that are approximately 25 MB in size, and classification then proceeds across the set of files. To determine where to split the files, Enterprise Vault operates as follows:

- If any single line in a text file causes the file to exceed the limit, Enterprise Vault places the line in a new text file. For example, the *cont* property line holds the content of an item and is usually the lengthiest line in the text file. In cases where this line and its predecessors exceed the limit, Enterprise Vault splits the file immediately before the line and creates a new file for the *cont* property.
- If the contents of a single line still exceed the limit, Enterprise Vault searches back from the limit until it finds a space character, and then splits the contents

there. If Enterprise Vault cannot find a space character within 300 characters, it splits the file precisely at the limit.

You can change the 25-MB limit by setting a registry entry, MaxTextFilterBytes. The following article on the Microsoft website describes this registry entry:

https://msdn.microsoft.com/library/ms692103.aspx

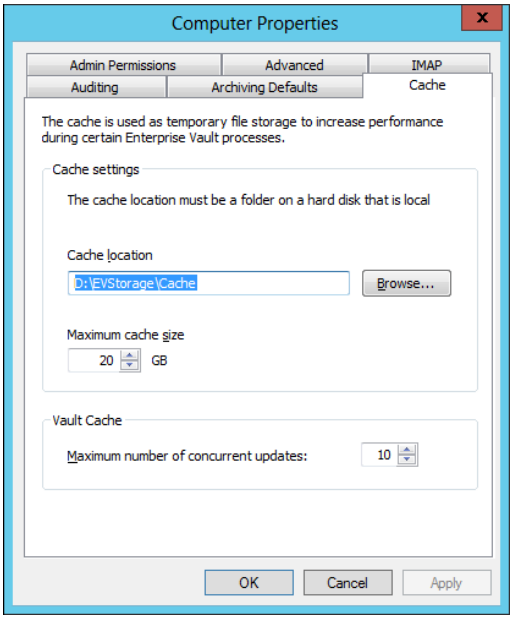
You may want to increase the limit if you have a complex rule that fails to match items because different parts of it match different files in the set. For example, this issue can arise if you have a rule that searches for both of the words *fraud* and *corruption*, when the first word is in one text file and the second word is in another.

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.

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.

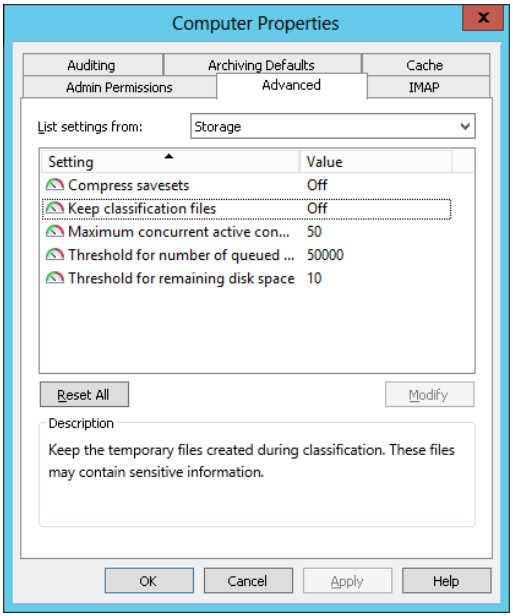
To configure Enterprise Vault to keep the classification files in the cache folder

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.

Chapter 3

Setting up the classification properties

This chapter includes the following topics:

About the Enterprise Vault classification properties

When an item matches a classification rule that you have defined, Enterprise Vault records the fact in the metadata properties of the item. The chosen property and the value that Enterprise Vault assigns to it determine what Enterprise Vault does with the item. As Table 3-1 explains, Enterprise Vault can process the classification values that are stored in four such properties.

Table 3-1 Enterprise Vault classification properties

Property	Description
evtag.category	This property assigns one or more category values to an item when the item is added to Enterprise Vault. For example, some of the example classification rules check the contents of items for credit card numbers and assign the category value "PII" (for "personally identifiable information") to those that do. You can search for the assigned property values in applications such as Enterprise Vault Search, Compliance Accelerator, and Discovery Accelerator.
evtag.exclusion	In environments where you use 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.) For example, the example classification rules use this property to exclude auto-generated news feeds, charity solicitations, and other unimportant items from Compliance Accelerator review sets. You can search for the assigned property values in applications such as Enterprise Vault Search, Compliance Accelerator, and Discovery Accelerator.
evtag.inclusion	In environments where you use 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. For example, the example classification rules use this property to include Company Confidential items and items that contain financial or legal data in Compliance Accelerator review sets. You can search for the assigned property values in applications such as Enterprise Vault Search, Compliance Accelerator, and Discovery Accelerator.

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

Property	Description
evaction.discard	By assigning the name of a retention category to this property of an item, you can mark the item for deletion. For example, one of the example classification rules uses this property to delete automated out-of-office messages. The way in which Enterprise Vault handles such items depends on the point at which it classifies them. ■ **During indexing**. If an item is classified when Enterprise Vault indexes it, Enterprise Vault sets the retention category of the item to the evaction.discard property value. 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. This property overrides the other classification properties, such as evtag.inclusion. So, if one classification rule marks an item for deletion then it is deleted, even if a second rule tags the item for inclusion in a Compliance Accelerator review set. 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.

All four properties are of type Multiple Choice List: you can assign several values to them. For example, an email that the example classification rules have processed could have two values assigned to its evtag.category property, "Many attachments" and "Personal", to indicate that it has ten or more attachments and that its author has assigned a sensitivity level of Personal to it. The evaction.discard property differs slightly because although it too is a Multiple Choice List property, Enterprise Vault uses the first assigned value only.

Setting up the Enterprise Vault classification properties manually

Enterprise Vault automatically sets up the four Enterprise Vault classification properties when you import the example rule set.

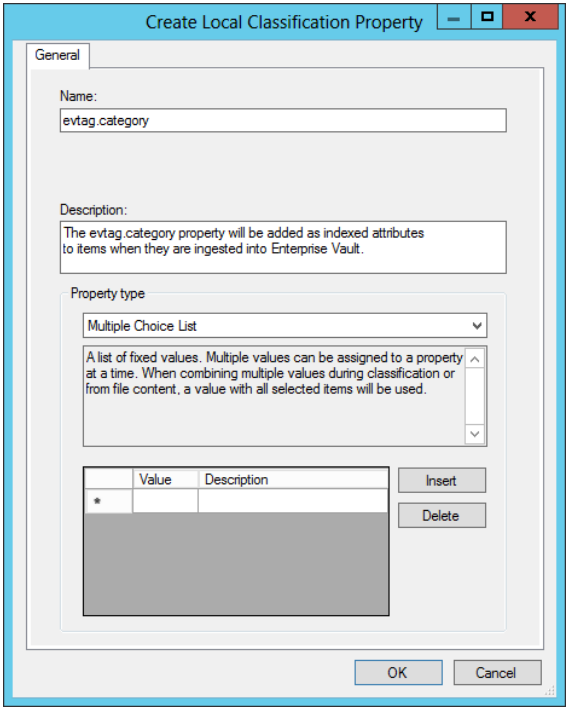
See "Importing the example rule set" on page 37.

If you do not import the rule set, you can still set up the properties manually.

To set up the Enterprise Vault classification properties manually

1. In the left pane of the File Server Resource Manager, expand the **Classification Management** container.
2. Right-click the **Classification Properties** node, and then click **Create Local Property**.

   The **Create Local Classification Property** dialog box appears.



3. Type the name and description of the new property.

   The required names and suggested descriptions are as follows:

evtag.category	Assigns one or more categories to an item when the item is added to Enterprise Vault. The property values are searchable and retrievable.
evtag.exclusion	Stops Compliance Accelerator from sampling an item that has this property. The property values are searchable and retrievable.
evtag.inclusion	Requires Compliance Accelerator to sample an item that has this property. The property values are searchable and retrievable.
evaction.discard	Marks an item for deletion if the name of a retention category is assigned to the property.

4. Set the property type to **Multiple Choice List**.
5. Add the values that your classification rules may assign to the property.
6. Click **OK** to save the classification property.
7. Repeat steps 2 through 6 for each of the other Enterprise Vault classification properties.

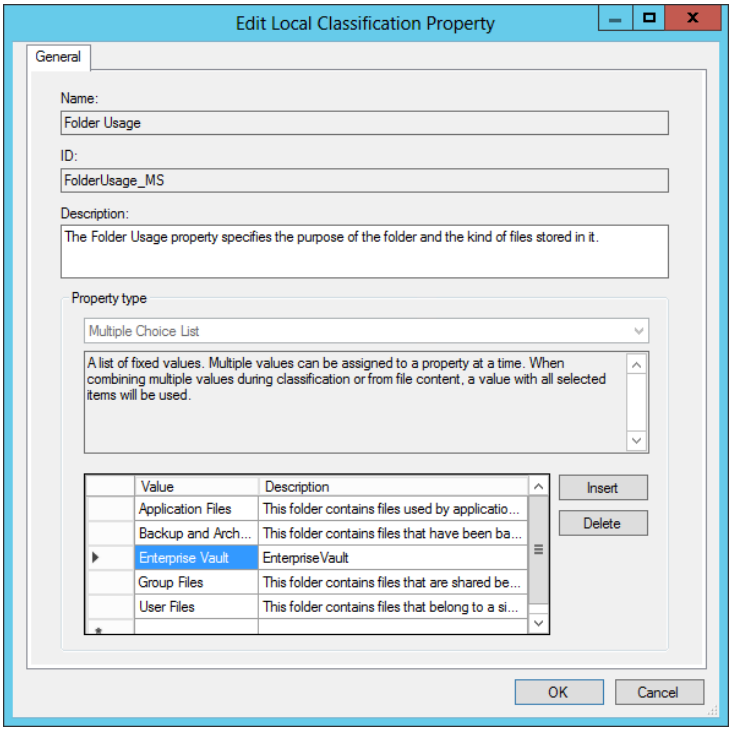
Checking the Folder Usage classification property

The Folder Usage property is a built-in classification property that tells the File Server Resource Manager about the purpose of certain folders on the local server and the kind of files that are stored in them. When you install Enterprise Vault and start the Storage service, it automatically adds an entry to the Folder Usage list that specifies the location of the classification cache folder. If you want to check that this entry is correct, you can do so by following the procedure below.

