About Enterprise Vault Advanced eDiscovery

This section includes the following topics:

- Introducing Enterprise Vault Advanced eDiscovery
- Advanced eDiscovery key features
- About classification
- Advanced eDiscovery term definitions

Introducing Enterprise Vault Advanced eDiscovery

This guide describes Veritas™ Enterprise Vault Advanced eDiscovery and describes how to use all of its key features.

Enterprise Vault Advanced eDiscovery is a web-based service that enables your company to respond proactively to litigation requests, ensure adherence to company communication policies, and meet regulatory requirements.

Advanced eDiscovery 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. Advanced eDiscovery provides case 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.

> “ ”

Note: This updated edition of theAdvanced eDiscovery User Guideincorporates information about the search feature that was previously included in theAdvanced eDiscovery Search Guide.

> “ ”

Recent updates to Advanced eDiscovery

Recent updates to Advanced eDiscovery include the following:

- Integration with the Veritas Information Classifier. Advanced eDiscovery's message search criteria now include options to search for the emails that are tagged with classification tags from the Veritas Information Classifier.

See About classification.

- Integration with the Microsoft Teams : The message search criteria in Advanced eDiscovery now include options to search from messages that are archived from Microsoft Teams. See About Targeted Collections. and the section called “Configuring Targeted Collection for Microsoft Teams”.

A list of the updates that were included with previous releases of Advanced eDiscovery is provided separately.

See About the Advanced eDiscovery updates in previous releases.

For full details of all the updates in each release of the Enterprise Vault.cloud service suite, see the Enterprise Vault.cloud release notes. You can access the release notes from the following article on the Veritas Support website:

http://www.veritas.com/docs/000100485

Advanced eDiscovery key features

Advanced eDiscovery includes the following features:

- Advanced iterative search capabilities

Advanced eDiscovery enables you to accelerate eDiscovery and investigations with powerful search capabilities to deliver fast results. Advanced eDiscovery 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. 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

Advanced eDiscovery provides a built-in collaborative workflow. Advanced eDiscovery's case management capabilities enable multiple reviewers to interact and collaborate on a specific case. Once a case is created, you can provision each reviewer with distinct privileges within the case. Reviewers can review messages, view case logs and reports, create exports, manage other reviewers, and edit a case, depending on their privileges. The external reviewers can have the additional privilege - download shared export - that allows them to download the exports shared by the administrator.

A reviewer with access to a case 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 status tags and labels, categorize information, and add notes for other reviewers.

- Classification with the Enterprise Vault.cloud Information Classifier.

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

See About classification.

- 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.

- Reporting

Advanced eDiscovery offers reporting functionality for reviewers and administrators to view audit trails for individual messages, or to view the history of an entire case.

About classification

The Veritas Information Classifier now integrates with Enterprise Vault.cloud to classify the emails that Enterprise Vault.cloud archives. The Veritas Information Classifier's built-in policies address many of the regulatory requirements and corporate standards for which you may want to classify emails.

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

For example, your company can enable the classification policies that detect personally identifiable information (PII) to help meet privacy regulations like the General Data Protection Regulation (GDPR).The PII policies match content like credit card numbers, email addresses, dates of birth, passport numbers, and driver's license numbers. When the Veritas Information Classifier identifies an email that matches the criteria for the policy, a PII classification tag is assigned in a header that gets added to the email. A Advanced eDiscovery reviewer can then perform a search for the emails that have the PII tag assigned. In this way, classification reduces review effort to meet your organization's regulatory requirements.

Note the following about the classification process:

- The classification tags that are associated with a policy get applied only to those matching emails that are ingested into Enterprise Vault.cloud after the policy is enabled. Any previously archived emails do not get tagged.
- If your system administrator changes or disables a classification policy, the changes affect the emails that are subsequently ingested into Enterprise Vault.cloud. The changes are not reflected in the existing archived emails. For example if you disable a previously enabled classification policy, any archived emails that were tagged as a result of matching the policy remain tagged in Enterprise Vault.cloud.

For information on how set up the classification of emails with the Veritas Information Classifier, see the Enterprise Vault.cloud Archive Administration Help.

Advanced eDiscovery term definitions

Table: Advanced eDiscovery definitions lists some specific terms that are used in Advanced eDiscovery and explains their meaning in this context.

Table: Advanced eDiscovery definitions

TERM	DESCRIPTION
Classification	If your company is enabled for the Veritas Information Classifier service, you can simplify data management decisions by categorizing data based on classification policies. The Veritas Information Classifier integrates with Enterprise Vault.cloud to analyze the emails that Enterprise Vault.cloud stores. The Veritas Information Classifier service assigns classification tags to those emails that match the classification policies your Enterprise Vault.cloud system administrator has enabled.
Classification tag	The Veritas Information Classifier service assigns classification tags to the incoming emails that match the conditions of an enabled classification policy. Advanced eDiscovery users can search on the classification tags as part of their eDiscovery work.
Custodian	In the context of Advanced eDiscovery, a custodian is anyone for whom your organization holds or has held an archive account. When a Discovery Administrator creates a case, they assign the custodians that the associated eDiscovery is to include.
eDiscovery	eDiscovery is the electronic aspect of identifying, collecting, and producing electronically stored information in response to a request for production in a law suit or investigation.
GDPR	General Data Protection Regulation. A regulation to strengthen and unify data protection for individuals within the European Union (EU). The GDPR aims primarily to give control back to citizens and residents over their personal data and to unify data protection regulation within the EU.

TERM	DESCRIPTION
Investigation	In the context of Advanced eDiscovery, this term means to examine and discover the factors of a potentially legal inquiry.
Label	Apply a label to an email typically to mark it as exempt from the review process. The default labels are: Spam , Privileged , and Personal . You can create custom labels to suit your company's requirements.
Legal Hold	A legal hold is a process that an organization uses to preserve relevant information for legal reasons.
Case	In law, a case is a subject that is in controversy or in dispute. In Advanced eDiscovery a Discovery Administrator creates a case to act as a container in which to associate all the related emails and attachments for such a subject.
Tag	In Advanced eDiscovery a tag is a marker that can be applied to emails to help organize the process of investigation or review.
	- In the E-Discovery tab you can tag an email with a review status tag to indicate its status in the eDiscovery review process.
	- You can apply your own custom tags to emails as you want, for example to retrieve identically tagged emails easily at a later time. These tags are visible only to the user that applies them.
	- You can tag emails with a managed tag, if you have any of these available to you. Managed tags are created in the Enterprise Vault.cloud Administration Console, under the My Config > Managed Tags node.

TERM	DESCRIPTION
	- If your company uses the Veritas Information Classifier service, the service can apply classification tags to the emails that match the enabled policies in the Veritas Information Classifier. You can search for these classification tags as part of your eDiscovery work. Note that the classification tags cannot be applied manually.

Getting started with Advanced eDiscovery

This section includes the following topics:

- Logging on to Advanced eDiscovery
- About the Advanced eDiscovery user interface
- Accessing your own archived emails

Logging on to Advanced eDiscovery

When your company signs up for Advanced eDiscovery, you are provided with a user name and password. With these credentials, you can log on to Advanced eDiscovery and start using the features that you have the permissions to access.

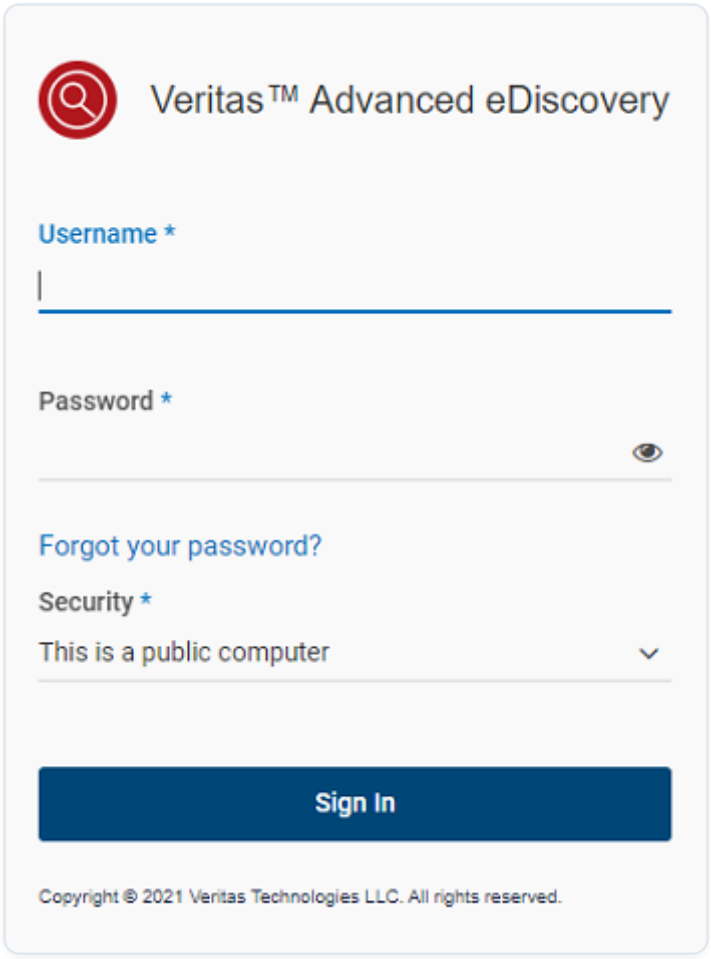
> “ ”

Note: Advanced eDiscovery users should exercise caution when accessing their accounts from public computers, to maintain the confidentiality of company emails. This note applies especially for administrators and reviewers. **Note:** If your company signed up for Advanced eDiscovery and you have not received your credentials, contact your administrator.

> “ ”

To log on to Advanced eDiscovery

1. Navigate to your Advanced eDiscovery URL.



2. Select a **Security** option.

Refer to the following table for more information:

THIS IS A PUBLIC OR SHARED COMPUTER	PROMPTS YOU FOR YOUR USER NAME AND PASSWORD EACH TIME YOU ACCESS THE LOGON SCREEN, AND LOGS YOU OUT AFTER 20 MINUTES OF INACTIVITY.
	DEFAULT OPTION SELECTED
This is a private computer	Your credentials are stored in your browser's local profile cache for one (1) year, letting you bypass the logon screen after your initial successful logon.
	You can clear this setting by logging out of Advanced eDiscovery.

1. Enter your user name and password.

If you have problems accessing your account, check with your administrator first. If you continue to have difficulty logging on, contact your Technical Support Staff through your administrator.

About the Advanced eDiscovery user interface

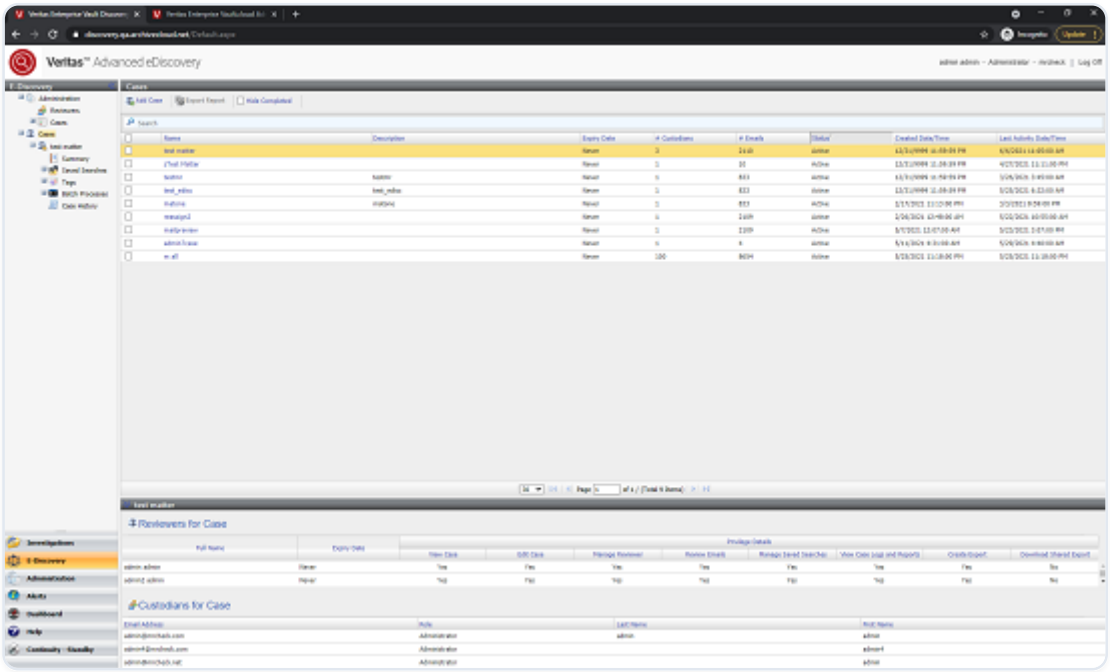
Figure: Advanced eDiscovery User Interface shows the Advanced eDiscovery user interface, with a typical view onto a case in the E-Discovery tab that a Discovery Administrator might see.

> “ ”

Note: 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 the roles and privileges of your Enterprise Vault.cloud account.

> “ ”

Figure: Advanced eDiscovery User Interface



The selection tabs at the bottom left control access to the various functions and features of Advanced eDiscovery:

- See About the Investigations tab.
- See About the E-Discovery tab.
- See About the Administration tab.

- See About the Alerts tab.
- See About the Dashboard tab.
- See About the Continuity tab. (not shown in the figure).

About the Investigations tab

The Advanced eDiscovery Investigations tab provides access to your own archived emails. Administrators and reviewers can also use this tab to access and review the archived emails of user accounts that they manage.

The following nodes are available from the Investigations tab, depending on your account permissions:

- The My Mailbox node is where you can view all of your archived emails, including the emails that were deleted from your email inbox.

Note that when viewing your archived emails, certain Personal.cloud features such as search filters and active folders are not available from Advanced eDiscovery.

See Accessing your own archived emails.

- The Managed Accounts node is available to users with the Reviewer role, and to administrators with the Monitor All Accounts privilege. The accounts that are assigned to you display when you select the Accounts sub-node.

You can use the features available from the Managed Accounts node to conduct initial, probative, or ad hoc investigations, outside of the legal discovery workflow.

See About Investigations.

- The Tags & Holds node lets you view and manage the custom tags and the emails with those tags, including those emails with legal hold, that have been applied in the Investigations tab.
- The Batch Processes node lets you view the status of email exports that you perform from the Investigations tab.

> “ ”

Note: External reviewers do not have access to theInvestigationstab.

> “ ”

About the E-Discovery tab

The E-Discovery tab includes the case management feature. This feature allows multiple reviewers to interact and collaborate on litigation cases during the eDiscovery process. Once a case has been created, the Discovery administrator or an assigned reviewer can use searches to find the emails relevant to the case. These searches can then be saved, and the resulting emails assigned to the various reviewers that have been nominated to work on the case. This distribution of the workload among the reviewers expedites the eDiscovery process.

During the review process, reviewers can place emails on legal hold, apply review status tags and labels, and apply custom tags. Reviewers can also add notes to emails that other reviewers who work on the case can view. Additionally, Collaborative eDiscovery includes various reporting features, that allow reviewers to view audit trails for individual emails or the history of an entire case.

See About cases in the E-Discovery tab.

About the Administration tab

The Administration tab provides administrators with access to the company's Enterprise Vault.cloud Administration Console. The Administration Console enables administrators to configure archive settings and to assign roles, including the roles that control the access to Advanced eDiscovery. Role assignment is only available to System Administrators or to Role Managers with the required permissions.

When you select the Administration tab the Administration Console appears in a new web browser tab, if you have the required permissions.

See About account roles and Advanced eDiscovery.

For reviewers and users with the Account role, the Administration tab displays options to change your password and personal time zone.

About the Alerts tab

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.

See Creating an alert.

About the Dashboard tab

The Dashboard tab provides administrators and reviewers with archive statistics. The statistics available from this tab include:

- Number of active accounts
- Top policy alerts trending
- Number of emails received
- Average mailbox size

About the Continuity tab

Email Continuity is an add-on service that provides a "standby mailbox". It enables users to continue to send and receive emails when your organization's mail server is unavailable.

For those companies that subscribe to the Email Continuity service the Continuity tab is provided. From this tab administrators can manage the service, and Advanced eDiscovery users can access a list of continuity emails.

See Managing Email Continuity.

See Viewing Continuity emails.

Email Continuity can also be managed from the Enterprise Vault.cloud Archive Administration console.

Accessing your own archived emails

Advanced eDiscovery users can view and access their own archived emails from the Investigations tab > My Mailbox node. You can view all of your archived emails, including the emails that were deleted from your email inbox.

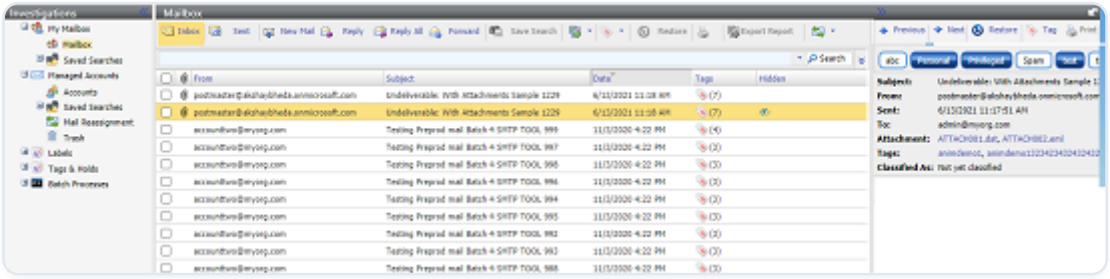
My Mailbox has similar functionality to your Personal.cloud archive. You can view and search your own emails. You can also reply and forward your emails from here. You cannot restore emails to your own account from Advanced eDiscovery and can only restore mails to the accounts which you monitor.

> “ ”

Note: When you view your archived emails, certain Personal.cloud features such as search filters and active folders are not available from Advanced eDiscovery.

> “ ”

When you select an email from the list, a preview pane displays the message. You can move this preview pane to underneath or to the right side of the main pane. The preview pane displays the message content and any attachments that are included with the original email.



You can double-click an email in the list to open the email in a separate window.

Below the Subject, From, Sent, and To information in the email header, you can see listed any attachments and also any custom tags or classification tags that are applied to the email. The custom tags and classification tags are typically for use with eDiscovery tasks.

Advanced eDiscovery roles

This section includes the following topics:

- About account roles and Advanced eDiscovery
- Account role
- Reviewer role
- Administrator role
- Assigning roles for Advanced eDiscovery

About account roles and Advanced eDiscovery

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

- Account
- Reviewer
- Administrator

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.

The role to which your account is assigned and the associated privileges that are granted to it determine the menu options and features that you can access from Advanced eDiscovery.

Account role

Available Advanced eDiscovery tabs: Investigations and Administration (for setting personal preferences only).

Users with the Account role have the least access to Advanced eDiscovery. They have access only to the Investigations tab, from where they can view their own archived emails.

Note that Personal.cloud is the preferred access method for users to view archived emails. Personal.cloud allows users to tag and restore archived emails into their own inbox.

Note: In one case, those accounts with theAccountrole can have greater access in Advanced eDiscovery. Administrators can configure the account in Archive Administration to make it anExternal Reviewer. These accounts are for users who are not part of your organization, but who need to review emails within the cases that are assigned to them#. External reviewers have their account disabled for archiving, and can only access theE-Discoverytab in Advanced eDiscovery. Within theE-Discoverytab the external reviewers can perform similar tasks as those accounts with theReviewerrole. See the Archive Administration help for more information about creatingExternal Revieweraccounts.

> “ ”

Reviewer role

Available Advanced eDiscovery tabs: Investigations, E-Discovery, Administration (for setting personal preferences only), and Alerts.

Users with the Reviewer role can monitor employee emails for the material that does not follow company communication policies. An administrator or HR representative typically reviews the email of reviewers, so that no employees are exempt from following company communication policies. Organizations should take special care in selecting the appropriate employees for the Reviewer role, since reviewers can see other employees' emails. Reviewers should not share their user name and password with anyone.

When you assign an account the Reviewer role, you can allow the account to monitor all of the accounts in Enterprise Vault.cloud, or a selected subset. You can use the Disable preview mail check box to prohibit email preview. It limits reviewers to only check the emails between sender and recipients.

In the Investigations tab, reviewers can perform open-ended investigative searches against one or all of the accounts that they have the permissions to monitor.

In the E-Discovery tab, reviewers have access only to those cases that are assigned to them.

When the Discovery Administrator creates a case, they assign the case to one or more reviewers. Each reviewer can be assigned a set of permissions within each case. A reviewer can perform some or all of the following functions within a case, depending on the permissions that they are assigned for that case:

- Review the emails that result from the searches that are associated with the case.

- View the case logs and reports.
- Manage saved searches of emails.
- Perform and manage searches on the emails that are associated with the case.
- Export emails.
- Place emails on legal hold.
- Edit the case for example to reassign searches to different reviewers.

> “ ”

Note: Accounts with theReviewerrole only see theE-Discoverytab once they have been assigned as a reviewer to at least one case.

> “ ”

Administrator role

Available Advanced eDiscovery tabs: Investigations, E-Discovery, Administration, Alerts, and Dashboard.

The Administrator role is for company administrators who need to configure and manage Advanced eDiscovery, or for HR personnel who need to monitor employee email usage.

Administrator roles must be assigned 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 only.

Accounts with the Administrator role and with the Monitor All Accounts privilege can be assigned to cases as reviewers, and can act as reviewers in the same way as the accounts with the Reviewer role.

Administrators can also receive email notifications each time a message is flagged in the Alerts area.

