Enterprise Vault 12 Feature Briefing

Classification

This document is about the new Classification feature in Enterprise Vault 12.

If you have any feedback or questions about this document, please email them to II-TEC@veritas.com stating the document title.

Feature Description

Enterprise Vault 12 offers new features for intelligent archiving with the introduction of Classification and Retention Plans. Deploying these features will allow organizations to automatically classify any ingested content, whether it be from Exchange, Domino, Files, PSTs, NSFs, SharePoint or the Content Management API.

Administrators are able to define policies and rules that will classify items based on the content or metadata of the item being archived. The system is then able to make intelligent decisions on whether an item needs to be kept for certain period, discarded, included in the supervisory review in Compliance Accelerator, or have searchable tags added to aid end user or eDiscovery searches.

Business Value

Automatic Classification of information can help organizations:

- make better **information retention decisions** by only keeping the information you need, or automatically deleting the information you definitely do not want to keep long term (news alerts, social media feeds, lunch menus, etc)
- make better **eDiscovery decisions** using searchable tags
- include items for **supervisory review** in Compliance Accelerator
- classify personally identifiable information (PII), and make better **information protection decisions**
- enable **risk analysis** and conduct any necessary remediation
- be compliant with **industry regulations** and avoid fines.

A large set of example rules ship with the product to aid customers in creating the initial set of classification rules, and includes identification of items such as: Social Security Number (US), Driving License (UK), VAT/TFA number (France), CPF number (Brazil), Identity Card (Germany), National Registry Identification Number (Singapore), Visa, MasterCard and American Express amongst others.

Enterprise Vault 12 also includes the ability to **re-classify** content in archives. This can potentially introduce storage savings by deleting unwanted items residing in older archives. Re-classification can also be used in cases where new regulations are introduced, or simply because the organization changed the policy and would like to retrospectively apply these changes to ensure they are compliant.

Additionally, Enterprise Vault 12 introduces a feature known as **Gated Deletion**. Gated Deletion forces any item manually deleted by end users or through automatic expiry to be presented to the classification rules first, to ensure the deletion action is compliant with the current policy. At this point the delete action can be denied, or the item’s retention category automatically changed if for example it’s found that the file was a contract that should be kept for a longer period.

Underlying Principles

EV12 Classification is powered by the Veritas Information Classifier (VIC) engine, developed as a plug-in to the Windows Server File Classification Infrastructure (FCI). One of the benefits of using the Windows FCI platform is that customers with an existing FCI compatible engine configured (Websense, Titus, etc.) can use that instead to perform classification.

All the classification processes are performed locally on the Enterprise Vault Server. Figure 1 shows a high level overview of the components involved in the Classification process.

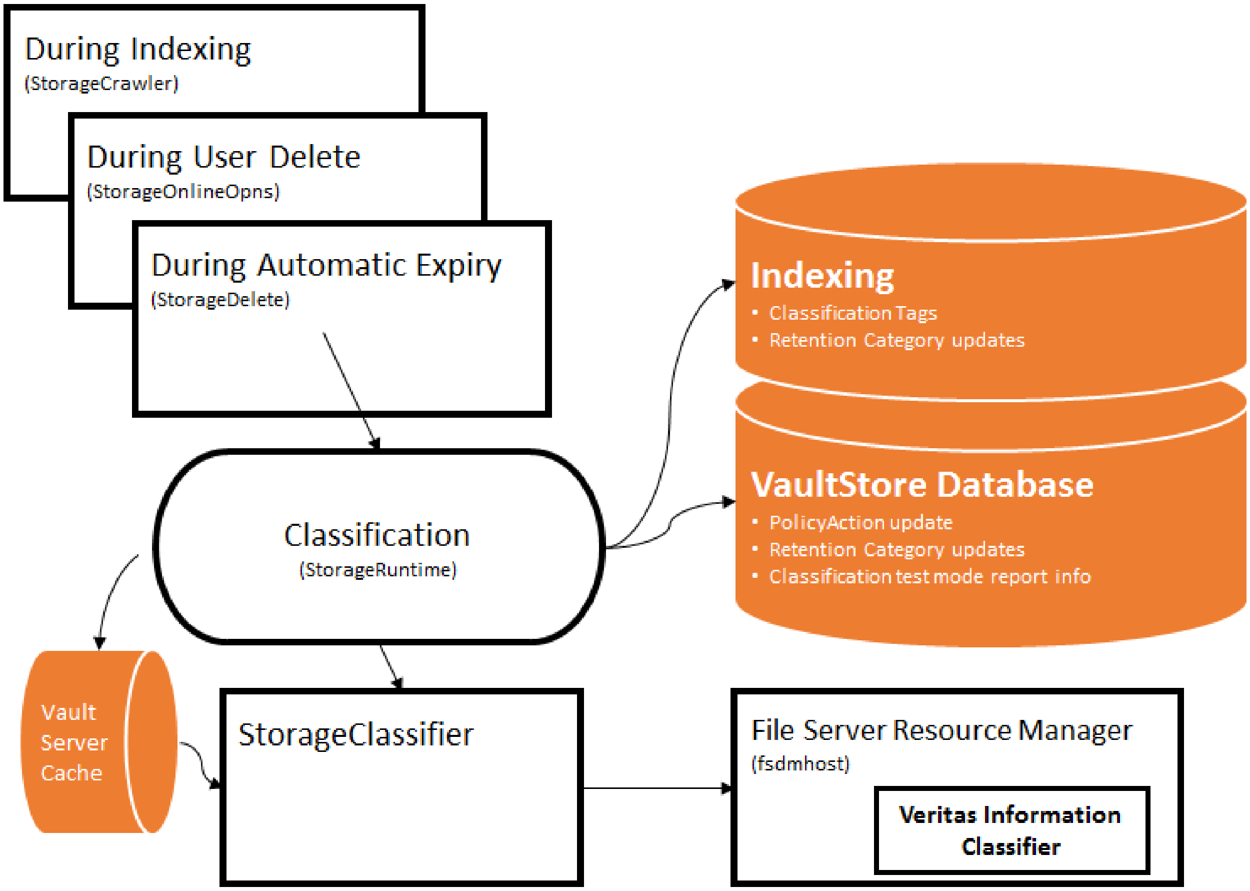


Figure 1 – Overview of Classification Components

Firstly, the item is ingested via an agent (for example File System Archiving Task, SMTP, Exchange Mailbox Archiving Task), and then passed to storage service to perform the content conversion. At this point if the destination archive is enabled for Classification with a Retention Plan, the converted index version of the original item is passed to the StorageClassifier process, which in turn will pass the item to the Veritas Information Classifier engine.

