About Arctera eDiscovery

This section includes the following topics:

Arctera eDiscovery key features

Arctera eDiscovery includes the following features:

- **Advanced iterative search capabilities**

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

  Arctera eDiscovery provides a built-in collaborative workflow. Arctera 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.

- **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 Arctera eDiscovery. An authorized reviewer or administrator can name and password-protect their exports.

- **Hit-highlighting**

  When reviewing search results, you can quickly identify where your search terms or applied tags appear using hit highlighting. The Preview pane also provides navigation controls to move between each occurrence within the item. For more details, See About Hit Highlighting.

- **Reporting**

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

- **Print to PDF**

  Arctera eDiscovery offers the Print to PDF feature in both, the Investigations and the eDiscovery tab. You can print collaboration messages collected from the *MS Teams* collectors using the Print to PDF feature.

  This feature is -

  - exclusive to *MS Teams* collaboration messages and is not supported for messages collected from other archive collectors.
  - not available for *Production Sets*, as it is not applicable in that context.

- **InsightAI assistant**

  The InsightAI icon is visible only if this service is enabled for your account. Acting as your built-in AI assistant based on Open AI GPT-4.1 Nano model, it delivers faster, smarter, and more

reliable answers from both new and saved searches by generating context from emails, collaboration messages, and files. You can use the predefined prompts or enter your own prompt (query) to generate context.

- **Translation**

  The Translation feature enables eDiscovery reviewers to translate non-English content directly in the item preview without downloading the item or using an external translation tool. The feature is available on both the **Investigations** tab and the **eDiscovery** tab. For more information, see Translating email, collaboration message, and file content.

Arctera eDiscovery term definitions

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

Table: Arctera eDiscovery definitions

TERM	DESCRIPTION
Custodian	In the context of Arctera eDiscovery, a custodian is anyone for whom your organization holds or has held an archive account. When an eDiscovery 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.
Investigation	In the context of Arctera 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.

TERM	DESCRIPTION
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 Arctera eDiscovery an eDiscovery Administrator creates a case to act as a container in which to associate all the related emails, attachments, collaboration chats, and files for such a subject.
Tag	In Arctera eDiscovery a tag is a marker that can be applied to emails, attachments, collaboration chats, and files to help organize the process of investigation or review.
	- In the eDiscovery 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, collaboration messages, and files as you want, for example to retrieve identically tagged items easily at a later time. These tags are visible only to the user that applies them.
	- You can tag items with a managed tag, if you have any of these available to you. Managed tags are created in the Arctera Management Console, under the My Config > Managed Tags node.

Introducing Arctera eDiscovery

This guide describes Arctera eDiscovery and describes how to use all of its key features.

Arctera 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.

Arctera eDiscovery provides the tools to search your company's archived items (emails, collaboration messages, and files) to discover those that are pertinent to litigation cases or infringements of corporate policies and regulations. Arctera eDiscovery provides case management features for eDiscovery work, including the ability for multiple reviewers to collaborate during the eDiscovery process. Items that are found to be of interest can be exported for external review.

> **Note:** This updated edition of the *Arctera eDiscovery User Guide* incorporates information about the search feature that was previously included in the *Arctera eDiscovery Search Guide*.

> Recent updates to Arctera eDiscovery

Recent updates to Arctera eDiscovery include the following:

- Integration with Microsoft Teams, OneDrive for Business, and Enterprise Vault: The search criteria in Arctera eDiscovery now include options to search from emails, messages, and files that are archived from Microsoft Teams, OneDrive, and Enterprise Vault. See About Targeted Collections. and See Adding targeted collection for Microsoft Teams.
- Filtering items in searches based on sentiment score: The filter criteria in searches now include option to filter items based on their sentiment score.
- Collection Defensibility Report: The Targeted Collections page displays an expansion icon for the Enterprise Vault, Microsoft Exchange, and Microsoft Teams reactive collectors that are successfully archived. You can expand the row to view details like Items Collected, Items Received, Items Archived, Items Duplicate, Items Rejected, and Items Failed.

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

Getting started with Arctera eDiscovery

This section includes the following topics:

About the Arctera eDiscovery user interface

[] shows a typical view of the Arctera eDiscovery user interface that an eDiscovery Administrator can see. All the tabs, options, and icons are clearly arranged with the modern layouts to ensure user friendliness. For easy navigation throughout the application, panes can be hidden and displayed as required. The options are easily available to navigate to the Arctera Management Console, the Arctera Personal Archive, and the Arctera Surveillance portals.

> **Note:** The tabs, the nodes within each tab, and the features varies with the roles and privileges of your Arctera Unified Platform account.

> The selection tabs in the left navigation pane control access to the various functions and features of Arctera eDiscovery.

After logging in to Arctera eDiscovery, the landing page visible to you by default depends on your role in Arctera eDiscovery. The following table explains the role and the corresponding landing page.

ROLE	DEFAULT LANDING PAGE
Administrator	eDiscovery > Reviewers
External reviewer	eDiscovery > Cases

ROLE	DEFAULT LANDING PAGE
Internal reviewer (if managed accounts are assigned)	Investigations > Managed Accounts > Accounts
Internal reviewer (if managed accounts are assigned)	Investigations > My Mailbox > Mailbox

- See About the left navigation pane.
- See About the title bar options.
- See About the search bar.
- See About the bottom navigation bar.
- See About the Details pane.

About the left navigation pane

The navigation pane that appears on the left side of the page contains the Investigations and the eDiscovery tabs. You can easily switch between these tabs as required. The Toggle icon allows you to expand and collapse the left navigation pane for a better visibility of the content in the panes available in the right side of the page.

eDiscovery tab

The eDiscovery 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, an eDiscovery 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.

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

- The Dashboard node lets you view and export cases summary reports.
- The Reviewers node lets you view Mailbox and Case access detail of the reviewers. You can export the reviewers summary reports for later use.
- The Review Status node lets you define the review status tags and define the active and default tags.
- The Redaction Reasons node lets you add and delete the reasons that you can use during creating production sets.
- The Cases node lets you manage cases that are assigned to you. After you select the case, the separate case-specific node appears below the Cases node to perform various operations.

Investigations tab

The 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. External reviewers do not have access to the Investigations tab.

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

- The Targeted Collection node is used to create a targeted collection in Arctera eDiscovery console. These collections are the cloned data of an archive collector that is configured in the Archive Administrator console.
- 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 Arctera 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 Active Directory hoc investigations, outside of the legal discovery workflow.

See About Investigations.

- The Labels node is where you can create labels. The emails are classified and displayed based on the labels applied to them. You can click the label to view emails and collaboration messages to which that label is applied.

- The Legal Holds node is where you can view emails with a legal hold.
- The Tags node lets you view and manage the custom tags and the emails with those tags that have been applied in the Investigations tab.
- The Retention Tags node displays the emails to which retention tags are applied.
- The Exports node lets you view the status of email exports that you perform from the Investigations tab.
- The Search Log node is where you can see the Search-specific logs.
- The Continuity - Standby node 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.

About the bottom navigation bar

This bar displays total number of pages, total number of records on a page, and the navigation options that are supported for multi-page lists.

- Click on the page number to display and navigate to a selected page.
- Click the |< icon to go to the First page of the list.
- Click the >| icon to go to the Last page of the list.
- Click the < icon to go to the Previous page of the list.
- Click the > icon to go to the Next page of the list.

About the Details pane

This pane displays the records with subsequent details. You can click on the column headings to sort the data either in ascending or descending order for one or more columns on the selected page.

For a better readability purpose, this pane shows limited columns. To view the additional columns on the page, click the Columns icon as shown in the sample image below. Select the additional columns you want to see and click Apply.

> **Note:** The **Columns** functionality is available for all the searches in the **Investigation** and **eDiscovery** tabs. However, for Advanced ECA searches, this functionality is available for **Files** tab only, and not for **Emails** and **Collaboration** tabs.

About the search bar

Use the quick search to quickly find content on the page. You can also click the arrow in the search field, to search using the Criteria Search filter.

See About Quick Search and Criteria Search.

About the title bar options

The title bar contains the following icons:

- Keyboard: You can use this icon to access (navigate to) the Arctera Management Console, the Arctera Personal Archive portal, and the Arctera Surveillance portal.
    - The Arctera Management Console option provides administrators with access to the Arctera Management Console. The Arctera Management Console appears in a new web browser tab. It enables administrators to configure archive settings and to assign roles, including the roles that control the access to Arctera eDiscovery. Role assignment is only available to System Administrators or to Role Managers with the required permissions.
    - The Arctera Personal Archive option provides administrators with access to the Arctera Personal Archive console.
    - The Arctera Surveillance option provides administrators with access to the Arctera Surveillance console.

See About account roles and Arctera eDiscovery.

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

- Help: You can use this icon to access user help documentation of Arctera eDiscovery.
- User Profile: You can use this icon to view the alerts, statistics, time zone, and change password options. These options varies with your role. You can log off your on-going session by selecting the log off option.
    - The Alerts option 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.

- The Statistics option provides administrators with archive statistics. The statistics available from this tab include Number of active accounts, Top policy alerts trending, Number of emails

received, and Average mailbox size. This option is not available for a reviewer or account users.

- The Set Time Zone option allows reviewers and account users to select the appropriate time zone for them.
- The Log Off option lets you to log off securely from the current session of Arctera eDiscovery.

Accessing your own archived emails

Arctera 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 Arctera Personal Archive 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 Arctera eDiscovery and can only restore mails to the accounts which you monitor.

> **Note:** When you view your archived emails, certain Arctera Personal Archive features such as search filters and active folders are not available from Arctera 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.

Logging off from Arctera eDiscovery

To log off from Arctera eDiscovery:

1. On the Arctera eDiscovery user interface, in the upper right-hand corner, click the user profile icon.
2. Click **Log Off**.

Resetting a forgotten password

If you forget your password and need help resetting it, Arctera eDiscovery can help you by sending a Reset Password link to your authenticated user name (email address).

To reset your forgotten password:

1. On the authentication screen, click the Forgot your password link.
2. In the User Name field, provide your user name (email address).
3. In the Validation Code field, enter the correct captcha from the image, without spaces. Letters are not case-sensitive.

   You cannot sign in if your archive fails to authorize your location or computer. You can contact system administrator for assistance.
4. Click **Send**.

   The application sends you an email with a reset password link. Check your email inbox, including the spam or junk folder, for this message. This link expires after 30 minutes from you receive the email.
5. Open the password reset email and click on the provided **Reset Password** link.

   The application directs you to a **Reset Password** page.
6. Type your user name, a new password, retype to confirm it, and click Submit.

   After successful reset, you receive an email notification that your password has been changed successfully.

Signing in to Arctera eDiscovery

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

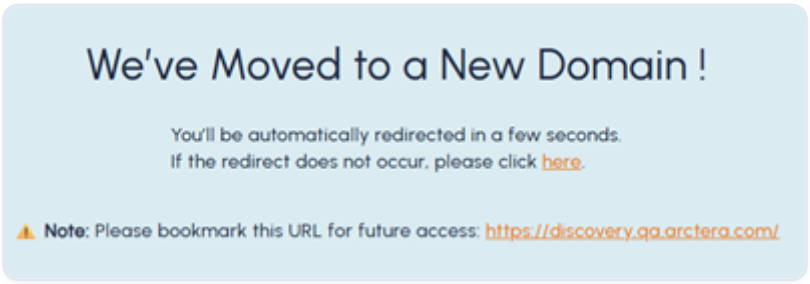
- Arctera eDiscovery users should exercise caution when accessing their accounts from public computers, to maintain the confidentiality of company emails. This note applies especially for administrators and reviewers.
- If your company signed up for Arctera eDiscovery and you have not received your credentials,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

To log on to Arctera eDiscovery:

1. Navigate to your Arctera eDiscovery URL.

Note

As of April 2026, the application is available at a new domain. If you access the application using a URL with the previous domain, an informational page appears.



The previously used URL is expected to automatically redirect you to the current application URL. If the automatic redirection does not occur, click the link provided on the page to continue. Do not bookmark the URL accessed through the *click here* link. To avoid future access issues, bookmark the new application URL provided in the note on the page.

Contact your administrator if you do not know your Arctera eDiscovery URL or you need access permission for Arctera eDiscovery. For more information on supported browsers, see Arctera Unified Platform Compatibility List.

1. Enter your username or DOMAIN\username 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.

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 three months, letting you bypass the logon screen after your initial successful logon.

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
	You can clear this setting by logging out of Arctera eDiscovery.

1. Click **Sign In**.
2. If the multi-factor authentication (MFA) is enabled for you, the **OTP** field appears on the authentication screen.

   This email-based authentication and the Time-based One Time Password (TOTP) authentication enhances the access and data security of Management Console. Administrators have the permission to enable or disable multi-factor authentication at the user and tenant level.

   - If the **email-based authentication** (EML) is enabled for you, a one-time password (OTP) is sent to your registered email address for authentication and access to the application. This OTP remains valid for 5 minutes from the time of receiving the email.

     Manually enter the OTP on the authentication screen within 5 minutes. Copy-pasting the OTP is not allowed. If you fail to provide OTP within 5 minutes of receiving it, the application displays a message that the OTP has expired. To obtain a new OTP, click **Resend OTP**. The application sends a new OTP.
   - If the **Time-based One Time Password authentication**(TOTP) is enabled for you, the application redirects you to an **Authenticator Setup** page as shown in the sample image below.