To check the Folder Usage classification property

1. In the left pane of the File Server Resource Manager, expand the **Classification Management** container.
2. Click the **Classification Properties** node to display the list of configured properties at the right.
3. Right-click the **Folder Usage** property, and then click **Edit Local Property**.

   The **Edit Local Classification Property** dialog box appears.
4. Check the list at the bottom of the dialog box. If there is no **Enterprise Vault** value in the list, you must add one.

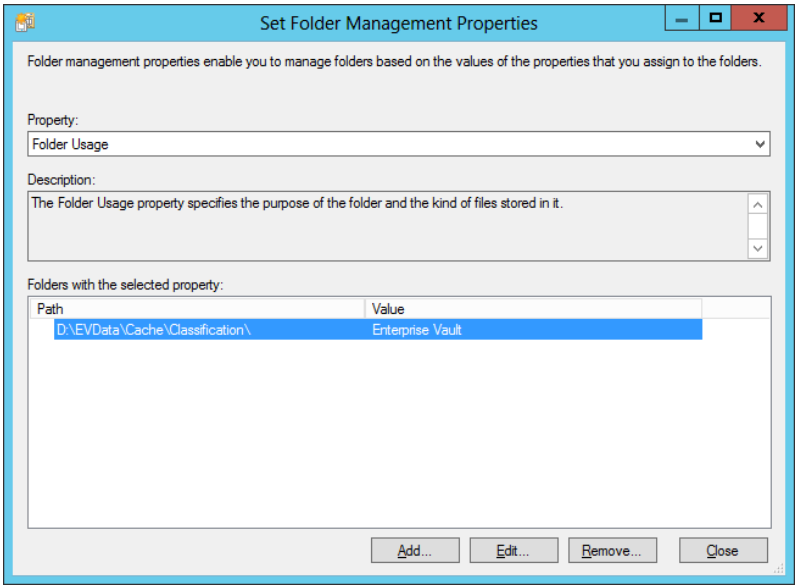


5 Click **OK** to save any changes that you have made and close the dialog box.

6 In the **Actions** pane at the right of the File Server Resource Manager, click **Set Folder Management Properties**.

7 In the **Property** list, choose **Folder Usage**.

8 In the **Folders with the selected property** area, ensure that there is an **Enterprise Vault** value and that it is mapped to the `Classification` subfolder of the server's Enterprise Vault cache location. For example:



9 Add the **Enterprise Vault** value and the associated folder path, if necessary.

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 classification rule:

- You have configured the classification policy to set the retention category of items.
  See "About classification policies" on page 46.
- The classification property value that the rule assigns to the item matches the name of an existing retention category. For example, if both the property value and the retention category are named "Financial", this is the retention category that Enterprise Vault tries to assign when it classifies the item.
  For instructions on how to create retention categories, see the *Administrator's Guide*.

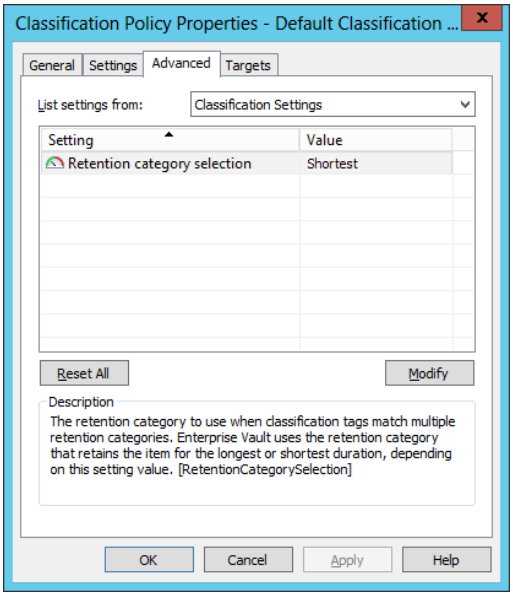
An item may sometimes match several classification rules, all of which are competing to assign a retention category to it. Where this is the case, the classification feature selects the winning retention category as follows:

- 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 rule 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.

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**.

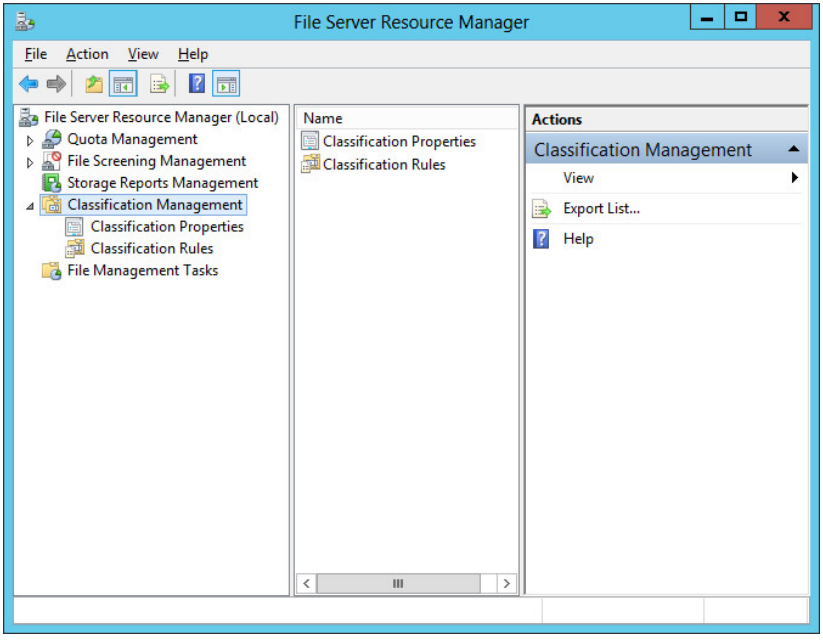


Setting up new values for the Enterprise Vault classification properties

You must configure the Enterprise Vault classification properties to receive the range of values that you want your classification rules to assign to those properties. For example, a rule that searches for instances of bad language in items may need to assign the value "Profanity" to the evtag.category property of any matching items. Before this can happen, you must add "Profanity" as a possible value for the evtag.category property.

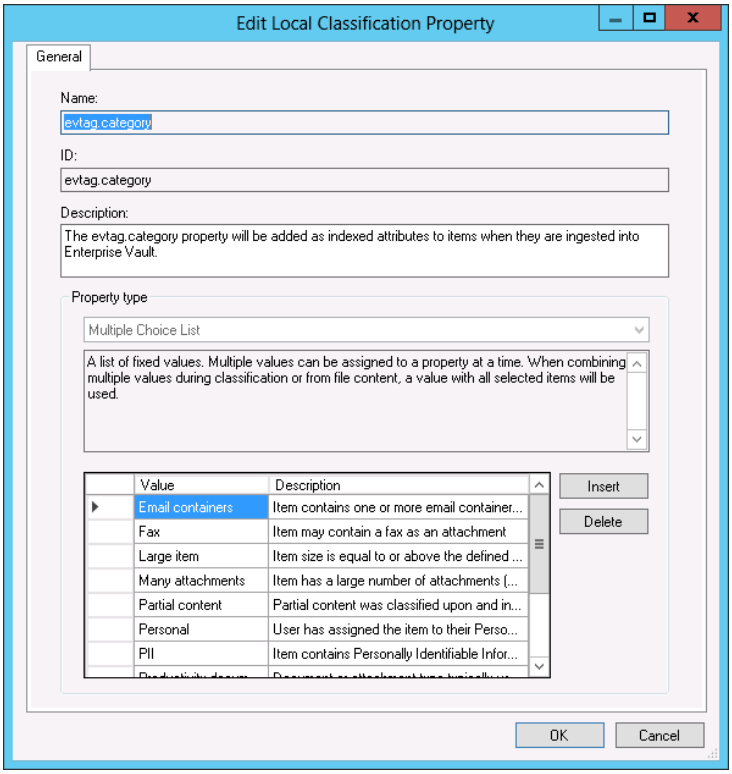
To set up a new value for an Enterprise Vault classification property

1 In the left pane of the File Server Resource Manager, expand the **Classification Management** container.



2 Click the **Classification Properties** node, and then double-click the Enterprise Vault property for which you want to set up one or more new values.