> “ ”

Note: Accounts with theAdministratorrole can be assigned additional privileges in Archive Administration, including the privileges that can be conferred by built-in group roles. The accounts

with theAdministratorrole that are also assigned theDiscovery Administratorbuilt-in role have full access to all the features of Advanced eDiscovery.

> “ ”

Discovery Administrators can configure and manage all aspects of Advanced eDiscovery, including the following:

- Creating, viewing, and editing cases
- Managing reviewers
- Adding and editing labels
- Assigning review status tags to emails
- Managing case review status tags
- Managing saved searches under cases
- Exporting emails from cases
- Viewing logs and saving reports

Given the sensitive nature of the information available to administrators, they should take special care to protect their logon credentials.

Assigning roles for Advanced eDiscovery

To assign roles to an account you must be a System Administrator or have the required Modify Privileges privilege.

Administrators can access the Administration Console from the Administration tab of Advanced eDiscovery.

- See Assigning the Reviewer role to an account.
- See Assigning the Administrator role to an account.

Assigning the Reviewer role to an account

To assign roles to an account you must be a System Administrator or have the Modify Privileges privilege.

To assign the Reviewer role to an account

1. In Advanced eDiscovery, select the Administration tab. The Enterprise Vault.cloud Administration Console sign-on screen opens in a new browser window.
2. Log on to the Administration Console as a System Administrator or with an account that has the Modify Privileges privilege.
3. Under the Role Management node, select **Assign Accounts**.
4. From the list of accounts, select the required user.
5. Select **Reviewer** from the Role drop-down menu.
6. Do the following:

    - Select the **Monitor All Accounts** check box to allow the user to monitor all user accounts.
    - If required, select the **Disable preview mail** to prohibit the reviewer from viewing preview of email content.
    - Or click **Add/Remove Monitored Accounts** and select the accounts for this reviewer to monitor.

When you have selected the required accounts, click **Update**and then click**Close** to close the Add/Remove Monitored Accounts window.

In the **Accounts to Monitor**list, if you want the reviewer privilege to expire for any account, clear the check box in the Never Expires column for that account. Then in the Expiration column, click the**Calendar** icon and select the date that you want the reviewer privilege to expire.

1. Click **Save** to save the role changes for the account.

Assigning the Administrator role to an account

To assign roles to an account you must be a System Administrator or have the Modify Privileges privilege.

To assign the Administrator role to an account

1. In Advanced eDiscovery, select the Administration tab. The Enterprise Vault.cloud Administration Console sign-on screen opens in a new browser window.
2. Log on to the Administration Console as a System Administrator or with an account that has the Modify Privileges privilege.
3. Under the Role Management node, select **Assign Accounts**.
4. Select the required user from the list of accounts.
5. From the Role drop-down menu, select **Administrator**.

6. To allow the account to monitor all user accounts, select the **Monitor All Accounts** check box.

If you do not select this option the account cannot view any user accounts other than their own.

1. If you want to assign Discovery Administrator privileges to the account, under Group Privileges select the **Discovery Administrator** check box.
2. Click **Save** to save the role changes for the account.

Investigations

This section includes the following topics:

- About Investigations
- About the Managed Accounts node
- Creating a label
- Performing a new search of accounts (Investigations tab)
- Saving a search of accounts (Investigations tab)
- Viewing or modifying a saved search (Investigations tab)
- Generating and exporting printable reports for searches (Investigations tab)
- Deleting saved searches (Investigations tab)
- Working with emails in the Investigations tab
- Hiding and unhiding emails
- Deleting emails permanently
- About the Mail Reassignment node
- Reassigning emails
- Viewing email reassignment status
- Canceling the email reassignment activity
- Generating a Mail Reassignment status report
- Sending notifications to the mail reassignment batch initiator
- About Collaboration
- Searching Collaboration messages during investigation
- Applying tags to Collaboration messages during investigation

About Investigations

From the Advanced eDiscovery 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 to corporate content or regulatory policies before deciding whether there is a requirement to create a tracked eDiscovery case.

Typically, an investigation is an internal search. For example, you can assess compliance to 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.

You can search the archives of the accounts that you manage from the Managed Accounts node. From here you can access, review, and work with the archived emails of interest as in the E-Discovery tab. The difference is that in the Investigations tab the search and the work that you do with the emails is not tracked as part of a case. Also in investigations the review status tags are not available.

In investigations, permission to view the emails of others is solely dependent on the roles and permissions of your account as configured in Archive Administration. The constraints that are enforced within a case and a Review Set are not present.

About the Managed Accounts node

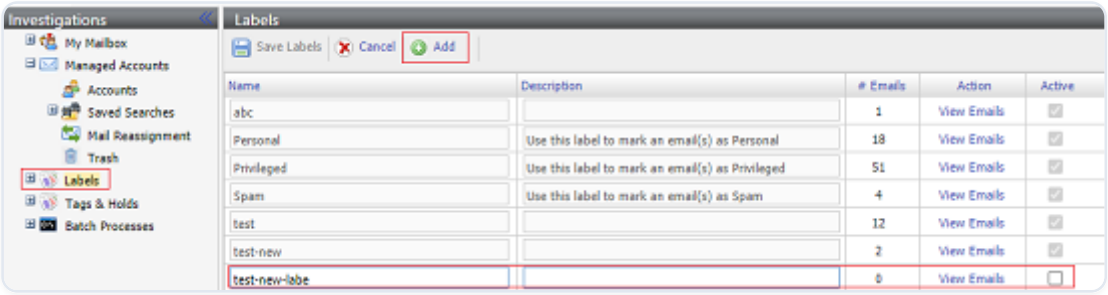
On the Investigations tab, the Managed Accounts node is available to those users with Administrator or Reviewer role privileges. The accounts to which you are assigned are listed when you select the Accounts sub-node. You can use the features available from the Managed Accounts node to conduct initial, probative, or ad hoc investigations, outside of the legal discovery workflow. When you are ready to conduct searches and reviews on a specific subject, you can create a case in the E-Discovery tab to track these searches.

Creating a label

Discovery Administrators 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.

To create a new label

1. On the Investigation tab, in the left navigation pane, select Labels.
2. Click **Add**.



3. Specify the following details:

NAME	SPECIFY A UNIQUE NAME FOR THE LABEL.
Description	Optionally enter a description for the label.
\# Emails	Displays number of emails to which this tag is applied. If this tag is not applied, the number of emails shown as zero.
Action	Click View Emails to view emails with the corresponding label.
Active	Select the Active check box for the label if you want to display this label while reviewers assign labels to emails. Clear the check box for any labels that you want to hide.

4. Click **Save Label**.

Performing a new search of accounts (Investigations tab)

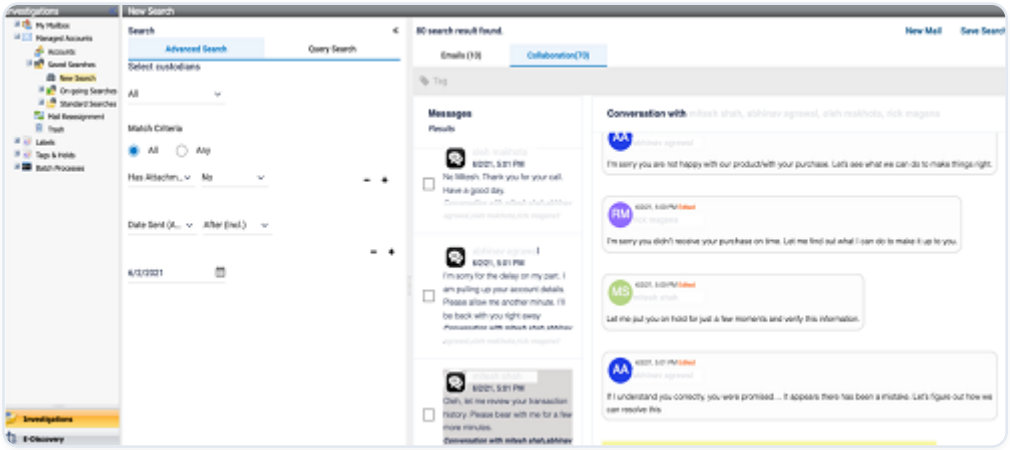
You can search the content of archive accounts from the Investigations tab, using Advanced Search and Query Search.

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 a sample Search page:



Perform step 2 for an Advanced Search, or step 3 for a Query Search.

1. To perform an Advanced Search, do the following:

   - Select the Advanced Search tab.
   - Select the custodian archives you want to search.
     - To search archives of all of the custodians that are associated with the case, select **All**.
     - To search archives of the particular custodians, select **Custom**. Click Manage to search for, add, and remove the custodians. Click Update to complete the custodian selection.
   - Specify the search criteria by using the following options.
     - Select All to match all conditions you have provided.
     - Select Any to match any of the conditions you have provided.
     - Click **+** to add new search clauses, and complete a new row for each clause.
     - Click **-** to remove search clauses that are not required.
     - Searches are not case-sensitive. The search supports phrase search, Boolean operators, proximity search, and wildcard search.

See Search syntax for Advanced Search.

- Search for and select the message attributes you want to search. Refer to the table below:

ENTIRE MESSAGE	CONTAINS / DOESN'T CONTAIN
Subject	Contains / Doesn't Contain
Body	Contains / Doesn't Contain
From	Contains / Doesn't Contain
	Note: Produces search results from theFromfield.
To	Contains / Doesn't Contain
	Note: Produces search results from theTo,BCC, andCCfields.
Has Attachment	Yes / No
Attachment Name	Contains / Doesn't Contain
Attachment Type	Contains / Doesn't Contain
	See Searchable attachment types .
Classified As	Contains / Doesn't Contain
	Note: This option is available if the Veritas Information Classifier service is enabled for your company. Select a classification tag from the drop-down list. The list shows all the classification tags that have been applied to your company's messages in Enterprise Vault.cloud. To see a tooltip with a classification tag's description, select the classification tag from the drop-down list and then point to the classification tag.
Date Sent (AND)	Is Equal To / Before / Before (Incl.) / After / After (Incl.)
From / To	Contains / Doesn't Contain
	Note: This option produces search results from theFromandTofields.

ENTIRE MESSAGE	CONTAINS / DOESN'T CONTAIN
Inbound Message (AND)	Yes / No
Outbound Message (AND)	Yes / No
Is Hidden	Yes / No
IP Header	Contains / Doesn't Contain

1. To perform a Query Search, do the following:

- Select the Query Search tab.
- Select the custodian archives you want to search.
  - To search archives of all of the custodians that are associated with the case, select **All**.
  - To search archives of the particular custodians, select **Custom**. Click Manage to search for, add, and remove the custodians. Click Update to complete the custodian selection.
- Specify the search query by providing keywords.

1. Click **Search**.

> “ ”

Note: The results of an Advanced Search include aRelevancecolumn. The length of the bar in this column represents how closely the email matches the search criteria, relevant to the other emails in the results.

> “ ”

2. Click **Save Search**.

See Saving a search of a case.

Saving a search of accounts (Investigations tab)

If you have the required permissions you can save an Advanced Search or a Query Search. The roles that can create saved searches from the Investigations tab are as follows:

- My Mailbox node: All users.
- Managed Accounts node: Administrators and reviewers with the appropriate permissions.

The Advanced or the Query Search that is performed from the Investigations tab can be saved as a Standard Search or an On-going Search:

- A Standard Search retains the results that were captured when the search was created.
- With an On-going Search, any new emails that meet the search criteria continue to be added after the search is created.

To save a search of accounts (Investigations tab)

1. Perform an Advanced Search or a Query Search in the Investigations tab.

See Performing a new search of accounts (Investigations tab).

1. Click **Save Search**.
2. Complete the information in the Save Search dialog. The following table describes the options.

ENTER SAVED SEARCH NAME	ENTER A NAME FOR THE SAVED SEARCH. THIS NAME IS ALSO THE DEFAULT TAG NAME, IF YOU SELECT THE ON-GOING CHECK BOX.
On-going	Select to make the saved search an On-going Search.
	If you do not check this check box, Advanced eDiscovery saves the search as a Standard Search.
Tag Name	This option is available only if the On-going check box is selected.
	Specify the name of a custom tag to assign to the associated emails. By default Advanced eDiscovery uses the saved search name as the tag name.
Legal hold	This option is available only if the On-going check box is selected.

ENTER SAVED SEARCH NAME	ENTER A NAME FOR THE SAVED SEARCH. THIS NAME IS ALSO THE DEFAULT TAG NAME, IF YOU SELECT THE ON-GOING CHECK BOX.
	Select to place all email in the saved search on legal hold. Emails on legal hold are not deleted from the archive.
Send to Case	You have an option to select this check box. In case the Search is an Ongoing search, then the Keep copy in investigation check box is selected and disabled by default. In addition, a Case needs to be selected from the Cases drop-down. This check box allows you to send along with keeping a copy in investigation to the E-Discovery Tab. This preserves chain of custody by recreating the search in E-Discovery. The case gets moved to the E-Discovery > Research Set.

3. Click **OK** to save the search. The search is saved under the Saved Searches node as follows:
    - If you selected the **On-going** check box, the search is saved under On-going Searches.
    - Otherwise the search is saved under Standard Searches.

If you have selected the Send to Case check box, accordingly the case gets moved to the E-Discovery > Research Set. A copy is created in the On-going/Standard searches, if the Keep copy in investigation check box is selected or not.

Viewing or modifying a saved search (Investigations tab)

You can edit a saved email search to update it or to create a new search with the modified criteria.

To view or modify a saved search (Investigations tab)

1. From the Investigations tab, under your Mailbox node or the Managed Accounts node, expand the Saved Searches node.
2. Under On-going Searches or Standard Searches, click the required search.

The search displays its results.

1. To modify the search, click **Update Saved Search**.

Then update the information in the Saved Search dialog as required. See the following table for more information.

ENTER SAVED SEARCH NAME	CHANGE THE NAME FOR THE SAVED SEARCH IF REQUIRED.
On-going	Select to make a Standard Search an On-going Search, or clear to make an On-going Search a Standard Search.
	For an On-going Search, new emails that meet the search criteria continue to be added after the search is created. A Standard Search retains only the results that were captured when the search was created.
Tag Name	This option is available only if the On-going check box is selected.
	Specify the name of the associated tag for selected emails. By default Advanced eDiscovery uses the saved search name.
Legal hold	This option is available only if the On-going check box is selected.
	Select to place all email in the Saved Search on legal hold. Emails on legal hold are not deleted from the archive.
Send to Case	You have an option to select this check box. In case the Search is an Ongoing search, then the Keep copy in investigation check box is selected and disabled by default. In addition, a Case needs to be selected from the Cases drop-down. This check box allows you to send along with keeping a copy in investigation to the E-Discovery Tab. This preserves chain of custody by recreating the search in E-Discovery. The case gets moved to the E-Discovery > Research Set.

1. Select an option for updating the search, as follows:

SAVE AS NEW	SELECT TO CREATE A NEW SAVED SEARCH WITH THE NEW NAME. THE ORIGINAL SAVED SEARCH IS UNCHANGED.
Update	Select to update the existing saved search with the new criteria.

If you clicked Save as New the new search is saved under the Saved Searches node as follows:

- If the **On-going** check box was selected, the search is saved under the On-going Searches node.
- Otherwise the search is saved under the **Standard Searches** node.

If you have selected the Send to Case check box, accordingly the case gets moved to the E-Discovery > Research Set. A copy is created in the On-going/Standard searches, if the Keep copy in investigation check box is selected or not.

Generating and exporting printable reports for searches (Investigations tab)

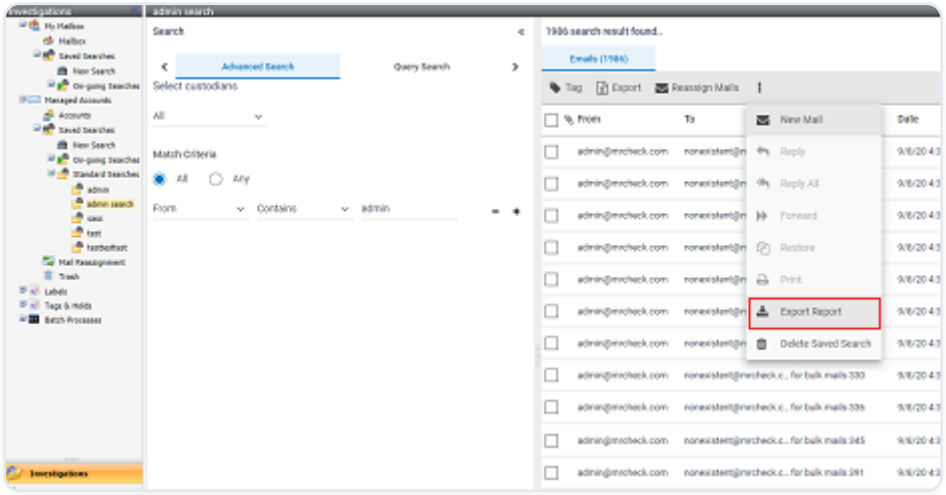
Any user who has access to Saved Searches can generate and export the Printable Reports in all searches in Investigations and eDiscovery.

To generate and export a printable report for Searches

1. In the Investigations pane, expand My Mailbox or Managed Accounts.
2. Go to any **Saved Search** Tree Node.
3. Search for and select any **On-going**or**Standard** search for which you want to export a report.

> “ ”

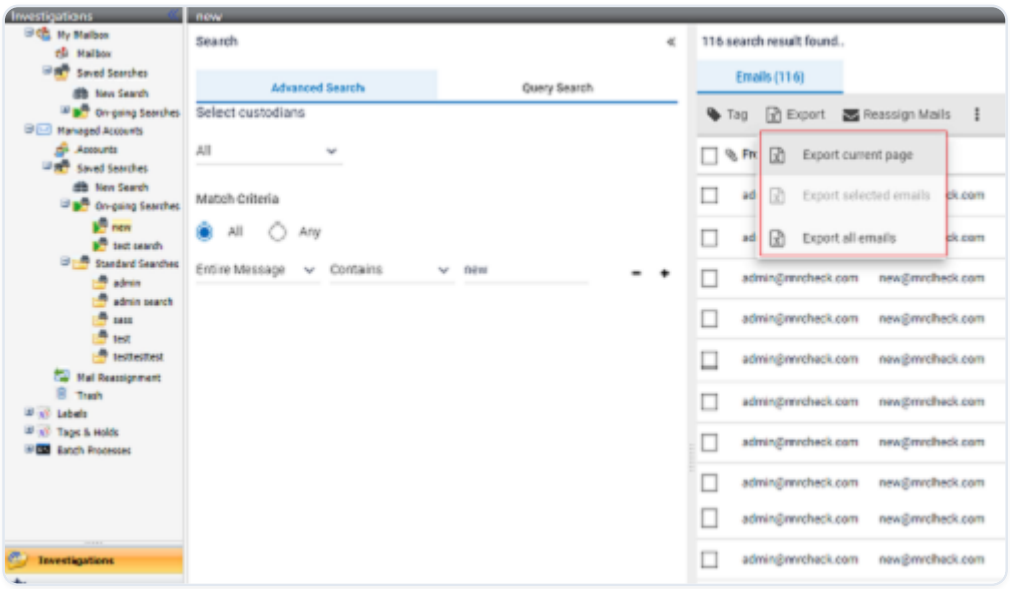
Note: In theAdvanced Searchtab, you can refine your criteria to search for records. Click the plus icon to add new criteria. Click the minus icon to remove the corresponding criteria. SelectMatch Allto find records that meet all specified criteria. SelectMatch Anyto find at least one specified criterion.



4. Click **Export Report** to generate a report with the custodians, the parameters, and the results.

Application downloads the zipped report to your Downloads folder. You can extract, save, and share this excel report with the concerned persons. This report specifies the date and time when the report is generated. It can contain a maximum of 100 Thousand records in a single file. If numbers of records exceeds 100 Thousand, application generates multiple files and downloads reports as a single zipped folder.

Alternatively, you can export and print the report for all records, only the selected records, or the records displayed on a single page.



- To export and print records on the current page, click the **Export Emails**icon, and select**Export current page**.

- To export and print selected records, select the records, click the **Export Emails**icon, and select**Export selected emails**.
- To export and print all records, click the **Export Emails**icon, and select**Export all emails**.

> “ ”

Note: It is vital to understand the difference between exporting reports and exporting email records. When you generate and export reports, the metadata displayed on the details pane is shown in the excel file. However, when you export emails, the actual email files are downloaded.

> “ ”

See Exporting emails.

Deleting saved searches (Investigations tab)

You can delete a saved search or multiple saved searches.

To delete a saved search (Investigations tab)

1. From the Investigations tab, under your Mailbox node or the Managed Accounts node, expand the Saved Searches node.
2. Under On-going Searches, Standard Searches, Research Sets, or Review Sets, click the search that you want to delete.
3. To delete a saved search, select the check box next to it in the grid and click the delete icon at the top of the page. Click **OK** to confirm that you want to delete the selected saved searches. Any selected searches are deleted.
4. To delete all the saved searches on a page, select the check box at the top of the page to select all the searches. Click **OK** to confirm that you want to delete the selected saved searches.
5. To delete all the saved searches for a node, select the check box at the top of each page and click the delete icon. Click **OK** to confirm that you want to delete the selected saved searches.

Working with emails in the Investigations tab

You can perform the following actions on emails in the Investigations tab. These actions are also available for emails in the E-Discovery tab:

- Tag emails with your own custom tag, or with a managed tag.

See Applying tags to emails.

> “ ”

Note: In theInvestigationstab, any custom tags you apply are listed in theTags & Holdsnode of the left pane. Click a tag to see the messages that have the tag applied. TheTags & Holdsnode does not show classification tags.

> “ ”

- Print emails.

See Printing emails.

- Restore emails to a selected email account.

See Restoring emails.

- Forward emails.

See Forwarding emails.

- Export emails, view the status of mail exports, and resubmit failed exports.