The Classification rules will now be applied to the item, and any tags (custom, discard, include or exclude from supervisory review) will be passed back to the StorageRuntime process before the item is stored. At this point if a Classification tag matches a Retention Category, the retention category of the item will be updated (if allowed by policy).

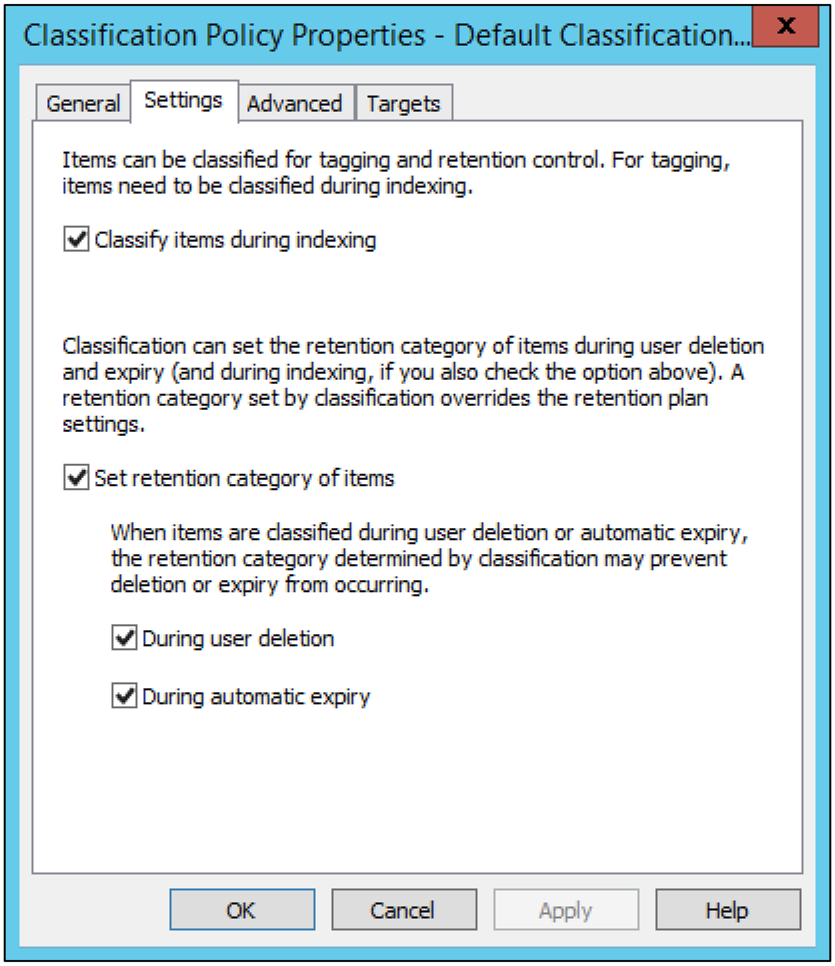
All the Classification functionality available to items at the point of ingestion also applies to items passed to Classification by user delete or automatic expiry operations.

Guided Tour

This section will provide a high level overview of how to configure Classification.

Step 1: Configure Classification Policy

The first step is to create and configure the Classification Policy. The policy will control how Classification is applied to items (Figure 2).


Classification Policy Properties - Default Classification...
X
General
Settings
Advanced
Targets

Items can be classified for tagging and retention control. For tagging, items need to be classified during indexing.

☑ Classify items during indexing

Classification can set the retention category of items during user deletion and expiry (and during indexing, if you also check the option above). A retention category set by classification overrides the retention plan settings.

☑ Set retention category of items

When items are classified during user deletion or automatic expiry, the retention category determined by classification may prevent deletion or expiry from occurring.

