

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

Copyright © 2017 Veritas Technologies LLC. All rights reserved.

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

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

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

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

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

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

<http://www.veritas.com>

Contents

About this Document	4
What's New in 9.0?	4
Processing Features.....	4
Information Classification.....	4
Analysis and Review Features	6
Bulk Redaction and Delete Bulk Redaction	6
Annotations in Review Mode.....	6
Redaction sets with preset reason codes	7
Legal Hold Features.....	9
Integrated Windows Authentication Single Sign-on for Legal Hold.....	9
System Administration Features	10
Case Backup Integrity.....	10
Obtaining More Product Information	10

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:

- [Processing Features](#)
- [Analysis and Review Features](#)
- [Legal Hold Features](#)
- [System Administration Features](#)

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.

Description: Sec vs. Tamas

Home Appliance: [Dropdown]

User Logins: Enabled [Dropdown]

Tagging: Enabled [Dropdown]

Document Dates & Times

Date Format: Use system format (mm/dd/yyyy) [Dropdown]

Time Format: Use system format (12 hr) [Dropdown]

Time Zone: Use system time zone (GMT-08:00) [Dropdown]

☐ Sort dates ascending by default

Document Security

☒ If a document is in a non-accessible folder, it is **still accessible** in other folders a user can access.

☐ If a document is in a non-accessible folder, it is **not accessible** in other folders a user can access.

Tagging and Other Administrative Dates & Times

☐ Use document dates and times [Dropdown]

☒ Use system dates and times [Dropdown] - Date Format: (mm/dd/yyyy) Thu May 25 2006
Time Format: (12 hr) 4:35:18 PM PDT
Time Zone: Use current appliance time zone (GMT-08:00)

☒ **Information Classification**

☒ Enable automatic classification of incoming data.
Note: Only policies enabled in the Information Classification portal will be utilized for classification.

[Define Active Directory parameters and specify internal domains](#)

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.

Filters [Docs] [Items]

► By Folder any

► By Tag any

▼ By Classification any

any | none [Icons]

- ☒ <Not Classified> (59) only
- ☒ ICD-10-CM (121) only
- ☒ PII (88) only
- ☒ US-FERPA (87) only
- ☒ US-FISMA (75) only
- ☒ Intellectual-Pr... (68) only
- ☒ US-CA-AB-1298 (41) only
- ☒ US-FFIEC (9) only
- ☒ US-HIPAA (8) only
- ☒ US-MA-201-CM... (6) only
- ☒ AU-Tax (4) only
- ☒ Corporate-Ethics (3) only
- ☒ US-CA-SB1 (2) only
- ☒ US-GLBA (2) only
- ☒ PCI-DSS (1) only
- ☒ Credit-Card (1) only
- ☒ Authentication (1) only
- ☒ US-SEC (1) only
- ☒ US-SSN (1) only

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

The screenshot shows a dialog box titled "Bulk Redact/Delete all redactions for Redaction Set". It has a "Redaction Set:" dropdown menu set to "Default". Under the "Settings" section, the "Action:" is set to "Bulk Redact" with the "Redact Text" option selected. Below this, there are fields for "Reason Code:" and "Redaction Color:". The "Redact Text" section includes a "Text to Redact" field with "SR02-12" entered, a "Find whole word only" checkbox, and a "Reason Code" dropdown set to "Corporate Confidential". There is also a "Redaction Color" dropdown set to black and a "Copy Reason Code for all rows" checkbox. At the bottom, there are three buttons: "Redact in Selected Items (0)", "Redact in All Items (23099)", and "Cancel".

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.

