Veritas eDiscovery Platform

Changes to Review User Interface 9.0-8.3

Preset Redaction Reason Codes

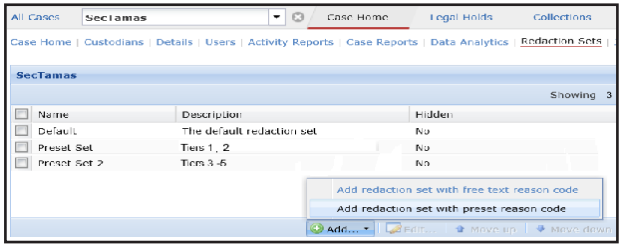
When the default redaction set is not sufficient, a redaction set with preset codes can be created, so users can apply codes consistently. See the *Review/Redaction User Reference Card* for the basic controls.

- Redaction set creation requires the Case Administrator to choose from free text or preset reason codes.

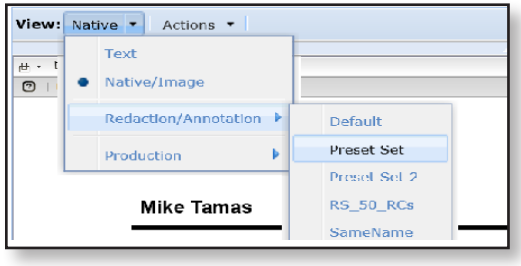
- For full redaction set creation requirements, see the *Case Administration Guide*, "Setting Up Redaction Sets".

- For Preset Reason Code instructions for use, see the *User Guide*, "Redacting Items."

Case Administrator



Case Reviewer



Annotation

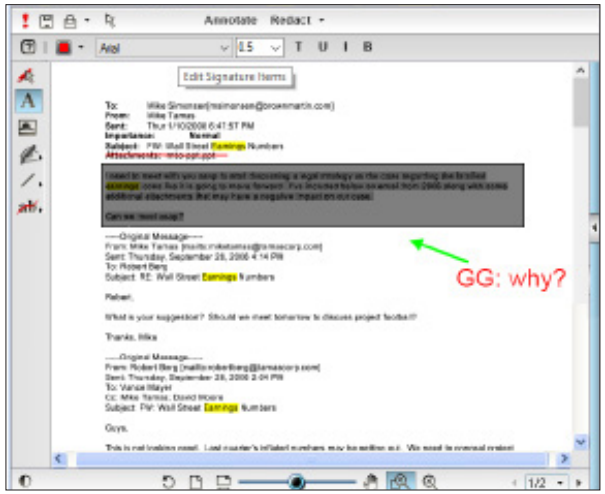
Annotation allows groups of reviewers to collaborate with increased detail about documents, employing a selection of editing tools that are distinct from the redaction tools. Reviewers can toggle between Annotate or Redact. See the *Review/Redaction User Reference Card* for the basic controls.

- Reviewers need access to review mode and privileges to redact/annotate.

- For redaction set creation requirements, see the Case Administration Guide.

- For Annotation details, see the *User Guide*, "Annotate an Item".

Case Reviewer



Bulk Redaction

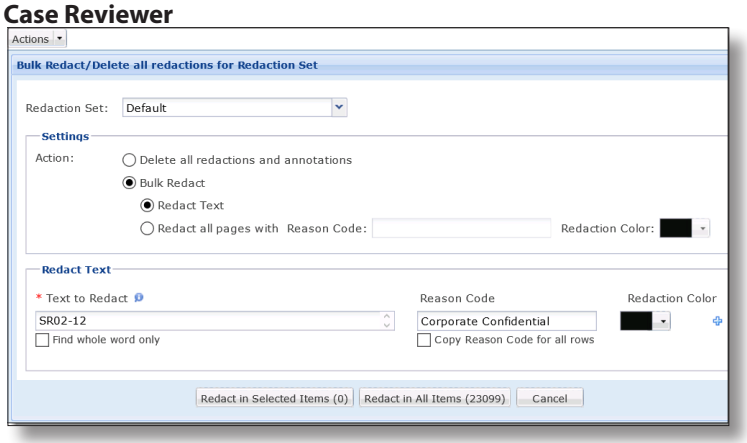
Bulk Redaction allows reviewers to redact multiple documents in a search result without reviewing each document in Native Viewer. Bulk redaction works on redaction sets with preset reason codes or with free-text reason codes.

- Any user with the "Allow Redacting" privilege can perform bulk redaction and delete bulk redaction operations.

- The System administrator will be able to see Bulk Redaction and Bulk Redaction Deletion in the Activity/Events reports.