     Scan the QR Code using the Google or Microsoft **Authenticator** app on your mobile phone at the time of your first login

     Configure the Authenticator app on your mobile phone.

     Click **Continue** to get a time-based OTP in the Authenticator app.

     Enter that OTP in the **OTP** field of the Authentication page, and click **Continue**.

     Configuring the Authenticator app on your mobile phone

If you have previously created an account for same user, please remove that entry and attempt to complete the setup again.

To install the Microsoft Authenticator app on your phone:

a. While installing the app, if prompted, allow notifications about the app.
b. Upon installation, open the app and click the plus (+) icon at top and select **Work or School account** or **Other account**.
c. Add your work account by using any of the following methods:
    - Use the installed authenticator app to scan the QR Code provided on the authentication page of Arctera Unified Platform application.
    - Sign in with your application credentials and follow the screen instructions.

    Upon successful scanning or signing in, your account gets connected to Microsoft Authenticator.

To install the Google Authenticator app on your phone:

a. While installing the app, if prompted, allow notifications about the app.
b. Upon installation, log in with your Google account credentials. Scroll down and click the plus (+) icon.
c. Scan the QR Code with the Google Authenticator app. Your account gets connected to the Google Authenticator app.

Resetting the Authenticator device

If you accidently remove the account from authenticator app or misplace the device on which the app is installed, you can contact your administrator to request for resetting the Authenticator device for you.

About the New Features updates

Upon successful sign-in, the New Features window appears, presenting the latest release updates for Arctera Management Console, Arctera eDiscovery, Arctera Personal Archive, Arctera Capture, and Arctera Surveillance as shown in the sample image below.

- To temporarily hide this window, click Close.
- To access this window later, click the profile icon and choose Show New Features.

- To permanently hide this window, click Do Not Show Again. Subsequently, upon next login, this window will no longer appear. To enable its visibility, contact your system administrator. However, it will reappear automatically with the next release updates.
- To read the complete release notes document, click View Detailed Release Notes.

What's new in this release

Arctera constantly works on improving the Arctera Unified Platform product and introduces new features and enhancements release by release. For an easy-to-reference source for all the ways the product is changing, refer to the Arctera Unified Platform Documentation.

Arctera eDiscovery roles

This section includes the following topics:

Assigning account roles

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

Administrators can access the Arctera Management Console from the Administration option on the Profile icon in the top-right corner of the application page.

- See Assigning the Reviewer role to an account.
- See Assigning the Administrator role to an 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 Arctera eDiscovery, click the profile icon available in the top-right corner of the application page and select **Arctera Management Console**. The management console opens in a new browser window.
2. Log on to the Arctera Management 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.

7. If you want to assign **eDiscovery Administrator** privileges to the account, under **Built-in Roles** select the **eDiscovery Administrator** check box.
8. Click **Save** to save the role changes for the 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 Arctera eDiscovery, click the profile icon available in the top-right corner of the application page and select **Arctera Management Console**. The management console opens in a new browser window.
2. Log on to the Arctera Management 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.

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

About account roles and Arctera eDiscovery

Arctera Unified Platform 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 Arctera Management 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 Arctera eDiscovery.

Account role

Available Arctera eDiscovery tabs: Investigations in the left navigation pane and the Administration option on the Profile icon in the top-right corner of the application page (for setting personal preferences only).

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

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

> **Note:** In one case, those accounts with the Account role can have greater access in Arctera eDiscovery. Administrators can configure the account in Arctera Management Console 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 the eDiscovery tab in Arctera eDiscovery. Within thee Discovery tab the external reviewers can perform similar tasks as those accounts with the Reviewer role. Refer to the Arctera Management Console help for creating External Reviewer accounts.

Administrator role

Available Arctera eDiscovery tabs: Investigations, eDiscovery tabs in the left navigation pane, and the Alerts and Statistics option on the Profile icon in the top-right corner of the application page.

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

Administrator roles must be assigned the Monitor All Accounts privilege in the Arctera Management 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 the **Administrator** role can be assigned additional privileges in Archive Administration, including the privileges that can be conferred by built-in group roles. The accounts with the **Administrator** role that are also assigned the **eDiscovery Administrator** built-in role have full access to all the features of Arctera eDiscovery.

> The eDiscovery Administrators can configure and manage all aspects of Arctera 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 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.

Reviewer role

Available Arctera eDiscovery tabs: Investigations and eDiscovery in the left navigation pane, and the Administration option on the Profile icon in the top-right corner of the application page (for setting personal preferences only), and Alerts option on the Profile icon in the top-right corner of the application page.

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 Arctera Unified Platform, 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 eDiscovery tab, reviewers have access only to those cases that are assigned to them.

When the eDiscovery 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 on-going and standard 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 the **Reviewer** role only see the **eDiscovery** tab once they have been assigned as a reviewer to at least one case.

Managing investigations

This section includes the following topics:

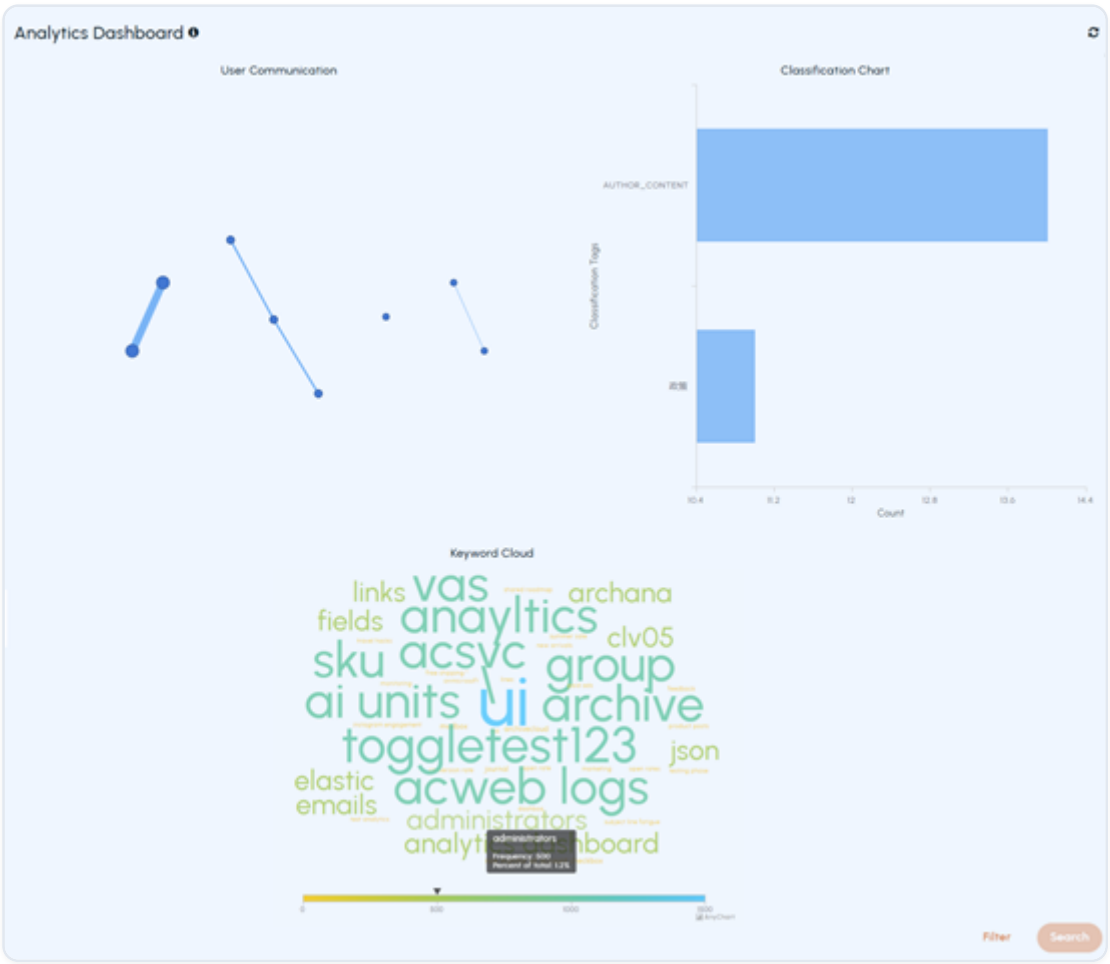
About Analytics Dashboard

Administrators can use the Analytics Dashboard to visualize the archived user communication data (emails only) of the top 50 users in the last 30 days. Analytics Dashboard displays this data in the form of charts for better visualization. Administrators can use this data to create searches for retrieving communication and classification information of a user. Based on the selected data, administrators can efficiently obtain more specific, limited, and accurate search results while investigation.

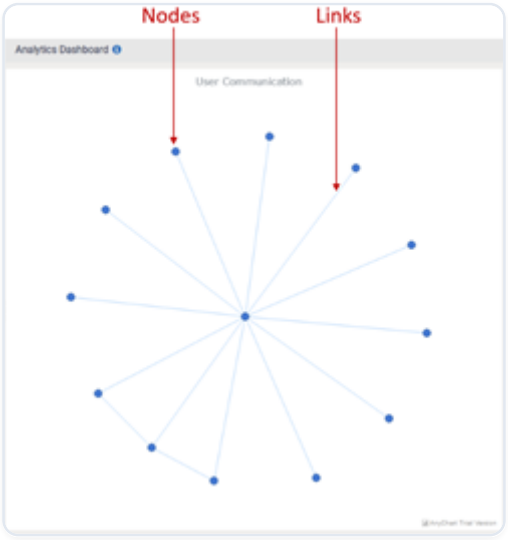
At present, the application provides you with the following charts:

- User communication chart
- Classification chart
- Keyword Cloud

The Analytics Dashboard is shown in the sample image below.



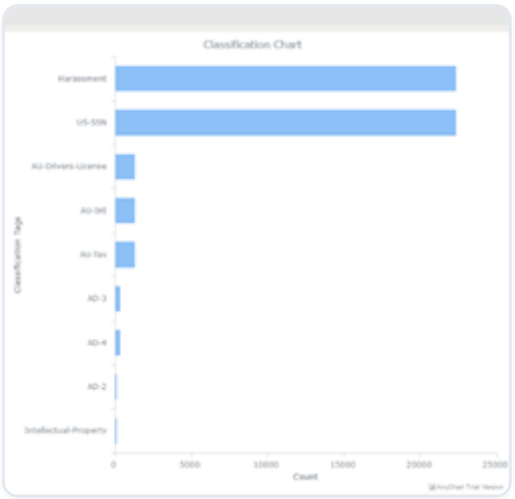
User Communication Chart



The chart has Nodes and Links connecting these nodes. Nodes in the chart represent users, and links represent the connections between or among these nodes. To select a node, click on the node. To select multiple nodes, press and hold the CTRL key on your keyboard, then click on the nodes you want to select. To enhance readability, you can drag any node away from crowded areas to separate it from neighboring nodes.

Hovering over nodes provides the user email address. Whereas hovering over links displays the user email addresses of individuals in communication.

Classification chart



This is a graphical representation of the user communication chart.

The charts are interconnected. Hence, selecting or filtering the data (nodes and links) in the *User Communication* chart leads to the automatic selection of corresponding data in the *Classification* chart and vice versa. You can only select one filter criteria at a time. If you wish to search communication data using a different filter, in such a scenario, click the Back icon, choose the desired link or node, and then click Search. Click the Refresh icon to refresh the monitoring data.

Keyword Cloud

The Keyword Cloud provides deeper communication insights, improving the accuracy and efficiency of investigations through interconnected dashboard views.

It displays the most exchanged keywords between users over the past 30 days to help identify key topics or emerging trends. It shows keyword frequency with trend lines, allows hover for details, and supports multi-select for focused searches across the dashboard.

Performing query searches using Analytics Dashboard

The Analytics Dashboard supports query searches only. Based on the data selected on charts, this query search provides you with the filtered archived review items.

To perform a query search using Analytics Dashboard:

1. On the **Investigation** tab, in the left navigation pane, select **Analytics Dashboard**.

   The application displays the *User Communication* and *Classification* charts for analysis of email communication of the top 50 users in the last 30 days.

2. On the **User Communication** chart, do the following:

   - Hover over nodes and links to view the user email addresses of individuals involved in communication.
   - Select the data in any chart, as convenient, for which you want further analysis.
     - If you want to select data from the *User Communication* chart, select nodes or links. To select a node, click on the node. To select multiple nodes, press and hold the CTRL key on your keyboard, then click on the nodes you want to select.