The **Edit Local Classification Property** dialog box appears. For example, in the case of the evtag.category property, the dialog box looks like this:



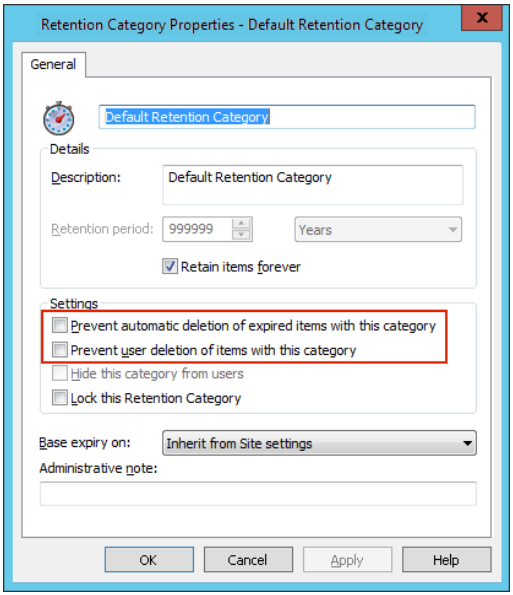
3 Click **Insert** to add a new value and description. To delete an unwanted value, click it and then click **Delete**. You cannot delete a value if it is in use in one or more classification rules.

4 Click **OK** to save the changes that you have made.

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 users from manually deleting items to which the category is assigned. Or you configure the retention category to prevent the automatic deletion of expired items with this category.



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 move the items from one folder to another folder that has a different retention category. This can potentially override the retention categories that the classification feature has set. However, you can choose to prevent retention category updates for moved items when you define a classification policy.
  See "About classification policies" on page 46.
  If you do not use the classification policy to prevent retention category updates for moved items, 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, Enterprise Vault waits until the old, later date before it deletes the item.

Chapter 4

Configuring your classification rules

This chapter includes the following topics:

About classification rules

A classification rule defines the criteria that an item must match to be awarded a specific classification value. For example, a rule that looks for emails that the sender has marked as unimportant may assign the value "Low importance" to those that it finds.

Enterprise Vault comes with a set of example classification rules, which you can import into the File Server Resource Manager and use as a starting point to create your own set of rules. Alternatively, you can create your own rules from the beginning.

About the example classification rules

Note: The example rules are for test purposes only and may not deliver the required results in a production environment.

The example rules are in a single XML file, `Example Rules.xml`, which is in the `Classification` subfolder of the Enterprise Vault program folder; for example, `C:\Program Files (x86)\Enterprise Vault\Classification\Example Rules.xml`.

The example rules have the following features in common:

- They have a scope of "Enterprise Vault": they classify items in the Enterprise Vault classification cache folder only.
  See "Checking the Folder Usage classification property" on page 24.
- They use the Veritas Information Classifier method to search for strings and regular expression patterns in items.
  See "Creating or changing classification rules" on page 38.
- When the rules find a match, they assign an appropriate value to one of the four Enterprise Vault classification properties on the matching item: evtag.category, evtag.exclusion, evtag.inclusion, or evaction.discard.
  See "About the Enterprise Vault classification properties" on page 20.
  For example, some of the rules search for strings in the form of credit card numbers. If the rules find an item that contains such a string, they assign the value "PII" to the item's evtag.category property, to indicate that the item contains personally identifiable information.

Table 4-1 describes the classification rules in the example rule set.

Table 4-1 Example classification rules

Rule name	Description	Property used	Assigned value
American Express Card	Detects items that may contain American Express credit card numbers.	evtag.category	PII
Auto-generated News Feeds	Detects items from the email domains of known news and research providers (alerts.yahoo.com, cnn.com, news.google.com, and so on).	evtag.exclusion	Auto-generated

Table 4-1 Example classification rules *(continued)*

Rule name	Description	Property used	Assigned value
Auto-Reply	Detects out-of-office messages.	evaction.discard	Default Retention Category
Charity Solicitations	Detects items containing terms and phrases that are commonly associated with charitable solicitations.	evtag.exclusion	Charity solicitations
Company Confidential	Detects items that were tagged in Microsoft Outlook as being Company Confidential.	evtag.inclusion	Company Confidential
CPF Number (Brazil)	Detects items that may contain Brazilian CPF numbers and associated words or phrases.	evtag.category	PII
Current Retention Category Name	Detects items that had an Enterprise Vault retention category named "1 Month" when they were submitted for classification.	evtag.category	Short retention
Date range	Detects items that were sent within a specified date range.	evtag.inclusion	Sensitive project
Discover Card	Detects items that may contain Discover Card credit card numbers.	evtag.category	PII
Driving License (UK)	Detects items that may contain UK driving license numbers.	evtag.category	PII
Email Containers (Attachments)	Detects items that have an attachment of type PST or NSF.	evtag.category	Email containers
Faxes (Attachments)	Detects fax attachments.	evtag.category	Fax
Financial Data	Detects items containing terms and phrases that are commonly associated with financial transactions.	evtag.inclusion	Financial

Table 4-1 Example classification rules *(continued)*

Rule name	Description	Property used	Assigned value
Identity Card (Germany)	Detects items that may contain current identity card numbers (issued in Germany since 2010).	evtag.category	PII
Large Items	Detects items that are 1000 KB or larger.	evtag.category	Large item
Large Number of Attachments	Detects items that have 10 or more attachments.	evtag.category	Many attachments
Legal	Detects items containing terms and phrases that are commonly associated with legal documents.	evtag.inclusion	Legal
Low Importance	Detects items that were tagged in Microsoft Outlook as being of low importance.	evtag.exclusion	Low importance
MasterCard	Detects items that may contain MasterCard credit card numbers.	evtag.category	PII
Message Sent to External Domain	Detects items that were sent to an external recipient.	evtag.inclusion	Sent externally
Message Sent to Specific External Domain	Detects items that were sent externally to a specific domain.	evtag.inclusion	Sent externally
National Insurance Number (UK)	Detects items that may contain UK national insurance numbers.	evtag.category	PII
National Registry Identification Number (Singapore)	Detects items that may contain Singaporean national registry identification numbers.	evtag.category	PII
Partial Content	Detects items for which Enterprise Vault was only able to supply partial content for classification (because, for example, their content was encrypted).	evtag.category	Partial content

Table 4-1 Example classification rules *(continued)*

Rule name	Description	Property used	Assigned value
Permanent Account Number (India)	Detects items that may contain Indian permanent account numbers and associated words or phrases.	evtag.category	PII
Personal	Detects items that were tagged in Microsoft Outlook as being Personal.	evtag.category	Personal
Productivity Documents	Detects items that have attachments in Microsoft Word or Excel format.	evtag.category	Productivity documents
Sensitive Project Code Names	Detects items that contain the user-defined code name of a project that is considered sensitive.	evtag.inclusion	Sensitive project
Social Security Number (US)	Detects items that may contain US social security numbers.	evtag.category	PII
VAT/TVA number (France)	Detects items that may contain French VAT/TVA numbers.	evtag.category	PII
Visa Card	Detects items that may contain Visa credit card numbers.	evtag.category	PII
Web Links	Detects items that include web links.	evtag.category	Web links

Importing the example rule set

If you decide to use the example rule set as the basis for your own classification rules, you can import it into the File Server Resource Manager on a selected Enterprise Vault storage server. Then, after you have configured the rules appropriately, you can publish them to the other storage servers in your environment.

To import the example rule set

1. Make sure that you have a copy of the example rule set file, `Example Rules.xml`. The file is installed in the `Classification` subfolder of the Enterprise Vault program folder.
2. Start the Enterprise Vault Management Shell.

   PowerShell opens and loads the Enterprise Vault snap-in. The cmdlets are now available in the shell.
3. Run the cmdlet `Import-EVClassificationRules` to import the rules.

   See "Import-EVClassificationRules" on page 84.

   For example, you might type the following:

   ```
   Import-EVClassificationRules -ImportRulesFile "c:\Program Files (x86)\Enterprise Vault\Classification\Example Rules.xml" -Servers localhost
   ```

   The cmdlet stops the Enterprise Vault Storage service on the server and then, after it has imported the classification properties and rules, it restarts the service.

Creating or changing classification rules

The following procedure guides you through the process of creating or changing a classification rule with the File Server Resource Manager. Each rule sets the value for a single classification property.

Caution: The simpler the rule, the more quickly Enterprise Vault classifies the matching items. Avoid overly complex rules, where possible.

To create or change a classification rule

1. In the left pane of the File Server Resource Manager, expand the **Classification Management** container.
2. Do one of the following:

   - To create a new rule, right-click the **Classification Rules** node and then click **Create Classification Rule**.
   - To change an existing rule, click the **Classification Rules** node and then double-click the rule.

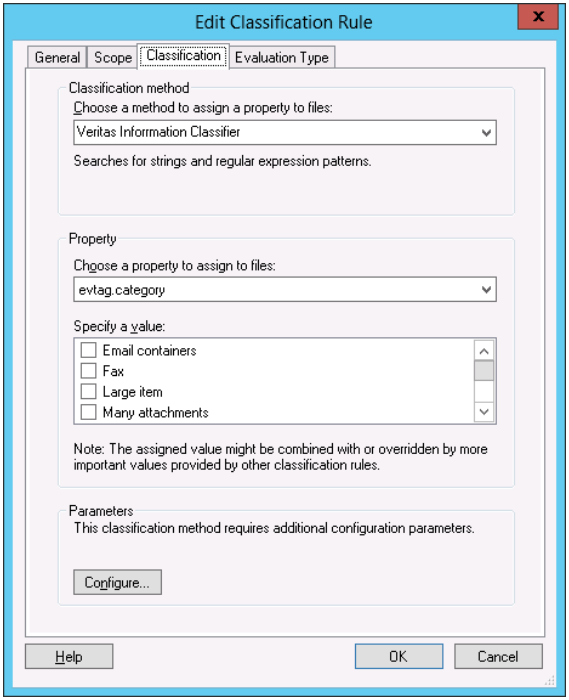
   A dialog box appears in which you can set the properties of the rule.
3. On the **General** tab, enter the following information:

- **Rule name**. Type a name for the rule.
- **Enabled**. This rule is only applied if the **Enabled** box is checked. To disable the rule, uncheck this box.
- **Description**. Type an optional description for this rule.

