Veritas eDiscovery Platform™

New Features Overview v1

9.0

VERITAS

Veritas eDiscovery Platform™: *New Features Overview*

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Last updated: 2017-12-06

Legal Notice

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

http://www.veritas.com

Contents

About this Document

This document provides a high-level overview of the new features and enhancements available in version 8.0, grouped into the following sections:

What's New in 9.0?

- Automatic Classification of data during processing based on pre-defined industry rules or manually defined policies
- The ability to Find and Redact any sensitive terms in bulk across a case in a single operation
- Ability to create preset redaction reason codes to streamline FOIA and other SAR workflows reducing errors in coding and reducing Quality Control times
- Provision of an Annotation Toolkit to allow for additional text, highlights or graphics to be added to documents before they are produced and exported
- Automatic conversion of OST files to PST files. This removes any manual steps required for conversion, reducing risk and time allowing processing of this data type to complete more quickly
- The ability to deploy Legal Hold Confirmation with Single Sign On using Integrated Windows Authentication

Processing Features

Information Classification

Starting with version 9.0, the eDiscovery Platform lets you automatically classify sensitive and critical case data based on a set of built-in and custom policies. Classification policies are all managed by the Veritas Information Classifier (VIC) interface. VIC is a common interface that is shared by a suite of Veritas applications including Enterprise Vault and Data Insight.

The platform integrates with VIC to analyze and classify eDiscovery data. VIC uses both predefined and user-defined policies to assign classification tags to your eDiscovery data during the processing phase. Once these tags have been applied, users can view pre-selected classification filters (system tags) in the Analysis and Review mode to quickly identify documents that match the VIC tags.

- In the eDiscovery Platform, the Case Administrator interacts with the VIC interface to enable and disable policies.
- Then the Case Administrator enables Information Classification in the case settings as a part of case processing setup.

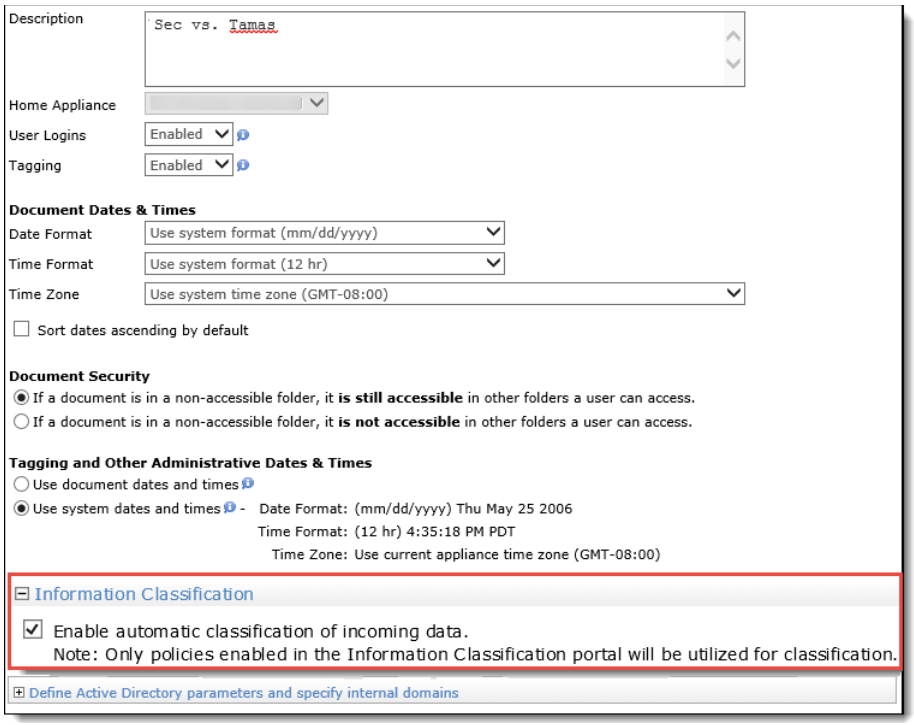

Figure 1 Enabling Information Classification

After the data has been processed, classification filters operate like predefined system tags in the eDiscovery platform. When the classification filter is expanded, Reviewers will see tags for every policy that has been enabled that has at least one matching document. Information classification tags function like all other tags in the eDiscovery platform.

Figure 2 Viewing Classification filters

Reviewers can select and use tags during Search and Review to apply single or multiple classification tags. Selecting **Include All Tags** during metadata and production export will cause the classification information to be included in the export load file.

Note: The Information Classification feature can only be enabled for cases created in version 9.0 and later. Cases created before version 9.0 are not supported.