See Exporting emails.

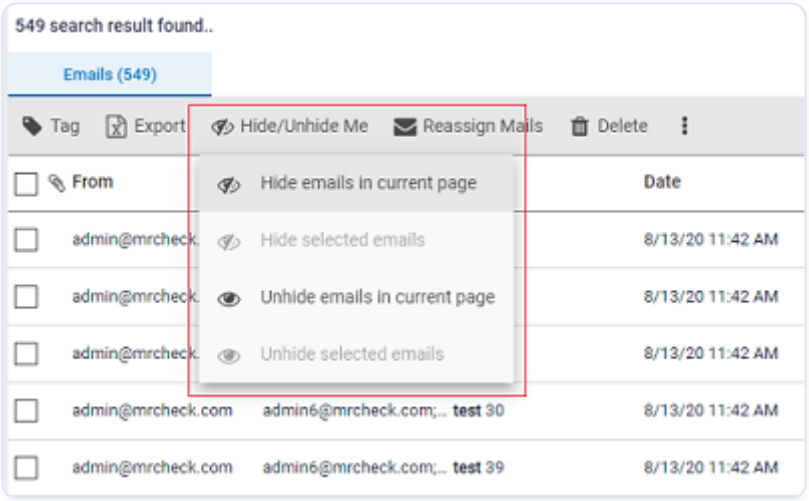
See Reviewing Export Status.

Hiding and unhiding emails

Administrators can use the Hide Me and the Unhide Me options to hide and unhide emails from users respectively. In Personal.cloud and Mobile Web Access, administrators cannot search the emails with the hidden state. However, in Advanced eDiscovery, administrators can search and view these hidden emails.

To hide emails

1. Navigate to **New search** under Monitored Accounts, and conduct a search.
2. If required, select the checkbox for one or more emails.
3. Click the **Hide me/Unhide me** icon, and select an option to specify which emails to hide.



4. Select the option to Hide selected emails or **Hide email in current page**.

> “ ”

Note: A maximum of 300 emails can be hidden in a single transaction. The Hide emails dialog box appears informing that the emails are hidden, and cannot be browsed by end-users. It may take up to 60 minutes to hide the emails from appearing in the end-user search results.

> “ ”

5. Click **OK**.

The Confirmation dialog box appears informing that action has been executed successfully, refresh search to see the output of this action.

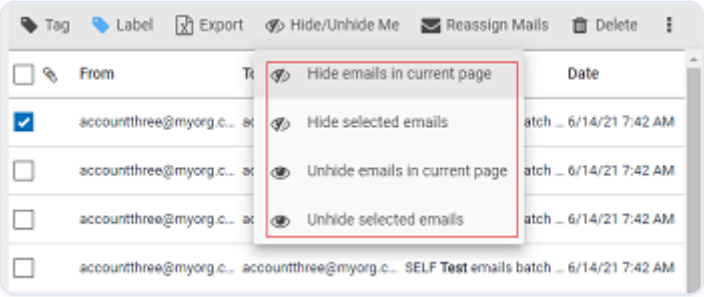
1. Execute the same search again.

The hidden emails are marked with a gray background, and the **Hide me** icon appears in the last column.

To unhide emails

1. Navigate to **New search** under Monitored Accounts, and conduct a search.

2. If required, select the checkbox for one or more emails.
3. Click the **Hide me/Unhide me** icon, and select an option to specify which emails to unhide.



4. Select the option to Unhide selected emails or **Unhide email in current page**.

> “ ”

Note: A maximum of 300 emails can be unhidden in a single transaction. The Unhide emails dialog box appears informing that the emails are unhidden, and cannot be browsed by end-users. It may take up to 60 minutes to unhide the emails from appearing in the end-user search results.

> “ ”

5. Click **OK**.

The Confirmation dialog box appears informing that action has been executed successfully, refresh search to see the output of this action.

1. Execute the same search again.

The unhidden emails are no longer marked with a gray background, and the **Hide me** icon disappears from the last column.

Deleting emails permanently

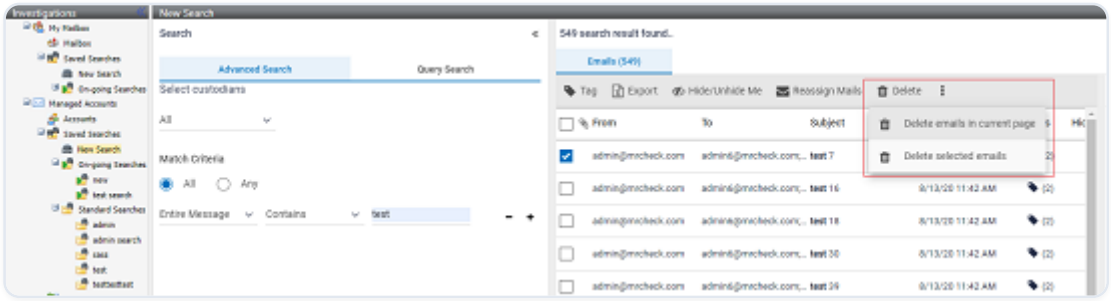
Administrators can use the Delete option to permanently delete emails from users. In Personal.cloud and Mobile Web Access, administrators or users cannot search the emails that have been deleted.

> “ ”

Note: For information on how to enablePrivilege Deleteto company level, seeConfiguring archive optionsin theEnterprise Vault.cloud Archive Administration Help. For information on how to enablePrivilege Deleteto administrators, seeEditing the built-in administrator rolesin theEnterprise Vault.cloud Archive Administration Help.

To delete emails

1. Navigate to **New search**under**Monitored Accounts** , and then conduct a search.
2. If required, select the checkbox for one or more emails.
3. Click the **Delete** icon, and then select an option to specify which emails to delete.



Note: A maximum of 300 emails can be deleted in a single transaction. The Permanently delete emails dialog box appears informing that once emails are deleted, they cannot be recovered or accessed and that this is permanent and irreversible action. It may take up to 60 minutes for deleted emails to stop appearing in the end-user search results.

4. Click **OK**.

The Confirmation dialog box appears informing that action has been executed successfully.

1. To check the status of the deleted emails, navigate to **Trash**under**Monitored Accounts** , and review the list of emails.

Note: A list shows the deleted emails in chronological order from most recent to older. You can sort by email Date or Date Added (default).

> “ ”

The status of the deleted email can be:

- Deleted \- the email has been deleted.
- Queued \- the email is queued to be deleted.
- On Legal Hold \- the email is on legal hold status, and it cannot be deleted.

The email on legal hold has Legal hold tag, Legal hold search, or Legal hold Custodian in a Case applied. To delete an email marked on legal hold, first, remove any applicable legal hold that has been previously applied .

About the Mail Reassignment node

On the Investigations tab, the Mail Reassignment node is available to those users with Administrator or Reviewer role privileges. Mail reassignment is used to send already processed emails back to go through the process of parsing, mail transfer, and sender-recipient mail address mapping.

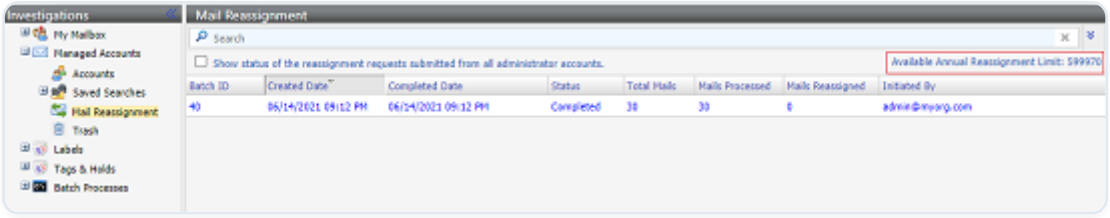
Emails are usually mapped to the unassigned legacy account because the domain or account has not been provided for email archiving or searching. Later, when such users are added as archive accounts, these previously mapped emails are required to assign again to map the mail addresses. After successful reassignment of such emails, new users can search and view these emails.

Reassigning emails

Every company has an unassigned legacy account. New users from the company cannot search or view the emails that were sent to their account before it was created. All such mails that do not find appropriate recipient of the mail goes to unassigned legacy account.

To enable such users to receive their previously assigned emails, you, as an administrator, need to reassign such emails to them. After you submit email batch for reassignment, application resends these emails to corresponding user accounts. All the new users can then search and view their emails.

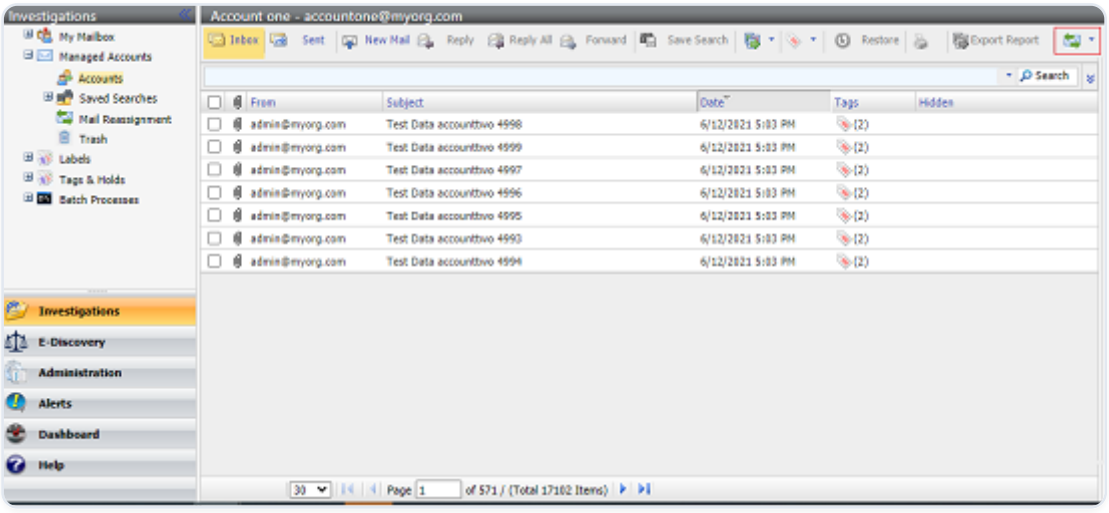
You can reassign emails from the unassigned legacy accounts, saved searches, and tags. You can select maximum 300 emails in one batch for reassignment. If there are more than 300 emails in the unassigned legacy account, you need to reassign emails in multiple batches. The maximum annual limit of mail reassignment is 600000 mails per customer, whereas the daily limit is 4500 per day per customer. When customers submit a batch for reassignment, customers can view a temporary notification (that fades out automatically) about their available reassignment limit. Alternatively, customers can check their mail reassignment limits on the Mail Reassignment node.



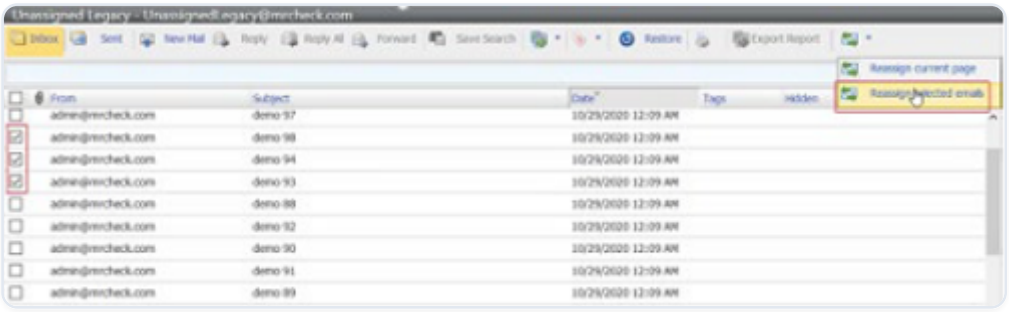
When customers use 90 percent of their annual mail reassignment limit, they receive an alert email.

To reassign emails

1. On the Investigations tab, search for and select emails from one of the following locations:
    - Go to Managed Accounts > Accounts.
    - Go to Managed Accounts > Saved Searches.
    - Go to Managed Accounts > Tags and Holds > Tags.
2. Click on the required unassigned legacy account to view all unassigned emails.
3. To reassign up to 30, 50, 100, and 300 emails in one batch, select number of emails you want to view on one page, and click the Reassign current page icon.



4. To reassign selected emails in one batch, select the required emails, and click the Reassign selected emails icon.



The application displays the following message:

1. Click OK.

Viewing email reassignment status

After you submit a batch for email reassignment, you need to know the status of every batch. There are four statuses, namely Queued, In-progress, Completed, and Failed.

To view email reassignment status

1. On the Investigations tab, select Managed Accounts > Mail Reassignment.
2. To view the status of email reassignment batches initiated by multiple admin accounts of the same company, select the Show status of the reassignment requests submitted from all administrator accounts check-box.
3. Use the Advanced Search option to search for the batch you want to check the status.
4. Select the batch.

The Status column displays the current reassignment status of the batch.

The Reassignment Details pane displays the Batch ID, name of the email reassignment initiator, total emails in the batch, successfully reassigned emails from the batch, date and time of the reassignment activity.

> “ ”

Note: If the batch status is either Queued or In-progress, then theCanceloption remains enabled. You can click theCanceloption to abort the reassignment activity. If the batch status is either Completed or Failed, then theCanceloption remains disabled. You cannot click theCanceloption to abort the reassignment activity.

> “ ”

Canceling the email reassignment activity

After you submit a batch for email reassignment, you need to know the status of every batch. There are four statuses, namely Queued, In-progress, Completed, and Failed. You can cancel the email reassignment activity only when the batch status is Queued or In-progress. You cannot cancel the reassignment for the Completed and Failed batches. You can cancel one batch at a time.

To cancel email reassignment activity

1. On the Investigations tab, select Managed Accounts > Mail Reassignment.
2. Use the Advanced Search option to search for the batch you want to cancel.
3. Select the batch whose status is either Queued or In-progress.
4. Under Reassignment Details, ensure that the Cancel option is enabled.
5. Click **Cancel**.

Generating a Mail Reassignment status report

If you want to share the email reassignment status report, you need to generate it from Enterprise Vault.cloud administration console. You must have an administrator role to access the reports section.

Refer to the Creating a Mail Reassignment status report section in the Enterprise Vault.cloud Archive Administration Help.

Sending notifications to the mail reassignment batch initiator

To confirm the batch reassignment status to the user who has initiated the mail reassignment batch, the application sends the email notifications. Email notifications is sent for the Completed mail reassignment batches.

To view a notification

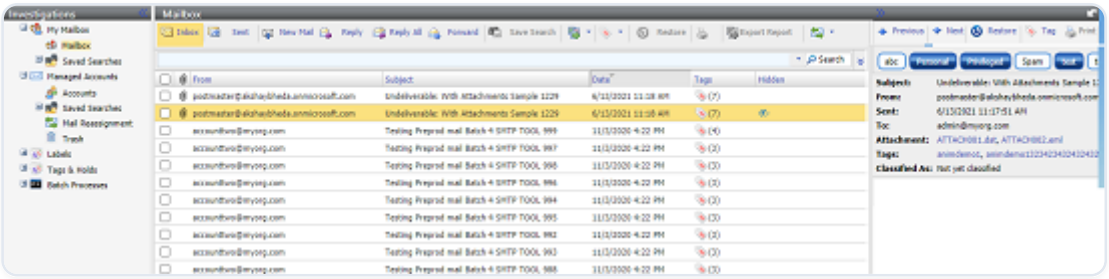
1. On the Investigations tab, select My Mailbox > Mailbox.
2. Click Inbox to view your emails regarding mail reassignment statuses.

> “ ”

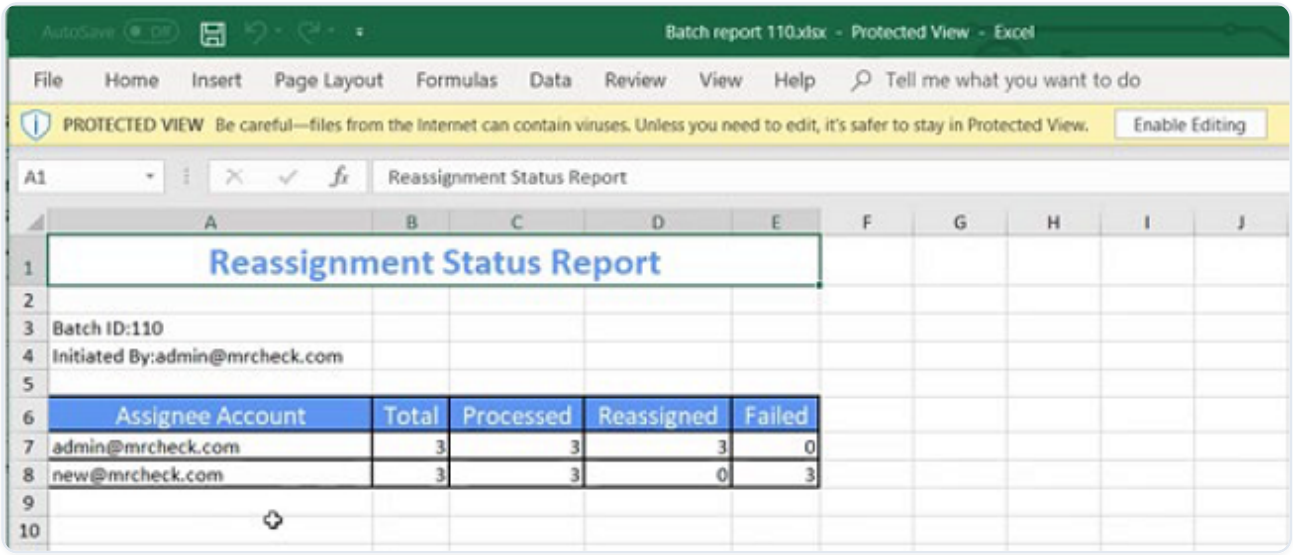
Note: You can use theAdvanced Searchoption to search for the emails regarding mail reassignment statuses.

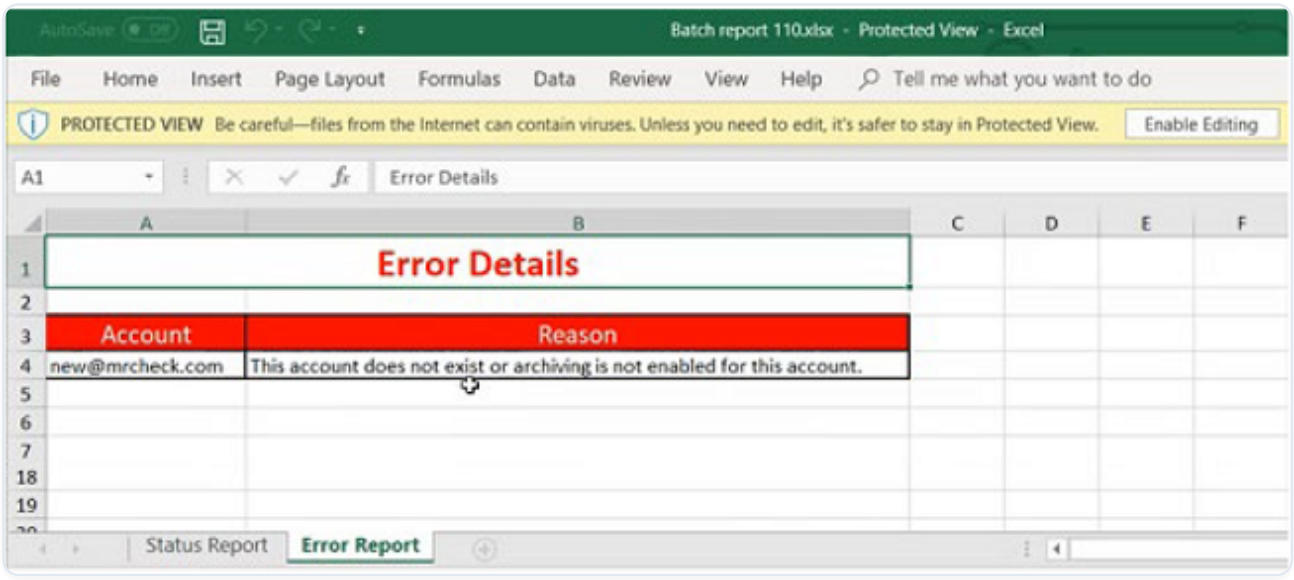
> “ ”

3. Select the email whose status is Completed.



Each email includes Batch Report as an attachment that includes the Status Report and the Error Report. The following image shows the sample reassignment status report worksheet.



