Introduction to Enterprise Vault.cloud™

Discovery.cloud

VERITAS™

Introduction to Enterprise Vault.cloud™ Discovery.cloud

Last updated: 2020-04-23

Legal Notice

Veritas Technologies LLC

2625 Augustine Drive

Santa Clara, CA 95054

http://www.Veritas.com

Table of contents

Overview

This document is intended for AdvisorMail customers transitioning to Veritas Advanced Supervision. This document provides a summary of some of the powerful discovery capabilities available to you with Advanced Supervision.

Introduction

With your transition from AdvisorMail to Veritas Advanced Supervision, your organization benefits from powerful new features that were previously only available to the Enterprise Vault.cloud™ customers. Advanced Supervision is now a part of the Enterprise Vault.cloud (EV.cloud) archiving platform. This transition offers you access to Enterprise Vault.cloud's Discovery.cloud – commonly referred to as Discovery Archive (DA).

Veritas recommends you refer to the EV.cloud user guides, Help documentation, and release notes, available at http://evcnews.veritas.com.

About Discovery.cloud

Discovery.cloud provides the tools to search your company's archived Enterprise Vault messages to discover those that are pertinent to litigation cases or infringements of corporate policies and regulations. Discovery.cloud provides matter management features for eDiscovery work, including the ability for multiple reviewers to collaborate during the eDiscovery process. Messages that are found to be of interest can be exported for external review.

Discovery.cloud key features

Discovery.cloud includes the following features:

- **Advanced iterative search capabilities**

  Discovery.cloud enables you to accelerate eDiscovery and investigations with powerful search capabilities to deliver fast results. Discovery.cloud enables you to build iterative searches using multiple criteria and to refine searches until the relevant information is located. If you add any criteria that narrow the search results too significantly, you can delete the term that limited the results, without re-building the entire search.

  Once the desired criteria are established, you can save the search. If you save the search as an on-going search, any new items that meet the criteria are automatically found, which significantly reduces review time. The phrase, Boolean, proximity, and wildcard search functionality enables relevant information to be found quickly and allows further refinement of search results before export.

- **Collaborative eDiscovery workflow**

  Discovery.cloud provides a built-in collaborative workflow. Discovery.cloud's matter management capabilities enable multiple reviewers to interact and collaborate on a specific matter. Once a matter is created, you can provision each reviewer with distinct privileges within the matter. Reviewers can review messages, view matter logs and reports, create exports, manage other reviewers, and edit a matter, depending on their privileges.

  A reviewer with access to a matter can use the extensive search capabilities to search the archives of the custodians involved. Searches can be saved and assigned to various reviewers to distribute the workload and expedite the eDiscovery process.

  A reviewer can place archived information on legal hold, apply review statuses and labels, categorize information, and add notes for other reviewers.

- **Flexible export options**

  Designated reviewers and administrators can perform online exports of search results. The ability for you to export data yourself minimizes your IT team's workload.

  You can export archived information from the archive in EML, PST, and NSF formats, with or without EDRM XML files. The archived information can then be imported into solutions like the Veritas™ eDiscovery Platform. An authorized reviewer or administrator can name and password-protect their exports.

  Note: Exports may not exceed 200,000 messages per request. Please refer to Customer Responsibilities in the EV.cloud service description for additional information on export restrictions.

- **Reporting**

   Discovery.cloud offers reporting functionality for reviewers and administrators to view audit trails for individual messages, or to view the history of an entire matter.

- **Classification with the Enterprise Vault.cloud Information Classifier**

   If your company has the Veritas Information Classifier service enabled[1], the service can apply classification tags to Enterprise Vault.cloud's incoming emails that match the enabled policies in the Veritas Information Classifier. Discovery.cloud users can then search for the emails that are tagged with these classification tags.

---

[1] Requires additional purchase. Contact your partner or Veritas sales representative for more information.

Getting started with Discovery.cloud

The following image shows a typical view of a matter in the **E-Discovery** tab for an approved Discovery Archive administrator.

The selection tabs you see at the bottom left of the user interface, and the features that are available within each tab depend on the roles and privileges of your Enterprise Vault.cloud account.