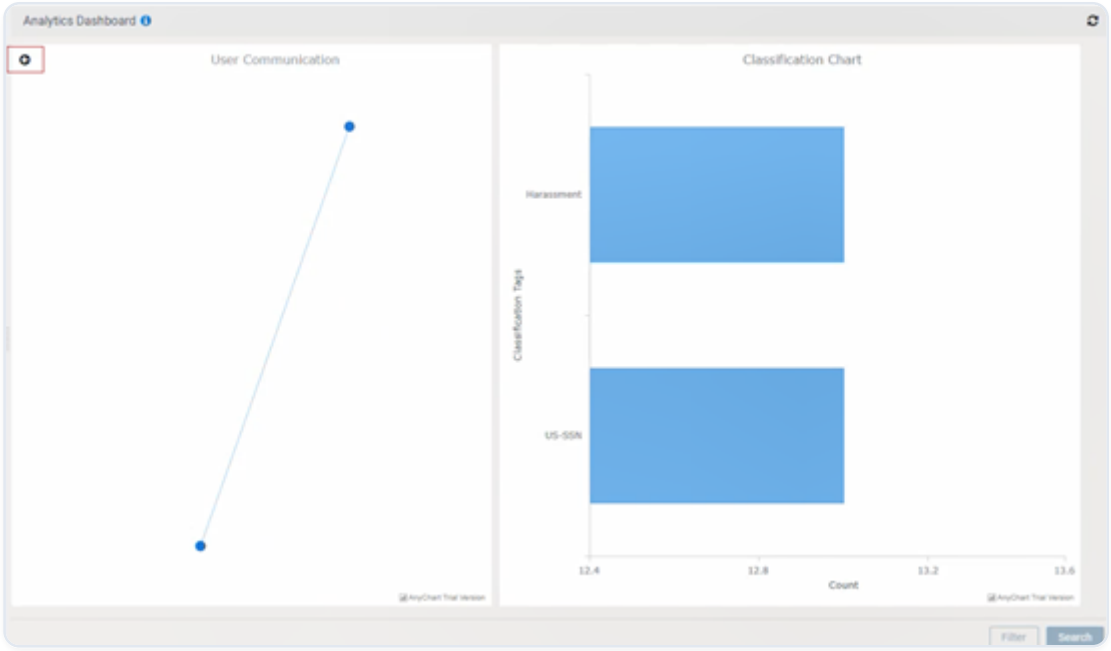
- If you want to select data from the *Classification* chart, select bars. To select a single bar, click on the bar. To select multiple bars, press and hold the CTRL key on your keyboard, then click on the bars you want to select.

As the charts are interconnected, selecting the data in the *User Communication* chart leads to the automatic selection of corresponding data in the *Classification* chart and vice versa.

- If required, click the **Refresh** icon to refresh the monitoring data.
- For better readability of charts:
  - You can select and drag the nodes away from crowded areas to separate them from neighboring nodes.
  - Keyboard and mouse users can use CTRL + Mouse wheel up/down to zoom in/out the chart view.
  - Touchpad users can use a two-finger pinch to zoom in or stretch out to zoom out the chart view.

3. In the bottom-right corner of the page, click **Filter**.

The application displays only the selected node or link and retrieves the communication threads among the individuals involved in the communication. In case there is no data for the selected node or link, the application prompts that the information is not available.



> **Note:** You can only select one filter criteria at a time. If you wish to search communication data using a different filter, in such a scenario, click the **Back** icon, choose the desired link or node.

4. Click **Search**.

   Before redirecting you to the search results, the application warns that your selected filter will be cleared if you click *Yes* on the confirmation message.

5. Click **Yes** on the confirmation message if you are sure with the data you have selected in the charts.

   Based on the data selected on charts, this query search provides you with the filtered archived review items.

About Labels

The eDiscovery 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.

Creating a label

To create a new label:

1. On the **Investigations** 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 items to which this tag is applied. If this tag is not applied, the number of items shown as zero.
Action	Click View Emails to view items with the corresponding label.

NAME	SPECIFY A UNIQUE NAME FOR THE LABEL.
Active	Select the Active check box for the label if you want to display this label while reviewers assign labels to items. Clear the check box for any labels that you want to hide.

4. Click **Save Label**.

About legal holds

This section describes the tasks that a user can perform with the legal holds.

Viewing legally hold items

While you tag the items, collaboration messages, and files, you can apply legal hold on the selected items. You can view those items under the Legal holds node.

To view legally hold items:

1. In the **Investigation** tab, select **Legal Holds**.
2. Select the tag name.

   In the details pane, the application displays the items that are tagged and marked as legal hold.
3. Select one item at a time to preview its details in the preview pane.
4. Click the Native View icon to view the item in the original format.
5. To download the item, click the **Download** icon.

Viewing the Legal Hold status of items

The Legal Hold icon reveals whether the searched emails, collaboration messages, and files are on legal hold and the reason for the hold. The application does not display this icon for items that are not on legal hold.

For a better understanding of the Legal Hold concept, let's explore the following terminologies:

- Tag Legal Hold: Legal hold is applied to the item by using a legal hold tag from the Investigations tab.
- Case Legal Hold: Legal hold is applied to the item inside a case by using one or more options below:

- An individual item is marked as Legal Hold inside a case.
- The Review set in which the item exists is marked as legal hold.
- The entire case in which any of the items custodian is present as case custodian is placed on legal hold.

> **Note:** For better application performance, it is recommended to deselect the **Legal Hold** column if it is no longer needed.

To view the Legal Hold status of items:

1. On the **Investigations** or **eDiscovery** tab, navigate to the appropriate Search from the required node, and select the **Email**,**Collaboration**, or **Files** tab.

   The searched items are displayed in the items grid.
2. Ensure that the **Legal Hold** column is displayed on the items grid.
3. If this column is not displayed, click the **Columns** icon.

   Select the **Legal Hold** check box and click **Apply**.

   The application displays the column as shown in the sample images below.
4. Hover over the icons to view tooltip that indicate the reason items are on legal hold as shown in the sample images below.

   In the **Investigation** tab, the legal hold icons and tooltip have the following meanings:

ICON	TOOLTIP	MEANING
	Tag Legal Hold	Legal hold applied by the current user using a tag. There might be additional legal holds on the same item, such as tag legal hold by another user or a legal hold inside a case.
	Tag Legal Hold	Legal hold applied by other users using a legal hold tag. additionally, the same item can also be on legal hold inside cases.

ICON	TOOLTIP	MEANING
	Case Legal Hold	Legal hold is applied only inside cases by any user and not by using a legal hold tag.

In the **eDiscovery** tab, the legal hold icons and tooltip have the following meanings:

ICON	TOOLTIP	MEANING
	Case Legal Hold	Legal hold applied inside the selected case. There might be additional legal holds on the same item, such as legal holds inside other cases or by using a legal hold tag from the Investigations tab.
	Case Legal Hold	Legal hold applied on the item, not in the current case but inside other cases. There might be additional legal holds applied on the same item using legal hold tags from the Investigations tab.
	Tag Legal Hold	The item is not on legal hold inside any case, but it is applied with legal hold tags by any user.

About Mail Reassignment

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.

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 Arctera Management Console. You must have an administrator role to access the reports section.

Refer to the Creating a Mail Reassignment status report section in the Management Console Help.

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, on-going and standard searches, holds, 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

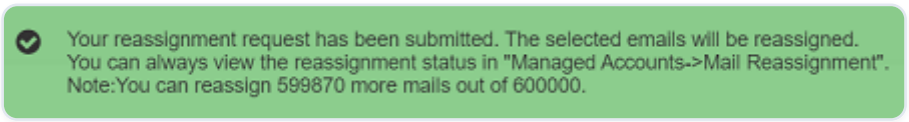
the daily limit is 4500 per day per customer. When customers submit a batch for reassignment, customers can view a temporary notification (that fades out automatically) about their available reassignment limit. Alternatively, customers can check their mail reassignment limits on the Mail Reassignment 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**>**On-going Searches**.
    - Go to **Managed Accounts**>**Standard Searches**.
    - Go to **Holds**.
    - Go to **Tags**.
2. Search for and select emails from the required unassigned legacy account, on-going and standard searches, hold, and the tags.
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. Click **Reassign Mails**, and do the following:
    - To reassign selected emails, click **Reassign selected emails**.
    - To reassign emails displayed on one page, click **Reassign emails in current page**.

    The application displays the sample message as follows:



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 the **Cancel** option remains enabled. You can click the **Cancel** option to abort the reassignment activity. If the batch status is either Completed or Failed, then the **Cancel** option remains disabled. You cannot click the **Cancel** option to abort the reassignment activity.

Viewing mail reassignment notifications and status reports

After performing the mail reassignment, the application notifies the user (who initiated the reassignment task) about the status of the mail reassignment task and the errors that occurred during reassignment. Email notifications are sent only for the batches that are completed.

To view a notification:

1. On the **Investigations** tab, select **My Mailbox**>**Mailbox**.
2. Click **Inbox** to view the list of emails regarding mail reassignment batch statuses.
3. Search for and select the emails for which you want to see the mail reassignment statuses.

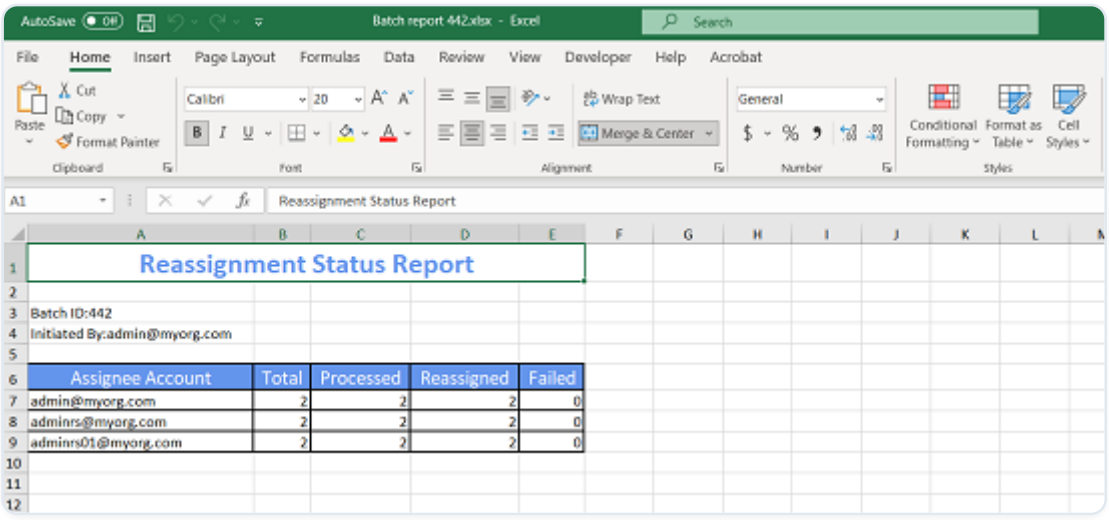
   > **Note:** Perform advanced search or query search to get the expected items. See Performing Advanced Search and Query Search.

4. Click the email to view details in the preview pane in the right side of the page.

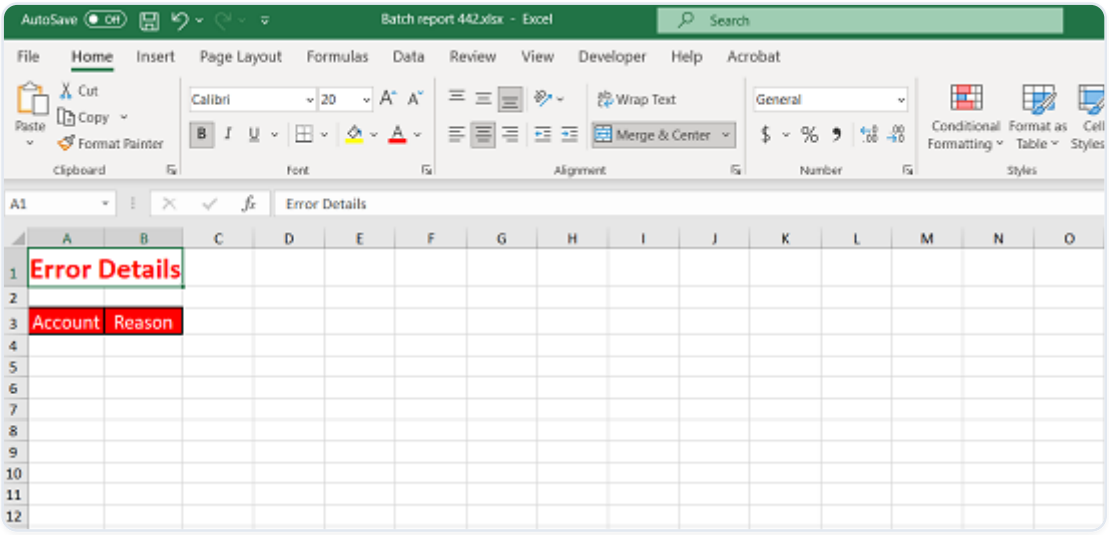
   - The **Subject** of the notification email shows the status of mail reassignment batch.
   - The **Attachment** shows the link to download the batch status summary report. The report is in the Microsoft Excel format and includes the***Status Report*** and the***Error Report*** sheets.

5. Click the link to download the report on your local computer.

   A sample **Status Report** sheet is shown as:



   A sample **Error Report** sheet is shown as below. It provides the reason of the failure or error occurred during email reassignment.



About search log

The search log provides you with the records of searches conducted in the Investigation and eDiscovery tabs, for auditing purpose. However, searches made under the Advanced ECA node in the Investigation tab and the Review Sets node in the eDiscovery tab are excluded from the log. It covers details of searches for emails, collaboration messages, and files, with separate logs for each search type.

The Advanced Search functionality of the Search Log node enables you to filter the record based on simple keyword values, user, or time period, enabling you to view specific records as needed. You can export search log records for a maximum duration of one year from the current date.

Viewing and exporting search log report

To view and export search log report:

1. On the **Investigations** tab, select **Search Log**.

   The application displays the record of all the searches, except for the searches performed under the **Advanced ECA** node in the Investigation tab and the **Review Sets** node in the eDiscovery tab.

2. To filter the appropriate records from the entire log, expand the **Advanced Search** pane (if it is not expanded already), and do the following:

SEARCH CRITERIA	TYPE THE SPECIFIC KEYWORDS TO BE QUERIED.
User	Select all users or the required user.
Search Date	Select the duration of the report from the available options.
	Note: The application allows exporting records of maximum one year. The **Export Report** option enables only if the selected data is within one year.