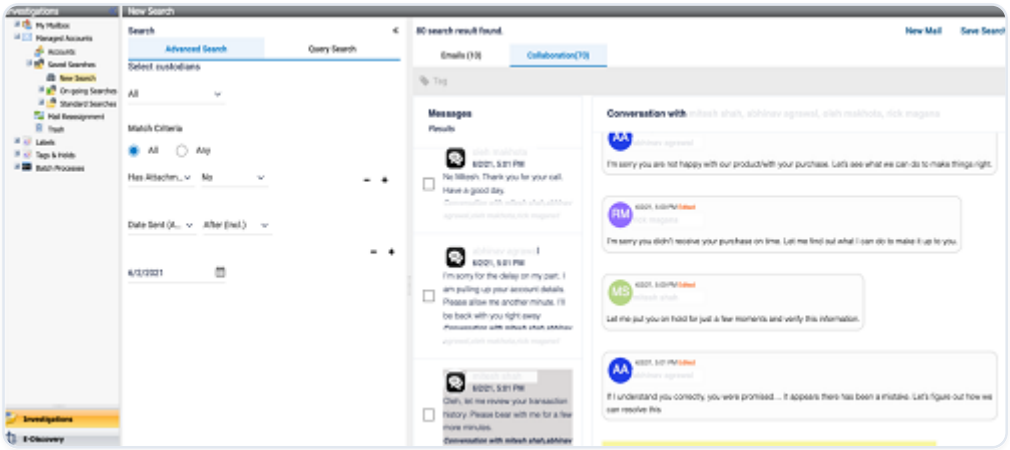


About Collaboration

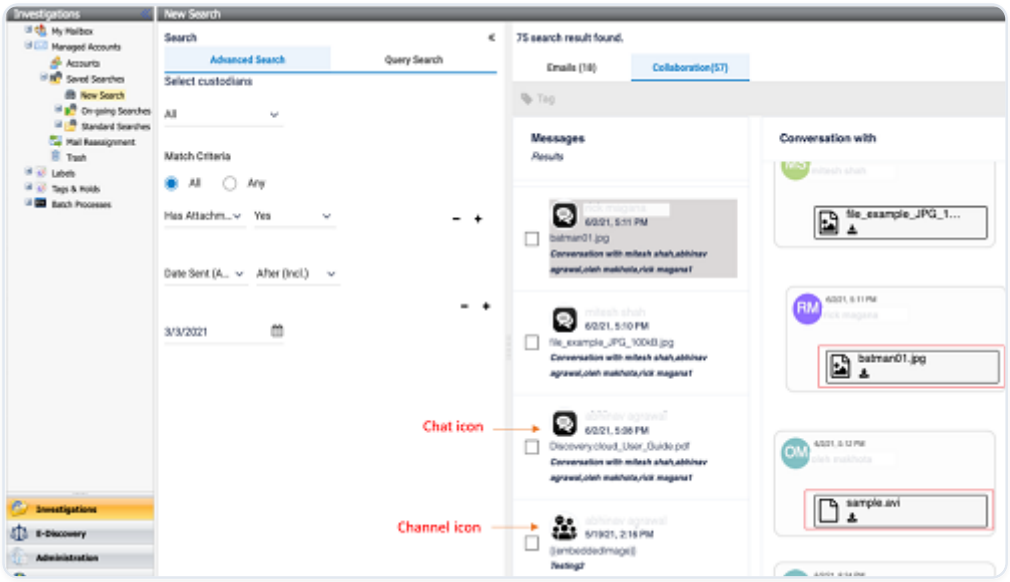
In the Advanced eDiscovery, the customer can collect the Microsoft Teams data. The customer can see the Collaboration tab while creating a search, if -

- The Microsoft Teams service is enabled
- The Microsoft Teams collector is configured

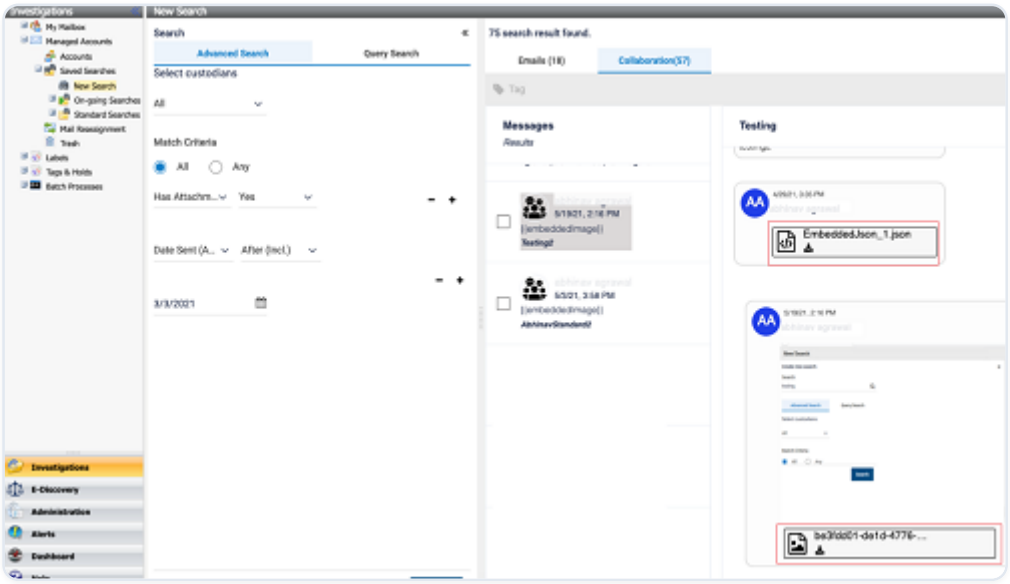
Besides emails, the customer can see and review the Microsoft Teams specific communication in the archives.



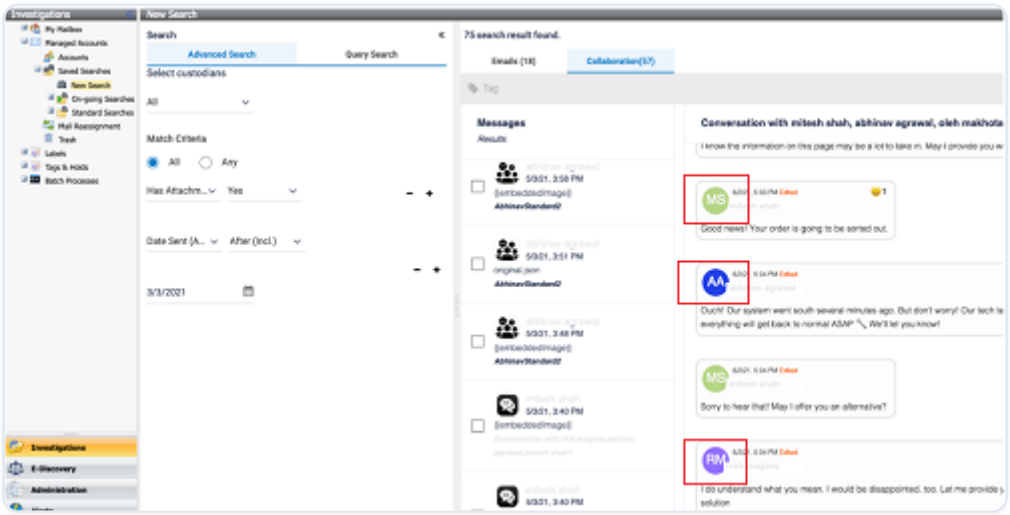
After executing a search, the Collaboration tab displays Chats or Channel conversations that matches with the Search criteria applied in the left pane. As the icons of the Chats and the Channel conversations are different, you can easily distinguish between the Chat and Channel messages.



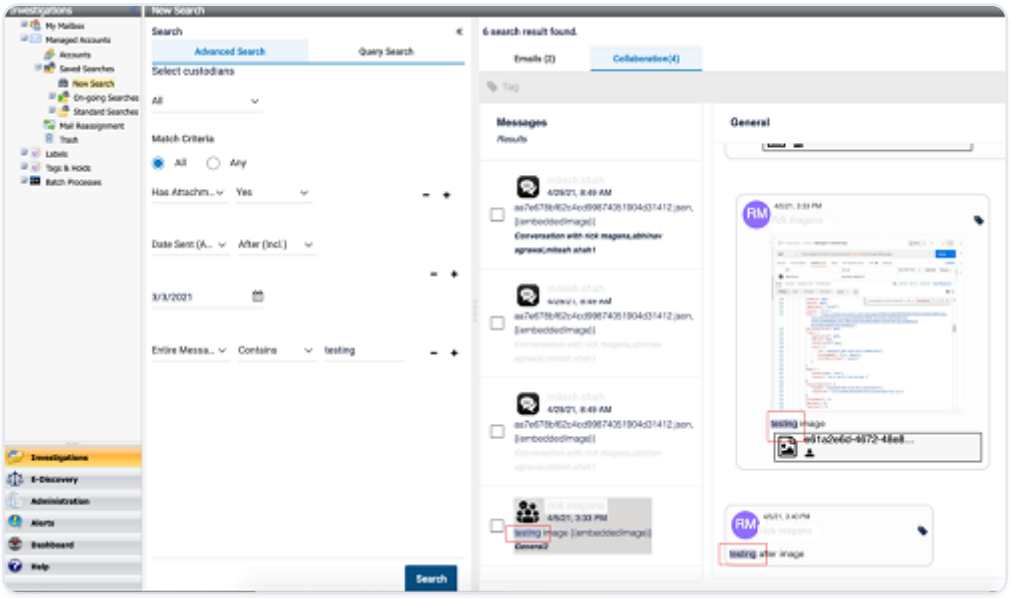
You can download the images and the attachments used in the Chat and Channel conversations.



To get a full context of the conversation, you can view the events, reactions, and link previews in the messages. To easily distinguish among the participants in the conversation, the participant icons are highlighted in different color.



When you search a term or a text in a conversation, it is highlighted in a different color for easy identification.



Searching Collaboration messages during investigation

You can search and view the Collaboration messages if the Microsoft Teams service is enabled and the archive collector is configured for you.

To search Collaboration messages during investigation

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.

Perform step 2 for an Advanced Search, or step 3 for a Query Search.

1. To perform an Advanced Search, do the following:
    - Select the Advanced Search tab.
    - Select the custodian archives you want to search.
        - To search archives of all of the custodians that are associated with the case, select **All**.

    - To search archives of the particular custodians, select **Custom**. Click Manage to search for, add, and remove the custodians. Click Update to complete the custodian selection.

- Specify the search criteria by using the following options.
    - Select All to match all conditions you have provided.
    - Select Any to match any of the conditions you have provided.
    - Click **+** to add new search clauses, and complete a new row for each clause.
    - Click **-** to remove search clauses that are not required.
    - Searches are not case-sensitive. The search supports phrase search, Boolean operators, proximity search, and wildcard search.

See Search syntax for Advanced Search.

- Search for and select the message attributes you want to search. Refer to the table below:

ENTIRE MESSAGE	CONTAINS / DOESN'T CONTAIN
Subject	Contains / Doesn't Contain
Body	Contains / Doesn't Contain
From	Contains / Doesn't Contain
	Note: Produces search results from theFromfield.
To	Contains / Doesn't Contain
	Note: Produces search results from theTo,BCC, andCCfields.
Has Attachment	Yes / No
Attachment Name	Contains / Doesn't Contain
Attachment Type	Contains / Doesn't Contain
	See Searchable attachment types .
Classified As	Contains / Doesn't Contain

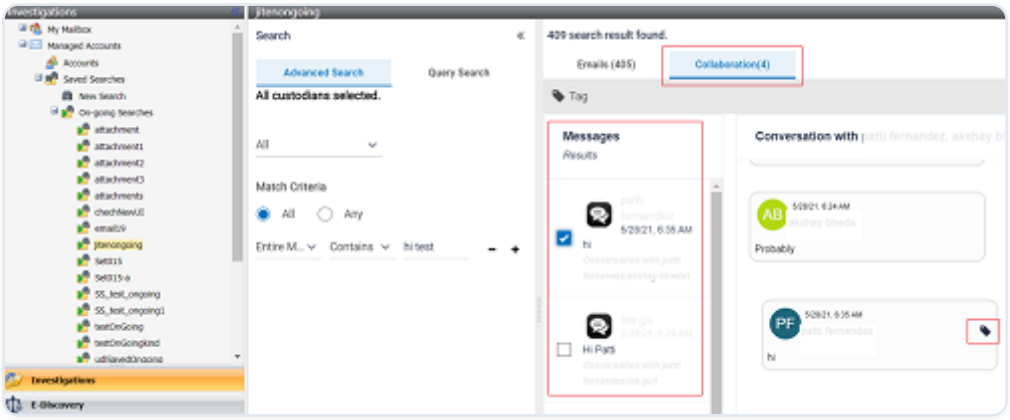
ENTIRE MESSAGE	CONTAINS / DOESN'T CONTAIN
	Note: This option is available if the Veritas Information Classifier service is enabled for your company. Select a classification tag from the drop-down list. The list shows all the classification tags that have been applied to your company's messages in Enterprise Vault.cloud. To see a tooltip with a classification tag's description, select the classification tag from the drop-down list and then point to the classification tag.
Date Sent (AND)	Is Equal To / Before / Before (Incl.) / After / After (Incl.)
From / To	Contains / Doesn't Contain
	Note: This option produces search results from theFromandTofields.
Inbound Message (AND)	Yes / No
Outbound Message (AND)	Yes / No
Is Hidden	Yes / No
IP Header	Contains / Doesn't Contain

1. To perform a Query Search, do the following:

- Select the Query Search tab.
- Select the custodian archives you want to search.
    - To search archives of all of the custodians that are associated with the case, select **All**.
    - To search archives of the particular custodians, select **Custom**. Click Manage to search for, add, and remove the custodians. Click Update to complete the custodian selection.
- Specify the search query by providing keywords.

1. Click **Search**.

The search result appears as shown in the following sample image.



1. Click **Save Search**.

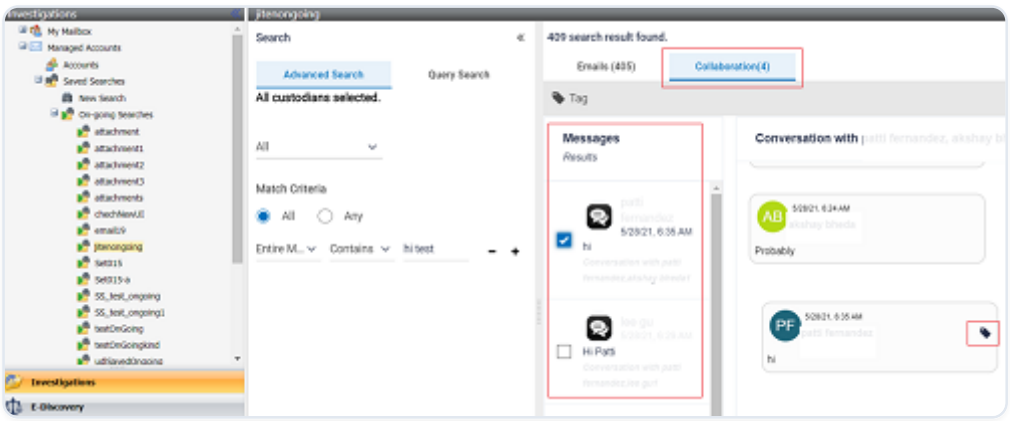
See Saving a search of a case.

Applying tags to Collaboration messages during investigation

To apply a tag to Collaboration messages

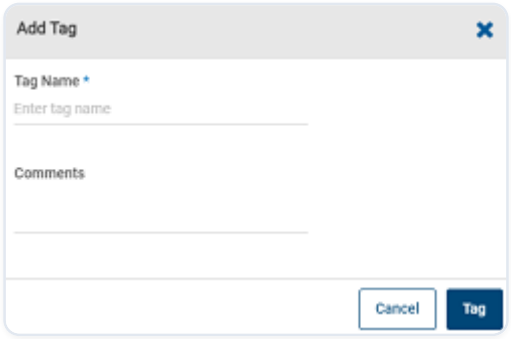
1. On the Investigations tab, select the node where you want to perform the new search:
   - To search your own mailbox select **My Mailbox > Mailbox**, or select**My Mailbox > Saved Searches > New Search**.
   - To search one or more of your managed accounts select **Managed Accounts > Saved Searches > New Search**.
   - Or to search a single managed account, select **Managed Accounts > Accounts** and click the required account.
2. Perform either an Advanced Search or a Query Search to search for the Collaboration messages. See Searching Collaboration messages during investigation.

The application displays result as shown in the following sample image.



1. Select the Collaboration message that you want to tag.

2. On the action menu, Click Tag.
3. In the Add Tag dialog box, enter a tag name and if required, provide your comments.



4. Click **Tag**.

Case management

This section includes the following topics:

- About Targeted Collections
- Configuring Targeted Collection for Microsoft Teams
- About cases in the E-Discovery tab
- Case workflow summary: Discovery Administrator
- Customizing the case review status tags
- Creating a case
- Viewing the details of a case
- Editing a case
- Performing a new search of a case
- Saving a search of a case
- Viewing and modifying a saved search of a case
- Applying a search-level legal hold
- Assigning Research Sets to reviewers
- Generating printable reports for searches
- Searching and tagging Collaboration messages in E-Discovery

About Targeted Collections

You can create a targeted collection in Advance Discovery console. These collections are the cloned data of an archive collector that is configured in the Archive Administrator console.

Before you create a targeted collection in Advanced Discovery console, ensure that, in Archive Administrator -

- the customer is already created
- the service for this collector is enabled for that customer
- the Archive Collector is configured

After you create a targeted collection, ensure that the configuration status is Complete. If the configuration is incomplete, user cannot be sent to case. User cannot remove the previously selected and saved options.

Configuring Targeted Collection for Microsoft Teams

To configure Targeted Collection for Microsoft Teams

1. On the E-Discovery tab, in the left navigation pane, select Targeted Collection.
2. Click Add to set up Microsoft Teams collector.

   > “ ”

   Note: At the time of adding the first collector, theSetup Collectionbutton appears in the middle of the screen. If one or more collectors are already added, theAddoption appears.

   > “ ”

3. On the Collection Information tab, specify the following:

COLLECTION NAME	PROVIDE A UNIQUE NAME FOR THIS COLLECTION.
Email	Enter email to get notification once the targeted collection has finished processing.
Select a collector	Select the Microsoft Teams collector that is already configured in Administration console.
Select matching method for the keyword search	Select the method to filter collection based on keywords.
Select date range	Specify the date range for collection. The available options are Before, After, and Between.

4. Click **Save and Next** to navigate to the User Source tab.
5. On the User Source tab, under User source configuration, select any of the following options:

   - Select the All users option to include all the available users.

- Select the Select users from list option to open the list of all users. Select the users whose activities you want to archive, and click **Confirm**.

6. Click **Save and Next** to navigate to the Send to Cases tab.
7. Search for and select cases that you want to send to this Microsoft Teams collector.
8. In the Research set name field, provide the collector name.
9. Click **Save and Next** to navigate to the Review tab.
10. On the Review tab, do the following:

    - Check the configuration information to ensure accuracy.
    - To modify configuration information, click the corresponding Edit link.

11. If the data is correct, click **Complete**.

The Microsoft Teams archive collector appears in the Targeted Collections page.

1. If the status of the targeted collector is Incomplete, modify the collector configuration. To modify the configuration, click on the targeted collection name.

   > “ ”

   Note: If the configuration is incomplete, user cannot be sent to case. User cannot remove the previously selected and saved options.

   > “ ”

2. After successful configuration, if you want to send the data to more cases, click Send to case in the respective row.

About cases in the E-Discovery tab

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

Cases are created and managed in the E-Discovery tab. When creating a case, the Discovery Administrator selects the user accounts (custodians) that the E-Discovery is to include. Within the case the Discovery Administrator can create and save the searches that find the custodian emails

and attachments that may be pertinent to the case. The searches and review actions within a case are traceable.

> “ ”

Note: Cases can never be deleted from Advanced eDiscovery. When a case is completed you can hide it from the cases list, but you cannot remove it.

> “ ”

Typically a case is set to place on legal hold all the emails that are associated with it. The legal hold ensures that the emails are retained in Enterprise Vault.cloud, regardless of the company's email retention policies. An email remains on legal hold until the reviewer or administrator removes the legal hold. Normally, the legal hold is removed for an email when a reviewer determines that it is not of interest to the case. Legal hold can also be applied to the results of individual searches.

When you save a search of a case, you can choose to save it as a Review Set, at which point you assign the search results to the case's reviewers for analysis. Multiple reviewers can interact and collaborate to review the search results to distribute the review work and expedite the discovery process. Once a search is saved as a Review Set it cannot be modified.

> “ ”

Note: While administrators can view all cases in Advanced eDiscovery, reviewers can only view the cases to which they are assigned.

> “ ”

Case workflow summary: Discovery Administrator

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

Table: Process for a Discovery Administrator to set up a new case

PHASE	ACTION	DESCRIPTION
Phase 1	Prepare the reviewers, labels, and review status tags for the cases.	- Prepare the reviewers. The System Administrator can assign Enterprise Vault.cloud accounts to the Reviewer and Administrator roles as required. See About account roles and Advanced eDiscovery . **Note:** Take care in selecting users for theReviewerrole, since reviewers can see other employees' emails. Review the current list of reviewers and the cases 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 Investigation > Labels node. See Creating a label .
		- Prepare the review status tags. You can create review status tags and choose which are available when creating

PHASE	ACTION	DESCRIPTION
		new cases. See Customizing the case review status tags .
Phase 2	In E-Discovery > Cases , add a new case.	The steps to add a new case are\:
		- Provide a name, description, and expiry date.
		- Apply legal hold for the case, if required.
		- Select the user accounts (custodians) on which to perform the eDiscovery.
		- Select one of more reviewers for the case.
		- Select the review status tags to use with the case.
		See Creating a case .
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.
		See Performing a new search of a case .
Phase 4	Apply labels and tags to the search.	Apply labels, tags, and notes to emails as required.
		See Applying tags to emails .

PHASE	ACTION	DESCRIPTION
		See Adding case notes to emails .
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.
		See Saving a search of a case .
		See Assigning Research Sets to reviewers .
		See Applying a search-level legal hold .

Customizing the case review status tags

Discovery Administrators can customize the case review status tags if required, to reflect their internal workflow. You can hide or rename the supplied status tags, and you can create new status tags.

Review status tags cannot be edited or hidden once they are applied to one or more emails.

To customize the case review status tags

1. From the E-Discovery tab, expand the Administration node. This node is only visible to Discovery administrators.
2. Expand the Cases node.
3. Select **Review Status Tags**.
4. Make changes in the Review Status Tags window. You can change the name or description for all the supplied review status tags except for the Not reviewed status. You can also add custom review status tags.

Select the **Is Active** check box for the status tags you want to display when creating a new case. Clear the check boxes for any statues that you want to hide.