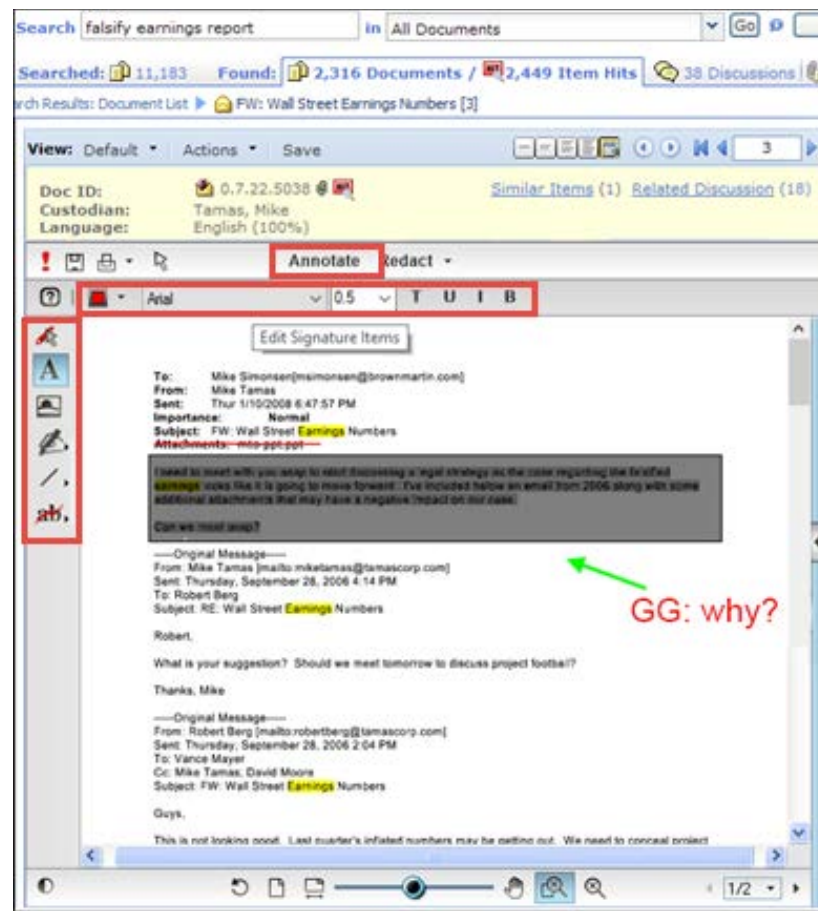


Figure 4 Annotation Controls

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.

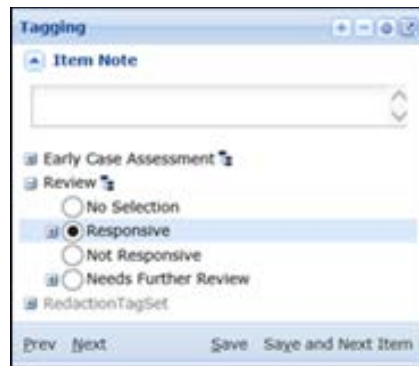


Figure 5 Choosing Preset Reason Codes in tagging panel

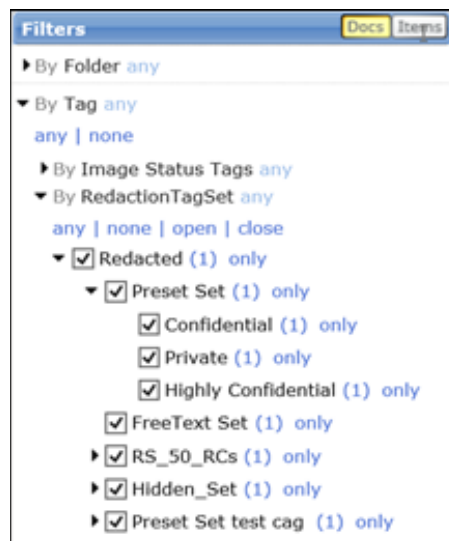


Figure 6 Using Preset Reason Codes as Filter Tags

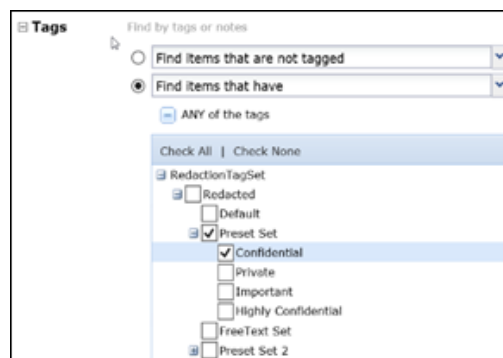


Figure 7 Using Preset Reason Codes in Advanced Search

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.

Veritas™ eDiscovery Platform

All Cases | Select a Case | All Legal Holds | All Collections | All Processing

Settings | Users | Appliances | Sessions | Backups | Directories and Servers | Known Files | Jobs | Schedules | License | Logs | Support Features | Patches

General | Locations | Indexing | Security | Print | Time & Date | Branding | Legal Hold Authentication

If authentication for Legal Holds is enabled, only custodians with valid LDAP accounts will be able to respond to notices.

Legal hold authentication ☒ Enable LDAP authentication for legal hold confirmations ⓘ

Connection URL* ldap://sso.local:389 ⓘ

Connection Username* administrator@sso.local ⓘ

Connection Password* ⓘ

User Base* dc=sso,dc=local ⓘ

Single Sign-On (SSO) ☒ Enable Integrated Windows Authentication (IWA) with LDAP ⓘ

☒ Use Kerberos only

☐ Use Kerberos first; if it fails, use NTLM ⓘ

Advanced LDAP Settings (Optional)

Validate LDAP Connectivity (Recommended)

Before saving the Legal Hold Authentication settings, test the LDAP connectivity by providing credentials of a valid LDAP user who is part of the User Base provided.

Test Account Username

Test Account Password

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.