4 On the **Scope** tab, in the first box, check **Enterprise Vault** to specify that you want to include the Enterprise Vault classification cache folder.

5 On the **Classification** tab, enter the following information:

- In the **Classification method** section, choose the method with which you want to assign an Enterprise Vault classification property to items.



The classification methods that are listed are as follows:

- **Content Classifier**. This method provides string and regular expression matching against the items.
- **Folder Classifier**. This method does not work with the Enterprise Vault classification feature, so do not choose it.
- **Windows PowerShell Classifier**. This method lets you write rules using PowerShell.

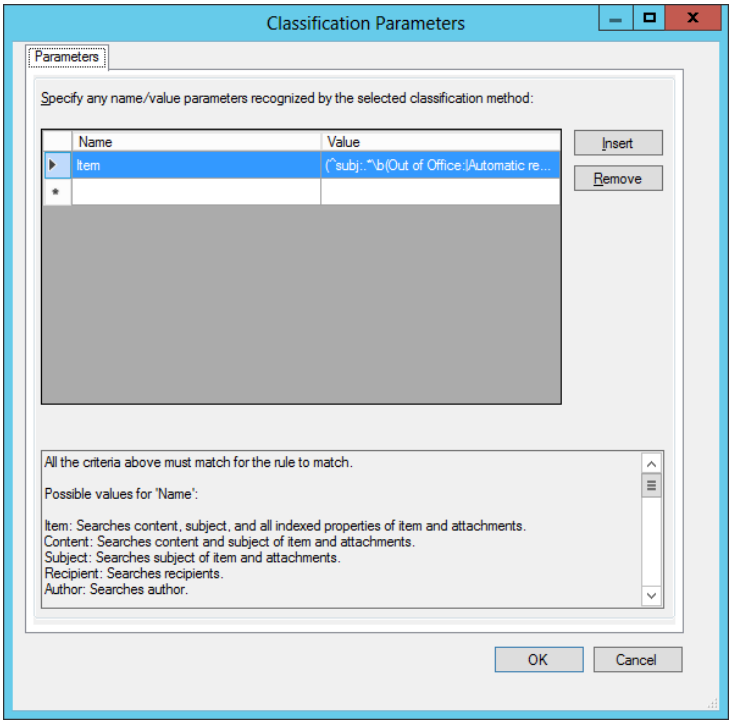
- **Veritas Information Classifier**. This method provides string, regular expression, and word proximity matching against items.

  Note: We recommend that you use the Veritas Information Classifier method rather than the alternative classification methods, as it has been expressly designed to process rules in the most efficient way: Processing multiple rules in parallel, ordering rules by average execution time and, for rules that contain multiple clauses, evaluating the quickest clause first. The Veritas Information Classifier also lets you target particular parts of messages only, such as their subject lines, so there is no need to search across the entire contents of items. The consequence of all these enhancements is drastically to reduce the overall rule processing time.

  Veritas Information Classifier has an additional advantage over other, similar methods, such as Content Classifier: You can export a set of rules that use the Veritas Information Classifier method from a server that is running one language version of Windows, such as English, and import them without problem into a server that is running another language version, such as Japanese. This is not the case when you export and import rules that use the Content Classifier method.

  The list may also include third-party classification methods, if you have installed any.

- In the **Property** section, choose the Enterprise Vault classification property to assign to items, and set the value of the property.
  See "About the Enterprise Vault classification properties" on page 20.
- In the **Parameters** section, click **Configure** to specify the content for which the rule is to search. For example:



For classification rules that use the Veritas Information Classifier method, you can specify a range of name and value parameters.

See "Supported configuration parameters for rules that use the Veritas Information Classifier method" on page 41.

6 Click **OK** without selecting any of the options on the **Evaluation Type** tab. Enterprise Vault does not take account of the settings on this tab.

Supported configuration parameters for rules that use the Veritas Information Classifier method

When you create a rule that uses the Veritas Information Classifier method, you must specify one or more additional configuration parameters. These parameters define the text strings or regular expressions for which you want to search in items. Each parameter consists of a *name* and a corresponding *value*.

You can specify multiple configuration parameters for the same rule. For example, you may want to create a rule that searches the subject lines of items for one word and their message bodies for a second word. Where this is the case, an item must

match all the parameters for the rule to match; the Veritas Information Classifier links the parameters together with Boolean AND operators rather than OR operators.

Note: To simulate the effect of linking multiple parameters with Boolean OR operators, create multiple rules that assign the same value to the same classification property. For example, you might create two rules that assign the same value to the evtag.category property: one rule that searches the subject lines of items for a word and a second rule that searches their message bodies for a different word.

Supported values for Name

The values that you type in the **Name** column of the **Classification Parameters** dialog box set the scope of the configuration parameter: they specify the properties of an item that you want to search.

You can search an individual property by typing its name in the **Name** column. For example, you might type *cont* to search the message body of an item or *rbea* to search the email addresses of its recipients. 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 the plain-text files in the classification cache folder.

See "About the Enterprise Vault properties" on page 62.

If you want to classify the items in one archive only, the *archiveid* property lets you specify the unique identifier of this archive. For example, by specifying an *archiveid* property value in one configuration parameter and a *cont* property value in a second configuration parameter, you can limit classification to the items in the nominated archive that have particular words in their message bodies.

A number of composite properties are also available with which you can search multiple properties of items at once. Table 4-2 describes these values.

Table 4-2 Composite properties

Name	Description
Attachment	Searches all the attachment-related properties: content, file name, size, type, and dates.
Author	Searches the author properties.
Content	Searches both the subject line and content of items and their attachments.
Item	Searches the item in its entirety: subject line, content, and all the classifiable properties of items and their attachments.

Table 4-2 Composite properties *(continued)*

Name	Description
Recipient	Searches the recipient list properties.
Subject	Searches the subject lines of items and their attachments.

You can combine multiple properties in a single Name value by separating them with a pipe symbol (|). For example, the following Name value is equivalent to the composite value *Subject* because it lets you search the subject lines of an item (*subj*) and its attachments (*a_subj*).

```
subj|a_subj
```

The next example searches the subject lines of an item and its attachments (*Subject*) and the content of those attachments (*a_cont*).

```
Subject|a_cont
```

Supported values for Value

In the **Value** column of the **Classification Parameters** dialog box, you specify what to search for: a word or phrase, for example, or a regular expression.

By default, the values that you enter are case-insensitive. So, the value *Fraud* matches not just *Fraud* but *fraud* and *FRAUD* as well. However, you can make a value case-sensitive by preceding it with *(?-i)*. For example, *(?-i)Fraud* matches *Fraud* only.

Specify date and time values as Coordinated Universal Time (UTC) values in the ISO 8601 format. According to ISO 8601, a combined date and time value has the following format:

yyyy-mm-dd`T`*hh*`:`*mm*`:`*ss*`Z`

For example, `2016-07-12T13:00:00Z`.

Table 4-3 describes the types of values that the Veritas Information Classifier supports.

Table 4-3 Supported values in the Value column

Value	Description
A string	Searches for the specified word or phrase, such as *fraud* or *cover up*.

Table 4-3 Supported values in the Value column *(continued)*

Value	Description
A regular expression	Searches for the specified regular expression. A regular expression 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` The regular expression *docx?* matches both *doc* and *docx*, so it is useful if you want to search for Microsoft Word documents. Your regular expressions must conform to the .NET Framework regular expression syntax. For more information on this syntax, see the following articles on the Microsoft website: https://msdn.microsoft.com/library/az24scfc.aspx http://go.microsoft.com/fwlink/?LinkId=180327 For many illustrations of regular expression syntax, see the example classification rules. See "About the example classification rules" on page 34.

A proximity search	Searches for words or regular expressions that are within the specified number of characters of each other. Punctuation and space characters count as normal characters. The syntax is as follows:
	`NEAR[proximity,regular_expression,regular_expression]`
	For example, type the following to find *fraud* and *cover up* within 100 characters of each other:
	`NEAR[100,fraud,cover up]`
	Type the following to find *fraud* and either *cover up* or *write off* within 150 characters of each other:
	`NEAR[150,fraud,(cover up|write off)]`

Table 4-3 Supported values in the Value column *(continued)*

Value	Description

A list of strings or regular expressions	Searches for multiple words, phrases, or regular expressions. The syntax is as follows:
	`LIST[`*`string_or_regular_expression`*`|`
	`string_or_regular_expression``|...]`
	For example, to find *cost of sales*, *earnings per share*, or *financial expenses*, type the following:
	`LIST[cost of sales|earnings per share|financial expenses]`
	If you want to enter a list that contains many hundreds of words or phrases, you may be able to maximize performance with the following, alternative syntax:
	`LARGELIST[`*`string1`*`|`*`string2`*`|`*`string3`*`|...]`
	LARGELIST uses a different method for evaluating the list against the item properties. You can further enhance performance by placing the words or phrases that are most likely to find a match at the start of the list. You cannot use regular expressions with the LARGELIST syntax.