Section	Description
Investigations	The Discovery.cloud **Investigations** tab provides access to your archived emails. Administrators and reviewers can also use this tab to access and review the archived emails of user accounts that they manage.
E-Discovery	The **E-Discovery** tab includes the matter management feature. This feature allows multiple reviewers to interact and collaborate on litigation matters during the eDiscovery process.
Administration	The **Administration** tab provides administrators with access to the company's Enterprise Vault.cloud Administration Console. For reviewers and users with the **Account** role, the **Administration** tab displays options to change your password and personal time zone.
Alerts	The **Alerts** tab allows administrators and reviewers to quickly and easily create alerts. Alerts are a helpful tool for administrators and reviewers, as they help monitor your company's email usage.
Dashboard	The **Dashboard** tab provides administrators and reviewers with archive statistics.
Help	The **Help** tab provides access to Discovery.cloud user guide.

About account roles and Discovery.cloud

Enterprise Vault.cloud accounts are each assigned to one of the following roles:

- **Account:** Tabs available are Investigations and Administration (for setting personal preferences only). Users with the Account role have the fewest privileges within Discovery.cloud. They have access only to the Investigations tab, from where they can view their archived emails.

- **Reviewer:** Tabs available are Investigations, E-Discovery, Administration (for setting personal preferences only), and Alerts. Users with the Reviewer role can monitor employee emails.

- **Administrator:** Tabs available are Investigations, E-Discovery, Administration, Alerts, and Dashboard. The Administrator role is for company administrators who need to configure and manage Discovery.cloud, or for HR personnel who need to monitor employee email usage. Administrator roles must be assigned by selecting the Monitor All Accounts privilege in the Administration Console if they are to monitor email usage. Unlike the accounts with the Reviewer role, the accounts with the Administrator role cannot be granted access to selected accounts.

System Administrators and Role Managers with the required privileges can assign accounts to one of these roles in the Role Management node of the Enterprise Vault.cloud Administration Console.

About investigations

From the Discovery.cloud Investigations tab, administrators or reviewers can conduct initial, probative, or ad hoc investigations on the archives of the accounts that they have the privileges to monitor. For example, you can assess compliance with corporate content or regulatory policies before deciding whether there is a requirement to create a tracked eDiscovery matter.

Typically, an investigation is an internal search. For example, you can assess compliance with corporate content policies, or respond to a request to find private information on a user. You can search for data in the emails of multiple user accounts all in one place.

Performing a new search of accounts (Investigations tab)

You can search the content of archive accounts from the Investigations tab, using Basic Search, Advanced Search, or Query Search.

To perform a new search for email content (Investigations tab):

1. Select the **Investigations** tab, and then select the node where you want to perform the new search:

    - To search your own mailbox, select **My Mailbox** > **Mailbox**, or select **My Mailbox** > **Saved Searches** > **New Search**.

    - To search one or more of your managed accounts, select **Managed Accounts** > **Saved Searches** > **New Search**.

    - Or to search a single managed account, select **Managed Accounts** > **Accounts** and click the required account.

    The following figure shows an example of the Basic Search box:
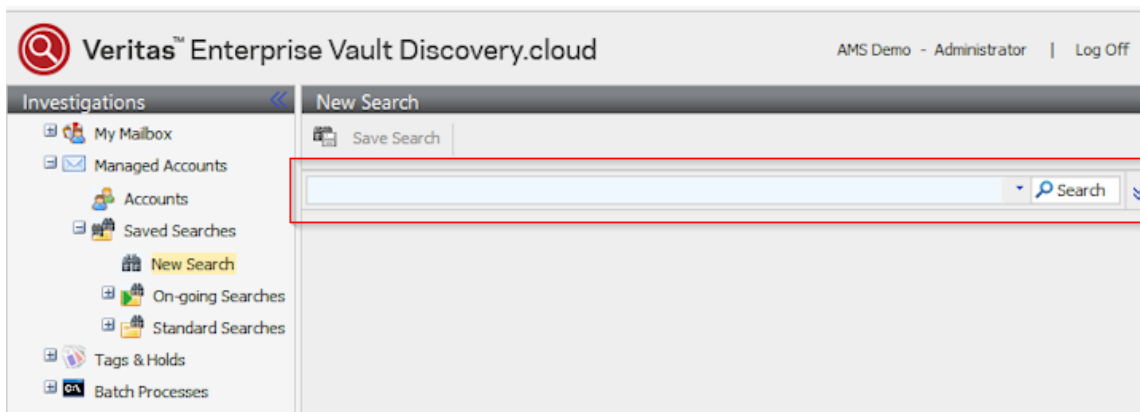
    Perform step 2 for a Basic Search, step 3 for an Advanced Search, or step 4 for an Advanced Search.