For bulk redaction considerations, corpus preparation, workflow, and job monitoring, see the *User Guide*, "Bulk Redaction".

Case Reviewer



Changes to User Interface 9.0-8.3

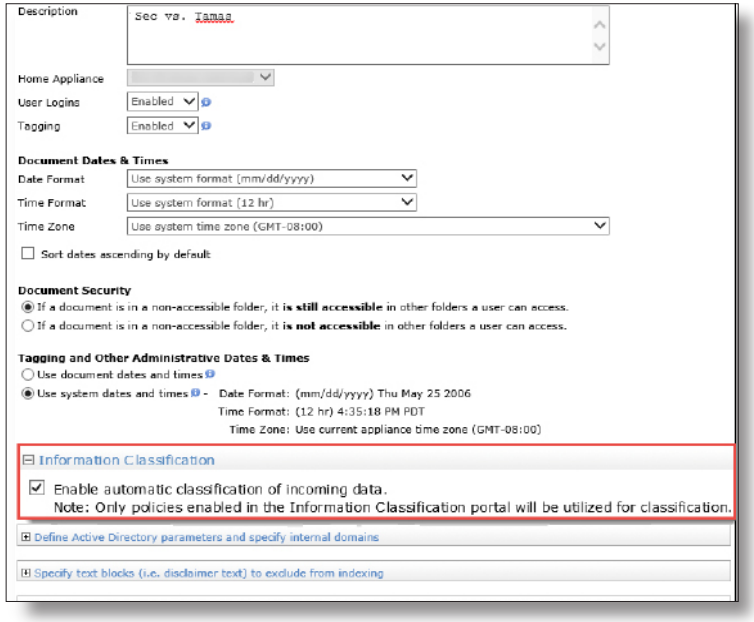
Veritas Information Classifier (VIC)

In release 9.0, Veritas eDiscovery Platform lets users automatically classify sensitive and critical data based on a set of built-in custom policies. The platform integrates with VIC to anyalyze and classify eDiscovery data. During processing, VIC uses both pre-defined and user-defined policies to assign classification tags to eDiscovery data.

Reviewers will be able to use classification filters in the Analysis and Review mode to identify documents that match the VIC tags.

Note: The Case Administrator needs to use the Veritas Information Classifier interface to enable or disable policies before case creation. See the Case Administration Guide "Information Classification" for full details.

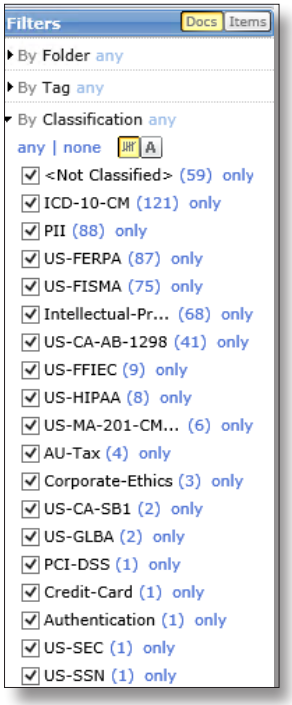
Case Administrator



After processing, Reviewers will see the policies appear as Classification tags. They can be used like any other filter in the Veritas eDiscovery Platform.

For more information, see the *User Guide* "Using Classification Information in eDiscovery".

Case Reviewer



More about Veritas Information Classifier:

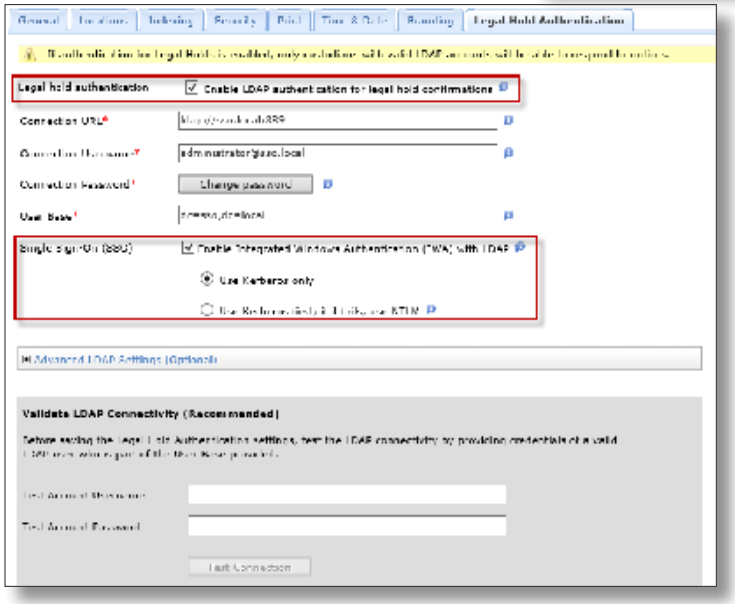
http://veritashelpsupport.com/Welcome?locale=EN_US&context=EV122VIC

Single Sign On for Legal Hold

Release 9.0 supports Integrated Windows Authentication (IWA) Single Sign-On (SSO) for Legal Hold authentication. When eDiscovery Platform is configured for IWA SSO, the logged-in Windows credentials of the custodian are used for authentication, and the custodian is directed to the Legal Hold Confirmation page without the need to enter login credentials.