Analysis and Review Features

Bulk Redaction and Delete Bulk Redaction

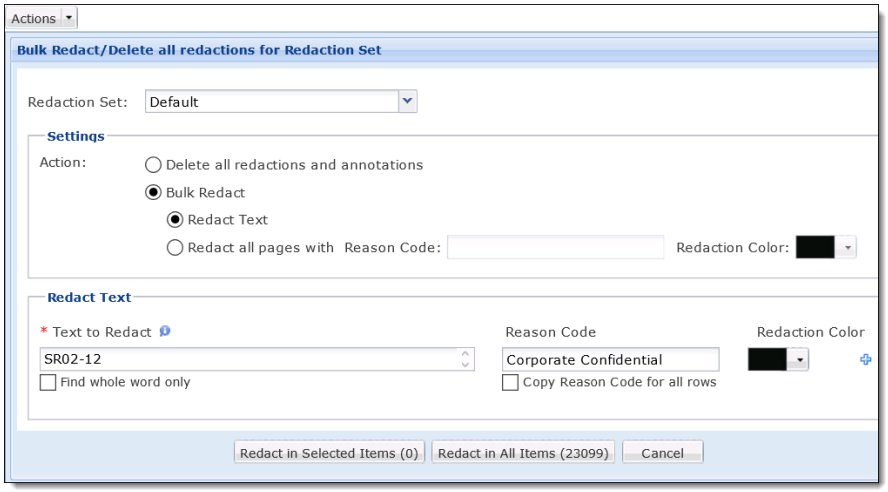

Figure 3 Bulk Redaction controls

Bulk redaction is an efficient way to apply redactions to multiple items in a redaction set without having to individually open and review every document in Native Viewer mode. Any user with the "Allow Redacting" privilege can perform bulk redactions, delete bulk redaction operations, and submit jobs.

Reviewers can easily specify the redaction set along with the reason code that needs to be applied to all the selected documents. Bulk redaction works on redaction sets with preset reason codes, or with free text reason codes.

Delete bulk redaction works in the same way, to correct misapplied redactions, or remove redactions on an entire redaction set.

Annotations in Review Mode

In addition to the existing capability to redact a document, this release adds the ability to annotate a document in review mode.

- Case reviewers can annotate a document by adding comments or graphical stamps, or strike out some text.
- Case reviewers are also allowed to delete annotations.
- Case reviewers can also search the document for the Redacted Tag.
- Once annotated, the document can be reviewed by another reviewer, who can also add annotations.

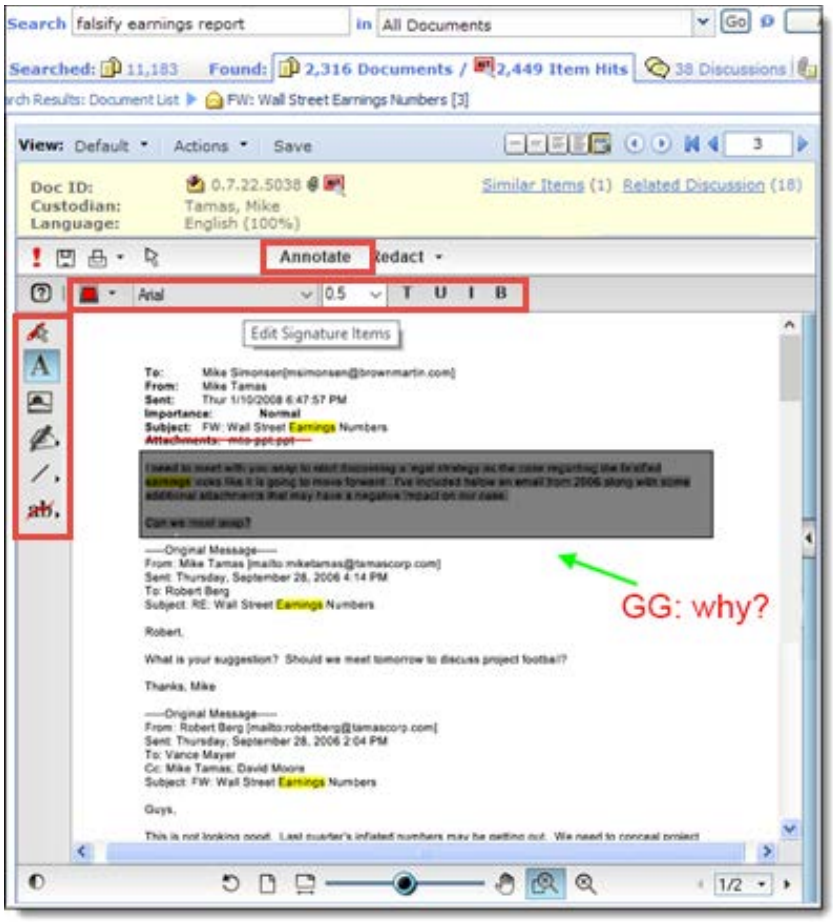

Figure 4 Annotation Controls

Redaction sets with preset reason codes

Now there are two ways to apply reason codes to redaction sets: free text and preset reason code. The previously existing free text option allows reviewers to enter reason codes. The preset reason code option allows an administrator to set up and control reason code choices for reviewers. Using preset reason codes can make it easier to adhere to standards that your organization follows or that comply with regulatory mandates (for example, Privacy Information, Confidential, Privileged).