☑ During user deletion

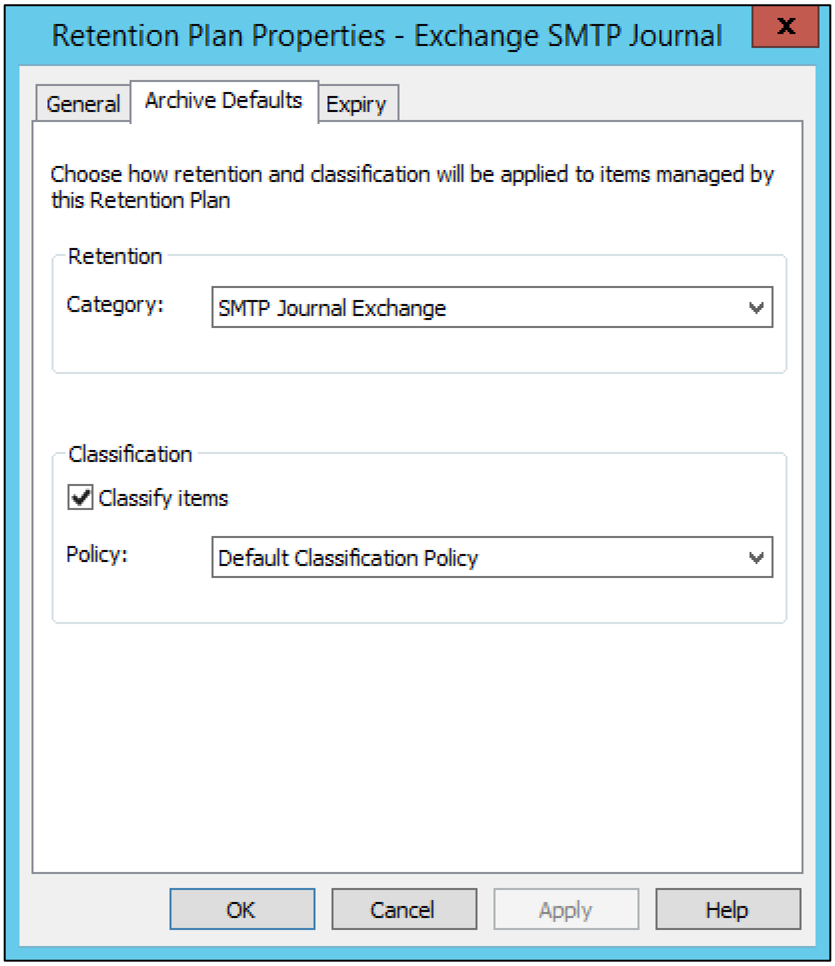
☑ During automatic expiry

Figure 2 – Classification Policy Configuration

Once the Classification policy is configured, the Retention Plan can be created and associated with the archive you wish to enable for Classification.

Step 2: Configure Retention Plans and associate with an archive

Retention Plans encapsulate a Retention Category and a Classification Policy, as shown in Figure 3.



Retention Plan Properties - Exchange SMTP Journal

Choose how retention and classification will be applied to items managed by this Retention Plan

Retention

Category: SMTP Journal Exchange

Classification

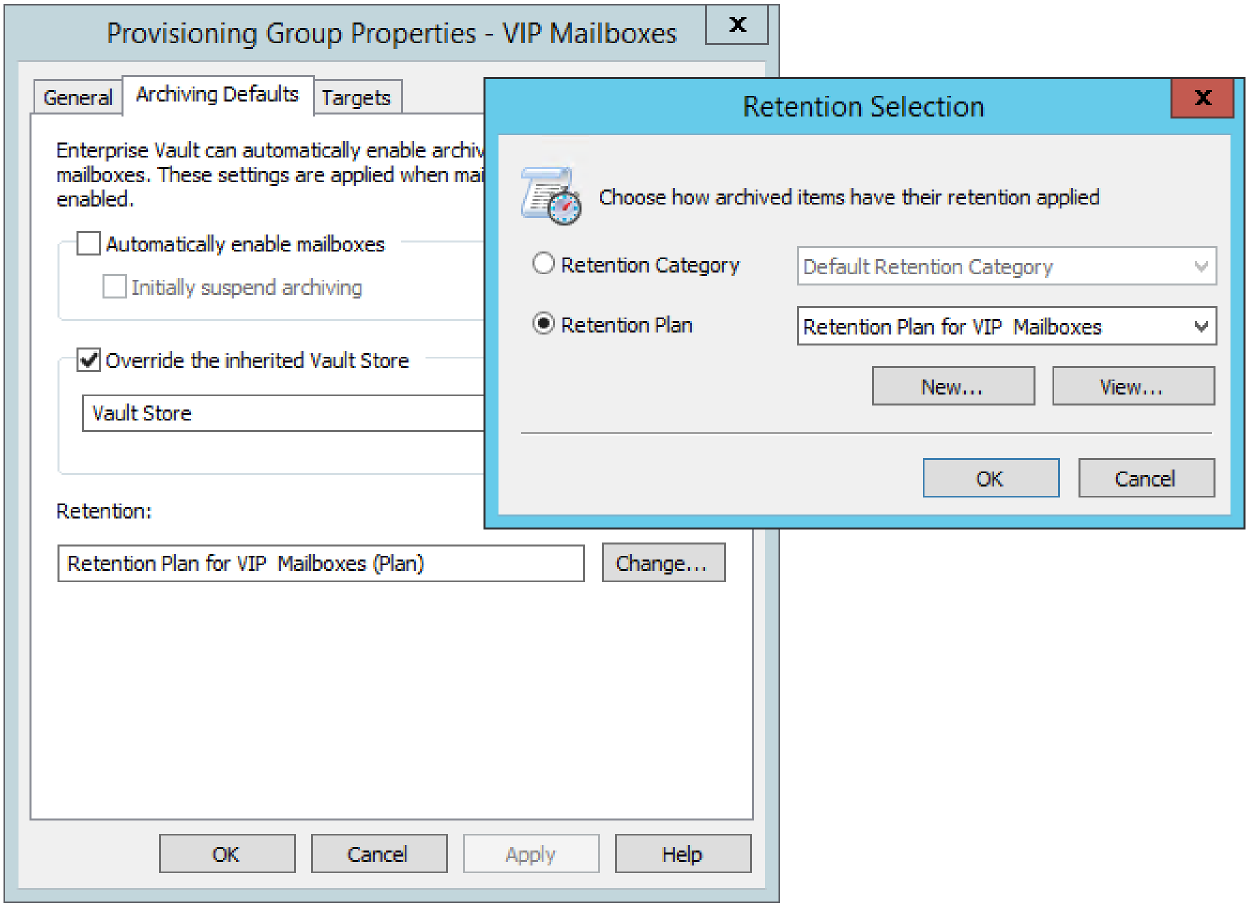
☑ Classify items

Policy: Default Classification Policy

Figure 3 – Retention Plan Properties

A Retention Plan will allow the administrator to specify a default Retention Category to apply to all items sent to that particular archive, and if no Classification rule matches or attempts to change the Retention Category for that item, the default Retention Category will be applied.