3. Ensure that the filtered result is as expected.
4. Click **Export Report**.

   The report is downloaded to your local downloads folder for further analysis.

About Searches in investigation

This section describes the tasks related to searches during investigation.

Updating on-going and standard searches

You can update the on-going and the standard searches from the Mailbox and the Managed Accounts nodes.

Updating an on-going or a standard search from Managed Accounts

You can update the on-going and the standard searches to change the search name, to specify the new tag name, and to apply a legal hold on a searches. While updating the searches from the Managed Accounts node, you can send the on-going and the standard searches to the cases available in the eDiscovery tab.

To update an on-going or a standard search from Managed Accounts:

1. On the **Investigations** tab, select **Managed Accounts**.
2. Expand the **On-going Searches** node or the **Standard Searches** node, as required.
3. **To update the on-going search**, select an on-going search, and click **Update Search**.

   Update the following information in the **Update Search** dialog box as required.

ENTER SAVED SEARCH NAME	CHANGE THE NAME FOR THE ON-GOING SEARCH IF REQUIRED.
Tag Name	You can modify the option only if the On-going check box is selected.
	Specify a new tag name. By default Arctera eDiscovery uses the saved search name.
On-going	Ensure that this check box is selected so that you can view this search under the on-going search list.
	For an on-going search, new items that meet the search criteria continue to be added after the search is created.
Legal hold	This option is available only if the On-going check box is selected.
	Select to place all items in this on-going search on legal hold. Emails on legal hold are not deleted from the archive.
Save as new	Click Save as new to save the selected on-going search as a new search. The original saved search remains unchanged.

ENTER SAVED SEARCH NAME	CHANGE THE NAME FOR THE ON-GOING SEARCH IF REQUIRED.
Send to Case	You have an option to select this check box. In case the Search is an on-going search, then the Keep copy in investigation check box is selected, but displayed as 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 eDiscovery tab. This preserves chain of custody by recreating the search in eDiscovery. The case gets moved to the eDiscovery > Research Set.
	Note: For AI-enabled cases, Send to Case supports only email items, and any non-email items (such as files and collaboration messages) are automatically skipped.

1. **To update the standard search**, select a standard search, and click **Update Search**.

   Update the following information in the **Update Search** dialog box as required.

ENTER SAVED SEARCH NAME	CHANGE THE NAME FOR THE STANDARD SEARCH IF REQUIRED.
Tag Name	You cannot change the Tag Name while updating the standard search. You can modify the option only if the On-going check box is selected. If you select the On-going check box, this standard search will be saved as the On-going search.
On-going	Select this option if you want to save the selected standard search as the on-going search. In this case, you can update the tag name and apply a legal hold to the items within the search.
	After you select this check box, the Advanced ECA option gets disabled.

ENTER SAVED SEARCH NAME	CHANGE THE NAME FOR THE STANDARD SEARCH IF REQUIRED.
Legal hold	You cannot change this option while updating the standard search. You can modify this option only if the On-going check box is selected.
Advanced ECA	Select this option if you want to move (save) the selected standard search under the Advanced ECA node.
	After you select this check box, the On-going and the Legal Hold options get disabled.
Send to Case	Select this check box if you want to send the selected standard search to the required cases on the eDiscovery tab.
	Select the case from the Cases drop-down. This check box allows you to send the selected search, along with keeping a copy in investigation, to the eDiscovery tab. This preserves chain of custody by recreating the search in eDiscovery. The case gets moved to the eDiscovery > Research Set.
	Note: For AI-enabled cases, Send to Case supports only email items, and any non-email items (such as files and collaboration messages) are automatically skipped.
Save as new	You cannot save the existing standard searches as a new standard search. This option remains disabled in case of updating the standard searches.

1. Click **Update** to save this updated search.

Updating on-going and standard searches from Mailbox

You can update the on-going and the standard searches to change the search name, to specify the new tag name, and to apply a legal hold on a searches. While updating the searches from the My

Mailbox node, you cannot send the on-going and the standard searches to the cases available in the eDiscovery tab.

To update an on-going or a standard search from your mailbox:

1. On the **Investigations** tab, select **My Mailbox**>**On-going Searches** or **Standard Searches** as required.
2. **To update the on-going search**, select an on-going search, and click **Update Search**.

   Update the following information in the **Update Search** dialog box as required.

ENTER SAVED SEARCH NAME	CHANGE THE NAME FOR THE SAVED SEARCH IF REQUIRED.
Tag Name	You can modify the option only if the On-going check box is selected.
	Specify a new tag name. By default Arctera eDiscovery uses the saved search name.
On-going	Ensure that this check box is selected so that you can view this search under the on-going search list.
	For an on-going search, new items that meet the search criteria continue to be added after the search is created.
Legal hold	This option is available only if the On-going check box is selected.
	Select to place all items in this on-going search on legal hold. Emails on legal hold are not deleted from the archive.
Save as new	Click Save as new to save the selected on-going search as a new search. The original saved search remains unchanged.

1. **To update the standard search**, select a standard search, and click **Update Search**.

   Update the following information in the **Update Search** dialog box as required.

ENTER SAVED SEARCH NAME	CHANGE THE NAME FOR THE STANDARD SEARCH IF REQUIRED.
Tag Name	You cannot change the Tag Name while updating the standard search. You can modify the option only if the On-going check box is selected.
On-going	Ensure that this check box is not selected. You can select this check box only if you want to save this search as an on-going search.
Legal hold	You cannot change this option while updating the standard search. You can modify this option only if the On-going check box is selected.
Save as new	You cannot save the existing standard searches as a new standard search. This option remains disabled in case of updating the standard searches.

1. Click **Update** to save this updated search.
    - When the **On-going** check box is selected, the search is saved under the **On-going Searches** node.
    - Otherwise the search is saved under the **Standard Searches** node.

Creating a new search

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

To create a new search:

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

- To search a single managed account, select **Managed Accounts > Accounts**, and click the required account. The **Search** pane appears.

2. To perform advanced search, specify the following inputs in the **Advanced Search** tab.

OPTION	DESCRIPTION
Custodians	• Select All to search archives of all of the custodians that are associated with the case.• Select Custom to search archives of the particular custodians. 1. The Manage button appears. Click Manage to open the Add/Remove Custodians. 2. Expand Selected Custodians to view the custodians selected for this search. 3. Expand Manage Custodians and select the custodians required for this search. 4. (Optional) Select Search Between Custodians at the bottom of the pop-up to retrieve emails exchanged exclusively among the selected custodians. For details, See Searching emails exchanged among specific custodians. 5. Click Update to add these selected custodians as a search input. These custodians are listed under the Selected Custodians section.
Custom Headers	**Note:** The **Custom Headers** option does not appear if there is no entry for a custom header for a particular group or tenant in database. Custom header does not work independently. You need to use the filter criteria to search the required items.Expand Custom Headers and set the header operator values.• Click + to add new search clauses.• Click - to remove search clauses that are not required.• In the first column, select the required header you want to search for. Based on the data type you have selected, the operator changes. For example, if you have selected the receiver date in header, the operator values can be Between, Before inclusive and After

OPTION	DESCRIPTION
	inclusive. For a numeric or integer header value, the operator values can be Is equal to, Less than, and Greater than. If you have selected a string value in header, then the operator will be Contains.• In the second column, select the available operator.• In the third column, specify the text, phrase, or date that you want to search for.
Filters	Expand Filters and set the filter operator values. The operators are explained in a table below.• 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.

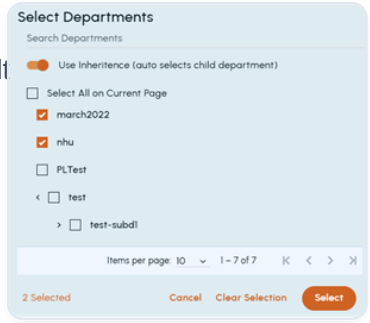
The **Filter** operators are listed below:

DROP-DOWN	DROP-DOWN	DROP-DOWN
Message	Entire Message	Contains / Doesn't Contain
	Subject + Body	Contains / Doesn't Contain
	Subject	Contains / Doesn't Contain
	Body	Contains / Doesn't Contain
	Inbound Message (AND)	Yes / No**Note:** The inbound message direction is decided differently based on the custodian selection:- Upon selecting all custodians, the message

DROP-DOWN	DROP-DOWN	DROP-DOWN
		direction is determined at the message level. Such message is treated as message-level inbound when it is sent to an internal domain from an external domain, independent of who the custodian is.- Upon selecting specific custodians, the message direction is determined at the custodian level. Such message is treated as custodian-level inbound when it is sent by the selected custodian, regardless of whether the recipient is internal or external.
	Outbound Message (AND)	Yes / No**Note:** The outbound message direction is decided differently based on the custodian selection:- Upon selecting all custodians, the message direction is determined at the message level. Such message is treated as message-level outbound when it is sent from an internal domain to an external domain, independent of who the custodian is.- Upon selecting specific custodians, the message direction is determined at the custodian level. Such message is treated as custodian-level outbound

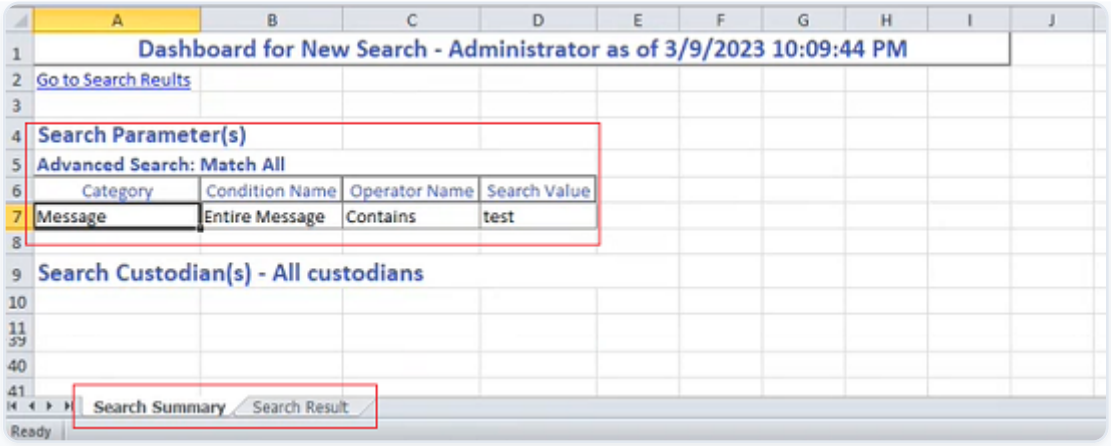
DROP-DOWN	DROP-DOWN	DROP-DOWN
		when it is sent by the selected custodian, regardless of whether the recipient is internal or external.
	Internal Message (AND)	Yes / No**Note:**- In Advanced Search, this option filters and retrieves only internal messages exchanged within the same organization.- In Query Search, use: `Internal:(3)` to include or `NOT Internal:(3)` to exclude
Date Sent/Modified(AND)	Subject + Body	Contains / Doesn't Contain
	Is Hidden	Yes / No
	IP Header	Contains / Doesn't Contain
	Is Equal To	Select a date
	Before	Select a date
	After	Select a date
	Within range	Select a date range
Participants	All Senders and Recipients	Contains / Doesn't Contain
	Senders Only	Contains / Doesn't Contain
	Recipients Only	Contains / Doesn't Contain
	To/Cc	Contains / Doesn't Contain
	To	Contains / Doesn't Contain
	Bcc	Contains / Doesn't Contain

DROP-DOWN	DROP-DOWN	DROP-DOWN
ClassificationNote: This option is available if the Arctera Classification service is enabled for a user.	Classified as	Contains / Doesn't ContainSelect 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 Arctera Unified Platform.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.
	Sentiment Score	Is Equal To / Below (Inc.) / Above (Inc.)
Attachment	Has Attachment	Yes / No
	File/Attachment Name	Contains / Doesn't Contain
	File Attachment Type	Contains / Doesn't ContainSee Searchable attachment types
Archive Date Filter archived data based on the date when emails, collaboration items, or files were archived.	Is Equal To: Finds items archived on a specific date.Before: Finds items archived before a certain date.After: Finds items archived after a certain date.Within Range: Finds items archived between two chosen dates.	Select date.Note: Use this filter only for the data archived after January 2021. Data before January 2021 will not appear in filtered results.Tip: If you want to use Query Search instead of Advanced Search, use the Archive Date:term and then build the search criteria.
Source Type	Is: Filters results that match the selected source type(s)Is Not: Excludes	Select one or more sources as needed.

DROP-DOWN	DROP-DOWN	DROP-DOWN
	results that match the selected source type(s).	
DepartmentNote: This option is available if the Arctera Surveillance service is enabled for a user.	All Senders & Recipients: Filters data where both the sender and recipient belong to the selected department(s).Senders Only: Filters data where only the sender belongs to the selected department(s).RecipientsOnly:Filt data where only the recipient belongs to the selected department(s).	Select Any or All operator and then click Select Department. A dialog box opens where you can choose one or more departments to apply as a filter.  Select Any or All operator and then click Select Department.1. Use the Search Departments field to quickly locate a department by name.2. Toggle the Use Inheritance to include child departments of a selected parent department.3. Click Select All on Current Page to select every department visible on the current page. Else, select the required departments individually. The count of selected departments appears in the bottom of the dialog box.4. Click Select to confirm and apply them as a filter.If you want to reset your choices, click Clear Selection. If you want to close the dialog without saving changes, click Cancel.