2. To perform a Basic Search:

    - Type a search term or phrase in the search box. You can enter up to 1000 characters. The search is not case-sensitive. The search supports phrase search, Boolean operators, proximity search, and wildcard search.

    - Click **Search** to start the search.

    - To filter the search results by date, click the single-arrow drop-down icon that is adjacent to the Basic Search box, and then select a date from the displayed calendar, or select a date option.
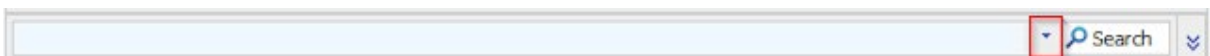
3. To perform an Advanced Search, click the **Expand** icon in the Search bar:
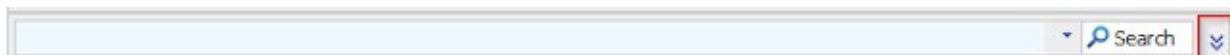
The Advanced Search options then appear. The **Search Custodian(s)** option appears only if you are searching the content of multiple accounts.
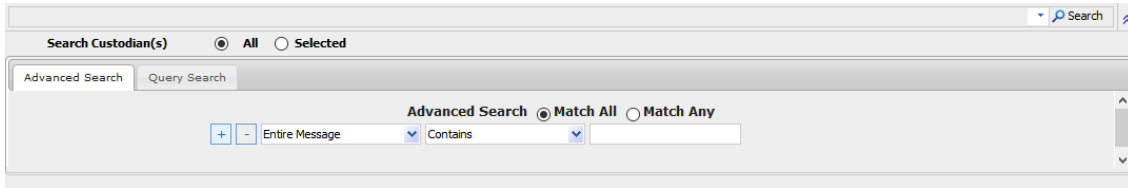
If you are searching content of multiple archive accounts, the **Search Custodian(s)** option lets you choose the accounts to include. To search all the accounts, select **All**. To search specific accounts, click **Selected** and then click **Add/Remove Custodian(s)** to select the required accounts.

Specify what to search for:

- o To define multiple search clauses, click the **+** icon and complete a new row for each clause.
- o Searches are not case-sensitive. The search supports phrase search, Boolean operators, proximity search, and wildcard search.

Choose from **Match All** or **Match Any** to indicate whether all the defined clauses must be matched, or whether the search results can include any matched clause.

Then click **Search** to start the Advanced Search.

4. To perform a Query Search, click the **Expand** icon in the Search bar.

The Advanced and Query Search options then appear.

- In the text box, write your required Query Search using Lucene Syntax. See https://lucene.apache.org/core/2_9_4/queryparsersyntax.html
- Click **Search** to start the Query Search.

5. To save the Basic, Advanced, or Query Search click **Save Search** and complete the Save Search dialog.

Generating printable reports for searches (Investigations tab)

Any user who has access to **Saved Searches** can generate the **Printable Reports** in all searches in **Investigations** and **E-Discovery**.

To generate a Printable Report for Searches:

1. Go to any of the Saved Search tabs in **Investigations**.
2. Go to any **Saved Search** Tree Node.
3. Go to a Saved Search.
4. Click the **Export** button and click **OK** on the pop-up.

When the button is clicked, it generates a report with the custodians, the parameters and the results.

About matters in eDiscovery

In Discovery.cloud the Discovery Administrator creates a matter as a container in which to associate the related emails and attachments for a subject on which they want to perform a traceable examination.

Matters are created and managed in the **E-Discovery** tab. When creating a matter, the Discovery Administrator selects the user accounts (custodians) that the eDiscovery is to include. Within the matter, the Discovery Administrator can create and save the searches that find the custodian emails and attachments that may be pertinent to the matter. The searches and review actions within a matter are traceable.

Matter workflow summary: Discovery Administrator

Process for a Discovery Administrator to set up a new matter shows the steps that are required for a Discovery Administrator to create and manage a matter.