Classification is enabled on a per archive basis, using Retention Plans. Retention Plans are assigned to archives either through Provisioning Groups in the Vault Admin Console, or via a PowerShell command (Figure 4).



Provisioning Group Properties - VIP Mailboxes

Enterprise Vault can automatically enable archiv
mailboxes. These settings are applied when mai
enabled.

□ Automatically enable mailboxes

□ Initially suspend archiving

☑ Override the inherited Vault Store

Vault Store

Retention: Retention Plan for VIP Mailboxes (Plan)

Retention Selection

Choose how archived items have their retention applied

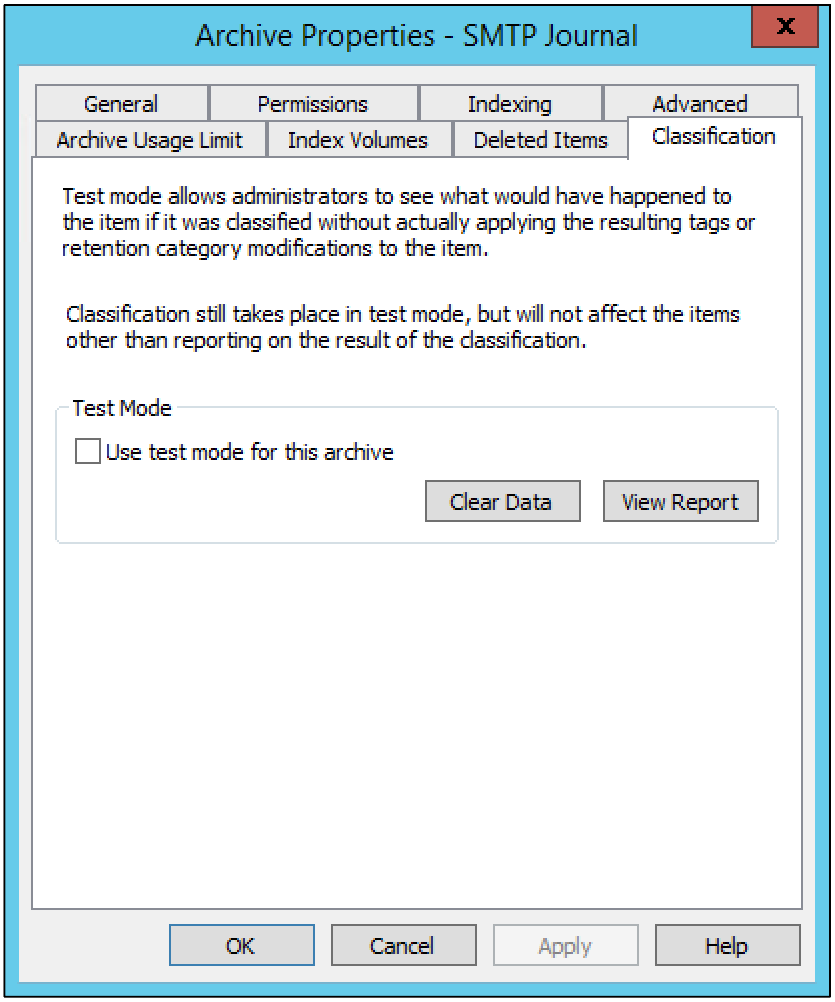
○ Retention Category: Default Retention Category

● Retention Plan: Retention Plan for VIP Mailboxes

Figure 4 – Retention Plan Provisioning

Step 3: Enable Test Mode for Classification

Once the archive is enabled for Classification, a Classification tab will appear in the properties of the archive (Figure 5).



Test mode allows administrators to see what would have happened to the item if it was classified without actually applying the resulting tags or retention category modifications to the item.

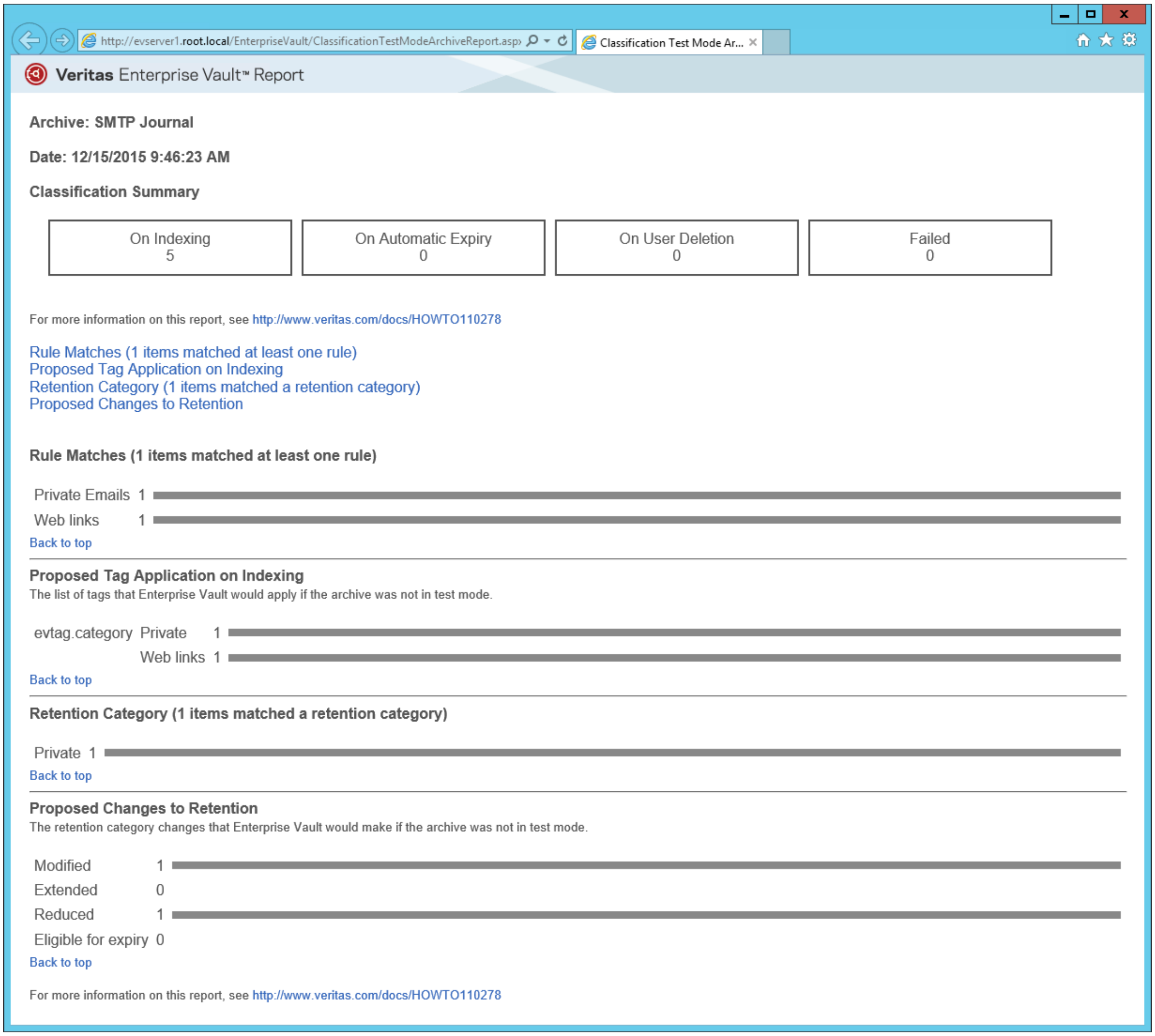
Classification still takes place in test mode, but will not affect the items other than reporting on the result of the classification.