Note:

- In Advanced Search, the search text input functionality is updated. In previous releases, when users were providing multiple text input with space, the default logical operator "AND" was getting applied. From now onwards, the default logical operator "OR" is getting applied to get user records. This operator change from "AND" to "OR" is applied to all kind of searches. If users have previously used spaces while providing the search text inputs, their saved records (saved searches/standard searches/Ongoing searches) will be impacted as the operator is changed from "AND" to "OR".
- Based on the selected attributes, when you export the search report, the **Search Summary** and **Search Report** is generated as shown in the sample image below.



3. To perform query search, specify the following inputs in the **Query Search** tab.

Note: Use the scroll bar to view the lengthy queries.

OPTION	DESCRIPTION
Custodians	- Select All to search archives of all of the custodians that are associated with the case.- Select Custom to search archives of the particular custodians.1. The Manage button appears. Click Manage to open the Add/Remove Custodians.2. Expand Selected Custodians to view the

OPTION	DESCRIPTION
	custodians selected for this search.3. Expand Manage Custodians and select the custodians required for this search.4. (Optional) Select Search Between Custodians at the bottom of the pop-up to retrieve emails exchanged exclusively among the selected custodians. For details, See Searching emails exchanged among specific custodians.5. Click Update to add these selected custodians as a search input. These custodians are listed under the Selected Custodians section.
Query Search	Specify the search query by providing keywords.

Guidelines for specifying queries

The application supports query searches only if the following necessary conditions are followed. Else, the application displays corresponding errors.

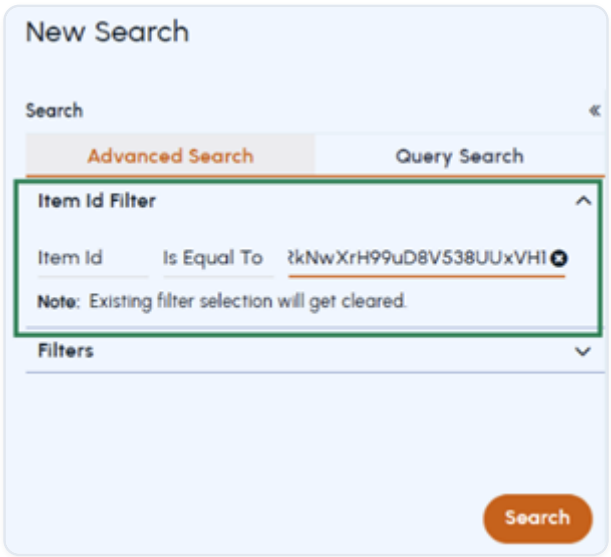
CONDITIONS		EXAMPLES
Operator-specific conditions	The search criteria must be used after the operator and before the query text.	**Correct**subject:hi OR attachments:test**Incorrect**subject:hi OR test
	The AND/OR/NOT operators must be written in capital letters.	**Correct**subject:text1 AND textbody:text2 OR attflag:true**Incorrect**subject:text1 and textbody:text2 or attflag:true
	The AND/OR logical operator is missing.	**Correct**EntireMessage:test AND NOT Entiremessage:hi**Incorrect**EntireMessage:te NOT Entiremessage:hi

CONDITIONS		EXAMPLES
Spaces-specific conditions	The extra space(s) between operators is not allowed.	**Correct**(NOT subject: test AND NOT textbody:test)
-	The space after bracket is not allowed.	**Correct**(NOT subject: text1)**Incorrect**(NOTsubject: text1)
-	The space before colon is not allowed.	**Correct**(NOT subject: test AND NOT textbody:test)**Incorrect**(NOT subject: test AND NOT textbody:test)

1. To search for the Arctera Surveillance item using the Item ID Filter, perform the following steps:

> **Note:** If you have a Arctera Surveillance subscription and the **Show Item ID Filter** feature is enabled in the Management Console, you can view the Id icon in the email preview pane as shown in the sample image below:

> Click the **Id** icon to copy the encrypted Item ID, then select **Advanced Filter**, expand **Item ID Filter**, choose **Is Equal To**, and paste the Item ID into the field as shown in the sample image below.



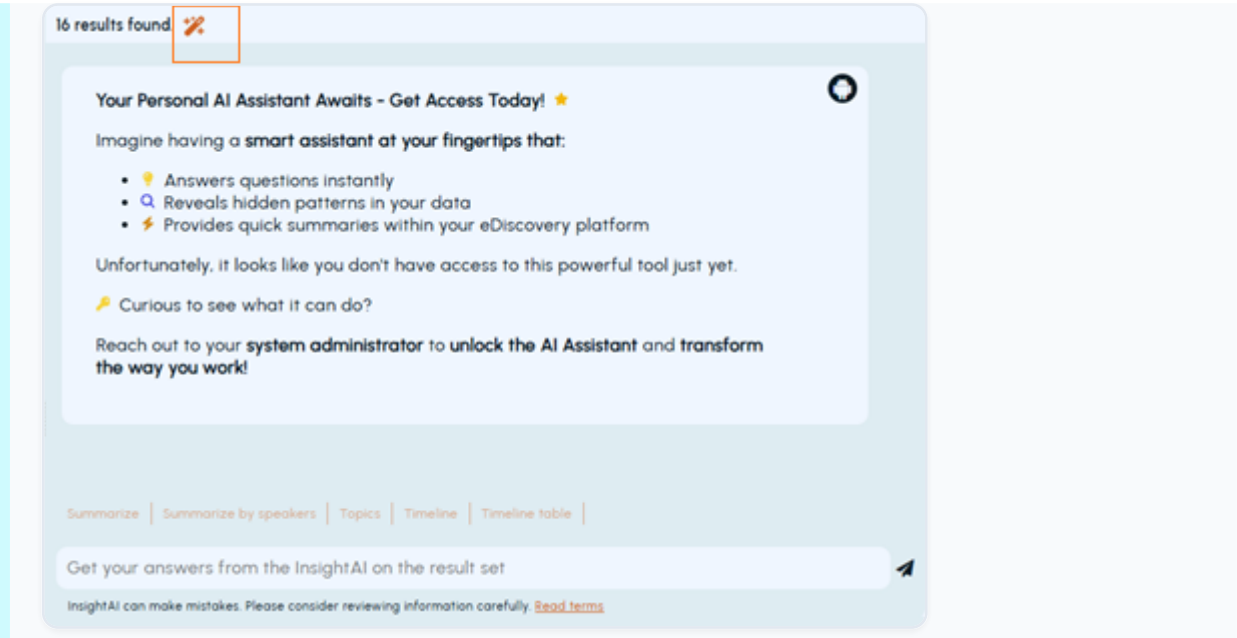
> **Note:** When the **Item ID Filter** is selected, all other filters are cleared to return the exact matching item

2. Click **Search**.
3. (Optional) To create a context of this search, click the **InsightAI** icon as shown in the sample image below.

   The **InsightAI** icon is visible only if this service is enabled for your account. Acting as your built-in AI assistant based on Open AI GPT-4.1 Nano model, it delivers faster, smarter, and more reliable answers from both new and saved searches by generating context from emails, collaboration messages, and files.

   You can use the predefined prompts or enter your own prompt (query) to generate context.

   > **Note:** For any support about this service, contact your system administrator.



4. Click **Save Search**.

   See Saving searches in Review sets and Research sets.

Deleting searches

You can delete a single search at a time.

To delete a saved search (Investigations tab):

1. On the **Investigations** tab, do any of the following:

- Expand **My Mailbox** to select search from the **On-going searches** or the **Standard searches** node.
- Expand **Managed Accounts** to select search from the **On-going searches**,**Standard searches**, or the **Advanced ECA** node.

2. Search for and select the Search you want to delete.

   The right-hand pane displays emails, collaboration messages, and files included in the search result.

3. Click **Delete Saved Search**.

   The application prompts you to confirm that you want to perform the operation.

4. Click **Yes** to complete the operation or click **No** to cancel it.

Exporting a summary report of searched items

In Investigations, any user who has access to searches can export the printable reports of emails. You can export all emails and a searched emails summary as a zip file for further use.

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

To export a report of searched items:

1. In the **Investigations** pane, expand **My Mailbox** or **Managed Accounts**.
2. Search for and select any new search, on-going search, or standard search for which you want to export a report.

   > **Note:** In the **Advanced Search** tab, 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. Select **Match All** to find records that meet all specified criteria. Select **Match Any** to find at least one specified criterion.

3. To export emails, click Export, and then do any of the following:

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

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

4. To export the searched email summary, click the **More Options** icon, and select **Export Report**.

   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.

Saving searches as on-going and standard searches

If you have the required permissions you can save an Advanced Search or a Query Search. The roles that can create the on-going and the standard 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 items that meet the search criteria continue to be added after the search is created.

To save a search as on-going or standard search:

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

   See Creating a new search.

2. Click **Save Search**.
3. 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, Arctera eDiscovery saves the search as a Standard Search.
	After you select the On-going check box, the application disables the Advanced ECA check box.
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 items. By default Arctera 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.
	Select to place all item 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 eDiscovery tab. This preserves chain of custody by recreating the search in eDiscovery. The case gets moved to the eDiscovery > Research Set.

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.
	Note: For AI-enabled cases,**Send to Case** supports only email items, and any non-email items (such as files and collaboration messages) are automatically skipped.

4. Click **OK** to save the search as follows:

   - If you have 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 eDiscovery > Research Set. A copy is created in the On-going/Standard searches, if the **Keep copy in investigation** check box is selected or not.

Searching emails exchanged among specific custodians

While performing a new search, the Search Between Custodians option allows you to retrieve the emails that are exchanged exclusively among selected custodians. Any additional internal or external participants are excluded.

> **Note:** This feature is disabled by default. To enable it, request your system administrator to contact Arctera Support.

> Before you use this feature, you must be familiar with the following facts. This feature:

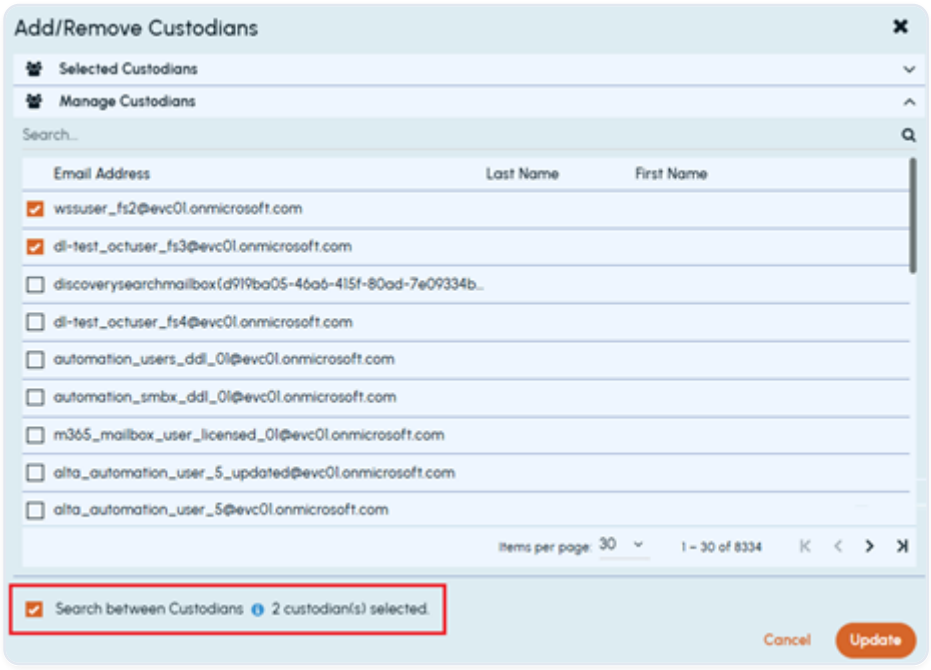
- is available in both *Advanced Search* and *Query Search* modes.
- supports searching for email items only and does not include collaboration messages or files.
- allows you to select minimum two to maximum 10 custodians.
- eliminates the need to manually look up or enter individual email addresses or aliases.

To search emails exchanged among specified custodians:

1. Do one of the following as needed:

- On the **Investigations** tab, select *My Mailbox > New Search* or *Managed Accounts > New Search*.
- On the **eDiscovery** tab, select *Archive Search > New Search*.

2. On the **Advanced Search** tab, under **Filters**, select the **Custom** option. The **Manage** button appears. Click **Manage** to open the **Add/Remove Custodians** pop-up as shown in the sample image below.



3. Select the **Search Between Custodians** option provided in the bottom on the pop-up.
4. Expand **Manage Custodians** and select the custodians required for this search.

> **Note:** Select minimum two to maximum 10 custodians as required. These custodians are listed under the **Selected Custodians** section.

5. Click **Update** to add these selected custodians as a search criterion and close the pop-up.

> **Note:** Do not select any additional criteria if you want to refine this search in **Previous Searches** or **Search Log** later.