A date range	For use with date-type properties only, such as *adat*, *date*, and *mdat*. Searches for items with a date property value that falls within the specified date range. Ranges can be open-ended. The syntax is as follows: ■ *YYYY-MM-DD..YYYY-MM-DD* For example, `2016-01-20..2016-06-19` finds items between these two dates. ■ *YYYY-MM..YYYY-MM* For example, `2015-01..2016-07` finds items between these two months. ■ *YYYY..YYYY* For example, `2015..2016` finds items between these two years. ■ *YYYY-MM-DD..* For example, `2016-01-20..` finds items after this date. ■ *..YYYY-MM-DD* For example, `..2016-01-20` finds items before this date. The dates are in the current time zone on the Enterprise Vault storage server.

Chapter 5

Defining and applying classification policies

This chapter includes the following topics:

About classification policies

A 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 classification rules. 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, the classification feature can update the retention categories of items. To determine which retention category to assign, Enterprise Vault examines the property values that the classification rules have assigned to the item. When the name of a property value matches that of one of the site's retention categories, Enterprise Vault assigns this retention category to the item.
  See "How classification property values and retention categories interact" on page 26.
- **Prevent retention category updates for moved items**. By default, Enterprise Vault updates the retention categories of archived items when users move the items from one folder to another folder that has a different retention category. This can potentially override the retention categories that the classification feature has set. With a 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 moving the items changes their record types.
- 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

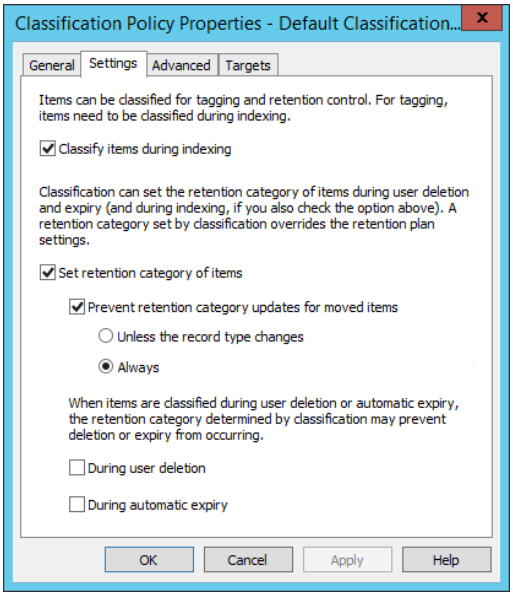
content sources. For example, your classification requirements for File System items may be different from those for Exchange mailbox items. Where this is the case, you can define a classification policy for each content source and then associate the two policies with different retention plans: one targeted 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 49.

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.

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 5-1 PowerShell cmdlets for creating or modifying classification policies

Cmdlet	Description
`Get-EVClassificationPolicy`	Returns a list of all the classification policies that you have configured in an Enterprise Vault site. See "Get-EVClassificationPolicy" on page 74.
`New-EVClassificationPolicy`	Creates a classification policy. See "New-EVClassificationPolicy" on page 76.
`Remove-EVClassificationPolicy`	Removes the specified classification policy, if it is not in use. See "Remove-EVClassificationPolicy" on page 80.
`Set-EVClassificationPolicy`	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*.

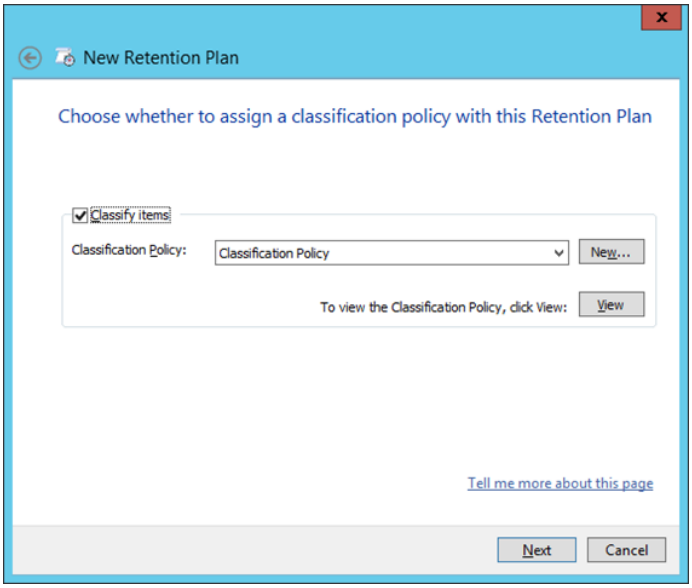
The following procedure describes how to use the Administration Console to associate a classification policy with a retention plan. However, you can also perform the same activity with PowerShell cmdlets.

See "About the PowerShell cmdlets for working with retention plans" on page 52.

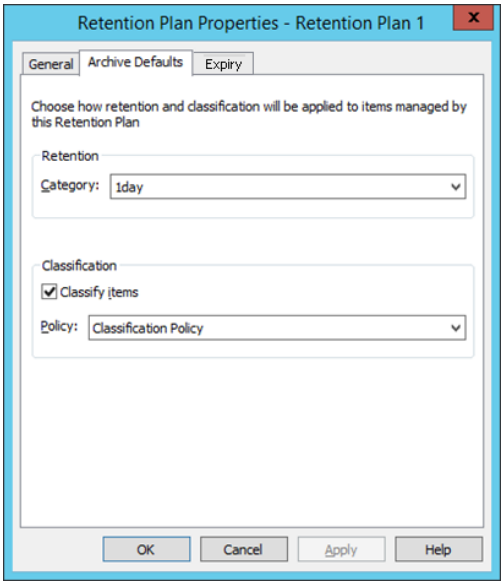
To associate a classification policy with a retention plan

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 check the **Classify items** option and then select the required classification policy.



- 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 5-2 PowerShell cmdlets for creating or modifying retention plans

Cmdlet	Description
`Get-EVRetentionPlan`	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.
`New-EVRetentionPlan`	Creates a retention plan and specifies the classification policy to associate with it.
`Remove-EVRetentionPlan`	Removes the specified retention plan, if it is not in use.

Table 5-2 PowerShell cmdlets for creating or modifying retention plans *(continued)*

Cmdlet	Description
`Set-EVRetentionPlan`	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.

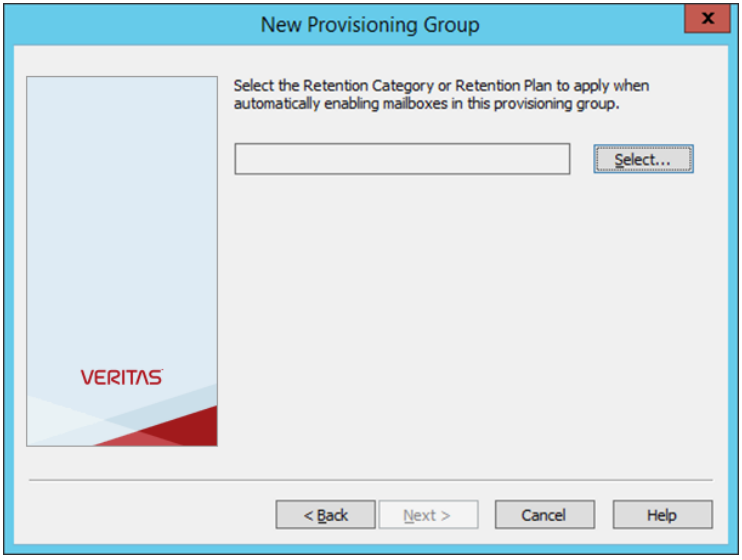
After you have associated the retention plan with the required feature, you must run the appropriate archiving task to apply it to the target archives. For instance, this is the Client Access Provisioning task in the case of an IMAP provisioning group or the Sharepoint Archiving task in the case of a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

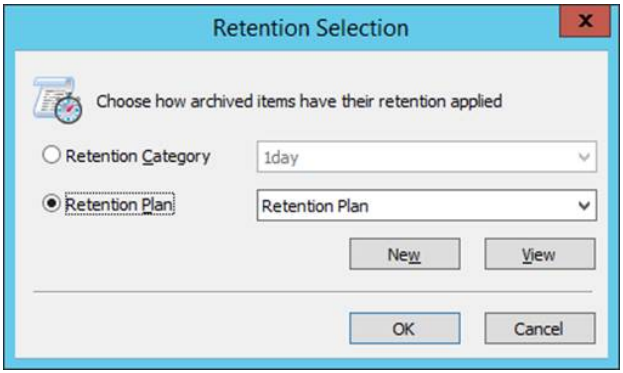
To associate a retention plan with an Exchange provisioning group

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 though 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**.

Chapter 6

Running classification in test mode

This chapter includes the following topics:

About classification test mode

By running the classification feature in test mode, you can identify and resolve any issues with your classification rules 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 extend the item's retention period or apply a retention category that blocks manual deletion or automatic expiry.