Advanced eDiscovery requires you to have at least two review status tags available to users. You can use the Is Default column to indicate the two default status tags.

1. Click **Save Review Status Tags**.

Creating a case

Discovery Administrators can create cases and select which custodians (email archives) to associate with the case. Once a case is created, all emails for the case can be placed on legal hold to ensure that the emails are retained.

To create a case

1. From the E-Discovery tab expand the Administration node. This node is only visible to Discovery Administrators.
2. Expand the Cases node and select the Case List node.
3. Click **Add Case**.
4. Complete the details in the Add New Case pane. Review the following table for more information.

APPLY LEGAL HOLD	CLICK YES TO TOGGLE THE OPTION BETWEEN YES AND NO. THE YES OPTION APPLIES A CASE-LEVEL LEGAL HOLD TO EMAILS, AND IS THE DEFAULT VALUE.
	NOTE: THIS OPTION KEEPS ALL EMAILS FOR THE CASE ON LEGAL HOLD UNTIL THE ADMINISTRATOR REMOVES THE LEGAL HOLD.
Name	Enter a unique name for the case.
Description	Optionally enter a description for the case.
Expiration date	Select Never Expires , or enter an expiration date for the case.
	After the expiration date a case's status changes to inactive. An inactive case

APPLY LEGAL HOLD	CLICK YES TO TOGGLE THE OPTION BETWEEN YES AND NO. THE YES OPTION APPLIES A CASE-LEVEL LEGAL HOLD TO EMAILS, AND IS THE DEFAULT VALUE.
	NOTE: THIS OPTION KEEPS ALL EMAILS FOR THE CASE ON LEGAL HOLD UNTIL THE ADMINISTRATOR REMOVES THE LEGAL HOLD.
	becomes read-only for reviewers, but all its associated data and any hold remains intact. The Discovery Administrator can revert an inactive case back to active status.

5. Under Custodians for Case, do one of the following:

   - Select **All Custodians** to include all the archive accounts as accounts that may be searched for this case.
   - Or click **Add/Remove Custodian(s)** and select the archive accounts that you want to include for search.

Then click **Update**to save your custodian selections, and click**Close** to close the dialog.

1. Under Reviewers for Case, click **Add/Remove Reviewer(s)** to add the reviewers for this case.

In the Add/Remove Reviewer(s) dialog, select the reviewers you want to act as reviewers.

Click **Update**to save your selections, and click**Close** to close the dialog.

1. In the reviewer permissions table, select the required reviewer permissions for each selected reviewer.

NEVER EXPIRES	SELECT THIS CHECK BOX IF YOU DO NOT WANT THE REVIEWER'S PERMISSIONS TO EXPIRE.
Expiration date	Enter an expiration date for the granted permissions, if you cleared the Never Expires check box.
Review Email	Allows the reviewer to review emails for the case.

NEVER EXPIRES	SELECT THIS CHECK BOX IF YOU DO NOT WANT THE REVIEWER'S PERMISSIONS TO EXPIRE.
View Case Logs/Reports	Allows the reviewer to view the logs and reports for the case.
Create Export	Allows the reviewer to create an export file of emails for the case.
Download Shared Export	Allows the external reviewer to see the shared exports that are shared by the Discovery administrators.
Manage Saved Searches	Allows the reviewer to manage the saved searches for the case.
Manage Reviewers	Allows the reviewer to manage the reviewers for the case.
Edit Case	Allows the reviewer to make edits to the case.
All	Selects all permission for the reviewer.

2. Under Reassign Emails, specify the following details. Click **Reassign** to implement the reassignment process.

REASSIGN FROM	SELECT THE REVIEWER FROM WHOM YOU WANT TO REASSIGN EMAILS TO ANOTHER CUSTODIAN.
Reassign To	Select a new reviewer to which you want to assign emails.
Percentage	Specify the amount of percentage for email reassignment from one reviewer to another for this case.

3. Under Customizations, select the list of values for the review status tags that are available to the reviewers when they review each message.

Under Select Review Status Tags LOV do one of the following:

- Select **Default values** to use the default list of review status tags in their default order.
- Or select **Custom LOV** to choose which review status tags are to be used with this case.

Click **Choose Review Status Tag** and in the Customize Review Status Tags LOV dialog, select the review status tag values to exclude.

Then if required, change the order in which the review status tags are to be displayed to the reviewers.

Click **Update** to save your selections, and then close the Customize Review Status Tags LOV dialog.

1. Click **Save** to create the case with your selected options.

Viewing the details of a case

To view the details of a case

1. From the E-Discovery tab, select the Cases node to display a list of cases.

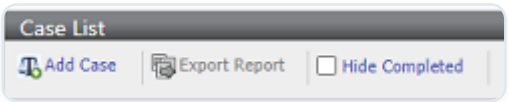
If you are a reviewer, Advanced eDiscovery lists only those cases to which you have been assigned.

> “ ”

Note: For Discovery Administrators, the list of all cases is also available from theAdministrationnode under> Cases > Case List.

> “ ”

1. If you have the required permissions the **Hide Completed** check box is available above the case list. To list only the active cases, select the check box.



2. To view the details of a case, select a case from the Case List. A summary of the reviewers and custodians for the case appears below the list.

Under the Cases node in the left pane a *case_name* node appears for the selected case. This node contains a number of sub-nodes that provide details of the case as follows. The available options depend on your permissions:

- *case_name* : Click this node to display the Edit Case pane. If you have the required permissions you can edit the details of the case in this pane.

See Editing a case.

- Summary: Click this node to view a Case Information Summary table.
- Saved Searches: From this node you can perform new searches or run any saved searches that are related to the case.

See Performing a new search of a case.

- Tags: Click this node to view all of the tag assignments for the case.
- Review Status Tags: Click this node to review the emails of the custodians that are associated with the case.

  > “ ”

  Note: Reviewers see only the emails that have been assigned to them.

  > “ ”

To view the mails according to their current review status tags, click the required review status tags node under the Review Status Tags node.

- Labels: Click this node to view details of the assigned labels.

To view all of the emails with a specific label, click the required label under the Labels node.

- Batch Processes: Click this node to view the exports that are associated with this case.
- Case History: Click this node to view a table of actions that were performed on this case.

Editing a case

Administrators and reviewers with the appropriate permissions can edit the cases to which they are assigned, and for which they have been granted edit permission.

To edit a case

1. From the E-Discovery tab, select the Cases node to display the cases list in the main pane.
2. Select the required case from the cases list.

Under the Cases node in the left pane a *case_name* node appears for the selected case.

1. Click the *case_name* node to display the Edit Case pane.
2. Edit the case details as required. Review the following table for more information.

> “ ”

Note: If you do not have edit permissions, the settings are not changeable.

> “ ”

EDIT CASE	YOU CAN EDIT THE CASE-LEVEL LEGAL HOLD STATUS, NAME, DESCRIPTION, AND EXPIRATION DATE FOR THE CASE.
	YOU CAN ALSO SET THE CASE STATUS TO INACTIVE OR COMPLETED . SETTING THE STATUS TO INACTIVE DISABLES ALL FUNCTIONALITY FOR WORKING WITH THE CASE.
Custodians for Case	You can add or remove the custodian archives to monitor for the case.
Reviewers for Case	You can add or remove reviewers or edit reviewer permissions for the case.
Reassign Emails	You can reassign emails from one reviewer to another reviewer.
Customizations	You can change the available Review Status Tags available for the case.

> “ ”

Note: ClickRefreshto update the number of emails that are included in the selected case and the number of emails on legal hold.

> “ ”

3. Click **Save** after you finish editing the case details.

Performing a new search of a case

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

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

> “ ”

Note: You can now use an advanced search to find the emails that include a classification tag. The Veritas Information Classifier assigns classification tags to emails that match an enabled classification policy. The built-in Veritas Information Classifier policies help you to locate any emails that may infringe your corporate policies or regulations.

> “ ”

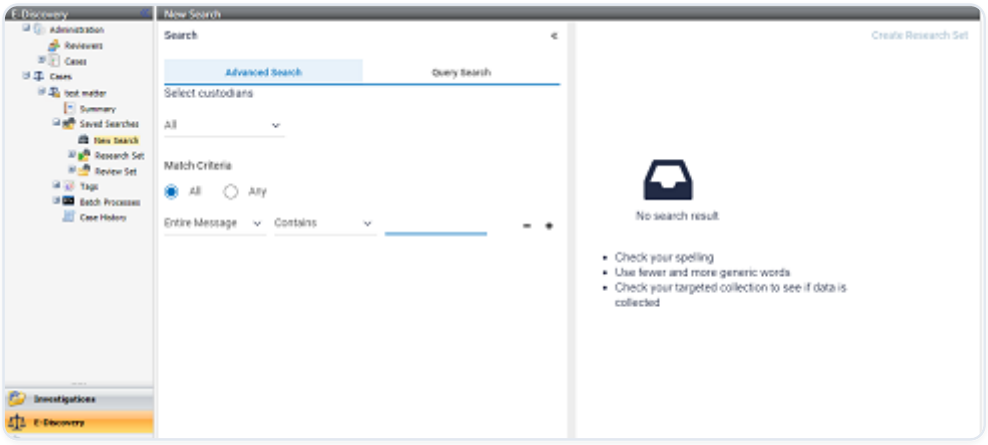
To perform a new search of a case

1. From the E-Discovery tab, select the Cases node to display the cases list in the main pane.
2. Select the required case from the cases list.

Under the Cases node in the left pane a *case_name* node appears for the selected case.

1. Under the Cases > *case_name* node, expand **Saved Searches**.
2. Click **New Search**.

You can perform an Advanced Search and a Query Search.



1. To perform an Advanced Search, do the following:

   - Select the Advanced Search tab.
   - Select the custodian archives you want to search.
     - To search archives of all of the custodians that are associated with the case, select **All**.
     - To search archives of the particular custodians, select **Custom**. Click Manage to search for, add, and remove the custodians. Click Update to complete the custodian selection.
   - Specify the search criteria by using the following options.
     - Select All to match all conditions you have provided.
     - Select Any to match any of the conditions you have provided.
     - Click **+** to add new search clauses, and complete a new row for each clause.
     - Click **-** to remove search clauses that are not required.
     - Searches are not case-sensitive. The search supports phrase search, Boolean operators, proximity search, and wildcard search.

See Search syntax for Advanced Search.

- Search for and select the message attributes you want to search. Refer to the table below:

ENTIRE MESSAGE	CONTAINS / DOESN'T CONTAIN
Subject	Contains / Doesn't Contain
Body	Contains / Doesn't Contain
From	Contains / Doesn't Contain

ENTIRE MESSAGE	CONTAINS / DOESN'T CONTAIN
	Note: Produces search results from theFromfield.
To	Contains / Doesn't Contain
	Note: Produces search results from theTo,BCC, andCCfields.
Has Attachment	Yes / No
Attachment Name	Contains / Doesn't Contain
Attachment Type	Contains / Doesn't Contain
	See Searchable attachment types .
Classified As	Contains / Doesn't Contain
	Note: This option is available if the Veritas Information Classifier service is enabled for your company. Select a classification tag from the drop-down list. The list shows all the classification tags that have been applied to your company's messages in Enterprise Vault.cloud. To see a tooltip with a classification tag's description, select the classification tag from the drop-down list and then point to the classification tag.
Date Sent (AND)	Is Equal To / Before / Before (Incl.) / After / After (Incl.)
From / To	Contains / Doesn't Contain
	Note: This option produces search results from theFromandTofields.
Inbound Message (AND)	Yes / No
Outbound Message (AND)	Yes / No
Is Hidden	Yes / No

ENTIRE MESSAGE	CONTAINS / DOESN'T CONTAIN
IP Header	Contains / Doesn't Contain

1. To perform a Query Search, do the following:

- Select the Query Search tab.
- Select the custodian archives you want to search.
  - To search archives of all of the custodians that are associated with the case, select **All**.
  - To search archives of the particular custodians, select **Custom**. Click Manage to search for, add, and remove the custodians. Click Update to complete the custodian selection.
- Specify the search query by providing keywords.

1. Click **Search**.

> “ ”

Note: The results of an Advanced Search include aRelevancecolumn. The length of the bar in this column represents how closely the email matches the search criteria, relevant to the other emails in the results.

> “ ”

2. Click **Save Search**.

See Saving a search of a case.

Saving a search of a case

If you have the required permissions you can save a search of a case. A search of a case can be saved as a Research Set or a Review Set:

- A Research Set is not assigned to reviewers. Emails continue to be added to Research Sets until a reviewer is assigned.
- A Review Set is assigned to the reviewers of the case. You can allocate a percentage of the search results to each reviewer.

- Additionally, you can select No Allocation in case you want to Assign 0% to all reviewers. In this case, emails are not assigned to any single reviewer. Any reviewer can again review and tag the emails that are reviewed and tagged before. The review tag can be changed any another reviewer.

To save a search of a case

1. Perform a new search on the case.

See Performing a new search of a case.

1. Click **Create Research Set**.
2. Complete the information in the Create Research Set dialog. The following table describes the options.

ENTER SAVED SEARCH NAME	ENTER A NAME FOR THE SAVED SEARCH.
Legal hold	Select to place all email in the saved search on legal hold. Emails on legal hold are not deleted from the archive.
Assign Create Review Set	Select this check box to assign the search results to the reviewers of the case.
	The Create Research Set dialog displays a list of reviewers of the case. Select one of the following options to assign emails to reviewers.
	- No assignment : No specific percentage of emails are assigned to any single reviewer. Emails that are reviewed and tagged by any of the reviewers can be edited and tagged by other reviewers.
	- Custom assignment : You can decide specific percentage of emails to reviewers. The total allocation percentage must be 100 percent. If the case has only one reviewer, Advanced eDiscovery automatically assigns all emails to the reviewer.

ENTER SAVED SEARCH NAME	ENTER A NAME FOR THE SAVED SEARCH.
	- Assign equally to all reviewers : The application equally distributes percentage of emails among reviewers.
	- Allow shared reviews : Select this check box to allow reviewers to access and review emails assigned to other reviewers. If you have selected the Custom Assignment or the Assign equally to all Reviewers option, you can clear this check box to restrict reviewers to access and review emails assigned to other reviewers. If you have selected the No Assignment option, this check box is selected by default. You cannot clear it.
	Note: If you do not selectCreate Review Set, the search is saved as a Research Set. Emails continue to be added to a Research Set until it is assigned to the reviewers and so becomes an Assigned Search.

3. Click **Save** to save the search.

The search is saved within the Saved Searches node as follows:

- If you selected the **Assign Save Search** check box, the search is saved under the Review Sets node.
- Otherwise the search is saved under the **Research Sets** node.

Viewing and modifying a saved search of a case

You can view the results of a saved search of a case. If the saved search is a Research Set, you can also change its name, create a new search with the same criteria.

> “ ”

Note: You cannot modify Assigned Searches.

“ ”

To view or update a saved search of a case

1. From the E-Discovery tab, select the Cases node to display the cases list in the main pane.
2. Select the required case from the cases list. Under the Cases node a *case_name* node appears for the selected case.
3. Under the Cases > *case_name* node, expand **Saved Searches**.
4. Click the required saved search under the Research Sets node or the Review Sets node.

The search displays its results.

1. To change the name of a Research Set or to clone it, click **Update Saved Search** in the menu bar.

   “ ”

   Note: You cannot modify Assigned Searches.

   “ ”

2. Update the information in the Saved Search dialog as required. See the following table for more information:

ENTER SAVED SEARCH NAME	PROVIDE A NEW NAME FOR THE SEARCH.

Then select an option for modifying the search as follows:

SAVE AS NEW	SELECT TO CREATE A NEW RESEARCH SET WITH THE NEW NAME.
	THE CURRENT SEARCH IS UNAFFECTED.
Update	Select to update the existing Research Set with the new name.

Applying a search-level legal hold

Accounts with the appropriate permissions can place emails from a search on legal hold. Applying a search-level hold ensures that specific emails remain on hold even if a case-level legal hold is removed.

You can apply a search-level legal hold to Research or Review sets.

To apply a search-level legal hold

1. From the E-Discovery tab, select the Cases node to display the cases list in the main pane.
2. Select the required case from the cases list.

Under the Cases node a *case_name* node appears for the selected case.

1. Under the Cases > *case_name* node, expand **Saved Searches**.
2. Expand the Research Sets or Review Sets node that contains the Saved Search to which you want to apply the search-level legal hold.
3. Select the required Saved Search.
4. In the top-right corner, click **Apply Search Legal Hold**.

> “ ”

Note: To remove a legal hold after it has been applied, clickRemove Search Legal Hold.

> “ ”

Assigning Research Sets to reviewers

Administrators or reviewers with the appropriate permissions can assign the results of a Research Set for a case to various reviewers to expedite the eDiscovery process.

Advanced eDiscovery treats Research Sets as on-going searches. Emails continue to be added to Research Sets until they are assigned to the reviewers.

> “ ”

Note: Once a search has been assigned to reviewers, it cannot be edited.

> “ ”

To assign a Research Set to reviewers

1. From the Research Sets node of a case, select a **Saved Search**.
2. Click **Create Review Set**. The Assign Emails for Review dialog displays a list of the case's reviewers.
3. Select one of the following options to assign emails to reviewers.

NO ASSIGNMENT	NO SPECIFIC PERCENTAGE OF EMAILS ARE ASSIGNED TO ANY SINGLE REVIEWER. EMAILS THAT ARE REVIEWED AND TAGGED BY ANY OF THE REVIEWERS CAN BE EDITED AND TAGGED BY OTHER REVIEWERS.
Custom assignment	You can decide specific percentage of emails to reviewers.
	The total allocation percentage must be 100 percent. If the case has only one reviewer, Advanced eDiscovery automatically assigns all emails to the reviewer.
Assign equally to all reviewers	The application equally distributes percentage of emails among reviewers.
Allow shared reviews	Select this check box to allow reviewers to access and review emails assigned to other reviewers.
	If you have selected the Custom Assignment or the Assign equally to all Reviewers option, you can clear this check box to restrict reviewers to access and review emails assigned to other reviewers.
	If you have selected the No Assignment option, this check box is selected by default. You cannot clear it.

4. Click **Save**.

Advanced eDiscovery automatically moves the search to the Review Sets node.

Generating printable reports for searches

Any user who has access to Saved Searches can generate the Printable Reports in all searches in Investigations and eDiscovery.

To generate a Printable Report for Searches

1. Go to any of the Saved Search tabs in Cases.
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.

Searching and tagging Collaboration messages in E-Discovery

You can search and view the Collaboration messages if the Microsoft Teams service is enabled and the archive collector is configured for you. For Collaboration feature overview, See About Collaboration.

To search Collaboration messages during investigation

1. In the E-Discovery tab, Select Administration > Cases > Case List.
2. Search for and select the case in which you want to search Collaboration messages.
3. In the E-Discovery tab, Select Case > Saved Searches > Case List.
4. To initiate a new search, , select **Saved Searches > New Search**.

Alternatively, to search in the existing research set, expand **Research Set** , and select the set you want.

1. To perform an Advanced Search, do the following:
    - Select the Advanced Search tab.
    - Select the custodian archives you want to search.
        - To search archives of all of the custodians that are associated with the case, select **All**.

- To search archives of the particular custodians, select **Custom**. Click Manage to search for, add, and remove the custodians. Click Update to complete the custodian selection.

- Specify the search criteria by using the following options.
  - Select All to match all conditions you have provided.
  - Select Any to match any of the conditions you have provided.
  - Click **+** to add new search clauses, and complete a new row for each clause.
  - Click **-** to remove search clauses that are not required.
  - Searches are not case-sensitive. The search supports phrase search, Boolean operators, proximity search, and wildcard search.

See Search syntax for Advanced Search.

- Search for and select the message attributes you want to search. Refer to the table below:

ENTIRE MESSAGE	CONTAINS / DOESN'T CONTAIN
Subject	Contains / Doesn't Contain
Body	Contains / Doesn't Contain
From	Contains / Doesn't Contain
	Note: Produces search results from theFromfield.
To	Contains / Doesn't Contain
	Note: Produces search results from theTo,BCC, andCCfields.
Has Attachment	Yes / No
Attachment Name	Contains / Doesn't Contain
Attachment Type	Contains / Doesn't Contain
	See Searchable attachment types .
Classified As	Contains / Doesn't Contain

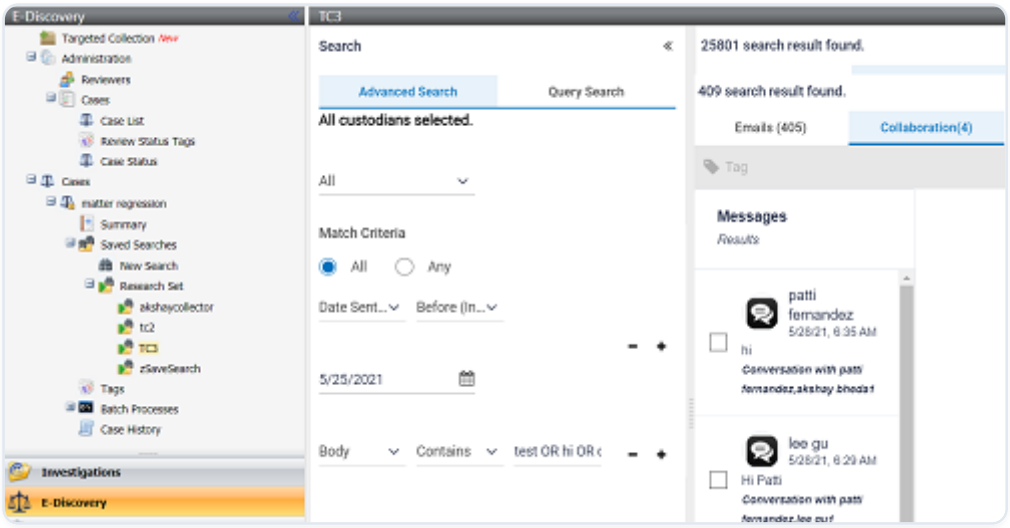
ENTIRE MESSAGE	CONTAINS / DOESN'T CONTAIN
	Note: This option is available if the Veritas Information Classifier service is enabled for your company. Select a classification tag from the drop-down list. The list shows all the classification tags that have been applied to your company's messages in Enterprise Vault.cloud. To see a tooltip with a classification tag's description, select the classification tag from the drop-down list and then point to the classification tag.
Date Sent (AND)	Is Equal To / Before / Before (Incl.) / After / After (Incl.)
From / To	Contains / Doesn't Contain
	Note: This option produces search results from theFromandTofields.
Inbound Message (AND)	Yes / No
Outbound Message (AND)	Yes / No
Is Hidden	Yes / No
IP Header	Contains / Doesn't Contain

1. To perform a Query Search, do the following:

- Select the Query Search tab.
- Select the custodian archives you want to search.
    - To search archives of all of the custodians that are associated with the case, select **All**.
    - To search archives of the particular custodians, select **Custom**. Click Manage to search for, add, and remove the custodians. Click Update to complete the custodian selection.
- Specify the search query by providing keywords.