Phase	Action	Description
Phase 1	Prepare the reviewers, labels, and review statuses for the matters.	• Prepare the reviewers. The System Administrator can assign Enterprise Vault.cloud accounts to the **Reviewer** and **Administrator** roles as required. Review the current list of reviewers and the matters to which they are assigned from the **E-Discovery** > **Administration** > **Reviewers** node. • Prepare the labels. You can use the default labels or create customized labels to suit your company's processes and requirements. Labels are applied to emails typically to mark them as exempt from the review process. The default labels are **Spam**, **Privileged**, and **Personal**. You can manage the labels from the **E-Discovery** > **Administration** > **Labels** node. Prepare the review statuses. • Prepare the review statuses. You can create review statuses and choose which are available when creating new matters.
Phase 2	In E-Discovery > Matters, add a new matter.	The steps to add a new matter are: • Provide a name, description, and expiry date. • Apply legal hold for the matter, if required. • Select the user accounts (custodians) on which to perform eDiscovery. • Select one or more reviewers for the matter. • Select the review statuses to use with the matter.
Phase 3	Create a search.	Use a search to find the data of interest. Run the search to check the results. The results of assigned searches determine the emails that the reviewers process. Typically, the reviewers do not see any other emails than these.
Phase 4	Apply labels and tags to the search.	Apply labels, tags, and notes to emails as required.
Phase 5	Save the search and assign it to a reviewer.	Assign the required searches to the reviewers for analysis. You can divide the search results between multiple reviewers. Apply a search-level legal hold, if required.

Performing a new search of a matter

Administrators or reviewers with the appropriate permissions can search the archives that are associated with a selected matter.

A search can then be saved and assigned to the matter's reviewers as required.

To perform a new search of a matter:

1. From the **E-Discovery** tab, select the **Matters** node to display the matters list in the main pane.
2. Select the required matter from the matters list.

   Under the **Matters** node in the left pane a **matter_name** node appears for the selected matter.
3. Under the **Matters** > **matter_name** node, expand **Saved Searches**.
4. Click **New Search**.
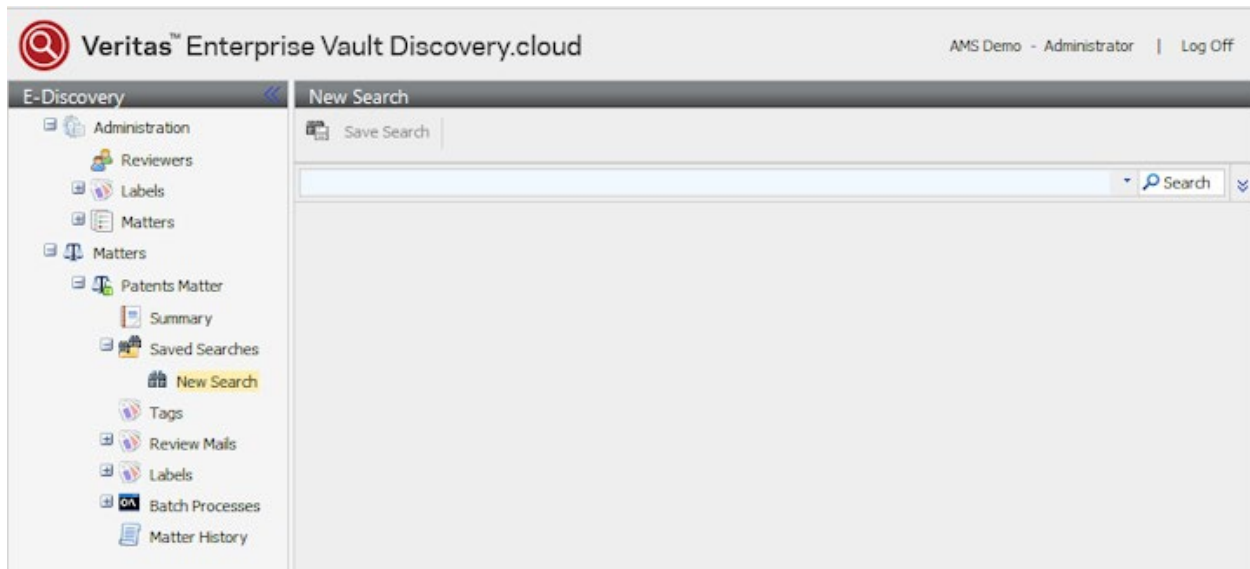
   From here you can perform a Basic Search or an Advanced Search on the matter.