Test Mode

□ Use test mode for this archive

Figure 5 – Classification Test Mode

The Test Mode setting in Figure 5 is very useful for confirming that the configured Classification rules work as expected, before actually enabling the functionality on production data. Test mode will generate a report based on the rules configured, and does not require a Retention license. Figure 6 shows an example report.


http://evserver1.root.local/EnterpriseVault/ClassificationTestModeArchiveReport.asp›
Classification Test Mode Ar...
Veritas Enterprise Vault™ Report

Archive: SMTP Journal

Date: 12/15/2015 9:46:23 AM

Classification Summary

On Indexing	On Automatic Expiry	On User Deletion	Failed
5	0	0	0

For more information on this report, see http://www.veritas.com/docs/HOWTO110278

Rule Matches (1 items matched at least one rule)
Proposed Tag Application on Indexing
Retention Category (1 items matched a retention category)
Proposed Changes to Retention

Rule Matches (1 items matched at least one rule)

Private Emails	1
Web links	1

Back to top

Proposed Tag Application on Indexing
The list of tags that Enterprise Vault would apply if the archive was not in test mode.

evtag.category	Private	1
	Web links	1

Back to top

Retention Category (1 items matched a retention category)

Private	1

Back to top

Proposed Changes to Retention
The retention category changes that Enterprise Vault would make if the archive was not in test mode.