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

Implementing classification test mode

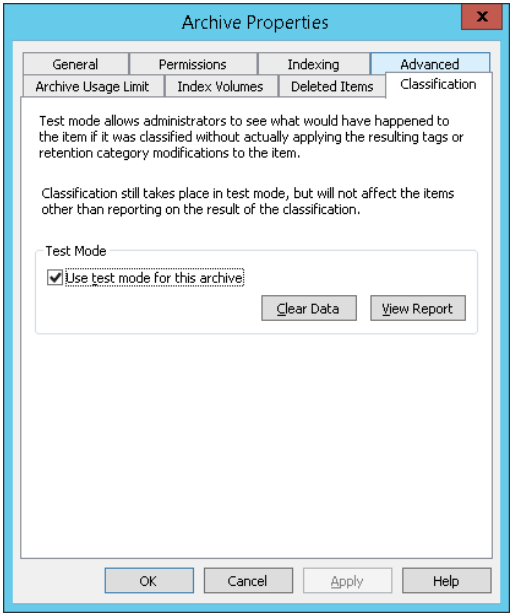
You implement classification test mode on individual archives. Only archives to which you have assigned a retention plan that has an associated classification policy are eligible for test mode.

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 58.

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. Check **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 6-1 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 92.
`Set-EVClassificationTestMode`	Enables or disables classification test mode in the nominated archive. See "Set-EVClassificationTestMode" on page 93.

Understanding the classification test mode reports

As Table 6-2 indicates, a classification test mode report contains several sections.

Table 6-2 Contents of a classification test mode report

This section	Shows
Rule Matches	The classification rules that the items match, and the number of items in each case.

Table 6-2 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 that match a classification rule whose assigned property value is the same as that of a retention category—and hence to which Enterprise Vault would apply the category.
Proposed Changes to Retention	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. This section also shows the number of items that would be eligible for expiry if Enterprise Vault were to classify them now.
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.

Chapter 7

Publishing classification properties and rules across your site

This chapter includes the following topics:

How to publish the classification properties and rules

When you are satisfied that your classification properties and rules work as expected, you can publish them to the other storage servers in your Enterprise Vault environment. To do this, run the PowerShell cmdlet `Import-EVClassificationRules` or `Publish-EVClassificationRules`.

See "Import-EVClassificationRules" on page 84.

See "Publish-EVClassificationRules" on page 87.

These two cmdlets perform a similar function. The difference is that `Publish-EVClassificationRules` first exports the classification properties and rules to an XML file before it publishes them to the target servers; `Import-EVClassificationRules` uses an existing XML file to perform the import part of the operation only.

For example, the following exports the classification properties and rules to the file `RulesFile.xml`, which it then publishes to all the Enterprise Vault servers in the specified site:

```
Publish-EVClassificationRules -StagingServer SERVERXYZ
-ExportRulesPath c:\Data\RulesFile.xml -SiteId 13E...EV.example.com
```

Other methods for publishing the classification properties and rules are available, such as running the PowerShell cmdlets that come with the Microsoft Data Classification Toolkit. However, these methods do not automatically turn off the Enterprise Vault Storage services on the target servers while they install the new classification properties and rules. As this can lead to classification errors, we recommend that you use the Enterprise Vault classification cmdlets instead. These cmdlets do stop the Storage service before they begin the installation, and then restart it afterwards.

Appendix A

Enterprise Vault properties for use in classification rules

This appendix includes the following topics:

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 File Classification Infrastructure for classification. When you create a rule that uses the Veritas Information Classifier method, you can configure it to search the values of these individual properties.

See "Supported configuration parameters for rules that use the Veritas Information Classifier method" on page 41.

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 `Get-EVArchive` 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.
auea	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.
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: ■ 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.
cont	String	The content of the item, up to the limit that the Windows File Classification Infrastructure imposes. See "Limits on the size of classification files" on page 16.
cpnm	String	The name of the extension content provider.
crcn	String	The current retention category name.
crre	Integer	Calendar recurrence exception.
crrp	String	Calendar recurrence pattern.
crrt	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.
dtyp	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.
isrc	String	Whether Enterprise Vault has marked the item as a record (True) or not (False). For use with Capstone and other approaches to records management. Can be referenced by either "isrecord" or "isrc". Not supported by queries that target 32-bit volumes.
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.
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.
rcid	String	The record ID of the item. For use with Capstone and other approaches to records management. Can be referenced by either "recordid" or "rcid". 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.
rtyp	String	The record type of the item, such as permanent or temporary. For use with Capstone and other approaches to records management. Can be referenced by either "recordtype" or "rtyp". Not supported by queries that target 32-bit volumes.

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

Property	Type	Description
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_cont*, *a_subj*, 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
a_comr	String	The reason for missing content (encrypted content, converter error, and so on). See the description of the *comr* property for more details. See "System properties" on page 63.
a_cont	String	The content of the attachment, up to the limit that the Windows File Classification Infrastructure imposes. See "Limits on the size of classification files" on page 16.
a_date	Date	The created, sent, received, or archived date of the attachment.
a_dtyp	String	The data type of the attachment. For example, DOCX, XLSX, or MSG.
a_mdat	Date	The last-modified date of the attachment.

Table A-2 Enterprise Vault attachment properties *(continued)*

Property	Type	Description
a_size	Number	The size of the attachment in KB.
a_subj	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	Provides the following details for an item that Enterprise Vault's Move Archive feature has copied: ■ The date and time at which the item was copied. ■ The identifier of the source archive. ■ The saveset identifier of the source item. The format is as follows: *UTC_datetime_of_copy*,*source_archive_ID*, *source_item_Saveset_ID* If an archive has been moved several times, there is a value for each move.
Vault.JournalType	String	For journal messages, the journal type. The options are as follows: ■ E2003 ■ E2007 ■ E2007ClearText ■ E2007RMS

Table A-3 Custom Enterprise Vault properties *(continued)*

Property	Type	Description
Vault.MsgDirection	String	The message direction. The options are as follows: ■ 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	The message type. The options are as follows: ■ 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.
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.

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

Property	Type	Description
EVSP.UniqueId	String	The GUID that uniquely identifies the item.
EVSP.Version	String	The version of the SharePoint document.
EVSPP.Attachments	String	Whether the item has attachments: true or false. This property applies to social content only, except for Wikis.
EVSPP.*display_name*	String	The display name of the archived item.
EVSPP.*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: ■ 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 built-in classification feature that was introduced in Enterprise Vault 12.)

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.

Table A-8 Custom properties for Enterprise Vault SMTP Archiving *(continued)*

Property	Type	Description
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.

Appendix B

PowerShell cmdlets for use with classification

This appendix includes the following topics:

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.

Get-EVClassificationPolicy

`Get-EVClassificationPolicy` returns a list of all the classification policies that are configured in an Enterprise Vault 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-1 Get-EVClassificationPolicy parameters

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

Examples

- `Get-EVClassificationPolicy`

  Returns a list of all the 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 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 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-2 Get-EVClassificationPolicy properties

Name	Type	Description
Name	String	The name of the classification policy.
EntryId	String	The directory entry ID of the classification policy.
IsADefaultPolicy	Boolean	Whether the 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 move the items from one folder to another folder that has a different retention category.

Table B-2 Get-EVClassificationPolicy properties *(continued)*

Name	Type	Description
AllowRCOnRecTypeChange	Boolean	Whether to allow retention category updates for moved items when this will change their record type (for example, from Temporary to Permanent).
Description	String	The description of the classification policy.
SiteId	String	The site ID to which the classification policy belongs.
Identity	Number	The identity number of the classification policy.

Related cmdlets

- See "New-EVClassificationPolicy" on page 76.
- See "Remove-EVClassificationPolicy" on page 80.
- See "Set-EVClassificationPolicy" on page 81.

New-EVClassificationPolicy

`New-EVClassificationPolicy` creates a classification policy for an Enterprise Vault 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-3 New-EVClassificationPolicy parameters

Parameter	Description
`-SiteId`	The ID of the Enterprise Vault site for which to create the classification policy. If you omit this parameter, and the cmdlet cannot determine the ID by looking in the registry, then `New-EVClassificationPolicy` prompts you to enter the required ID. You can use `Get-EVSite` to obtain the site ID.
`-Name` (required)	The name of the classification policy. The name must be unique, and it can contain up to 40 alphanumeric or space characters.
`-Description`	The description to set for the 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 (`$true`) or not (`$false`). The default is `$true`. This setting also determines whether Enterprise Vault reclassifies items when you rebuild the indexes.
`-DetermineRC`	Specifies whether to allow the classification feature to update the retention categories of items (`$true`) or not (`$false`). The default is `$true`.
`-RCDuringDeletion`	When `DetermineRC` is `$true`, specifies whether to enable classification on user deletion (`$true`) or not (`$false`). The default is `$false`. You cannot set `RCDuringDeletion` to `$true` when `DetermineRC` is set to `$false`.
`-RCDuringExpiry`	When `DetermineRC` is `$true`, specifies whether to enable classification on automatic expiry (`$true`) or not (`$false`). The default is `$false`. Note the following: ■ You cannot set `RCDuringExpiry` to `$true` when `DetermineRC` is set to `$false`. ■ You must set `RCDuringExpiry` to `$true` when `DuringIndexing` is `$false` and `DetermineRC` is `$true`.

Table B-3 New-EVClassificationPolicy parameters *(continued)*

Parameter	Description
`-PreventRCDuringMove`	When `DetermineRC` is `$true`, specifies whether to prevent Enterprise Vault from updating the retention categories of archived items when users move the items from one folder to another folder that has a different retention category. The default for `PreventRCDuringMove` is `$false`. Enterprise Vault can update the retention categories of moved items, subject to site archive settings.
`-AllowRCOnRecTypeChange`	For use in environments where you use the Enterprise Vault records management feature to mark selected items as records. When `PreventRCDuringMove` is `$true` (do not allow retention category updates for moved items), `AllowRCOnRecTypeChange` specifies whether to allow these updates in instances where moving the items will change their record type. The default for `AllowRCOnRecTypeChange` is `$true`. When `PreventRCDuringMove` is `$false`, `AllowRCOnRecTypeChange` has no effect.