5. To perform a Basic Search on all the custodian archives:
   - Enter a keyword or phrase in the search field. The search is not case-sensitive. You can enter up to 1000 characters. The search supports phrase search, Boolean operators, proximity search, and wildcard search.
   - To start the Basic Search, click **Search**.
   - To filter the search results by date, click the single-arrow drop-down icon that is adjacent to the Basic Search box, and then select a date from the displayed calendar, or select a date option.
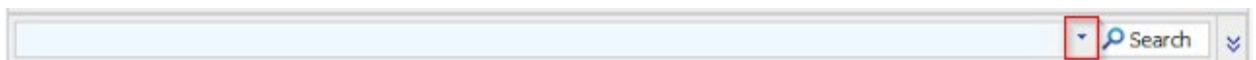
6. To perform an Advanced Search, click the **Expand** icon in the Search bar:
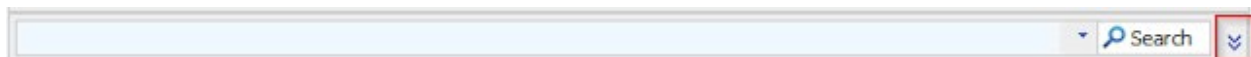
   The Advanced Search options then appear.
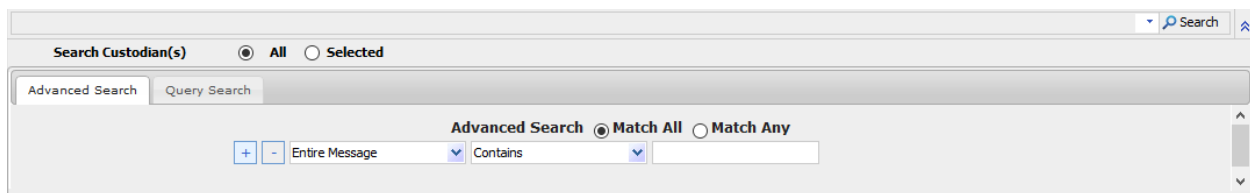
7. Next to **Search Custodian(s)**, choose the custodian archives you want to search. To search the archives of all the custodians that are associated with the matter, select All. To choose the custodians, click **Selected** and then click **Add/Remove Custodian(s)** to select the required custodians.

8. Specify what to search for:

   - To define multiple search clauses, click **+** and complete a new row for each clause.
   - Searches are not case-sensitive. The search supports phrase search, Boolean operators, proximity search, and wildcard search.

9. Select either **Match All** or **Match Any** to indicate whether all the defined clauses must be matched, or whether the search results can include any one matched clause or more.

10. To run the Advanced Search, click **Search**.

11. (Optional) To perform a Query Search, click the **Expand** icon in the Search bar.

    The Advanced and Query Search options appear.

    - In the text box, write your required Query Search using Lucene Syntax.
      See https://lucene.apache.org/core/2_9_4/queryparsersyntax.html.
    - Click **Search** to start the Query Search.

12. To save the Basic, Advanced, or Query Search, click **Save Search** and complete the Save Search dialog.

About reviewing matters

As a reviewer of a matter in the E-Discovery tab, you see only the resulting emails from the matter searches that are assigned to you. You work with those emails to identify the content of interest. Discovery.cloud provides review status tags, custom tags, and labels, all of which you can apply to emails to help you manage the review process. You can then discover the emails by tag name.

If your organization is enabled for the Veritas Information Classifier service, some emails may be tagged with classification tags. The presence of a classification tag indicates that the email matches a classification policy that has been enabled in the Veritas Information Classifier.

You can also add matter-specific notes to an email that another reviewer who works on the same matter can see.

Additionally, the eDiscovery function includes various reporting features. These features allow reviewers to view audit trails for individual emails or the history of an entire matter.

Matter workflow summary: reviewer

The Discovery Administrator configures a reviewer's permissions within each matter. The roles and permissions that can be granted to reviewers in Enterprise Vault.cloud and Discovery.cloud are very flexible. The reviewer process that is described in this documentation is for a typical company setup. Your company may give more permissions to a reviewer if required.