Modified	1
Extended	0
Reduced	1
Eligible for expiry	0

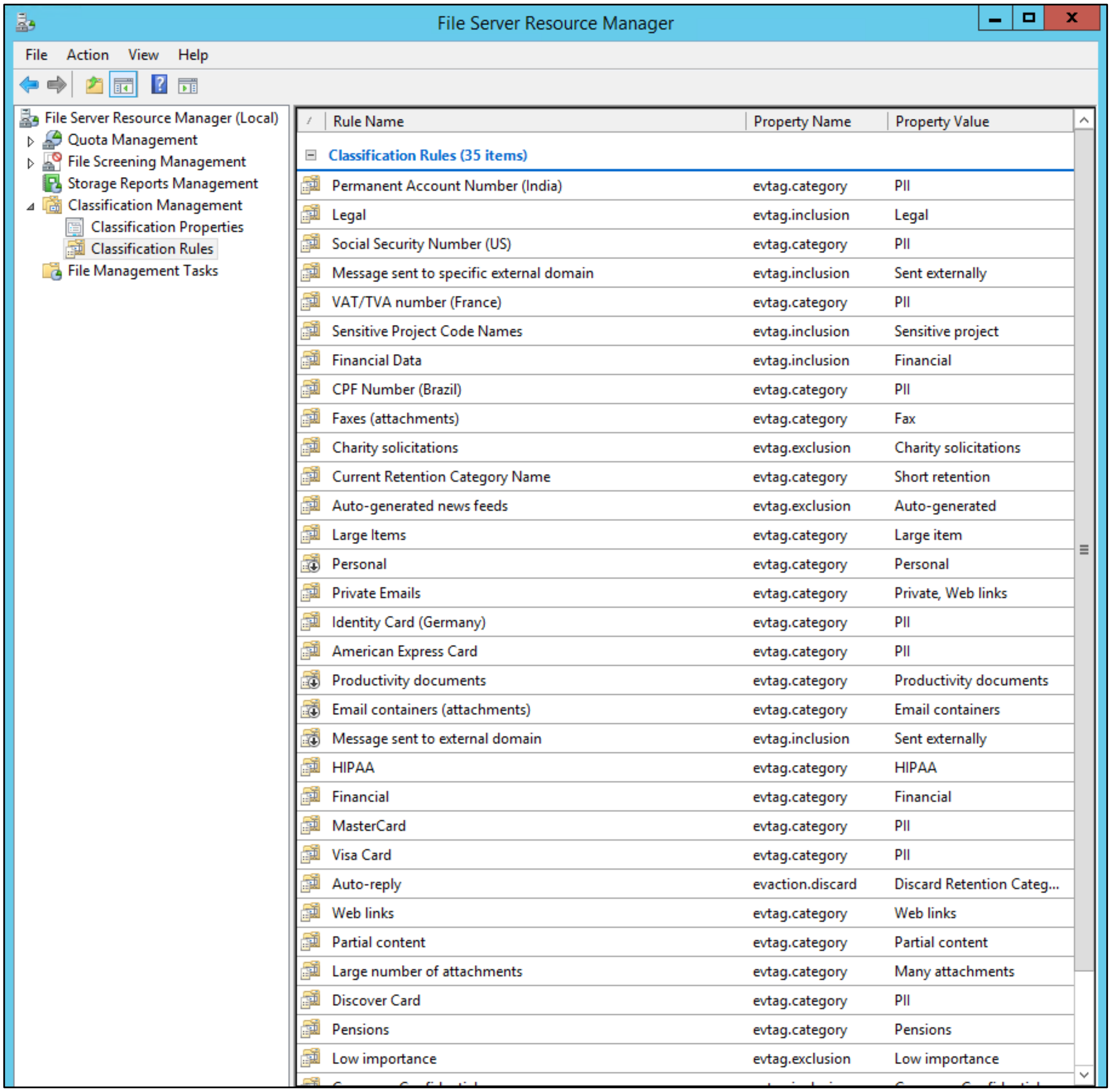
Back to top

For more information on this report, see http://www.veritas.com/docs/HOWTO110278

Figure 6 – Example Classification Test Mode Report

Step 4: Configure Classification Rules

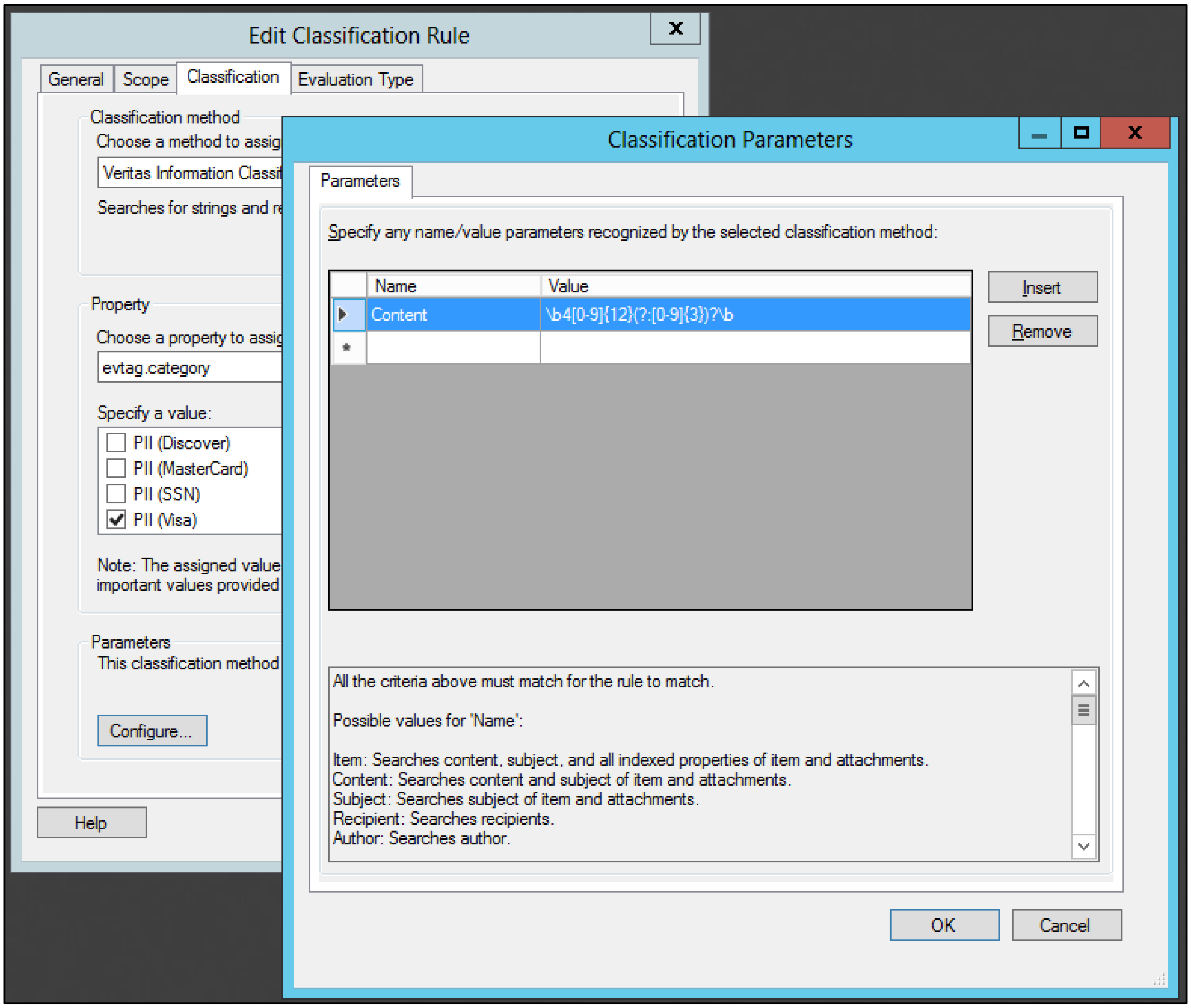
After importing the example rules, the administrator is presented with the following interface in the File Server Resource Manager console. It is recommended that administrators review the example rules before deleting or disabling them. New rules are easily created and will become immediately active.