Note: To use the SSO option, LDAP must be configured and enabled against the Active Directory domain from which Windows users will be authenticating. The custodians must be present in the Active Directory.

For more information, see the *Legal Hold User Guide* "Integrated Windows Authentication Single Sign-On for Legal Hold".



Changes to User Interface 8.2-8.x

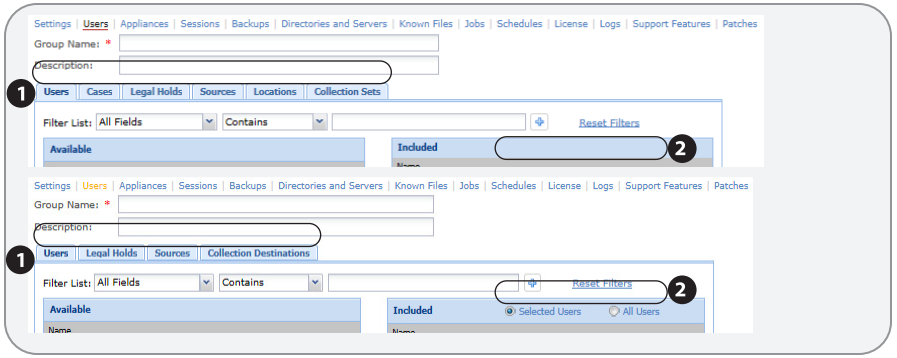
Access Groups or Case Authorization

In Veritas eDiscovery release 8.2, the **Access Groups** feature provides a greater level of access control across the entire workflow.

Note: Use of **Access Groups** is NOT required. Case and document access can still be assigned individually.

1. **Access Groups** now includes Cases and Locations.
2. When assigning any of these, there is no longer an add all option.

8.2



8.1.1

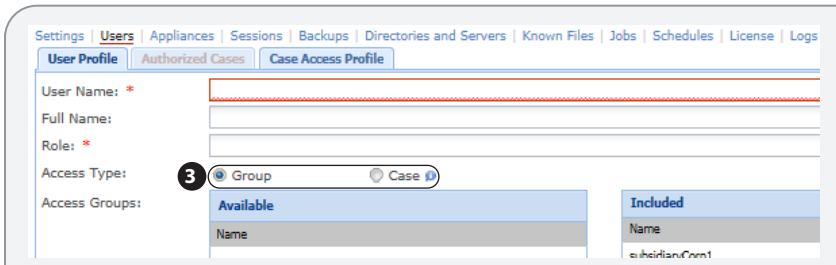
When creating users you now have the option to assign them to **Access Groups**, or give them specific case authorization.

Note: In version 8.2, you cannot give a user both group access and case authorization.

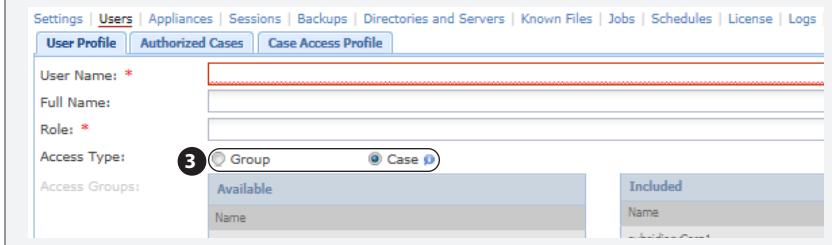
3. The Access Group option is now shown when viewing an existing user or creating a new user. Clicking on the **Case** radio button grays out the **Access Groups** selection windows. Previous versions did not offer **Access Group** selection when creating or editing users.
4. Clicking on the **Authorized Cases** tab presents a list of cases to be assigned or removed from that user.

For more information refer to the *System Administration Guide* section *Managing User Accounts: Access Group and User Creation* and *Managing Security of eDiscovery Platform: Access Groups*. Also, refer to the *Case Administration Guide: About Access Groups and Roles*.