The Discovery Administrator typically saves one or more searches based on the criteria of interest for the matter and assigns the results to one or more reviewers for analysis. As a reviewer, when you open a matter in Discovery.cloud, you see the list of emails that are assigned to you for that matter.

Phase	Action	Description
Phase 1	In E-Discovery > Matters, open a matter	Under the Matters node in the left pane, a matter_name node appears for the selected matter. This node contains a number of sub-nodes that provide details of the matter as follows. The available options depend on your permissions: • **matter_name**: Click this node to display the Edit Matter pane. If you have the required permissions, you can edit the details of the matter in this pane. • **Summary**: Click this node to view a Matter Information Summary table. • **Saved Searches**: From this node, you can perform new searches or run any saved searches that are related to the matter. • **Tags**: Click this node to view all the tag assignments for the matter. • **Review Mails**: Click this node to review the emails of the custodians that are associated with the matter. • **Labels**: Click this node to view details of the assigned labels. • **Batch Processes**: Click this node to view the exports that are associated with this matter. • **Matter History**: Click this node to view a table of actions that were performed on this matter.
Phase 2	View the emails that are assigned to you.	Review your assigned emails under the **Review Mails** node. Work through the emails and attachments one by one to assess the content of interest. Your Discovery Administrator can inform you of the details to look out for.
Phase 3	Review each email for any content that is pertinent to the matter.	You can work with each email in the following ways as required: • **Apply a review status**: By default, all emails have the **Not reviewed** status applied. As you process each email, apply the appropriate review status. • **Apply a tag**: Add your own tags to emails to help organize your work, if required, or apply a managed tag. • **Add a note**: Add a note to an email if required. • **Manage legal holds**: Typically, all emails for a matter have legal hold applied. As you review the individual emails, you can remove or retain the legal hold as appropriate. • You can also perform other actions on the emails, as required.
Phase 4	Export emails.	You can export emails in a variety of formats. For example, you can export contentious emails to an internal HR representative or an external legal counsel. You can export emails, view the status of mail exports, and resubmit failed exports.

Exporting emails

During the review process, reviewers can export emails in EML, NSF, PST, EML with EDRM, msg with EDRM, and PST with EDRM format.

To export emails:

1. Browse the archives for the accounts that are assigned to you or conduct a search.
2. Select the emails you want to export.
3. Click the export icon and select an export option.
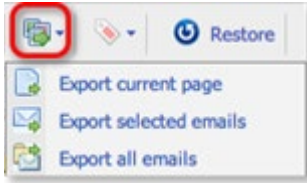
4. Enter the required information in the **Export Options** dialog.

5. Click **Export** Items.

6. To review export status, expand the **Batch Processes** node and select **Exports**.

About collaborative eDiscovery reporting

Discovery administrators and reviewers with the appropriate permissions can review the reports that contain matter-related actions. They can review reports by email, by matter, or by an archive.

Collaborative eDiscovery reports contain the following information:

- Created Matter
- Created Search
- Search criteria used
- The number of emails that are assigned to a specific reviewer

Report	Description
Report by email: Audit trail	Reviewers can review the audit trail for a specific email that includes actions performed, such as review status or the applied labels and export details.
Report by Matter: Matter History	Reviewers can see and search all actions which are performed within a matter such as edits on matter details, reviewer permission changes, or created exports. Only Discovery administrators or reviewers with the View Matter Logs/Reports permission can view reports for a matter.
Report by Matter: Matter Summary	Discovery administrators and reviewers can view a report for individual matters, which includes the number of reviewers, custodians, emails, and legal holds. The matter expiration date is also displayed.
Report by Archive: eDiscovery dashboard	Discovery administrators can view a report for the entire archive. This report includes the number of emails within each matter and the number of matters that are assigned to a reviewer.

Creating an alert

Administrators and reviewers can create an alert that sends an email notification each time a user sends or receives an email that meets flagged criteria. For example, Administrators and Reviewers can create alerts to flag emails with profanity in the subject line, message body, or attachment.

To create an alert:

1. Create a saved search that defines the criteria for the alert.
2. Select the **Alerts** tab.
3. Click the plus icon to display the **Add Policy Alert** page.
4. Enter the information for the alert in the **Add Policy Alert** window.
5. Click **Save**.