File Server Resource Manager
File
Action
View
Help
File Server Resource Manager (Local)
Quota Management
File Screening Management
Storage Reports Management
Classification Management
Classification Properties
Classification Rules
File Management Tasks

Rule Name	Property Name	Property Value
Classification Rules (35 items)		
Permanent Account Number (India)	evtag.category	PII
Legal	evtag.inclusion	Legal
Social Security Number (US)	evtag.category	PII
Message sent to specific external domain	evtag.inclusion	Sent externally
VAT/TVA number (France)	evtag.category	PII
Sensitive Project Code Names	evtag.inclusion	Sensitive project
Financial Data	evtag.inclusion	Financial
CPF Number (Brazil)	evtag.category	PII
Faxes (attachments)	evtag.category	Fax
Charity solicitations	evtag.exclusion	Charity solicitations
Current Retention Category Name	evtag.category	Short retention
Auto-generated news feeds	evtag.exclusion	Auto-generated
Large Items	evtag.category	Large item
Personal	evtag.category	Personal
Private Emails	evtag.category	Private, Web links
Identity Card (Germany)	evtag.category	PII
American Express Card	evtag.category	PII
Productivity documents	evtag.category	Productivity documents
Email containers (attachments)	evtag.category	Email containers
Message sent to external domain	evtag.inclusion	Sent externally
HIPAA	evtag.category	HIPAA
Financial	evtag.category	Financial
MasterCard	evtag.category	PII
Visa Card	evtag.category	PII
Auto-reply	evaction.discard	Discard Retention Categ...
Web links	evtag.category	Web links
Partial content	evtag.category	Partial content
Large number of attachments	evtag.category	Many attachments
Discover Card	evtag.category	PII
Pensions	evtag.category	Pensions
Low importance	evtag.exclusion	Low importance

Figure 7 – Configuring Classification Rules

Figure 8 shows an example of the rule to detect Visa bank cards. The example rule will search for the card string across the whole item, and stamp a PII tag to the message or file, and optionally change the retention category of the item.



Choose a method to assig

Veritas Information Classi

Searches for strings and r

Choose a property to assig

evtag.category

Specify a value:

□ PII (Discover)
□ PII (MasterCard)
□ PII (SSN)
☑ PII (Visa)

Note: The assigned value
important values provided

This classification method

Specify any name/value parameters recognized by the selected classification method:

Name	Value
Content	\b4[0-9]{12}(?:[0-9]{3})?\b

All the criteria above must match for the rule to match.

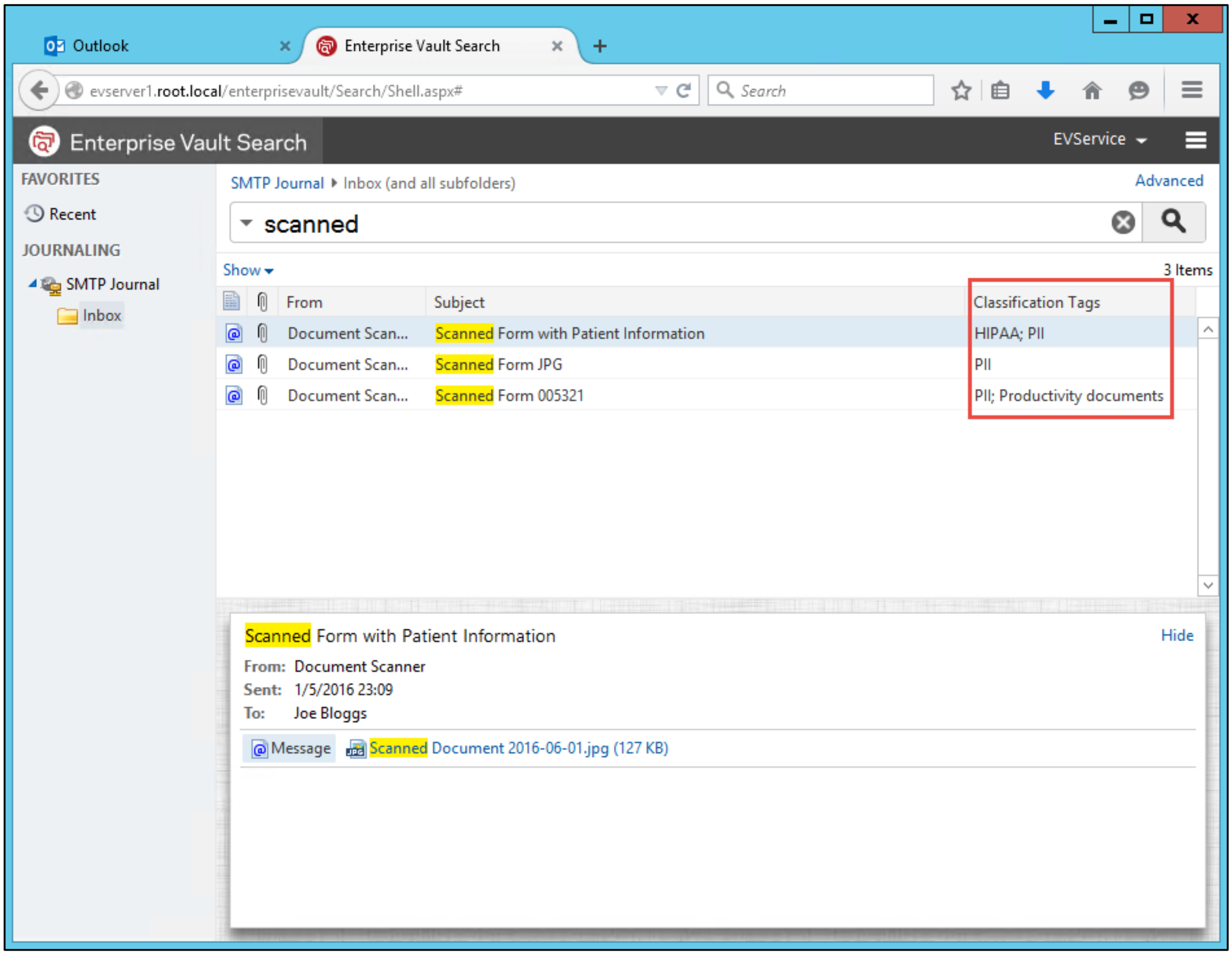
Possible values for 'Name':

Item: Searches content, subject, and all indexed properties of item and attachments.
Content: Searches content and subject of item and attachments.
Subject: Searches subject of item and attachments.
Recipient: Searches recipients.
Author: Searches author.