Applying a preset reason code is even easier than entering free text. Once the Case administrator has defined preset reason codes for a redaction set, reviewers simply choose from the available options.

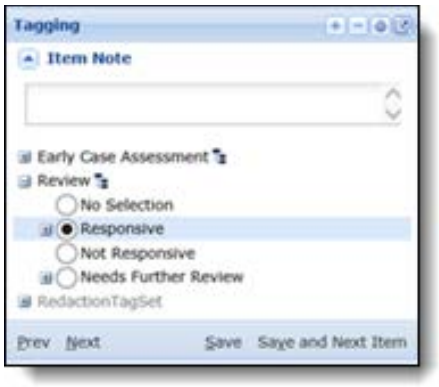

Figure 5 Choosing Preset Reason Codes in tagging panel

Figure 6 Using Preset Reason Codes as Filter Tags

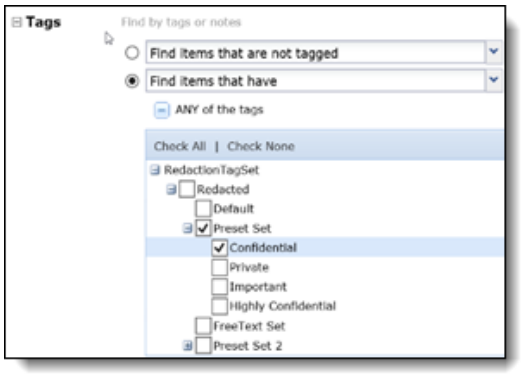

Figure 7 Using Preset Reason Codes in Advanced Search

Legal Hold Features

Integrated Windows Authentication Single Sign-on for Legal Hold

Veritas eDiscovery Platform supports Integrated Windows Authentication (IWA) Single Sign-On (SSO) for Legal Hold authentication. When IWA SSO is configured, the logged-in Windows credentials of the custodian are used for authentication, and the custodian is subsequently directed to the Legal Hold Confirmation page without the need to enter login credentials. To use the SSO option, LDAP must be configured and enabled against the Active Directory domain from which Windows users will be authenticating.

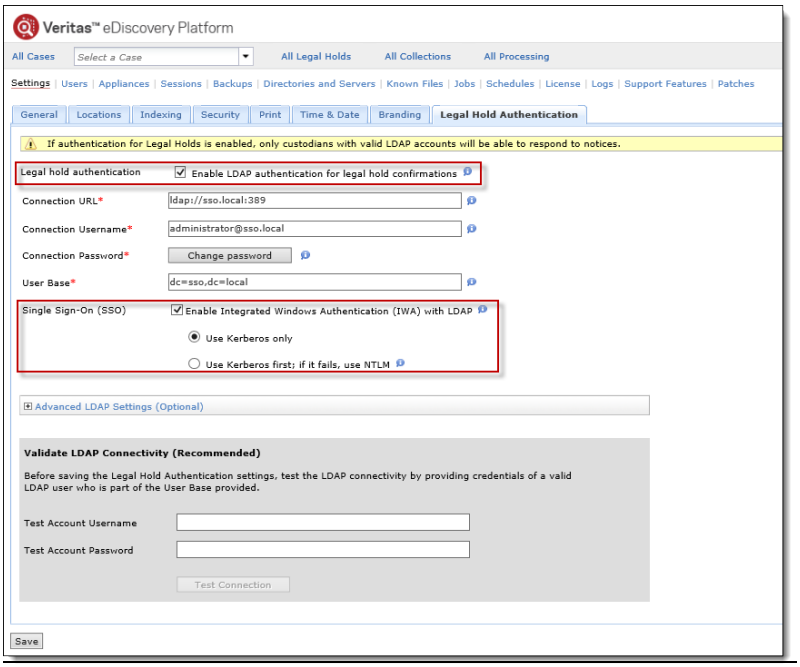

Figure 8 Setting up custodian IWA SSO for Legal Hold authentication

System Administration Features

Case Backup Integrity

During an eDiscovery Platform backup, empty directories may be created in the backup structure. If a case backup directory is then moved and empty directories are not copied, a restore job will subsequently fail. With this release, restore job for a case backup with empty directories does not fail. With the Case Backup Integrity feature, a checksum of the case backup directory is created during both the backup and the restore job. The checksum file created during the restore job is compared with the checksum file created during the backup job. If any empty directory is identified, then these empty directories are created at their specific paths during restore. This results in the success of the restore jobs.

Obtaining More Product Information

To obtain more information:

Sign in and use the MyVeritas portal for downloading product software, licensing and support:

- Information and the replacement options are located here: https://www.veritas.com/support/en_US/article.000001129
- For cumulative hotfix information and downloads, visit the Veritas eDiscovery Platform support site: https://www.veritas.com/content/support/en_US/DocumentBrowsing.html?product=eDiscovery%20Platform

You can download the appropriate Veritas eDiscovery Platform product files from the Veritas Entitlement Management System (VEMS), previously the Veritas Licensing Portal.