Examples

- `New-EVClassificationPolicy -SiteId 13E...EV.example.com -Name "Classification policy" -Description "Classification policy created using PowerShell"`

  Creates a 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 a 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 a classification policy to classify items during indexing and allow the classification feature to update the retention categories of items. This policy prevents Enterprise Vault from updating the retention categories of moved items

in those archives to which you apply the classification policy, 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-4 New-EVClassificationPolicy properties

Name	Type	Description
Name	String	The name of the classification policy.
EntryId	String	The directory entry ID of the classification policy.
IsADefaultPolicy	Boolean	Whether the 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 move the items from one folder to another folder that has a different retention category.
AllowRCOnRecTypeChange	Boolean	Whether to allow retention category updates for moved items when this will change their record type (for example, from Temporary to Permanent).
Description	String	The description of the classification policy.
SiteId	String	The site ID to which the classification policy belongs.

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

Name	Type	Description
Identity	Number	The identity number of the classification policy.

Related cmdlets

- See "Get-EVClassificationPolicy" on page 74.
- See "Remove-EVClassificationPolicy" on page 80.
- See "Set-EVClassificationPolicy" on page 81.

Remove-EVClassificationPolicy

`Remove-EVClassificationPolicy` removes the specified 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-5 Remove-EVClassificationPolicy parameters

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

Examples

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

  Removes the classification policy that is named "Classification policy" from the specified Enterprise Vault site.

Output

None.

Related cmdlets

- See "Get-EVClassificationPolicy" on page 74.
- See "New-EVClassificationPolicy" on page 76.
- See "Set-EVClassificationPolicy" on page 81.

Set-EVClassificationPolicy

`Set-EVClassificationPolicy` sets or updates the properties of an existing 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-6 Set-EVClassificationPolicy parameters

Parameter	Description
`-SiteId`	The ID of the Enterprise Vault site for which to set or update the classification policy details. If you omit this parameter, and the cmdlet cannot determine the ID by looking in the registry, then `Set-EVClassificationPolicy` prompts you to enter the required ID. You can use `Get-EVSite` to obtain the site ID.
`-Name` (required)	The name of a specific 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 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 (`$true`) or not (`$false`). The default is `$true`. This setting also determines whether Enterprise Vault reclassifies items when you rebuild the indexes.
`-DetermineRC`	Specifies whether to allow the classification feature to update the retention categories of items (`$true`) or not (`$false`). The default is `$true`.
`-RCDuringDeletion`	When `DetermineRC` is `$true`, specifies whether to enable classification on user deletion (`$true`) or not (`$false`). The default is `$false`. You cannot set `RCDuringDeletion` to `$true` when `DetermineRC` is set to `$false`.

Table B-6 Set-EVClassificationPolicy parameters *(continued)*

Parameter	Description
`-RCDuringExpiry`	When `DetermineRC` is `$true`, specifies whether to enable classification on automatic expiry (`$true`) or not (`$false`). The default is `$false`. Note the following: ■ You cannot set `RCDuringExpiry` to `$true` when `DetermineRC` is set to `$false`. ■ You must set `RCDuringExpiry` to `$true` when `DuringIndexing` is `$false` and `DetermineRC` is `$true`.
`-PreventRCDuringMove`	When `DetermineRC` is `$true`, specifies whether to prevent Enterprise Vault from updating the retention categories of archived items when users move the items from one folder to another folder that has a different retention category. The default for `PreventRCDuringMove` is `$false`. Enterprise Vault can update the retention categories of moved items, subject to site archive settings.
`-AllowRCOnRecTypeChange`	For use in environments where you use the Enterprise Vault records management feature to mark selected items as records. When `PreventRCDuringMove` is `$true` (do not allow retention category updates for moved items), `AllowRCOnRecTypeChange` specifies whether to allow these updates in instances where moving the items will change their record type. The default for `AllowRCOnRecTypeChange` is `$true`. When `PreventRCDuringMove` is `$false`, `AllowRCOnRecTypeChange` has no effect.

Examples

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

  Updates the description of an existing 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 classification policy to prevent Enterprise Vault from updating the retention categories of moved items, including when this will change the record type of the items, in those archives to which you apply the policy.

Output

There is a confirmation message on completion.

Related cmdlets

- See "Get-EVClassificationPolicy" on page 74.
- See "New-EVClassificationPolicy" on page 76.
- See "Remove-EVClassificationPolicy" on page 80.

Import-EVClassificationRules

`Import-EVClassificationRules` imports all the Enterprise Vault classification properties and rules from a file into the target servers. Before the cmdlet does this, it clears any existing properties and rules from those servers.

This cmdlet performs a similar function to the `Publish-EVClassificationRules` cmdlet. The difference is that `Publish-EVClassificationRules` first exports the classification properties and rules to an XML file before it publishes them to the target servers; `Import-EVClassificationRules` uses an existing XML file to perform the import part of the operation only.

Note the following:

- To run this cmdlet, you must have the system administrator role on both the server where you run the cmdlet and on all the target servers.
- Install the Microsoft Data Classification Toolkit on the server where you run this cmdlet. You can download the toolkit from the following webpage:
  http://www.microsoft.com/download/details.aspx?id=27123
- If you do not run the cmdlet on an Enterprise Vault server, you must specify either the `-SiteId` or `-Servers` parameter. If you run the cmdlet on an Enterprise Vault server and omit these parameters, the cmdlet uses the site of the current server to publish to all the other Enterprise Vault servers in the site.
- In a cluster configuration (either Windows Server Failover Clustering or Veritas Cluster Server), if you import the classification properties and rules into one

cluster node then all the other nodes are also updated. So, after a failover to another node, classification continues with the same rules as before.

- In an Enterprise Vault Building Blocks environment, this cmdlet imports only to servers that are currently hosting Enterprise Vault tasks and services.
- This cmdlet stops the Enterprise Vault Storage service on each target server and then, after it has imported the classification properties and rules, restarts the service.

Note: Other methods for publishing the classification properties and rules do not automatically stop and then restart the Storage service, and this can lead to classification errors. For example, this is the case if you use the PowerShell cmdlets that come with the Microsoft Data Classification Toolkit. Therefore, we strongly recommend that you use `Import-EVClassificationRules` (or `Publish-EVClassificationRules`) to publish the classification properties and rules.

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

Syntax

```
Import-EVClassificationRules [-ImportRulesFile <string>] [-SiteId
<string>] [-Servers <string>] [-TimeoutSecs <integer>] [-Confirm
<Boolean>]
```

Parameters

Table B-7 Import-EVClassificationRules parameters

Parameter	Description
`-ImportRulesFile` (required)	Specifies the file from which the cmdlet imports the classification properties and rules. The file must have a `.xml` file name extension.
`-SiteId`	Identifies the site to which you want to publish the classification properties and rules. If you set this parameter, you cannot set the `-Servers` parameter as well.

Table B-7 Import-EVClassificationRules parameters *(continued)*

Parameter	Description
`-Servers`	Nominates the servers that will receive the set of classification properties and rules. Type the NETBIOS name, IP address, or fully-qualified domain name of each server in a comma-separated list. To specify the local computer, type the computer name "localhost". If you set this parameter, you cannot set the `-SiteId` parameter as well.
`-TimeoutSecs`	Sets the timeout value in seconds when the cmdlet stops or starts the Enterprise Vault Storage service on each of the target servers. The default is 300 seconds. **Note:** If the cmdlet fails to restart a service within the specified period, check the state of the classification rules and Storage services on the failed servers. A server can be left without classification rules if the cmdlet clears the existing rules without also importing the new ones.
`-Confirm`	When set to `$true` (the default value), causes the cmdlet to prompt you for confirmation before it imports the classification properties and rules. Set to `$false` to suppress the prompts.

Examples

- `Import-EVClassificationRules -ImportRulesFile c:\Data\RulesFile.xml`
  Imports the classification properties and rules that are in the specified file into all the Enterprise Vault servers that are in the current site (that is, the same site as the server on which you run the cmdlet).
- `Import-EVClassificationRules -ImportRulesFile c:\Data\RulesFile.xml -SiteId 13E...EV.example.com`
  Imports the classification properties and rules that are in the specified file into all the Enterprise Vault servers that are in the specified site.
- `Import-EVClassificationRules -ImportRulesFile c:\Data\RulesFile.xml -Servers SERVER1,SERVER2.ABC.DEF.COM`
  Imports the classification properties and rules that are in the specified file into all the specified servers.

Output

This cmdlet returns objects of type Symantec.EnterpriseVault.PowerShell.Commands.ServerInfo, which has the following default properties.

Table B-8 Import-EVClassificationRules properties

Name	Type	Description
ServerName	String	The name of the Enterprise Vault server.
ServerFQDN	String	The fully qualified domain name of the Enterprise Vault server.
Result	String	The import result (Succeeded/Failed/DuplicateServer).
ErrorMessage	String	The error reason, if the import to the server was not successful.

Related cmdlets

- See "Publish-EVClassificationRules" on page 87.

Publish-EVClassificationRules

`Publish-EVClassificationRules` exports all the Enterprise Vault classification properties and rules from a nominated server to an XML file in the specified location. Enterprise Vault then uses this file to import the classification properties and rules into the target servers. Before the cmdlet does this, it clears any existing properties and rules from those servers.