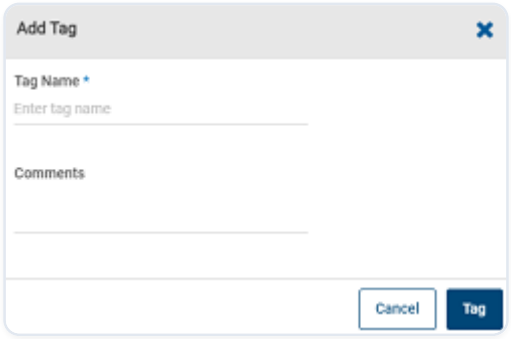
1. Click **Search**.

The search result appears as shown in the following sample image.



The application displays Chat and Channel messages for your review.

1. Select the message, and click **Tag**.
2. On the action menu, Click Tag.
3. In the Add Tag dialog box, enter a tag name and if required, provide your comments.



4. Click **Tag**.

Reviewing and working with emails in eDiscovery

This section includes the following topics:

- About reviewing cases
- Case workflow summary: reviewer
- Reviewing emails of cases
- Applying a case review status tag to emails
- Applying tags to emails
- Adding case notes to emails
- Printing emails
- Restoring emails
- Forwarding emails

About reviewing cases

As a reviewer of a case in the E-Discovery tab, you see only the resulting emails from the case searches that are assigned to you. You work with those emails to identify the content of interest. Advanced eDiscovery 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 case-specific notes to an email that another reviewer who works on the same case can see.

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

Case workflow summary: reviewer

The Discovery Administrator configures a reviewer's permissions within each case. The roles and permissions that can be granted to reviewers in Enterprise Vault.cloud and Advanced eDiscovery 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 case, and assigns the results to one or more reviewers for analysis. As a reviewer, when you open a case in Advanced eDiscovery you see the list of emails that are assigned to you for that case.

Table: Process for a reviewer working on a case describes the process to review content in the emails that result from an eDiscovery search within a case.

Table: Process for a reviewer working on a case

PHASE	ACTION	DESCRIPTION
Phase 1	In E-Discovery > Cases , open a case.	See Viewing the details of a case .
		Note: You see only the cases that are assigned to you.
Phase 2	View the emails that are assigned to you.	Review your assigned emails under the Review Set 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.
		You can view emails in the following scenarios:
		- When the emails are directly assigned to you.
		- When you are one of the assigned reviewers, and the

PHASE	ACTION	DESCRIPTION
		Allow Shared Reviews check box is selected while creating a Review Set.
Phase 3	Review each email for any content that is pertinent to the case.	You can work with each email in the following ways as required\:
		- Apply a review status tag: By default, all emails have the Not reviewed status applied. As you process each email, apply the appropriate review status. See Applying a case review status tag to emails .
		- Apply a tag: Add your own tags to emails to help organize your work, if required, or apply a managed tag. See Applying tags to emails .
		- Add a note: Add a note to an email if required. See Adding case notes to emails .
		- Manage legal holds: Typically, all emails for a case 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. See Printing emails . See Restoring

PHASE	ACTION	DESCRIPTION
		emails . See Forwarding emails .
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 to an external legal counsel.
		You can export emails, view the status of mail exports, and resubmit failed exports.
		See Exporting emails .
		See Reviewing Export Status .

Reviewing emails of cases

To review emails of a case

1. From the E-Discovery tab, select the Cases node in the left pane, to display a list of cases.

If you are a reviewer, Advanced eDiscovery lists only those cases to which you have been assigned.

> “ ”

Note: For Discovery Administrators, the list of all cases is also available from theAdministrationnode under> Cases > Case List.

> “ ”

1. If you have the required permissions the **Hide Completed** check box is available above the case list. To list only the active cases, select the check box.
2. Select the required case from the list.

Under the Cases node in the left pane a *case_name* node appears for the selected case.

1. Under the *case_name* node, select Saved Searches > Review Set. The Review Set then lists the associated emails for review. You can view emails in the following scenarios:
    - When the emails are directly assigned to you.
    - When you are one of the assigned reviewers, and the Allow Shared Reviews check box is selected while creating a Review Set.

From the list you can select emails to review their content. You can perform actions on a selected email such as change its review status tag, apply a message legal hold, or apply a new tag.

1. Open a Review Set to filter the emails based on filter criteria. Select the filters you want to apply. See the following table for more information.

INCLUDE REVIEW SET	CLICK THE FIELD AND SELECT FROM YOUR LIST OF REVIEW SETS TO INCLUDE ONLY THE EMAILS FROM THE SELECTED REVIEW SETS.
Labels	Click the field and select the required labels, to include only the emails that have the selected labels applied.
From	Enter the email sender.
Subject	Enter the subject of the email.
Has Attachment	Click the field to include emails that have attachments.
Attachment Type	Select the attachment type from the drop-down to include emails having that attachment type.
Assigned To	Click the field to include emails that are assigned to the respective reviewer.
Review Status	Click the field to include emails that are having the corresponding review status.

Click **Apply**.

Applying a case review status tag to emails

Case reviewers can apply one of the following default review status tags to an email, to indicate its status in the eDiscovery review process:

- Not reviewed
- Escalate
- Irrelevant
- Privileged
- Redact
- Relevant

In addition, Discovery administrators can customize the available review status tags.

To apply a case review status tag to emails

1. Under the associated case, select Review Set, and open the corresponding review set node

See Reviewing emails of cases.

1. To apply a review status tag to one or more emails directly from the **Review Set** :
    - Select the check box for one or more emails in the list, and click **Review Status Tags**.
    - Then select the required review status tag.
2. To apply a review status tag to an email while you view its details:
    - Select the email from the **Review Set** list to display its details.

The review status tag is shown at the top of the preview pane that displays the details of the message.

- Click the required review status tag from the row of review status tags options.

Note that to view emails based on their review status tag, you can filter the required review status tags node under the Filter section.

Applying tags to emails

To help organize your work you can tag emails with custom tags of your own choosing, which are visible only to you. You can also tag emails with a managed tag, if you have any of these available to you. Managed tags are created in the Enterprise Vault.cloud Administration Console, under the

My Config > Managed Tags node. For more information on managed tags, see the Archive Administration Help.

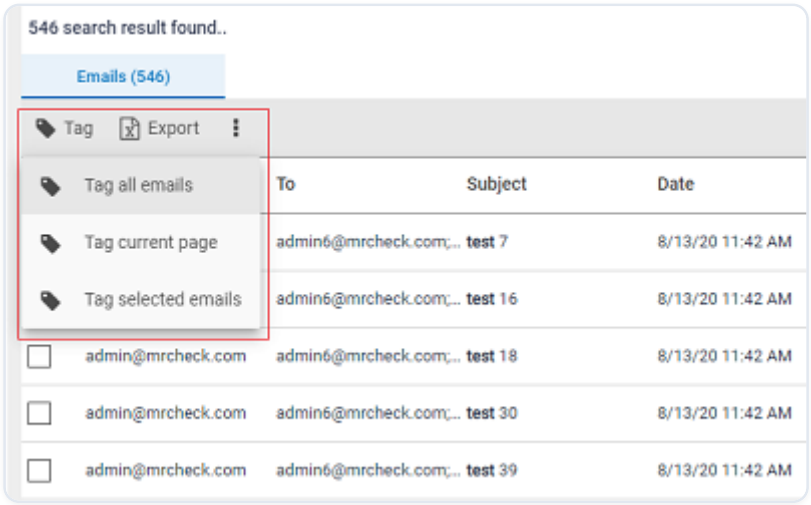
> “ ”

Note: The Veritas Information Classifier assigns classification tags to emails that match an enabled classification policy. You cannot add classification tags manually.

> “ ”

To apply tags to emails

1. Browse the archives of accounts that are assigned to you, or conduct a search, or view the **Review Status Tags** for a case that is assigned to you.
2. If required, select the check box for one or more emails, or select a message to view the message in the Advanced eDiscovery preview pane.
3. Click the tag icon, and select an option to specify which emails to tag.



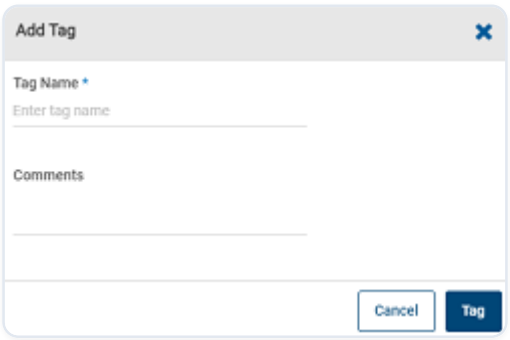
4. Enter a tag name and description for the custom tag. Alternatively you can select a retention tag, if any are available to you.

> “ ”

Note: Retention tags are the managed tags that are created in Archive Administration, under theMy Config > Managed Tagsnode.

> “ ”

If you entered a custom tag name and you want to place the tagged emails on legal hold, select the **Legal Hold** check box



1. Click **OK**.

> “ ”

Note: In theE-Discoverytab, any custom tags you create are listed in theTagsnode of the selected case. TheTagsnode does not show classification tags.

> “ ”

Adding case notes to emails

Notes are case-specific. A note that is applied to an email in one case does not appear for the same email in a different case. Reviewers can apply notes to an email that are visible to other reviewers of that case.

To apply a case note to emails

1. Display the **Review Status Tags** list of emails for the associated case.

See Reviewing emails of cases.

1. Select a message to display it in the message preview pane.
2. In the preview pane for the message, click **Notes** to add or review the notes for this email.

Printing emails

You can print emails of interest, if required.

To print emails

1. Right-click the email and select **Print this message**. The details of the message are shown. Click**Print**.
2. You can also click the **Print** icon when viewing the details of a message in the message preview pane.

Restoring emails

The restore feature in Advanced eDiscovery sends an exact copy of a selected email back to the selected user's mailbox. The restoration process only takes a few seconds to complete. The restored email appears in the top of the user's Inbox with the date and time you restored the email. You can see the original timestamp of the email by opening it in your Outlook or Notes Inbox.

To restore an email

1. Right-click the email and select **Restore**, or to select multiple emails select the check boxes and click**Restore** in the toolbar.
2. Select the user's account that you want to restore the selected email.

   > “ ”

   Note: UseQuick Searchto quickly find a user's account. You can also click the arrow in the search field, to search using theCriteria Searchfilter.

   > “ ”

3. Click **Restore**.
4. Click **Close** to close the restore window or select additional user accounts if you want to restore the selected email to additional accounts.

Forwarding emails

The forwarding functionality is only available if enabled for your organization.

> “ ”

Note: We recommend you only forward emails during the investigation phase. Forwarding an email changes its metadata and is not an appropriate means for collecting files during legal proceedings.

> “ ”

You can use Advanced eDiscovery's forward feature to share emails with other reviewers or outside counsel.

To forward an email from Advanced eDiscovery

1. Browse the archives of the accounts that are assigned to you, or conduct a search.
2. Select the emails you want to forward.
3. Click **Forward**.
4. Enter the email address for the recipient of the emails.

Advanced eDiscovery automatically sends the emails to the recipient as individual emails, in the original mail format.

Email export

This section includes the following topics:

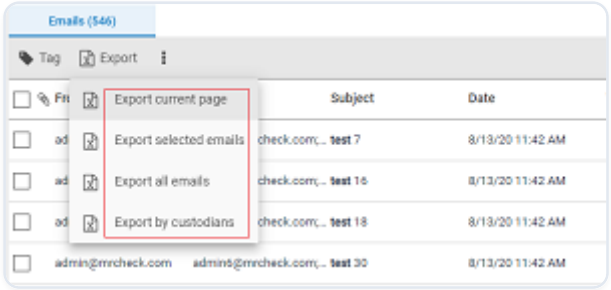
- Exporting emails
- Sharing exports with Discovery administrators
- Sharing exports with the external reviewers
- Reviewing Export Status
- Resubmitting failed export items
- Option to maintain folder structure in the export
- Canceling Export Batch
- Email export FAQ

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. Review the following table for more information.

MESSAGE FORMAT	SELECT ONE OF THE FOLLOWING FILE FORMATS FROM THE DROP-DOWN MENU\:
	- EML
	- NSF
	- PST
	- EML WITH EDRM
	- MSG WITH EDRM
	- PST WITH EDRM WARNING: FOR CLEARWELL AND FTI-RINGTAIL, DO NOT USE EXPORT OPTIONS WHEN EXPORTING EMAILS FROM THE INVESTIGATIONS TAB. THESE OPTIONS ARE USED FOR THE DISCOVERY PROCESS AND SHOULD ONLY BE AVAILABLE TO EXPORT EMAILS FROM THEE-DISCOVERYTAB.
Include Journaling Envelope	Select this option to include journaling envelopes, which contain information about email recipients such as distribution lists.
Exclude Exported Emails	Select this option to exclude previously exported emails from the current export.
	This option is case-specific. The same email in another case may or may not be exported depending if it was already exported for that case.
Export Name	Enter a name for the export file.
Export Password	Enter an access password for the export file. The password is required to open the export file after it is downloaded to your computer.
Confirm Password	Enter your export password again to confirm.

5. Click **Export Items**.

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

More Information

Email export FAQ

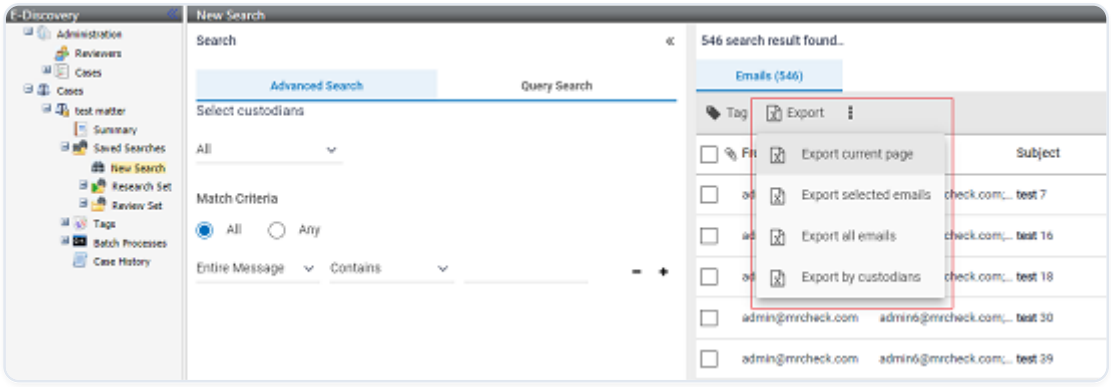
Sharing exports with Discovery administrators

During the investigation process, administrators can share exported email batch allowing to download or resubmit the exported emails.

This feature is available only when Share Export is enabled for the Discovery Administrator built-in role. For information on how to enable or disable this feature, see *Editing the built-in administrator roles* in the Enterprise Vault.cloud Archive Administration Help.

To share the exported emails batch

1. Navigate to the archives for the accounts or conduct a search using **New Search**under**Monitored Accounts** in the Investigations section.
2. If required, select checkbox for one or more emails.
3. Click the export icon, and then select an export option.



4. Enter the required information in the Export Options dialog. Review the following table for more information.

MESSAGE FORMAT	SELECT ONE OF THE FOLLOWING FILE FORMATS FROM THE DROP-DOWN MENU\:
	- EML
	- NSF
	- PST
	- EML WITH EDRM
	- MSG WITH EDRM
	- PST WITH EDRM
	WARNING: FOR CLEARWELL AND FTI-RINGTAIL, DO NOT USE EXPORT OPTIONS WHEN EXPORTING EMAILS FROM THE INVESTIGATIONS TAB. THESE OPTIONS ARE USED FOR THE DISCOVERY PROCESS AND SHOULD ONLY BE AVAILABLE TO EXPORT EMAILS FROM THEE-DISCOVERYTAB.
Include Journaling Envelope	Select this option to include journaling envelopes, which contain information about email recipients, such as distribution lists.
Enable AES-256 Encryption	Select this option to enable AES-256 encryption.
Export Name	Enter a name for the export file.
Export Password	Enter an access password for the export file. The password is required to open the export file after it is downloaded to your computer.
Confirm Password	Enter your export password again to confirm.
Share Export	Click this option to load the list of administrators to share export.
	Note: The list only displays the Discovery Administrators.

5. Click **Export Items**.
6. To review the export status, expand the Batch Processes node and select **Exports.**>**Note:** Follow your company's security guidelines while manually sharing the export password between Advanced eDiscovery administrators.

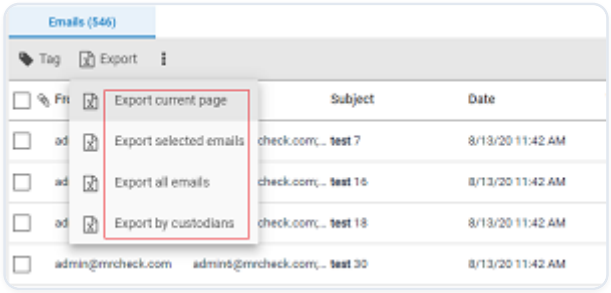
Sharing exports with the external reviewers

Discovery administrators can share exported emails batch within that case with the external reviewers during the case review process. External reviewers can access the shared export batches from the Batch Process tab when the shared export is successful.

This feature is available only when the Download Export permission is enabled for the Discovery Administrator built-in role. For information on how to enable or disable this feature, see *Editing the built-in administrator roles* in the Enterprise Vault.cloud Archive Administration Help.

To share the exported emails batch

1. Navigate to the **Case**in eDiscovery and conduct a search using**New Search**.
2. If required, select check box for one or more emails.
3. Click Export, and then select an export option.



4. Enter the required information in the Export Options dialog. Review the following table for more information.

MESSAGE FORMAT	SELECT ONE OF THE FOLLOWING FILE FORMATS FROM THE DROP-DOWN MENU\:
	- EML
	- NSF
	- PST
	- EML WITH EDRM
	- MSG WITH EDRM
	- PST WITH EDRM
	WARNING: FOR CLEARWELL AND FTI-RINGTAIL, DO NOT USE EXPORT OPTIONS WHEN EXPORTING EMAILS FROM THE INVESTIGATIONS TAB. THESE OPTIONS ARE USED FOR THE DISCOVERY PROCESS AND SHOULD ONLY BE AVAILABLE TO EXPORT EMAILS FROM THEE-DISCOVERYTAB.
Include Journaling Envelope	Select this option to include journaling envelopes, which contain information about email recipients, such as distribution lists.
Enable AES-256 Encryption	Select this option to enable AES-256 encryption.
Export Name	Enter a name for the export file.
Export Password	Enter an access password for the export file. The password is required to open the export file after it is downloaded to your computer.
Confirm Password	Enter your export password again to confirm.
Share Export	Click this option to load the list of external reviewers to share export.

MESSAGE FORMAT	SELECT ONE OF THE FOLLOWING FILE FORMATS FROM THE DROP-DOWN MENU\:
	- EML
	- NSF
	- PST
	- EML WITH EDRM
	- MSG WITH EDRM
	- PST WITH EDRM
	WARNING: FOR CLEARWELL AND FTI-RINGTAIL, DO NOT USE EXPORT OPTIONS WHEN EXPORTING EMAILS FROM THE INVESTIGATIONS TAB. THESE OPTIONS ARE USED FOR THE DISCOVERY PROCESS AND SHOULD ONLY BE AVAILABLE TO EXPORT EMAILS FROM THEE-DISCOVERYTAB.
	Note: This list only displays the external reviewers who are added as reviewers for that case.

5. Click **Export Items**.
6. To review the export status, expand the Batch Processes node and select **Exports.**>**Note:** Follow your company's security guidelines while manually sharing the export password between Advanced eDiscovery administrators and external reviewers. After you share the exports with the external reviewer, Discovery administrator needs to enable the external administrator to see the export. Discovery administrator must enable theDownload Shared Exportprivilege (under case reviewers) for the external reviewer. This step is done while creating/editing a case. After Discovery administrator assigns this privilege to the external reviewer, external reviewers can view the shared exports from the admin.

> “ ”

Note: If discovery admin revokes the permission forDownload Shared Export, then the external reviewer cannot access the shared exports.

> “ ”

Reviewing Export Status

From the Export Status page, you can view details on mail exports, download exports and resubmit failed export items.