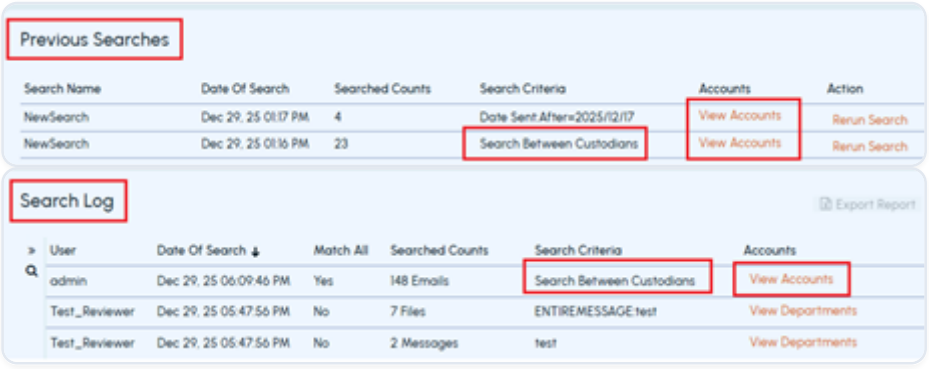
6. Click **Search**.

   After performing a search, if you had selected only the **Search Between Custodians** option and not specified any additional search criteria, the **Search Log**,**Previous Searches**, and **Case History** display the search criteria as *Search Between Custodians*.

You can view selected custodians from both Investigations and eDiscovery tabs.

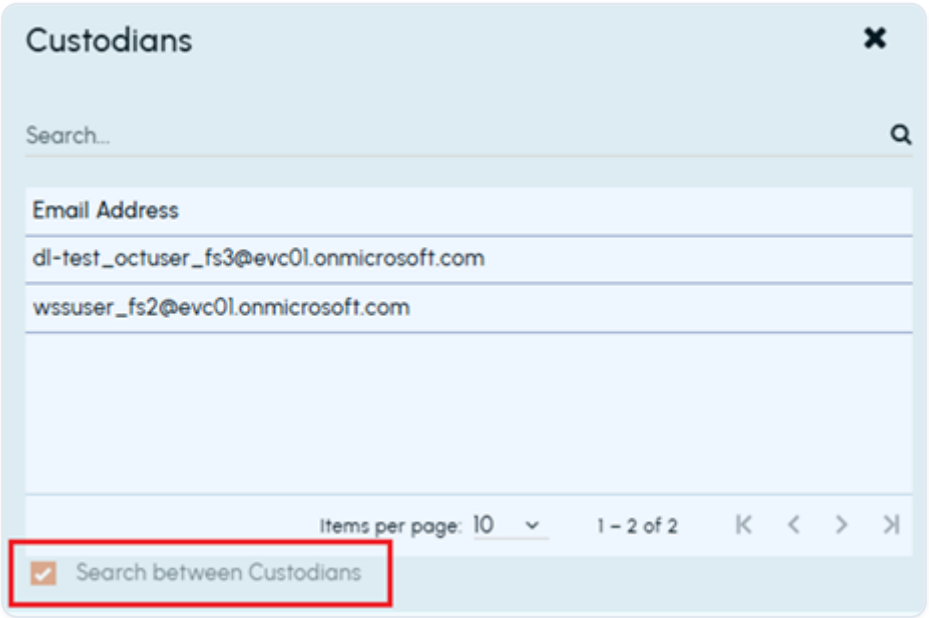
- In **Investigations**, open **Previous Searches** or **Search Log**.
- In **eDiscovery**, open **Previous Searches**.

The *Search Criteria* column shows *Search Between Custodians* as the applied criteria for the search. Refer to the sample images below.

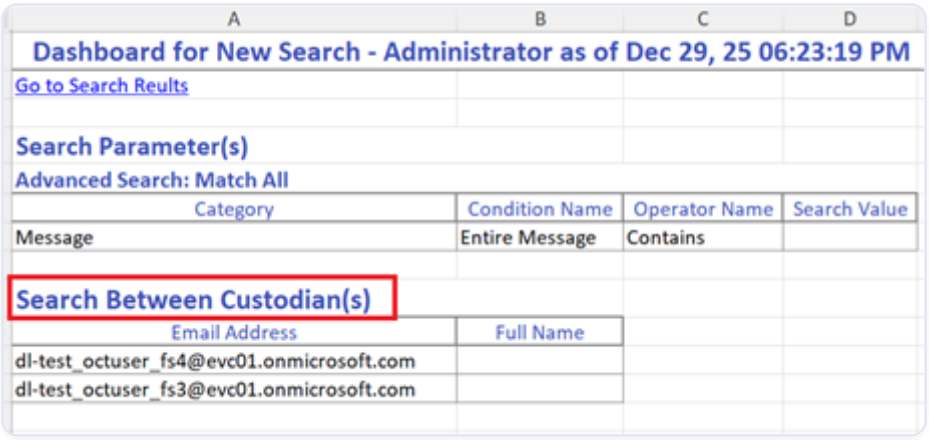


7. Click **View Accounts** in the same row.

The application opens a pop-up to show the selected custodians. Refer to the sample images below.



When you export the report for such searches with criteria as *Search Between Custodians*, the exported report shows the details as shown in the sample report image below.



Dashboard for New Search - Administrator as of Dec 29, 25 06:23:19 PM

Go to Search Reults

Search Parameter(s)

Advanced Search: Match All

Category	Condition Name	Operator Name	Search Value
Message	Entire Message	Contains	

Search Between Custodian(s)

Email Address	Full Name
dl-test_octuser_fs4@evc01.onmicrosoft.com	
dl-test_octuser_fs3@evc01.onmicrosoft.com	

Viewing previously executed but unsaved searches during an investigation

While investigating data references, you may often run a search and retrieve the data, but knowingly or unknowingly do not save it. In such scenarios, the application logs the search under *Investigation > Managed Accounts > Previous Searches* node. This allows you to refer to your previously executed but unsaved searches when needed. You can rerun the same search and save it for future investigative purposes.

To view previously executed but unsaved searches during an investigation:

1. In the left navigation pane, select **Investigation**>**Managed Accounts**>**Previous Searches** node.

   A list of previously executed but unsaved searches during investigation appears. Use the page navigation arrows to access cases displayed on other pages.
2. To retrieve the search result, click **Rerun Search** in the **Action** column of the row corresponding to the search you want to run again.
3. If needed, do the following:

   - Click **Save Search** for future investigative purposes.
   - Click **Send to Case** to send the review items retrieved in a search to one or more cases available in the **eDiscovery** tab, while keeping a copy of items in the **Investigation** tab.

> **Note:** For AI-enabled cases,**Send to Case** supports only email items, and any non-email items (such as files and collaboration messages) are automatically skipped.

> **Note:** Department Reviewers may encounter certain role-specific limitations. For details, these are known, low-impact issues targeted for resolution in the next release.

About Tags

This section describes the tasks that a user can perform with the tags.

Deleting tags

To delete a tag:

1. On the **Investigations** tab, select **Tags**.
2. Select the tag you want to delete.

   The application displays all items to which the selected tag is applied.
3. Click **Delete Tag**.

   The application prompts you to confirm that you want to perform the operation.
4. Click **Yes** to complete the operation or click **No** to cancel it.

Removing items from tags

To remove items from tags:

1. On the **Investigations** tab, select **Tags**.
2. Select the tag to view all items to which the selected tag is applied.
3. In the **Collaboration** tab, select the message which tag you want to remove.
4. Click **Remove from Tag**.

   The application prompts you to confirm that you want to perform the operation.
5. Click **Yes** to complete the operation or click **No** to cancel it.

Updating tags

To update a tag:

1. On the **Investigations** tab, select **Tags**.
2. Select the tag you want to update.

   The application displays all items to which the selected tag is applied.
3. Click **Update Tag**.
4. In the **Tag** dialog box, do the following:

   - In the **Tag Name** field, modify the existing tag name, if required.

- In the **Comments** field, specify the reason to update the tag.
- To apply legal hold on the items with this tag, select the **Legal Hold** check box.

5. Click **OK** to complete the operation or click **Cancel** to abort updating task.

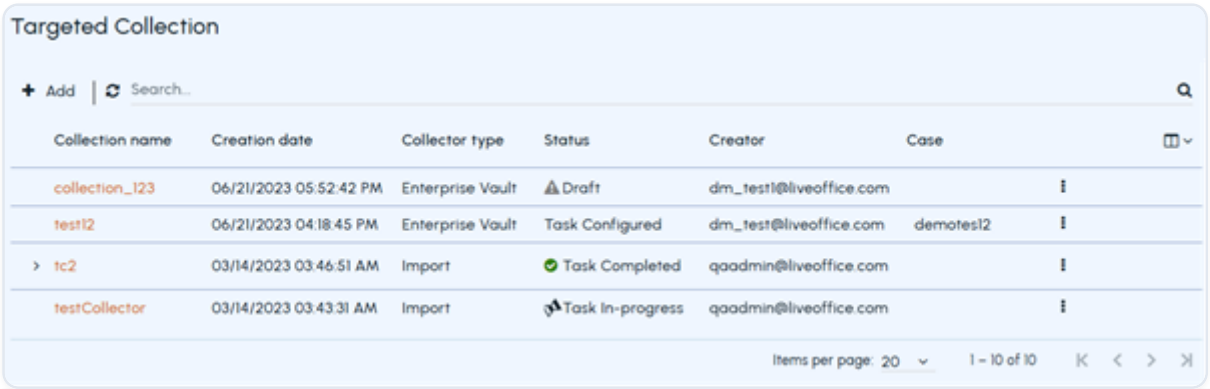
About Targeted Collections

A targeted collection is a cloned data set of an archive collector which is configured in the Arctera Management Console. You can create and manage targeted collections in the Arctera eDiscovery. These collections allow retrieval of filtered content for eDiscovery purposes. After an administrator configures the archive collector for your organization, the content that matches the filter criteria can be collected in Arctera eDiscovery.

Before creating a targeted collection in Arctera eDiscovery, make sure the following prerequisites are met in the Management Console

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

After creating a targeted collection, the Targeted Collection table displays all collectors along with their configuration status, type, and metadata. Use the table to monitor collector readiness before assigning them to a case. Refer to the sample image below.



COLUMNS	DESCRIPTION
Collection name	Displays the name of the targeted collection.
	You can expand the row to view collection details such as items collected, items received, items archived, items duplicate, items rejected,

COLUMNS	DESCRIPTION
	and items failed. You can also download the Collection Defensibility Report.
Creation date	Shows the date and time the collection was created.
Collector type	Indicates the type of a collector.
Status	Displays the current status of the collector.
	- Draft: The collection status is not yet configured or the task is in an incomplete state.
	- Task In-progress: The collector is configured and the collection task is automatically queued or resumed for data collection.
	- Stopped: The collector is stopped manually for some reason. If you want to restart the stopped collection, you can start the collector from the More actions icon. The status then again updates to Task In-progress.
	- Task Completed: The collection task is successfully completed and the Collection Defensibility Report is available to download.
Creator	Displays a name of a user who has created the collector.
Case	Displays the name of cases (to which the items are sent) assigned to the collector, if applicable.
More actions icon	Provides options to manage the collector. The available options are Start, Stop, Restart, Hide, and Show. See Managing Arctera Capture collectors from Arctera eDiscovery.

Adding targeted collection for data import

The data (files) import collector lets your organization collect files. This collector supports files with extension ZIP, PDF, DOC, DOCX, PPT, PPTX, XLS, XLSX, CSV, PST, EML, MSG, and DAT. You can compress these extension files into ZIP file for import. After an administrator configures this importer, the files uploaded in this importer gets processed.

Prerequisite: Before you configure a file importer in Arctera eDiscovery, the Arctera Management Console administrator must create and enable the Data Uploading archive collector in Arctera Management Console.

Before you import files in the importer, you must understand the following conditions:

- This type of collector supports ZIP, PDF, DOC, DOCX, PPT, PPTX, XLS, XLSX, CSV, PST, EML, MSG, and DAT file extensions.
- Each file should not exceed 2 GB size.
- Total upload size should not exceed 20 GB size.
- ZIP file inside ZIP file will not get processed.
- After you upload the files using collector, you cannot upload more files in same collector.

To configure targeted collection for data import:

1. On the **Investigations** tab, in the left navigation pane, select **Targeted Collection**.
2. Click **Add** to set up data importer.

   The **Select Collector Type** pop up appears.
3. Select **Import**, and specify the following details:.

IMPORTER NAME	ENTER A UNIQUE NAME FOR THE IMPORTER. THIS IS A MANDATORY FIELD.
Description	Provide the description (purpose) for the importer. This is an optional field.

4. Click **Create Importer**.
5. On the **Upload files and import data** page, Click **Import** or **Browse** to add files that you want to upload.

   The selected files are listed with corresponding details. To remove files from this list, select the check box in the file details row, and click the **Delete** icon.

6. Click **Upload**. Do not refresh the screen while uploading is in progress.

   The file upload status is displayed after uploading is completed. If you have uploaded several files, use the page navigation bar to view the files.

7. Click the **Targeted Collection** node to view the import details report.
8. After successful data uploading, the importer appears on the **Targeted Collections** page.

> **Note:** If the status of the importer is **Archived**, you can expand the importer row to view the **Collection Defensibility Report** of the importer-specific data. It displays the details like Items Collected, Items Received, Items Archived, Items Duplicate, Items Rejected, and Items Failed. To download the **Collection Defensibility Report**, click the **Download** icon. The collection defensibility report consists of two sections: **File Details** and **EML Details**. The **File Details** section provides details of ZIP, PDF, DOC, DOCX, PPT, PPTX, XLS, XLSX, CSV, and DAT files. The **EML Details** section provides details of loose PST, EML,and MSG files.