This cmdlet performs a similar function to the `Import-EVClassificationRules` cmdlet. However, `Import-EVClassificationRules` does not create the XML file that Enterprise Vault subsequently imports into the target servers; the cmdlet uses an existing XML file to perform the import part of the operation only.

Note the following:

- You can run the cmdlet on a different server from the server on which you have configured the classification properties and rules.
- To run this cmdlet, you must have the system administrator role on both the server where you run the cmdlet and on all the target servers.
- You must install the Microsoft Data Classification Toolkit on the computer where you run this cmdlet. You can download the toolkit from the following webpage: http://www.microsoft.com/download/details.aspx?id=27123
- If you do not run the cmdlet on an Enterprise Vault server, you must specify either the `-SiteId` or `-Servers` parameter. If you run the cmdlet on an Enterprise Vault server and omit these parameters, the cmdlet uses the site of the current server to publish to all the other Enterprise Vault servers in the site.

- In a cluster configuration (either Windows Server Failover Clustering or Veritas Cluster Server), if you publish the classification properties and rules to one cluster node then all the other nodes are also updated. So, after a failover to another node, classification continues with the same rules as before.
- In an Enterprise Vault Building Blocks environment, this cmdlet imports only to servers that are currently hosting Enterprise Vault tasks and services.
- This cmdlet stops the Enterprise Vault Storage service on each target server and then, after it has imported the classification properties and rules, restarts the service.

Note: Other methods for publishing the classification properties and rules do not automatically stop and then restart the Storage service, and this can lead to classification errors. For example, this is the case if you use the PowerShell cmdlets that come with the Microsoft Data Classification Toolkit. Therefore, we strongly recommend that you use `Publish-EVClassificationRules` (or `Import-EVClassificationRules`) to publish the classification properties and rules.

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

Syntax

```
Publish-EVClassificationRules [-StagingServer <string>]
[-ExportRulesFile <string>] [-SiteId <string>] [-Servers <string>]
[-TimeoutSecs <integer>] [-Confirm <Boolean>]
```

Parameters

Table B-9 Publish-EVClassificationRules parameters

Parameter	Description
`-StagingServer` (required)	Specifies the name of the server on which you have configured the classification properties and rules and from which you now want to export them.
`-ExportRulesFile` (required)	Specifies the path to a file to which the cmdlet exports the classification properties and rules, before importing them into the target servers. The cmdlet creates the file locally, so you must specify a local path such as `c:\Data\RulesFile.xml`. Ensure that the file name has a `.xml` extension.

Table B-9 Publish-EVClassificationRules parameters *(continued)*

Parameter	Description
`-SiteId`	Identifies the Enterprise Vault site to which you want to publish the classification properties and rules. If you set this parameter, you cannot set the `-Servers` parameter as well.
`-Servers`	Nominates the servers that will receive the set of classification properties and rules. Type the NETBIOS name, IP address, or fully-qualified domain name of one or more servers in a comma-separated list. To specify the local computer, type the computer name "localhost". If you set this parameter, you cannot set the `-SiteId` parameter as well.
`-TimeoutSecs`	Sets the timeout value in seconds when stopping or starting the Enterprise Vault Storage service on each of the target servers. The default is 300 seconds. **Note:** If the cmdlet fails to restart a service within the specified period, check the state of the classification rules and Storage services on the failed servers. A server can be left without classification rules if the cmdlet clears the existing rules without also importing the new ones.
`-Confirm`	When set to `$true` (the default value), causes the cmdlet to prompt you for confirmation before it publishes the classification data. Set to `$false` to suppress the prompts.

Examples

- `Publish-EVClassificationRules -StagingServer SERVERXYZ -ExportRulesFile c:\Data\RulesFile.xml`

  Exports the classification properties and rules from server SERVERXYZ to the specified local file. The cmdlet then publishes the properties and rules to all the Enterprise Vault servers that are in the current site (that is, the same site as the server on which you run the cmdlet).

- `Publish-EVClassificationRules -StagingServer SERVERXYZ -ExportRulesPath c:\Data\RulesFile.xml -SiteId 13E...EV.example.com`

  Publishes the exported classification properties and rules to all the Enterprise Vault servers that are in the specified site.

- `Publish-EVClassificationRules -StagingServer SERVERXYZ -ExportRulesPath c:\Data\RulesFile.xml -Servers SERVER1,SERVER2.ABC.DEF.COM`

  Publishes the exported classification properties and rules to the specified servers.

Output

This cmdlet returns objects of type Symantec.EnterpriseVault.PowerShell.Commands.ServerInfo, which has the following default properties.

Table B-10 Publish-EVClassificationRules properties

Name	Type	Description
ServerName	String	The name of the Enterprise Vault server.
ServerFQDN	String	The fully qualified domain name of the Enterprise Vault server.
Result	String	The publish result (Succeeded/Failed/DuplicateServer).
ErrorMessage	String	The error reason, if the import to the server was not successful.

Related cmdlets

- See "Import-EVClassificationRules" on page 84.

Get-EVClassificationTags

For the specified plain-text (`.txt`) file in the classification cache folder, `Get-EVClassificationTags` returns details of the rules that it matches and the associated classification properties and property values. You may find this useful when you create a classification rule, as the cmdlet lets you verify that the rule is operating correctly without repeatedly having to rearchive the same item.

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 18.

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

Syntax

```
Get-EVClassificationTags [-File] <string>
```

Parameters

Table B-11 Get-EVClassificationTags parameters

Parameter	Description
`-File` (required)	The path to the plain-text file for which to return the classification details. Only `.txt` files are eligible. File names that contain a dollar sign ($) must be escaped using single quotation marks (').

Examples

- `Get-EVClassificationTags -File E:\EVCache\Classification\ClassificationFile.txt`

  Returns the classification details for the file `ClassificationFile.txt`.

- `Get-EVClassificationTags -File 'E:\EVCache\Classification\EV$90B2291D1E3417B67AB88BDDC2195091~02B5EDB8.txt'`

  Returns the classification details for a file that has a dollar sign in its name. For this reason, the entire path is enclosed in single quotation marks.

Output

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

Table B-12 Get-EVClassificationTags properties

Name	Type	Description
RuleName	String	The classification rule that the file has matched.
PropertyName	String	The classification property in which the rule assigns one or more values.
PropertyValue	String	The values that the rule assigns to the classification property.

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-13 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-14 lists the properties that are available.

Table B-14 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 (`$true`) or disabled (`$false`).

Related cmdlets

- See "Set-EVClassificationTestMode" on page 93.

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-15 Set-EVClassificationTestMode parameters

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

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 92.

Appendix C

Troubleshooting and performance monitoring

This appendix includes the following topics:

Troubleshooting classification

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

Table C-1 Potential classification issues

Issue	Explanation/solution
Enterprise Vault fails to classify items.	Ensure all of the following: ■ The File Server Resource Manager service is running and correctly configured. ■ You have a valid license for the Enterprise Vault retention feature. ■ The correct classification rules are in place. ■ You have correctly configured the retention plan and classification policy for the target archives. Each archive must have an associated retention plan that has a classification policy. ■ You are running classification in normal mode rather than test mode. See "About classification test mode" on page 56. In addition, check the Application event log. If the File Server Resource Manager returns an error when it evaluates a classification rule, an Error event may provide an explanation. For example, event 41620 may indicate an invalid Veritas Information Classifier rule. You may also want to examine the files in the classification cache folder. See "Configuring Enterprise Vault to keep the classification files in the cache folder" on page 18.

Table C-1 Potential classification issues *(continued)*

Issue	Explanation/solution
Items are not classified as you expect.	Try the following: ■ 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 56. ■ Run the PowerShell cmdlet `Get-EVClassificationTags` to identify the rules that each item matches. See "Get-EVClassificationTags" on page 90. ■ 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 18. Then you can review the file contents for any anomalies that you did not anticipate. ■ If you use the Veritas Information Classifier to classify items, run the DTrace utility against the fsdmhost process to determine why a rule does not match. For guidelines on running DTrace, see the *Utilities* guide.
Classification operates in test mode only.	You have associated one or more classification policies with one or more retention plans, but Enterprise Vault cannot detect a valid license for the retention feature.
Timeouts occur during classification.	In Windows Server 2012 R2, the File Classification Infrastructure has a default timeout of 10 minutes. If a rule is particularly complex, this timeout is reached and Error event 12351 is logged in the Application event log. Enterprise Vault makes four more attempts to classify the item and then records Error event 29075 in the Veritas Enterprise Vault event log ("Failed to classify item content"). To resolve this issue, simplify the rules that are responsible for the timeouts. **Note:** Timeouts do not occur in Windows Server 2012 Original Release, so classifying complex rules can theoretically take many hours to process. This can affect system performance because the process is CPU-intensive. For this reason we recommend that you run Windows Server 2012 R2 on all Enterprise Vault servers.

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 C-2 describes the counters.

Table C-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.
Items blocked from discard on classification	The number of items that meet an evaction.discard classification rule 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 they meet an evaction.discard classification rule.
Items failed classification	The number of items that Enterprise Vault has failed to classify.
Items successfully classified	The number of items that Enterprise Vault has passed to the Windows File Classification Infrastructure for classification with a success result. The count includes any items that meet an evaction.discard classification rule, whether or not Enterprise Vault was able to discard them. 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.

Index

F

G

I

K

L

M

N

P

R

S

T

V

W