The following table provides more information on the Export Status page sections:

EXPORT TABLE	PROVIDES A LIST OF EXPORT BATCHES.
	NOTE: ADVANCED EDISCOVERY SPLITS LARGE EXPORTS INTO 2-GIGABYTE BATCHES. THEREFORE, MULTIPLE EXPORT BATCHES CAN BE ASSOCIATED WITH ONE EXPORT
Download Details	Provides the export details and export download link. Details include: export file type, expiration date for download link, output file type, and export status.
Resubmit Failed Items	This section appears when the selected export contains failed export items. Exports contain failed items when Completed with Errors or Error is listed in the Step field.

Following are the export table column definitions:

BATCH ID	ID NUMBER FOR THE EXPORT BATCH.
Export Name	Name of the export file.
Create Date	Date and time export was created.
Start Date	Date and time export started processing.
End Date	Date and time export process ended.

BATCH ID	ID NUMBER FOR THE EXPORT BATCH.
Step	Describes the export status\:
	- Complete - export without any errors
	- Completed with Errors - export with failed export items
	- Error - export failed
	- Terminated - export canceled
\# Total	Total number of export items.
\# Exported	Number of successful export items.
\# Failed	Number of failed export items.

Resubmitting failed export items

Exports contain failed items when Completed with Errors or Error is listed in the Step field.

Exports with failed items can be resubmitted three times.

> “ ”

Note: Exports can only be resubmitted after all associated export batches have finished processing. Advanced eDiscovery splits large exports into 2-gigabyte batches. Therefore, multiple export batches can be associated with one export.

> “ ”

For more information on failed items, see the error list in the download file.

To resubmit failed export items:

1. Expand the Batch Processes node.
2. Select **Export**.
3. Select the export batch you want to resubmit.

4. In the Resubmit Failed Items section, click **Go**.

> “ ”

Note: TheResubmit Failed Itemssection appears only when the selected batch contains failed export items. The batch contains failed items whenCompleted with ErrorsorErroris listed in theStepfield.

> “ ”

5. Complete the information in the Resubmit Fail Items window. Review the following table for more information.

EXPORT NAME	ENTER A NAME FOR THE EXPORT FILE.
	NOTE: THE MINIMUM LENGTH IS 5 CHARACTERS AND THE MAXIMUM IS 160.
Export Password	Enter an access password for the export file. The password is required to open the export file after it is downloaded to your computer.
Confirm Password	Enter your export password again to confirm.

6. Click **Export Items**.

> “ ”

Note: Only failed items are included in the resubmitted exports. For example, if an export with 20 items includes 5 failed items, only the 5 failed items are exported to the file.

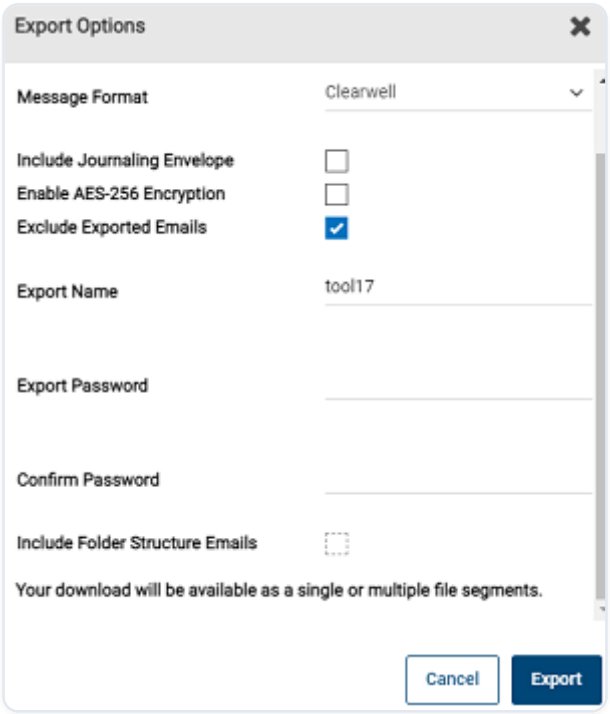
> “ ”

Option to maintain folder structure in the export

The option to Include Folder structure in the export is displayed to the Customer only when all the listed conditions are satisfied:

- Customer has purchased Folder Synchronization
- Customer exports a single custodian's email
- Customer is on the E Discovery Tab

The Include Folder Structure check box is displayed and disabled by default. The check box is enabled for selection only when the user selects the value PST from the Message Format drop-down.

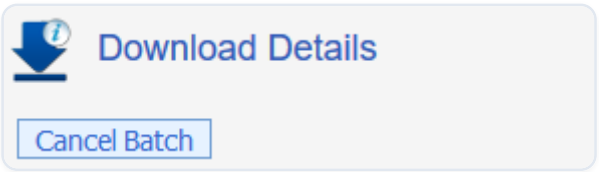


Canceling Export Batch

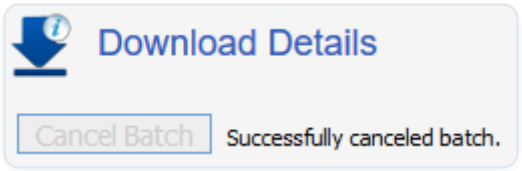
When you cancel an export batch, the export is abandoned, and the status of the batch is set to Terminated. The option to resubmit failed items is disabled on the terminated batch.

To cancel an export batch

1. Select an export batch in the table of exports. The download details section for the selected export displays a **Cancel Batch** button.



2. Click **Cancel Batch**.
3. Click **OK** to confirm.



After the batch is successfully canceled, the status of the batch is set to Terminated. The option to resubmit failed items is disabled on the terminated batch.

Email export FAQ

The following frequently asked questions provide more information about data exports in Advanced eDiscovery.

- What is the maximum number of messages that I can export?

You can export up to 200,000 messages.

- Why is the export to NSF option unavailable?

The NSF export option is only available when a Domino server has been configured as the mail server type in the archive settings. Contact your Archive Administrator for more information.

Collaborative reports

This section includes the following topics:

- About collaborative eDiscovery reporting
- Report by email: Audit trail
- Report by Case: Case History
- Report by Case: Case Summary
- Report by Archive: eDiscovery dashboard

About collaborative eDiscovery reporting

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

Collaborative eDiscovery reports contain the following information:

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

Report by email: Audit trail

Reviewers can review the audit trail for a specific email that includes actions performed, such as review status tags or the applied labels and export details.

To review the audit trail for an email

1. Expand the node for a case.
2. Expand the Review Status Tags node.
3. Select **All** to display all emails or one of the review status tags under the Review Status Tags node.
4. Select the email you want to audit.
5. Click **Audit**.

6. Review the information in the Email History window that displays.

Report by Case: Case History

Reviewers can see and search all actions which are performed within a case such as edits on case details, reviewer permission changes, or created exports.

> “ ”

Note: Only Discovery administrators or reviewers with theView Case Logs/Reportspermission can view reports for a case.

> “ ”

To review the history for a case

1. Expand the node for a case.
2. Select **Case History** from the node for the case you selected. The Case History pane displays.
3. Click the arrow to display the Case History search menu.
4. Use the filters that are provided to search for specific Case History items. Review the following table for more information.

SCOPE	SELECT THE GENERAL SCOPE OF THE CASE HISTORY ITEM.
Action	Select the specific action of the Case History item.
User	Select the user that performed the action.
Date From	Enter the start date for the search range.
Date To	Enter the end date for the search range.
Before Value	Enter the before state of an item.
	You can enter the original review status tag for an email.

SCOPE	SELECT THE GENERAL SCOPE OF THE CASE HISTORY ITEM.
After Value	Enter the after state of an item.
	You can enter the final review status tag for an email.

5. Click **Search**.
6. Click **Export Report** to export the report for review at a later time.
7. Review the information in the Email History window that displays.

Report by Case: Case Summary

Discovery administrators and reviewers can view a report for individual cases, which includes the number of reviewers, custodians, emails, and legal holds. The case expiration date is also displayed.

To review the summary for a case

1. Expand the node for a case.
2. Select **Summary** from the node for the case you selected.
3. Review the Case Summary report that displays.
4. Click **Export Report** to export the report for review at a later time.

Report by Archive: eDiscovery dashboard

Discovery administrators can view a report for the entire archive. This report includes the number of emails within each case and the number of cases that are assigned to a reviewer.

To review the summary for the archive

1. From the E-Discovery tab, expand the Administration node. This node is only visible to Discovery administrators.
2. Select the Cases node.
3. Review the information on the Discovery Admin Dashboard.
4. Click **Export Report** to export the report for review at a later time.

Advanced eDiscovery alerts

This section includes the following topics:

- Creating an alert

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.

Refer to the following table for more information:

POLICY NAME	ENTER A NAME FOR THE NEW ALERT.
Saved Search	Click the down arrow and select the required Saved Search .
Alert Email(s)	Enter your email address.
Comment	Enter comments relating to the alert.
In Dashboard	Select the check box if you want the alert to appear in the Administration dashboard .

Email Continuity

This section includes the following topics:

- Managing Email Continuity
- Viewing Continuity emails

Managing Email Continuity

The Continuity tab is available to your organization if it subscribes to the Email Continuity feature.

If your account has the required permissions, you can access the Continuity Management page to do the following:

- Control whether users can send, reply to, and forward emails from Personal.cloud when your mail server is unavailable.
- Control whether users receive a notification when your organization's mail server is unavailable and Email Continuity is active.
- View the list of domains and mail servers that are configured for Email Continuity, and the Email Continuity status in each case.

To manage Email Continuity

1. Select the Continuity tab.
2. Select the Continuity Management node.
3. Review or configure the Email Continuity settings as required. The configurable settings are as follows:

ENABLE SEND, REPLY AND FORWARD	SELECT TO ALLOW USERS TO SEND, REPLY, AND FORWARD EMAILS FROM PERSONAL.CLOUD WHEN YOUR ORGANIZATION'S MAIL SERVER IS UNAVAILABLE.
Indicate EC Active	Select to notify users when your organization's mail server is unavailable and Email Continuity is active.

The table below the settings lists each domain and corresponding mail server that are configured for Email Continuity, and the Email Continuity status in each case.

1. Click **Save** to save any changes you made.

Viewing Continuity emails

From the Continuity Emails page of the Continuity tab, administrators can view a list of the emails that Email Continuity has handled during an outage.

To view continuity emails

1. Select the Continuity tab.
2. Select the Continuity Emails node.

Methods for searching cases and accounts

This section includes the following topics:

- About Advanced Search
- Search syntax for Advanced Search
- About stop words and special characters
- Phrase searches
- Boolean operator searches
- Wildcard searches
- Proximity searches
- Double-byte character set searches
- About enhanced searches in Japanese
- Searchable attachment types
- Search examples and tips

About Advanced Search

Advanced eDiscovery provides the following methods for searching the content of cases and archive accounts:

- Search provides a quick way to search the content of every message.
- Advanced Search lets you focus the search within chosen email components such as the subject or body, and on email attributes such as the sent date.

Advanced Search are available from:

- The Investigations tab when you search your own account or the accounts that you manage.
- The E-Discovery tab when you perform searches of the custodian accounts within cases.

Advanced Search support the use of phrase search, Boolean operators, proximity search, and wildcard search.

See Search syntax for Advanced Search.

You can perform a new search and optionally save it, or you can view the results of a previously saved search:

- See Performing a new search of accounts (Investigations tab).
- See Performing a new search of a case.

Search syntax for Advanced Search

Table: Search methods and their syntax for Advanced Search describes the search methods that are available in Advanced Search.

Table: Search methods and their syntax for Advanced Search

SEARCH METHOD	SYNTAX	EXAMPLE AND MORE DETAILS
Phrase search	Use double quotation marks around one or more words to search for the exact phrase.	"cloud computing" finds archived messages with this phrase.
		See Phrase searches .
AND operator search	Use the AND operator between two search terms to find items that contain both search terms.	cloud AND computing finds archived messages with both of the search terms cloud and computing .
		See Boolean operator searches .
OR operator search	Use the OR operator between two search terms to find items that contain at least one of the search terms.	cloud OR computing finds archived messages with the search term cloud , or the search term computing , or both terms.
		See Boolean operator searches .
NOT operator search	Use the NOT operator between search terms to	cloud NOT computing finds archived messages with the

SEARCH METHOD	SYNTAX	EXAMPLE AND MORE DETAILS
	exclude specific search terms.	search term cloud but not the search term computing .
		See Boolean operator searches .
Single character wildcard search	Use a question mark at the end of a search term to represent a single unspecified character.	appl? finds archived messages with search terms such as apple or apply .
	Note: You must enter a search term with at least three characters before the wildcard character.	See Wildcard searches .
Multiple character wildcard search	Use an asterisk at the end of a search term to represent one or more unspecified characters.	comp* finds archived messages with search terms such as computing , computer , or company .
	Note: You must enter a search term with at least three characters before the wildcard character.	See Wildcard searches .
Proximity search	Place quotation marks around two search terms, followed by a tilde and a numerical value to indicate the maximum word count between them.	"cloud computing"~5 finds archived messages with the search terms cloud and computing within five words of each other.
	Note: Personal.cloud limits the word count between the 2 search terms to under 50 words.	See Proximity searches .

> “ ”

Note: Searches are not case-sensitive. Capitalizing a search term has no effect on the search results. Invalid search terms are shown in red; hover over invalid search terms to get additional help via Tool Tip.

> “ ”

About stop words and special characters

Stop words

Stop words are a set of commonly used words that Personal.cloud ignores when it performs a Search or Advanced Search. Personal.cloud treats the following words as stop words:

- `a, an, and, are, as, at` - `be, but, by` - `for` - `if, in, into, is, it` - `no, not` - `of, on, or` - `such` - `that, the, their, then, there, these, they, this, to` - `was, will, with` >**Note:** The stop words are supported in English only, unless your company subscribes to the option to perform enhanced searches in Japanese.

Note the following special cases:

- In phrase searches a stop word acts as a placeholder for any stop word, or nothing.

See Phrase searches.

- The words AND, OR, and NOT act as operators in a Boolean operator search.

See Boolean operator searches.

Special characters

Personal.cloud omits the following special characters from searches:

`* @ # $ % ^ & - + = _ { } [ ] , < > ; : / \ ?` **Advanced eDiscovery prevents you from entering the following special characters into the search boxes:** `/ \ < > #`

Note the following special cases:

- In phrase searches a special character acts as a placeholder for any special character, or nothing.

See Phrase searches.

- Question marks and asterisks act as wildcard characters in a wildcard search.

See Wildcard searches.

Phrase searches

To search for a phrase, enclose the phrase within double quotation marks. For example:

`"cloud computing"`

The search returns those items that contain the exact phrase *cloud computing*.

> “ ”

Note: A search produces unexpected results if it contains nothing between the quotes, or only white space between the quotes.

> “ ”

About stop words and special characters within search phrases

A phrase search that includes stop words or special characters can return any of the following:

- The exact phrase, including the stop word or special character.
- The phrase with the supplied stop word or special character replaced by other stop words or special characters.
- The phrase without the stop word or special character.

For example:

- The phrase `"test and verification"` returns items that include the exact phrase, and also phrases such as *test not verification*,*test verification*.
- The phrase with two stop words `"cat in the hat"` returns items that include the exact phrase, and also phrases such as *The cat has no hat*, and*cat hat*.

If the exact phrase occurs in the search results, it is highlighted. Otherwise the phrase is not highlighted.

> “ ”

Note: In phrase searches, the*and?characters are treated as special characters, not wildcards.

> “ ”

Boolean operator searches

You can use the Boolean operators AND, OR, and NOT to include or exclude search terms in Quick Search and Advanced Search.

> “ ”

Note: The Boolean operators are supported in English only, unless your company subscribes to the option to perform enhanced searches in Japanese.

> “ ”

- See AND operator search.
- See OR operator search.
- See NOT operator search.
- See About using multiple Boolean operators.
- See About using Boolean operators with phrase searches.
- See About Boolean operators and special characters.

AND operator search

The AND operator is inserted in between two search terms, for example:

```
cloud AND computing
```

The returned results contain both terms.

> “ ”

Note: Personal.cloud treats a space between two search terms as an AND operator.

> “ ”

The following searches are treated identically:

```
cloud computing
```

```
cloud AND computing
```

OR operator search

The OR operator is inserted in between two search terms, for example:

```
cloud OR computing
```

The returned results contain either or both of the terms.

NOT operator search

The NOT operator can be inserted in between two search terms to specify that the first term must be present, and the second term must be absent. For example:

```
cloud NOT computing
```

Enterprise Vault.cloud also lets you begin a search with a NOT operator. For example:

```
NOT "cloud computing"
```

This search attempts to return every item that does not include the phrase *cloud computing*.

> “ ”

Note: Searches that begin with a NOT operator may fail to complete due to the large number of matching results, especially if you have a large message archive.

> “ ”

About using multiple Boolean operators

You can use multiple Boolean operators in a search to create more complex searches. For example:

`cloud AND computing OR public`

In this example `cloud AND computing` represents one term.

The following items are returned:

- Items with *cloud*and*computing*- Items with*cloud*,*computing*, and*public*- Items with*public*

You can also use brackets to group multiple terms for Boolean processing. For example:

`(cloud (computing OR public)) NOT software`

In this example, the space between `cloud` and `(computing OR public)` is treated as an AND operator.

The following items are returned:

- Items with both *cloud*and*computing*, with no reference to*software*.
- Items with both *cloud*and*public*, with no reference to*software*.

The maximum number of Boolean operators that is allowed in a search is 249.

About using Boolean operators with phrase searches

Boolean operators can be used with phrase searches. For example:

`"cloud computing " OR "public cloud" NOT software`

This search returns the following:

- Items with *cloud computing*, with no reference to*software*.
- Items with *public cloud*, with no reference to*software*.
- Items with *cloud computing*and*public cloud*, with no reference to*software*.

About Boolean operators and special characters

Boolean searches with special character search terms result in invalid searches. For example, if you enter the following:

`cloud OR +`

The special character + is dropped. The effect is a Boolean search with no second term, which is an invalid search.

Here is another example:

`cloud AND - AND computing`

The special character " - " is dropped. The effect is a Boolean search with two adjacent AND operators, which is an invalid search.

Wildcard searches

A wildcard search uses a wildcard character at the end of a search term to represent one or more unspecified characters. The question mark `?` **represents a single character, and the asterisk** `*` represents one or more characters.

For example:

- `appl?` finds archived messages with search terms such as *apple*or*apply*.
- `comp*` finds archived messages with search terms such as *computing*,*computer*, or*company*.

> “ ”

Note: The wildcard character must be placed at the end of the search term. The search term must contain at least three characters before the wildcard character.

> “ ”

In phrase searches, the `*` **and** `?` characters are treated as special characters, not wildcards.

Proximity searches

Use a proximity search to find two words within a specified distance of each other. To create a proximity search, enclose the two words within quotation marks, and follow them with a tilde character (~) and a numerical value. For example:

`"cloud computing"~5`.

The numerical value specifies the maximum number of words that can exist between the words in quotes.

Note the following when using proximity searches:

- The returned results are not highlighted.
- Personal.cloud limits the proximity word count to a maximum of 49 words.
- Wildcard characters cannot be used in a proximity search.
- The results from a proximity search can contain stop words, but the stop words are excluded from the proximity word count.

Double-byte character set searches

Enterprise Vault.cloud provides some ability to search those languages that contain double-byte characters.

Phrase searches can be used to search for exact phrases with double-byte characters. For example:

```
"敏捷的棕色狐狸" AND 3515431
```

An enhanced search is available for Japanese terms, if you subscribe to the option for enhanced searches in Japanese.

More Information

About enhanced searches in Japanese

About enhanced searches in Japanese

An option is available to enable the ability to perform enhanced searches in Japanese. This option employs a Japanese language analyzer to provide better search results for different Japanese scripts.

To find out if your company's Enterprise Vault.cloud supports enhanced searches in Japanese, ask your Enterprise Vault.cloud administrator.

> “ ”

Note: Administrators can contactVeritas Services & Supportfor more information on the configuration of this option.

> “ ”

If your company's Enterprise Vault.cloud supports enhanced searches in Japanese, note the following about the enhanced search capabilities:

- Searches are supported in any combination of hiragana, kanji, katakana, and romaji scripts.
- Searches are valid for text in the message subject, the message body, attachment extensions, and attachment content.
- Advanced eDiscovery's Search supports a minimum of one English or Japanese character.
- The wildcard character limit for any search is one English or Japanese character.

Searchable attachment types

Advanced Search lets you search the content of message attachments.

> “ ”

Note: Password-protected attachments and encrypted attachments are not included in searches.

> “ ”

Table: Searchable attachments lists the attachment types that Enterprise Vault.cloud can search.