Adding targeted collection for Enterprise Vault

The Enterprise Vault reactive collector lets your organization collect items that are associated with your Enterprise Vault. After an administrator configures this collector for your organization, the items that match the filter criteria can be collected in Arctera eDiscovery.

You must configure the filter criteria for each Enterprise Vault reactive collector. Based on the filter criteria, the Enterprise Vault reactive collector collects the archive-level and vault-level data in Arctera eDiscovery to perform all eDiscovery operations.

Prerequisite: Before you use the Enterprise Vault collector Arctera eDiscovery to collect Enterprise Vault content, you need to enable this service. To enable Enterprise Vault service, do the following:

1. Contact Arctera support team to enable the Enterprise Vault collector in Arctera Unified Platform.
2. Install the Enterprise Vault Agent on a server that can access your Enterprise Vault environment.

   You can download the Enterprise Vault Agent from here

3. Refer the following procedure to configure the Targeted Collection for Enterprise Vault.

   To configure Targeted Collection for Enterprise Vault:

4. On the **Investigations** tab, in the left navigation pane, select **Targeted Collection**.
5. Click **Add** and select the Enterprise Vault collector.

> **Note:** At the time of adding the first collector, the **Set up Collection** button appears in the middle of the screen. If one or more collectors are already added, the Add option appears.

6. On the **Collection Information** tab, specify the following:

COLLECTION NAME	PROVIDE A UNIQUE NAME FOR THIS COLLECTION. ARCTERA UNIFIED PLATFORM
Email	Enter email to get notification once the targeted collection has finished processing.
Select a site	If you have multiple sites in your Enterprise Vault environment or have multiple individual Enterprise Vault environments, the application displays a list of all sites which this tenant has as a part of direct migration agent configuration.
	Select a required site from the displayed options.

7. Click **Save and Next** to navigate to the **Filter** tab.
8. On the **Filter** tab, do the following:

DATE	SPECIFY THE DATE RANGE FOR COLLECTION. THE AVAILABLE OPTIONS ARE BEFORE, AFTER, AND BETWEEN.
Vault stores and Archives	Select the appropriate vault stores or archives in which you want to search the data.
	It supports selecting vault stores and archives from multiple sites.

DATE	SPECIFY THE DATE RANGE FOR COLLECTION. THE AVAILABLE OPTIONS ARE BEFORE, AFTER, AND BETWEEN.
	- Select the All vault stores option to consider all the available vault stores to search items.
	- Select the Selected vault store(s) option to select the required vault stores for the selected archives. The Select vault(s) button appears. Click Select vault(s) to search for and select the required vaults for searching items. You can remove the selection from the same dialog box.
	- Select the All archives option to consider all the available archives to search items.
	- Select the Selected archive(s) option to select the required archives. The Select archive(s) button appears. Click Select Vault(s) to search for and select the required archives for searching items. You can remove the selection from the same dialog box.
	- If you have many archives for targeted collection, use the Import functionality that supports importing data in the CSV format. Click Import, and choose a CSV file with the list of archives. The CSV file must contain Archive IDs in the first column. The file should not contain any other information. It may lead to error during the import.
Search terms	Specify the criteria with the help of keywords. It helps you to restrict searching items from the selected vault stores and archives.
	Use the plus-icon to save the search term and add a new criteria under the Search terms section.

DATE	SPECIFY THE DATE RANGE FOR COLLECTION. THE AVAILABLE OPTIONS ARE BEFORE, AFTER, AND BETWEEN.
	Use the minus-icon to remove an existing criteria.
Attachments	Specify the file types (Enterprise Vault compatible file extensions such as .pdf, .doc, .zip, and so on) that you want to collect during data collection from Enterprise Vault.
Custom attributes	Specify attributes that you want to include in the search configuration.
	If you want to provide several attributes, specify either All of or Any of option under the Attribute inclusion section. It determines whether the search results should match any of the
	attributes or all of them.

9. Click **Save and Next** to navigate to the **Send to Cases** tab.
10. On the **Send to Cases** tab, specify the following:

SEND TO EXISTING CASE	**ALTHOUGH THIS FIELD IS OPTIONAL, THE CHECK BOX IS SELECTED BY DEFAULT.**
	- IF YOU WANT TO SEND A SEARCH RESULT TO CASES, SELECT THIS CHECK BOX AND CHOOSE ONE OR MORE CASES FROM THE LIST OF AVAILABLE CASES. NAVIGATE TO THE NEXT AND PREVIOUS PAGES TO ACCESS THE AVAILABLE CASES.
	- IF YOU DO NOT WANT TO SEND A SEARCH RESULT TO CASES, CLEAR THIS CHECK BOX. UPON CLEARING THIS CHECK BOX, THE APPLICATION DISPLAYS A CONFIRMATION PROMPT THAT YOU HAVE NOT SELECTED ANY CASE TO SEND THE COLLECTED ITEMS. DO THE FOLLOWING AS REQUIRED: CLICK NO TO ASSIGN A CASE AND COMPLETE THE SETUP. CLICK YES TO PROCEED WITHOUT SELECTING A CASE. THIS ALLOWS YOU TO ARCHIVE THE ITEMS FIRST AND SEND THEM TO THE REQUIRED CASES LATER.
Collection set name	Enter the collection set name.
	When you select a single or multiple cases in the eDiscovery tab, the node of this name is displayed under the Case Documents node.
	After the targeted collector is configured and the displayed status is Archived, all the items are sent to this Collection Set in the respective cases under the Case Documents node.

11. Click **Save and Next** to navigate to the **Review** tab.
12. On the **Review** tab, do the following:
    - Check the configuration information to ensure accuracy.
    - To modify configuration information, click the corresponding **Edit** link.

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

    The Enterprise Vault reactive collector appears in the Targeted Collections page.

    > **Note:** If the status of the Enterprise Vault targeted collector is **Archived**, you can expand the targeted collector row to view the **Collection Defensibility Report** of the Enterprise Vault reactive data. It displays the details like Items Collected, Items Received, Items Archived, Items Duplicate, Items Rejected, and Items Failed. To download the Collection Defensibility Report, click the **Download** icon.

14. 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, items cannot be sent to case. User cannot remove the previously selected and saved options.

15. If the status of the targeted collector is **Archived**, and you want to send items to cases, click **Send to case** in the respective row.

    See Sending collected data to cases.

Adding targeted collection for Exchange Online

To configure Targeted Collection for Exchange Online:

1. On the **Investigations** tab, in the left navigation pane, select **Targeted Collection**.
2. Click **Add**.

   The **Select Collector Type** pop up appears.
3. Select **Exchange Online**.
4. 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.

COLLECTION NAME	PROVIDE A UNIQUE NAME FOR THIS COLLECTION.
Select a collector to get data from	Select the Exchange Online collector that is already configured in Arctera Unified Platform Management Console.

5. Click **Save and Next** to navigate to the **Filters** tab.
6. On the **Filters** tab, specify the following:

USER SOURCE CONFIGURATION	- 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 COLLECT., AND CLICK CONFIRM.
	SYNCHRONIZING USER ACCOUNTS:
	TO GET THE LATEST USER LIST, CLICK THE SYNC ICON. THIS SYNCHRONIZATION PROCESS MAY TAKE SEVERAL MINUTES AS IT SYNCHRONIZES ALL THE ACCOUNTS FROM THE CONTENT SOURCE.
	RESETTING CURRENT USER SELECTION:
	CLICK THE RESET ICON TO RESET THE LIST OF MONITORED USERS TO THE LASTLY-SAVED SELECTION.
Select matching method for the keyword search	Provide any words that you want to search in the email subject and email body content. Press ENTER to confirm the word or a phrase.
	You can enter multiple words and phrases.
	Select All to consider all the specified words and phrases you want to search and collect.

USER SOURCE CONFIGURATION	**- 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 COLLECT., AND CLICK CONFIRM.
	SYNCHRONIZING USER ACCOUNTS:
	TO GET THE LATEST USER LIST, CLICK THE SYNC ICON. THIS SYNCHRONIZATION PROCESS MAY TAKE SEVERAL MINUTES AS IT SYNCHRONIZES ALL THE ACCOUNTS FROM THE CONTENT SOURCE.
	RESETTING CURRENT USER SELECTION:
	CLICK THE RESET ICON TO RESET THE LIST OF MONITORED USERS TO THE LASTLY-SAVED SELECTION.
	Select Any to consider any of the specified words and phrases you want to search and collect.
Select date range	Specify the date range for collection. The available options are Before, After, and Between.
Captured Modern Attachment	Select any of the following options as required\:
	- Latest version: Select this option to capture the latest saved version of the shared document that is available at connector runtime.
	- Shared version: Select this option to capture the saved version of the document at the time of sharing in Microsoft Teams.

7. Click **Save and Next** to navigate to the **Send to Cases** tab.

8. On the **Send to Cases** tab, specify the following:

SEND TO EXISTING CASE	**ALTHOUGH THIS FIELD IS OPTIONAL, THE CHECK BOX IS SELECTED BY DEFAULT.**
	- IF YOU WANT TO SEND A SEARCH RESULT TO CASES, SELECT THIS CHECK BOX AND CHOOSE ONE OR MORE CASES FROM THE LIST OF AVAILABLE CASES. NAVIGATE TO THE NEXT AND PREVIOUS PAGES TO ACCESS THE AVAILABLE CASES.
	- IF YOU DO NOT WANT TO SEND A SEARCH RESULT TO CASES, CLEAR THIS CHECK BOX. UPON CLEARING THIS CHECK BOX, THE APPLICATION DISPLAYS A CONFIRMATION PROMPT THAT YOU HAVE NOT SELECTED ANY CASE TO SEND THE COLLECTED ITEMS. DO THE FOLLOWING AS REQUIRED: CLICK NO TO ASSIGN A CASE AND COMPLETE THE SETUP. CLICK YES TO PROCEED WITHOUT SELECTING A CASE. THIS ALLOWS YOU TO ARCHIVE THE ITEMS FIRST AND SEND THEM TO THE REQUIRED CASES LATER.
Collection set name	Enter the collection set name.
	When you select a single or multiple cases in the eDiscovery tab, the node of this name is displayed under the Case Documents node.
	After the targeted collector is configured and the displayed status is Archived, all the items are sent to this Collection Set in the respective cases under the Case Documents node.

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 Exchange Online archive collector appears on the Targeted Collections page.

    > **Note:** If the status of the Microsoft Teams targeted collector is **Archived**, you can expand the targeted collector row to view the **Collection Defensibility Report** of the Exchange Online-specific reactive data. It displays the details like Items Collected, Items Received, Items Archived, Items Duplicate, Items Rejected, and Items Failed. To download the Collection Defensibility Report, click the **Download** icon.

12. 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 collect items properly. User cannot remove the previously selected and saved options.

13. If the status of the targeted collector is **Archived**, and you want to send items to cases, click **Send to case** in the respective row.

    See Sending collected data to cases.

Adding targeted Collection for Google Workspace

The Google Collection archive collector collects enterprise-level Google-specific conversation data. The collected data includes data from Google Chat, Gmail, and Drive. You can view the Google Workspace collector only if the *Google Workspace Service* is enabled for you in the Arctera Management Console. For more information, contact your system administrator.

Performance Best Practices:

To ensure efficient processing of Google Workspace collections, the following performance guidelines apply. While the system is designed to handle large-scale data, processing speeds are affected by Google Vault API limits, data volume, and item complexity. To maintain consistent processing speeds and responsiveness, large collections should be divided into smaller, manageable jobs as follows:

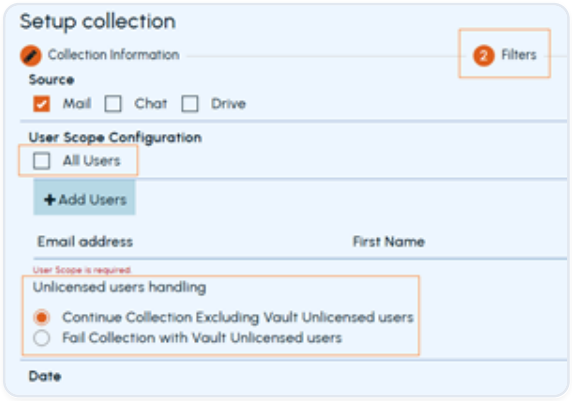
DATA TYPE	RECOMMENDED LIMIT PER JOB	RATIONALE
Gmail	Under 5 GB	Large historical exports require substantial time for end-to-end conversion and download. Smaller batches reduce the risk of processing bottlenecks.
Google Drive	Under 5 GB	Drive exports involve complex ZIP expansion and metadata parsing. Limiting to 5 GB or less improves turnaround time.
Google Chat	25000 Messages	High-volume spaces with frequent edits or deletes demand additional processing resources to reconstruct data accurately.

To add the Google Collection archive collector:

1. On the **Investigations** tab, in the left navigation pane, select **Targeted Collection**.
2. Click **Add**. The **Select Collector Type** pop up appears.
3. Select **Google Workspace**.
4. On the **Collection Information** tab, specify the following details, and click **Save and Next**.

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 to get data from	Select the Microsoft Teams collector that is already
	configured in Management Console.