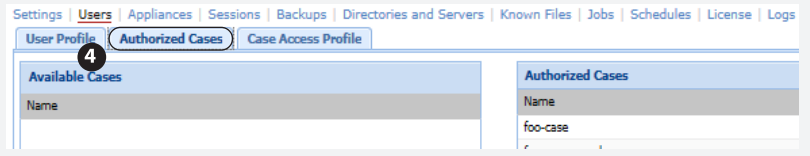
8.2



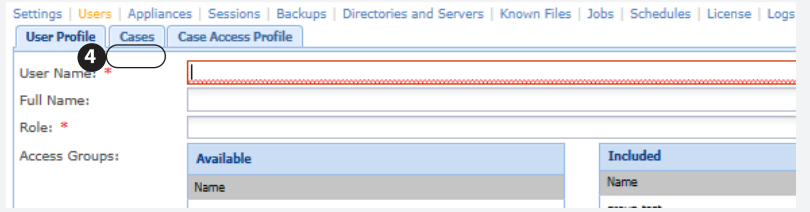
8.2



8.2



8.1.1



User Role Changes

Note: Starting with version 8.2, the **Group Admin** role has been created. It can add users, assign them to roles, and assign them to cases within a group.

At least one person must have the System Manager role to create **Access Groups** and apply the **Group Admin** role.

Refer to the *Veritas Upgrade Guide* and *Veritas Upgrade Overview* for more information.

Changes to User Interface 8.2-8.x

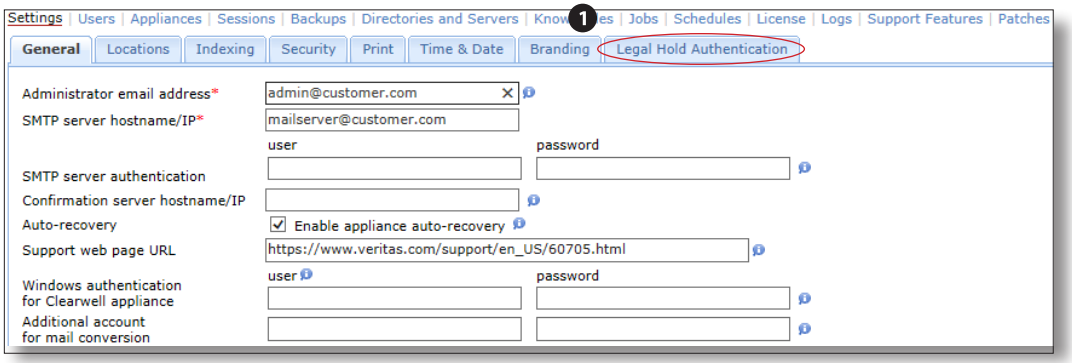
Legal Hold Authentication

1. Release 8.2 offers a legal hold authentication mechanism, in which **System Managers** can limit access to a legal hold confirmation page only to the intended custodian. Only the intended custodian, who must have a valid LDAP account, will be able to see the notice.

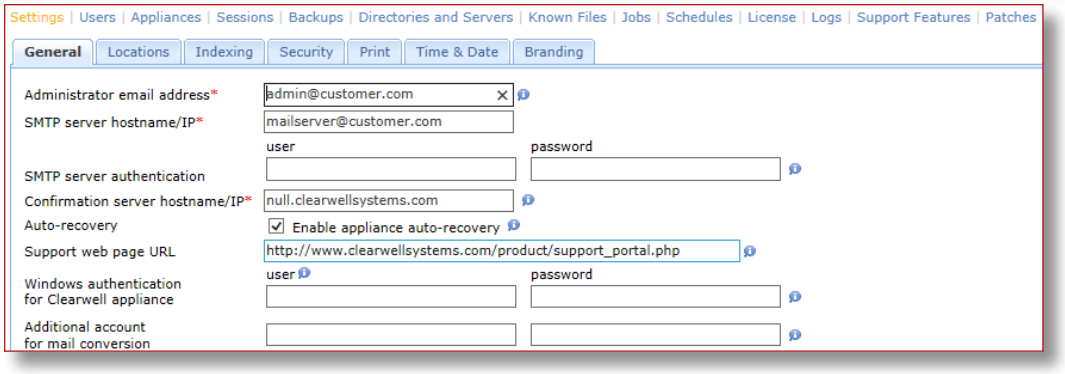
   Refer to *Legal Hold User Guide: Legal Hold Authentication* for more information.

2. Note: The **System Manager** must ensure that the required custodians exist in Active Directory before enabling LDAP authentication for legal holds. Refer to the *Identification and Collection Guide: Importing Custodians to Your Data Map* for details on adding or importing custodians.

8.2



8.1



8.2