Figure 8 – Configuring Classification Rules

Step 5: View or search on Classification tags

Enterprise Vault Search can be configured to display and search for specific Classification tags. Figure 9 shows the Classification tags displayed in an SMTP Journal archive.



From	Subject	Classification Tags
Document Scan...	Scanned Form with Patient Information	HIPAA; PII
Document Scan...	Scanned Form JPG	PII
Document Scan...	Scanned Form 005321	PII; Productivity documents

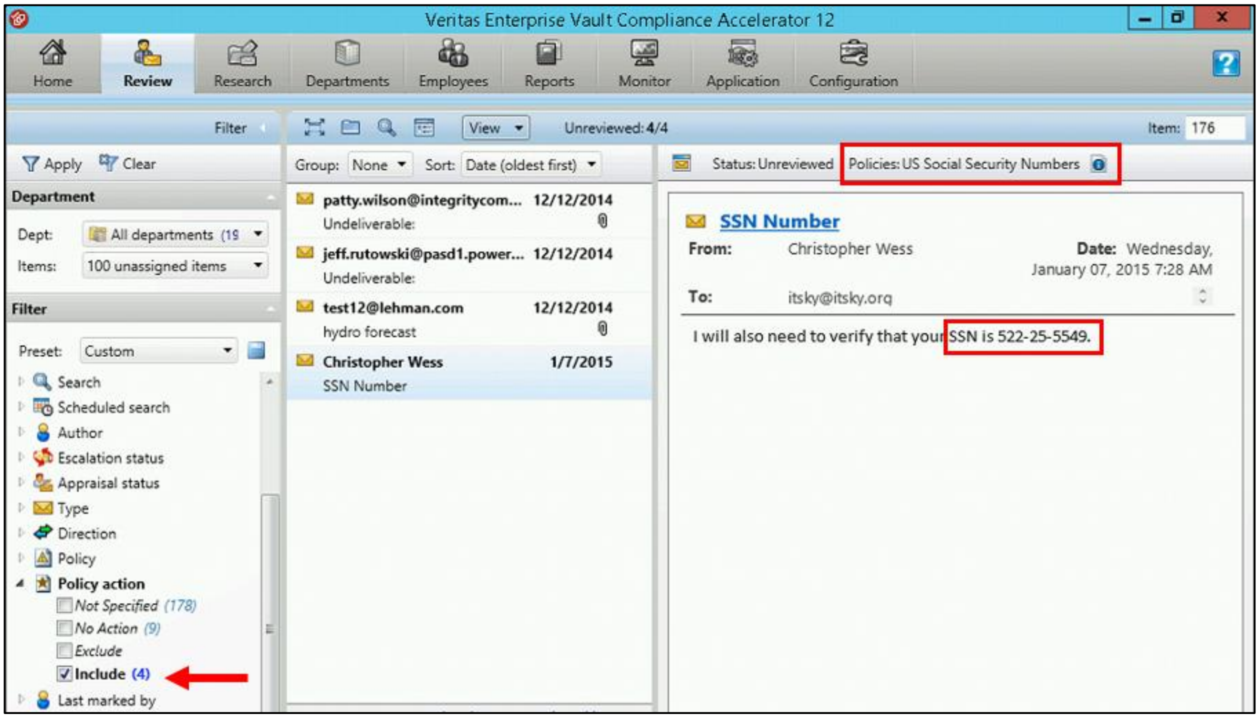
Scanned Form with Patient Information

From: Document Scanner
Sent: 1/5/2016 23:09
To: Joe Bloggs

Message   Scanned Document 2016-06-01.jpg (127 KB)

Figure 9 – Configuring Classification Rules

Figure 10 shows the tags being used in Compliance Accelerator to include any emails where a Social Security Number was used.



Unreviewed: 4/4

Item: 176

Group: None Sort: Date (oldest first)

Status: Unreviewed Policies: US Social Security Numbers

Dept: All departments (19

Items: 100 unassigned items

Preset: Custom

Policy action:
- ☐ Not Specified (178)
- ☐ No Action (9)
- ☐ Exclude
- ☑ Include (4)

patty.wilson@integritycom... Undeliverable:	12/12/2014
jeff.rutowski@pasd1.power... Undeliverable:	12/12/2014
test12@lehman.com hydro forecast	12/12/2014
Christopher Wess SSN Number	1/7/2015

SSN Number

From: Christopher Wess

Date: Wednesday, January 07, 2015 7:28 AM

To: itsky@itsky.org

I will also need to verify that your SSN is 522-25-5549.

Figure 10 – Using Classification Tags in Compliance Accelerator

Licensing and support considerations

Retention Plans, Classification, Re-Classification & Gated Deletion are included in the Enterprise Vault Retention license. To try out classification in test mode, no license is required.

Enterprise Vault 12's Classification replaces Enterprise Vault Data Classification Services (DCS). DCS is still supported, and if required can be used in conjunction with Classification, but no new license sales will be accepted. To add additional user licenses to DCS, contact the Veritas Enterprise Vault Pricing & Licensing team.

About Veritas:
Veritas Technologies LLC enables organizations to harness the power of their information, with solutions designed to serve the world's largest and most complex heterogeneous environments. Veritas works with 86 percent of Fortune 500 companies today, improving data availability and revealing insights to drive competitive advantage. More information is available at www.veritas.com.

For specific country offices and contact numbers, please visit our Web site: **www.veritas.com**

Veritas World Headquarters
500 East Middlefield Road
Mountain View, CA 94043 USA

+1 (650) 933 1000

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.