Table: Searchable attachments

FILE EXTENSION	SEARCHABLE ATTACHMENT TYPES
.accdb	Microsoft Access (text only) 1.0, 2.0, 95 - 2010
.ai	Adobe Illustrator
.asf	Windows Media ASF (metadata only)
.avi	AVI (metadata only)

FILE EXTENSION	SEARCHABLE ATTACHMENT TYPES
.csv	Microsoft Excel for Windows
.dbf	Dbase III, IV, V
	Enable Spreadsheet
.doc	Microsoft Word for Windows 1.0 - 2013
	Microsoft Word 2003 XML (text only)
	Microsoft Word 98 (J)
.docx	Microsoft Word for Windows
	Microsoft WordPad
.docm	Microsoft WordPad
.dwg	AutoCAD Drawing 9.0 - 14.0
.emf	Enhanced Metafile (EMF)
	Visio (Page Preview mode WMF/EMF)
.eml	Microsoft Outlook Express (EML)
.htm	HTML (CSS rendering not supported) 1.0 - 4.0
.html	HTML (CSS rendering not supported)
.hwp	Hangul
	97 - 2010
.ics	vCalendar 2.1
.keynote	Apple iWork Keynote (MacOS, text, and PDF preview) 9
.mht	Encoded mail messages
.mp3	MP3 (ID3 metadata only)

FILE EXTENSION	SEARCHABLE ATTACHMENT TYPES
.mp4	MPEG-4 (metadata only)
.mpp	Microsoft Project (table view only) 98 - 2003, 2007, 2010
.msg	Microsoft Outlook (msg) 97 - 2013
.numbers	Apple iWork Numbers (MacOS, text, and PDF preview) 9
.odg	OpenOffice Draw
.odp	IBM Lotus Symphony Presentations 1.x
.ods	Oracle Open Office Calc 3.x
	StarOffice Calc
.odt	OpenOffice Writer 1.1 - 3.0
	Oracle Open Office Writer 3.x
	StarOffice Writer
.oft	Microsoft Outlook Forms Template (OFT) 97 - 2013
.one	Microsoft OneNote (text only) 2007, 2010
.ots	Oracle Open Office Calc
	StarOffice Calc
.ott	OpenOffice Writer
	Oracle Open Office Writer
.pages	Apple iWork Pages (MacOS, text, and PDF preview) 9
.pdf	Adobe PDF

FILE EXTENSION	SEARCHABLE ATTACHMENT TYPES
	1.0 - 1.7 (Acrobat 1 - 10)
	Adobe PDF Package 1.7 (Acrobat 8 - 10)
	Adobe PDF Portfolio 1.7 (Acrobat 8 - 10)
	Graphic embeddings in PDF
.pot	Microsoft PowerPoint for Windows Template 2007 - 2013
.potx	Microsoft PowerPoint for Windows Template
.pps	Microsoft PowerPoint for Windows slide show 2007 - 2013
.ppsx	Microsoft PowerPoint for Windows slide show
.ppt	Microsoft PowerPoint for Windows 3.0 - 2013
.pptx	Microsoft PowerPoint for Windows
.rtf	IBM DCA/RFT
	Microsoft WordPad
	Rich Text Format (RTF)
.stc	Oracle Open Office Calc
.stw	Oracle Open Office Writer
.swf	Flash (text extraction only) 6.x, 7.x, Lite
.sxw	Oracle Open Office Writer
	StarOffice Writer 5.2 - 9.0
.txt	ANSI Text
	7 & 8 bit

FILE EXTENSION	SEARCHABLE ATTACHMENT TYPES
	Unicode Text 3.0, 4.0
.vcf	vCard
	2.1
.vcs	vCalendar
.vsd	Visio 5.0 - 2007
.wav	WAV (metadata only)
.wk1	Lotus 1-2-3
.wk3	Lotus 1-2-3
.wma	Windows Media Audio (metadata only)
.wmf	Visio (Page Preview mode WMF/EMF) 4
	Windows Metafile
.wml	Wireless Markup Language
.wmv	Windows Media Video WMV (metadata only)
.xhtml	XHTML (file ID only)
.xls	Microsoft Excel for Windows 3.0 - 2013
.xlsb	Microsoft Excel for Windows 2007 - 2013 (Binary)
.xlsm	Microsoft Excel for Windows
.xlsx	Microsoft Excel for Windows
.xlt	Microsoft Excel for Windows
.xltm	Microsoft Excel for Windows
.xml	Extensible Markup Language files

FILE EXTENSION	SEARCHABLE ATTACHMENT TYPES
	Microsoft Excel for Windows
	2003 XML (text only)
	XML (text only)
.xmp	Adobe Illustrator XMP CS1 - 6
.xps	Microsoft XPS (text only)
.zip	Compressed file

Search examples and tips

Examples of using Basic, Advanced, and Quick Search

Suppose that you want to search for the messages that relate to the resetting of a password. You can enter `password reset` **into the Search box and click Search to perform a Search. The space between** `password` **and** `reset` is treated as an AND operator, so the returned results contain any messages that include both the word *password* and the word *reset*.

Suppose that you now decide to search for the phrase *password reset*, and to exclude from the results any emails that reference the word *Box*. You can use an Advanced Search for this purpose. Click the expand icon to display the Advanced Search options. Your original Search is now shown in the first criteria row.

Insert double quotation marks around `password reset` **to specify it as a phrase. Then click + to add a second criteria row. In the new criteria row, select Doesn't Contain and enter** `Box` in the text field.

Click Search to perform the Advanced Search. The search returns any items that do not contain *Box* but that contain the exact phrase *password reset*.

You could obtain the same results if you entered the following term in the Search bar:

```
"password reset" NOT box
```

Table: List of query search terms lists some possible query search terms along with examples.

Table: List of query search terms

SEARCH TERM	DATA TYPE	DESCRIPTION	EXAMPLE
`_All, Entiremessage`	Text	Searches through all default fields. Similar to simple search or not specifying a field.	_All:(test or test2)
			"hello world"
			Entiremessage:test
`Attachments.content`	Text	Search by attachment content.	Attachments.content: "Hello World"
`Attachments.extension`	Text	Search by attachment file type (PDF, DOC, docx, and so on.)	Attachments.extension:docx
`Attachments.filename`	Text	Search by the file name of the attachment.	Attachments.filename:Report.PDF
`Attcount`	Integer	Search by the amount of attachments.	Attcount:6
`Attflag`	Boolean	Search by whether there is an attachment.	Attflag:true
`Atttext`	Text	Search the content of the attachments.	Atttext:Computers
`Atttypes`	Text	Search by the attachment type.	Atttypes:PDF
`Cc`	Text	Search by carbon copy recipients.	Cc:JoeBlogs@example.com
			Sender:*@example.com

SEARCH TERM	DATA TYPE	DESCRIPTION	EXAMPLE
`Classification.tags`	Text	Search by classification tags.	Classification.tags:PII
`Hidden`	Boolean	Search whether email is visible to end user or not.	Email Hidden\:
			Hidden:(1)
			Email Visible:
			NOT Hidden:(1)
`Inbound`	Boolean	Search inbound emails.	Inbound:false
`Ipheader`	IP Address	Search by the IP header of the email.	Specific IP Address\:
			Ipheader: (10.201.1.1)
			IP Address using wildcards:
			Ipheader:(10.*.1.1) AND Ipheader: (10.201.?.1)
`Maildate`	Date Time	Search by the date the message was sent.	Closed Range\:
			Maildate: [2018-01-01T00:00:00 TO
			2019-12-31T23:59:59]
			Open Range:

SEARCH TERM	DATA TYPE	DESCRIPTION	EXAMPLE
			Maildate: {2018-01-01T00:00:00 TO 2019-12-31T23:59:59}
`Messagesizeinkb`	Floating Point Number	Search by total size of the email.	Messagesizeinkb: \[2.5 TO 5\]
`Outbound`	Boolean	Search whether a user sent the email.	Outbound:true
`Sender`	Text	Search by the sender address(es).	Sender:JoeBlogs@example.com
			Sender:*@example.com
`Subject`	Text	Search by the subject of the email.	Subject:IT
`Textbody`	Text	Search the text content of the email.	Textbody: "Hello World!"
`To`	Text	Search by recipient.	To:JoeBlogs@example.com
			To:*@example.com

Examples of Query Searches:

- MailDate:
- Messagesizeinkb:
- Subject:(export OR report)
- MailDate: AND subject:archive
- Sender:(@*domain.com OR*@domain2.com OR*@domain3.com)
- Atttypes:(pdf OR docx) AND atttext:process
- Attachments.filename:(Report.PDF or Export.docx)

Searching the From, To, BCC and CC fields

The To, From, and From/To search options are available within an Advanced Search.

- The To option provides search results from the To, BCC, and CC fields.
- The From option provides search results from the From field.
- The From/To option provides search results from the From and To fields.

Searching within specific email domains

One way to search for items within a specific domain is to enter the domain name in the To field of an Advanced Search.

You can use wildcards to search for results from a group of similar domains. For example: `mycloud*` returns emails for the domains that begin with *mycloud*.

Methods for searching tables and reports

This section includes the following topics:

- About Quick Search and Criteria Search
- Searching tables, lists, and reports

About Quick Search and Criteria Search

The following search interfaces are provided for searching the lists or tables that Advanced eDiscovery displays, such as lists of user accounts, reviewers, cases, tags, or reports:

- Quick Search provides a search based on complete or partial words.
- Criteria Search. On some of the pages that provide Quick Search, an additional option named Criteria Search lets you search on specific table criteria.

  > “ ”

  Note: Quick Search and Criteria Search do not support phrase search, Boolean operators, proximity search, or wildcard search.

  > “ ”

Quick Search is available on the following Advanced eDiscovery pages. The pages that also have Criteria Search are indicated in brackets:

- Investigations tab:
  - Managed Accounts > Accounts (Criteria Search also available)
  - Tags and Holds > Holds
  - Tags and Holds > Tags
  - Tags and Holds > Retention
  - Batch Processes > Exports

E-Discovery tab:

- Administration > Reviewers (Criteria Search also available)
- Cases > Case List
- Cases > Status
- Cases > *Case Name* > Tags
- Cases > *Case Name* > Batch Processes > Exports
- Cases > *Case Name* > Case History (Criteria Search also available)

Alerts tab:

- Search Log
- Policy Alert (Criteria Search also available)

See Searching tables, lists, and reports.

Searching tables, lists, and reports

Quick Search provides a fast way to search tables and reports in Advanced eDiscovery. For some of the more complex tables and reports Criteria Search is also available. Criteria Search enables you to search within specific table columns.

> “ ”

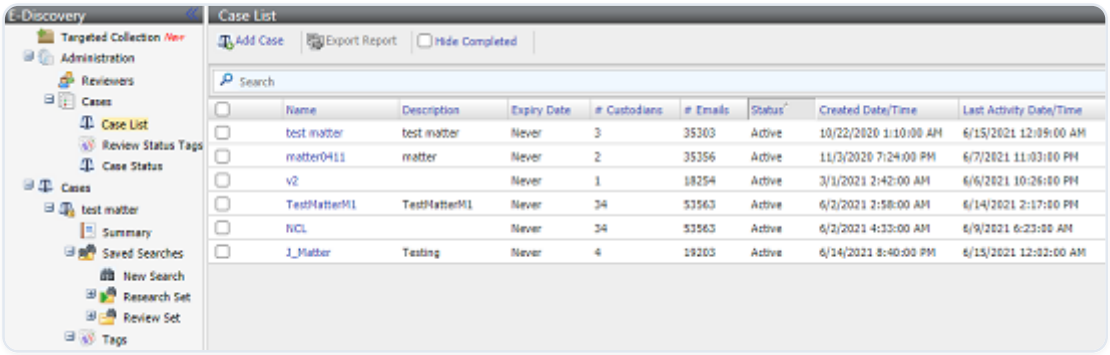
Note: Quick Search and Criteria Search do not support phrase search, Boolean operators, proximity search, or wildcard search. Searches are not case-sensitive.

> “ ”

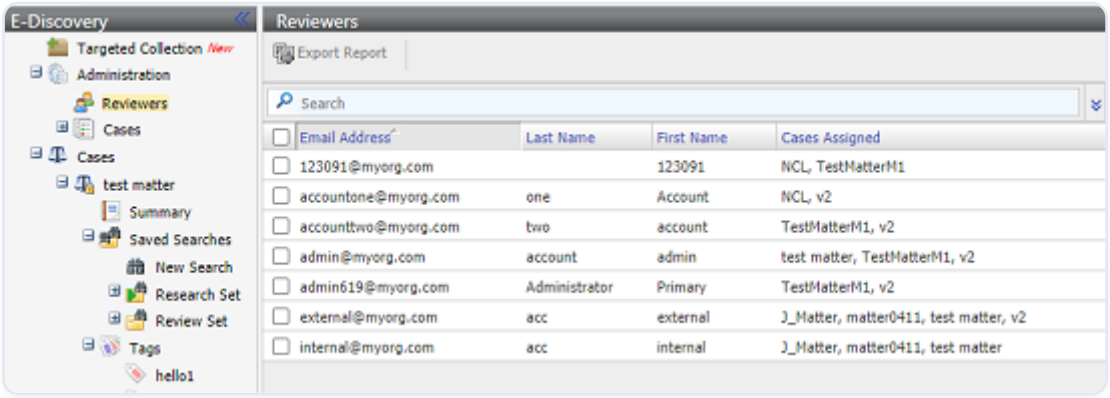
To search tables, lists, and reports

1. In Advanced eDiscovery browse to the page that contains the table, list or report that you want to search.

The following figure shows an example of the Quick Search interface, in this case in the Case List node on the E-Discovery tab:



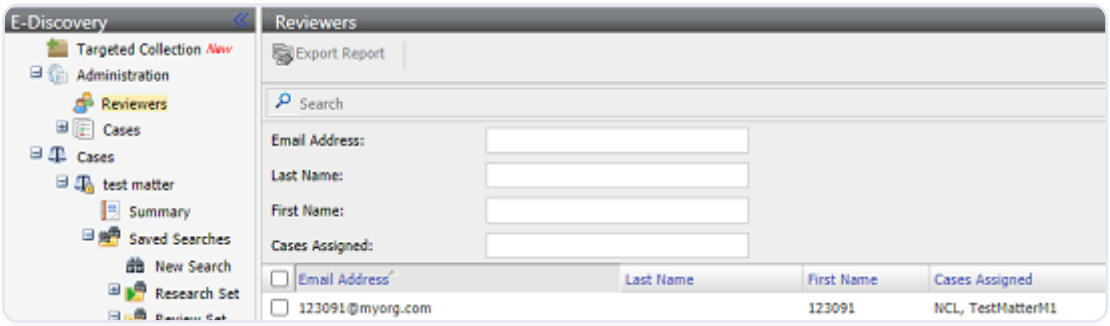
If a Criteria Search is available in addition to the Quick Search, an Expand icon is present at the end of Search box, as shown here on the Reviewers node:



1. To perform a Quick Search, enter a search term in the Search box. Note the following:
    - In most cases the search begins as soon as you enter the text.
    - The search is performed on the most significant column of the table, such as the email address, the case name, the user, the export name, the search criteria, or the after value.
    - Search terms can consist of complete or partial words. Quick Search does not support phrase search, Boolean operators, proximity search, or wildcard search.
    - Searches are not case-sensitive.
2. On pages that support Criteria Search you can perform a search on specific table criteria. Criteria Search is available on the following pages:
    - Investigations tab > Managed Accounts > Accounts
    - E-Discovery tab > Administration > Reviewers
    - E-Discovery tab > Cases > *Case Name* > Case History
    - Alerts tab > Policy Alert

To perform a Criteria Search, click the **Expand** icon at the end of the Quick Search box The Criteria Search options are displayed.

The following figure shows an example of the Criteria Search interface. The search fields vary, depending on the table or report.



Enter your search terms in one or more of the search boxes. Search terms can consist of complete and partial words. Searches are not case-sensitive. Phrase search, Boolean operators, proximity search, and wildcard search are not supported.

Advanced eDiscovery returns the search results as you enter the criteria. As you add more criteria the search is filtered on those criteria.

Advanced eDiscovery Frequently Asked Questions

This section includes the following topics:

- Frequently Asked Questions

Frequently Asked Questions

The following frequently asked questions provide more information about using Advanced eDiscovery.

- What browsers does Advanced eDiscovery support?

Advanced eDiscovery support is limited to the browsers that are listed in the Enterprise Vault.cloud Compatibility List.

See the Enterprise Vault.cloud Compatibility List.

- Can I use Advanced eDiscovery to access my archived messages in Enterprise Vault.cloud?

Yes, you can use Advanced eDiscovery to access your messages that are archived in Enterprise Vault.cloud. However, certain Personal.cloud features such as search filters and active folders are not available from Advanced eDiscovery.

- What happens to archived messages when my organization deletes a user account?

The archived messages of a deleted user remain in your organization's archive. The messages are also searchable by reviewers and administrators with the appropriate permissions.

- When are archived messages removed from my organization's archive permanently?

Archived messages are permanently removed in accordance with the retention polices in place for your organization.

- What happens to the messages that are sent to a disabled or deleted user account?

The messages that are sent to a disabled user account are excluded from archiving and do not appear in the archive of the disabled user or the Unassigned Legacy Account. The messages that are sent to a deleted user account appear in the Unassigned Legacy Account.

- Can disabled users access their archived messages in Enterprise Vault.cloud?

No, disabled users cannot access their archived messages in Enterprise Vault.cloud.

- What attachment types does Advanced eDiscovery support?

Advanced eDiscovery supports a wide range of attachment types:

See Searchable attachment types.

- Can I search for calendar items or contacts?

No, currently archive calendar items and contacts are not archived.

- What is the character limit of search strings?

You can enter up to 1000 characters in the search field of the Search box.

- Does capitalizing a word affect search results?

No, search terms are not case-sensitive.

- Are there "stop words" that are excluded from search?

Yes. In Advanced Search, common words or "stop words" are automatically dropped from searches.

See About stop words and special characters.

- How can I search for an exact phrase?

In Advanced Search, to search for an exact phrase place double quotation marks around the search term.

See Phrase searches.

- How can I search for two terms at once?

In Basic and Advanced Search enter an uppercase AND between two search terms to find emails containing both term. Use an uppercase OR between two search terms to find emails containing at least one of the terms.

See Boolean operator searches.

- Can I use Boolean Search Logic?

Yes, in Basic and Advanced Search you can use a combination of AND, OR, and NOT with your search terms to construct Boolean search criteria.

See Boolean operator searches.

- Can I conduct a wildcard search?

Yes, in Basic and Advanced Search you can use an asterisk or a question mark at the end of a word to conduct a wildcard search.

See Wildcard searches.

- Can I use the proximity of words as a search criteria?

Yes, in Basic and Advanced Search you can enter two search terms in quotation marks followed by a tilde and a numerical value to represent the word count proximity.

See Proximity searches.

- What is the maximum number of messages that I can export?

You can export up to 200,000 messages.

- Why is the export to NSF option unavailable in the Export Options?

The NSF export option is only available when a Domino server has been configured as the mail server type in the archive settings. Contact your Archive Administrator for more information.

Best practices, limitations, and known issues

This section includes the following topics:

- Best practices and limitations with Advanced eDiscovery
- Known issues with Advanced eDiscovery

Best practices and limitations with Advanced eDiscovery

General

- Although the users that are provisioned for archive access can view their messages from Advanced eDiscovery, we recommend that users work with their messages using Personal.cloud. Additional functionality such as search filters and active folders is provided when users work with archived messages in Personal.cloud.

Search

- Search times improve after a user performs their first search during each session because Advanced eDiscovery keeps the index in memory during each session.
- Inaccurate search results may be returned if the hyphen in a domain name is included because the hyphen is dropped.
- Use Advanced Search to cut down search results If you see a message stating that you have exceeded the number of search results that can be returned.
- Search terms are limited to 1,000 characters.
- Use Query Search to accurately find and to reduce search results.
- Searching with empty quotes or whitespace within quotes produces unexpected results.
- Searching with an empty field produces an error.
- Tags are only searchable on the Tags & Holds page, which is located within the Investigations tab.
- The search interface prevents the user from entering the following special characters: / \ # \< \>
- The maximum number of Boolean operands in a search is 249. Note that *roof rusted OR paint* has two Boolean operands: the OR, and the space between the first two terms. The space is treated as an AND operator.

Foreign language search constraints

- Unable to search for DBCS/hiascii char in the Quick Search field in Alerts.
- Unable to search for DBCS/hiascii char in Policy Names - Alerts.
- Unable to search for DBCs/hiascii char in Advanced/Query search - comments
- Unable to search for DBCs/hiascii char in Advanced/Query search - Alert Emails
- Search fails in Managed Account if last name includes non-ASCII characters
- Search fails in Reviewers Account if last name includes non-ASCII characters
- Corrupted DBCS/hiascii character results in Case Review Status Tag name and description
- Case Status has the hard-code issue risk

Known issues with Advanced eDiscovery

- Saved searches named using Japanese double-byte characters are not saved correctly and result in the search results not being displayed.
- Keywords within a message body may be highlighted inconsistently.
- You may receive a security error message when downloading data from Advanced eDiscovery.

Workaround - close the security error message window and retry the download.

- Bcc recipients are currently not searchable in Advanced eDiscovery.
- Due to limitations of Microsoft Exchange journaling, the Bcc recipients currently displayed depends on the version of Exchange the message sender and Bcc recipients use. Please refer to the following table for more information.

Table: Exchange versions displayed in Bcc field

SENDER EXCHANGE VERSION	EXCHANGE VERSIONS DISPLAYED IN BCC FIELD WHEN VIEWED FROM EXCHANGE 2010 ENVIRONMENT	EXCHANGE VERSIONS DISPLAYED IN BCC FIELD WHEN VIEWED FROM EXCHANGE 2007 ENVIRONMENT	EXCHANGE VERSIONS DISPLAYED IN BCC FIELD WHEN VIEWED FROM EXCHANGE 2003 (STANDARD) ENVIRONMENT	EXCHANGE VERSIONS DISPLAYED IN BCC FIELD WHEN VIEWED FROM EXCHANGE 2003 (ENVELOPE) ENVIRONMENT
Exchange 2010	All	Exchange 2007	None	None
Exchange 2007	Exchange 2010	All	None	Exchange 2003 (Envelope)
Exchange 2003 (Standard)	Exchange 2010	Exchange 2007	None	None
Exchange 2003 (Envelope)	Exchange 2010	Exchange 2007	None	All

Advanced eDiscovery updates in previous releases

This section includes the following topics:

- About the Advanced eDiscovery updates in previous releases

About the Advanced eDiscovery updates in previous releases

About the Advanced eDiscovery updates in previous releases

The following page describes the most recent updates for Advanced eDiscovery:

See Introducing Enterprise Vault Advanced eDiscovery.

For full details of all the updates in each release of the Enterprise Vault.cloud service suite, see the Enterprise Vault.cloud release notes. You can access the release notes from the following article on the Veritas Support website:

https://www.veritas.com/support/en_US/article.100040129