5. On the **Filters** tab, specify the following details, and click **Save and Next**.

SOURCE	SELECT THE DATA SOURCES TO ARCHIVE. YOU CAN SELECT THE MAIL, CHAT, AND DRIVE OPTIONS.
	BASED ON THE SELECTED SOURCES, THE SYSTEM CREATES SEPARATE COLLECTOR INSTANCES FOR EACH TYPE (GMAIL, CHAT, OR DRIVE). EACH INSTANCE USES A CORRESPONDING SUFFIX: -GMAIL, -CHAT, OR -DRIVE.
	NOTE:
	- IF YOU SELECT ONLY THE MAIL OPTION, THE ALL USERS CHECKBOX IS AVAILABLE UNDER THE USER SCOPE CONFIGURATION SECTION.
	- IF YOU SELECT THE CHAT OR DRIVE OPTIONS, THE ALL USERS CHECKBOX IS DISABLED. IN THIS CASE, CLICK ADD USERS TO MANUALLY SELECT SPECIFIC USERS.
User Scope Configuration	 Add users whose data the collector has to archive.
	- Select the All Users checkbox to include all users, or clear it to select specific users.
	- Clear the All Users checkbox to select specific users. Click the Add Users option to open the list of available users. Select the

SOURCE	**SELECT THE DATA SOURCES TO ARCHIVE. YOU CAN SELECT THE MAIL, CHAT, AND DRIVE OPTIONS.**
	BASED ON THE SELECTED SOURCES, THE SYSTEM CREATES SEPARATE COLLECTOR INSTANCES FOR EACH TYPE (GMAIL, CHAT, OR DRIVE). EACH INSTANCE USES A CORRESPONDING SUFFIX: -GMAIL, -CHAT, OR -DRIVE.
	NOTE:
	- IF YOU SELECT ONLY THE MAIL OPTION, THE ALL USERS CHECKBOX IS AVAILABLE UNDER THE USER SCOPE CONFIGURATION SECTION.
	- IF YOU SELECT THE CHAT OR DRIVE OPTIONS, THE ALL USERS CHECKBOX IS DISABLED. IN THIS CASE, CLICK ADD USERS TO MANUALLY SELECT SPECIFIC USERS.
	users whose data you want to collect, and click Update.
	Note:
	When the All Users checkbox is cleared, the Unlicensed Users Handling section appears.
	Select one of the following options:
	- Continue Collection Excluding Vault Unlicensed Users: The collection process continues even if Google Vault unlicensed users are encountered. These users are automatically excluded, and data is collected only for licensed users.
	- Fail Collection with Vault Unlicensed Users: The collection process stops if any Google Vault unlicensed users are encountered. No data is collected.

SOURCE	**SELECT THE DATA SOURCES TO ARCHIVE. YOU CAN SELECT THE MAIL, CHAT, AND DRIVE OPTIONS.**
	BASED ON THE SELECTED SOURCES, THE SYSTEM CREATES SEPARATE COLLECTOR INSTANCES FOR EACH TYPE (GMAIL, CHAT, OR DRIVE). EACH INSTANCE USES A CORRESPONDING SUFFIX: -GMAIL, -CHAT, OR -DRIVE.
	NOTE:
	- IF YOU SELECT ONLY THE MAIL OPTION, THE ALL USERS CHECKBOX IS AVAILABLE UNDER THE USER SCOPE CONFIGURATION SECTION.
	- IF YOU SELECT THE CHAT OR DRIVE OPTIONS, THE ALL USERS CHECKBOX IS DISABLED. IN THIS CASE, CLICK ADD USERS TO MANUALLY SELECT SPECIFIC USERS.
Select a collector to get data from	Select the Microsoft Teams collector that is already
	configured in Management Console.
Date	Specify the date range for collection. The available options
	are Before, After, and Between.
Search Terms	Provide any words that you want to search in the
	collection.
	Press ENTER to confirm the word
	or a phrase.
	You can enter multiple words and phrases.

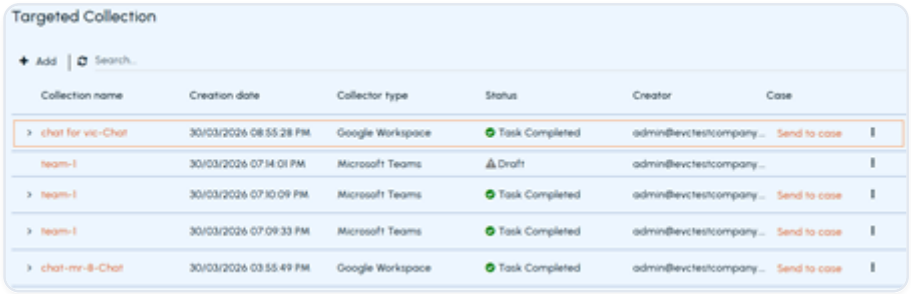
SOURCE	**SELECT THE DATA SOURCES TO ARCHIVE. YOU CAN SELECT THE MAIL, CHAT, AND DRIVE OPTIONS.**
	BASED ON THE SELECTED SOURCES, THE SYSTEM CREATES SEPARATE COLLECTOR INSTANCES FOR EACH TYPE (GMAIL, CHAT, OR DRIVE). EACH INSTANCE USES A CORRESPONDING SUFFIX: -GMAIL, -CHAT, OR -DRIVE.
	NOTE:
	- IF YOU SELECT ONLY THE MAIL OPTION, THE ALL USERS CHECKBOX IS AVAILABLE UNDER THE USER SCOPE CONFIGURATION SECTION.
	- IF YOU SELECT THE CHAT OR DRIVE OPTIONS, THE ALL USERS CHECKBOX IS DISABLED. IN THIS CASE, CLICK ADD USERS TO MANUALLY SELECT SPECIFIC USERS.
	Select All to consider all the specified words and phrases
	you want to search and collect.
	Select Any to consider any of the specified words and
	phrases you want to search and collect.

6. On the **Send to Cases** tab, specify the following details, and click **Save and Next**.

SEND TO EXISTING CASE	THIS FIELD IS OPTIONAL.
	TO SEND A RESULT TO CASES, SELECT THIS CHECK BOX AND CHOOSE ONE OR MORE CASES FROM THE LIST OF AVAILABLE CASES. NAVIGATE TO THE NEXT AND PREVIOUS PAGES TO ACCESS THE AVAILABLE CASES.
Collection set name	Enter the collection set name.
	When you select a single or multiple cases in the eDiscovery tab, the node of this name is displayed under the Case Documents node.
	After the targeted collector is configured and the displayed status is Archived, all the items are sent to this Collection Set in the respective cases under the Case Documents node.

7. Click **Save and Next** to navigate to the **Review** tab.
8. On the **Review** tab, do the following:
   - Check the configuration information to ensure accuracy.
   - To modify configuration information, click the corresponding **Edit** link.
9. If the data is correct, click **Complete**.

   The **Google Workspace** archive collector appears on the **Targeted Collections** page.



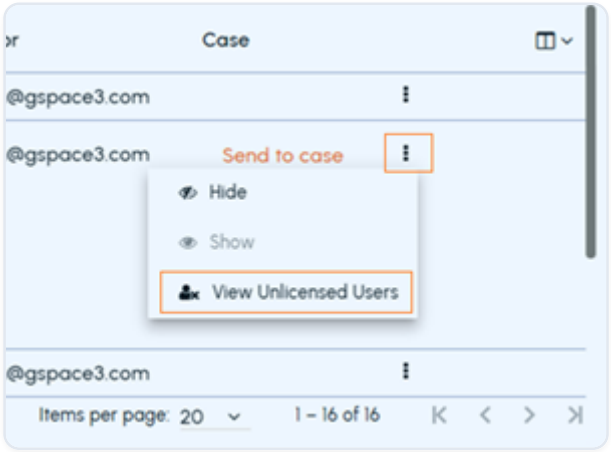
   - If the status is **Task Completed**, you can do the following:
     - To view the **Collection Defensibility Report** of the collection, expand the targeted collector row. It displays the details like Items Collected, Items Received, Items

Archived, Items Duplicate, Items Rejected, and Items Failed. To download this, click the **Download** icon.

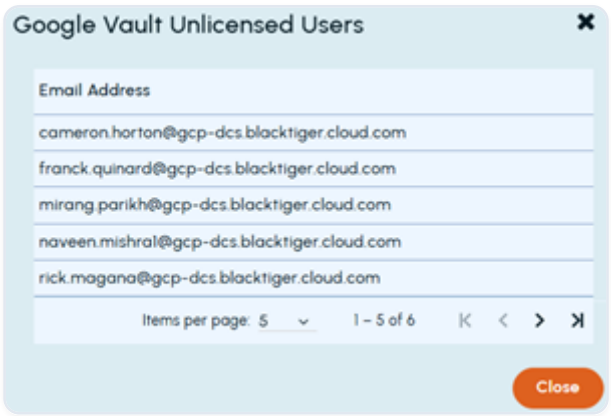
- To send items to cases, click **Send to case** in the respective row.

See Sending collected data to cases.

- If the status is *Task Completed* and only the specific users are added (the *All Users* option was not selected) during collector configuration, you can view the users who are not licensed for Google Vault. On the **Targeted Collections** page, click the **kebab** icon (three vertical dots) provided in the selected collectors's row, and then click **View Unlicensed Users**. Refer to the sample image below:



The **Google Vault Unlicensed Users** pop-up appears as displays the user list. Refer to the sample image below:



- If the status is **Incomplete**, modify the collector configuration. To modify the configuration, click on the targeted collection name. If the configuration is incomplete, user cannot collect items properly. User cannot remove the previously selected and saved options.

Adding targeted collection for Microsoft Teams

To configure Targeted Collection for Microsoft Teams:

1. On the **Investigations** 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, the **Setup Collection** button appears in the middle of the screen. If one or more collectors are already added, the **Add** option 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 to get data from	Select the Microsoft Teams collector that is already configured in Arctera Unified Platform Management Console.
	Note: If the **EV Folder Target** field is set to **No** while configuring the Microsoft Teams archive collector in the Management Console, the collector does not appear in the drop-down list during targeted collection configuration in Arctera eDiscovery. This is because items from such collectors are not ingested into Arctera Unified Platform - whether through regular, proactive, or cloned targeted collection.

4. Click **Save and Next** to navigate to the **Filters** tab.
5. On the **Filters** tab, specify the following:

USER SOURCE CONFIGURATION	**- 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 COLLECT., AND CLICK CONFIRM.
	SYNCHRONIZING USER ACCOUNTS:
	TO GET THE LATEST USER LIST, CLICK THE SYNC ICON. THIS SYNCHRONIZATION PROCESS MAY TAKE SEVERAL MINUTES AS IT SYNCHRONIZES ALL THE ACCOUNTS FROM THE CONTENT SOURCE.
	RESETTING CURRENT USER SELECTION:
	CLICK THE RESET ICON TO RESET THE LIST OF MONITORED USERS TO THE LASTLY-SAVED SELECTION.
Select matching method for the keyword search	Provide any words that you want to search in the collaboration messages. Press ENTER to confirm the word or a phrase.
	You can enter multiple words and phrases.
	Select All to consider all the specified words and phrases you want to search and collect.
	Select Any to consider any of the specified words and phrases you want to search and collect.
Select date range	Specify the date range for collection. The available options are Before, After, and Between.
Captured Modern Attachment	Select any of the following options as required\:

USER SOURCE CONFIGURATION	**- 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 COLLECT., AND CLICK CONFIRM.
	SYNCHRONIZING USER ACCOUNTS:
	TO GET THE LATEST USER LIST, CLICK THE SYNC ICON. THIS SYNCHRONIZATION PROCESS MAY TAKE SEVERAL MINUTES AS IT SYNCHRONIZES ALL THE ACCOUNTS FROM THE CONTENT SOURCE.
	RESETTING CURRENT USER SELECTION:
	CLICK THE RESET ICON TO RESET THE LIST OF MONITORED USERS TO THE LASTLY-SAVED SELECTION.
	- Latest version: Select this option to capture the latest saved version of the shared document that is available at connector runtime.
	- Shared version: Select this option to capture the saved version of the document at the time of sharing in Microsoft Teams.

6. Click **Save and Next** to navigate to the **Send to Cases** tab.
7. On the **Send to Cases** tab, specify the following:

SEND TO EXISTING CASE	**ALTHOUGH THIS FIELD IS OPTIONAL, THE CHECK BOX IS SELECTED BY DEFAULT.**
	- IF YOU WANT TO SEND A SEARCH RESULT TO CASES, SELECT THIS CHECK BOX AND CHOOSE ONE OR MORE CASES FROM THE LIST OF AVAILABLE CASES. NAVIGATE TO THE NEXT AND PREVIOUS PAGES TO ACCESS THE AVAILABLE CASES.
	- IF YOU DO NOT WANT TO SEND A SEARCH RESULT TO CASES, CLEAR THIS CHECK BOX. UPON CLEARING THIS CHECK BOX, THE APPLICATION DISPLAYS A CONFIRMATION PROMPT THAT YOU HAVE NOT SELECTED ANY CASE TO SEND THE COLLECTED ITEMS. DO THE FOLLOWING AS REQUIRED: CLICK NO TO ASSIGN A CASE AND COMPLETE THE SETUP. CLICK YES TO PROCEED WITHOUT SELECTING A CASE. THIS ALLOWS YOU TO ARCHIVE THE ITEMS FIRST AND SEND THEM TO THE REQUIRED CASES LATER.
Collection set name	Enter the collection set name.
	When you select a single or multiple cases in the eDiscovery tab, the node of this name is displayed under the Case Documents node.
	After the targeted collector is configured and the displayed status is Archived, all the items are sent to this Collection Set in the respective cases under the Case Documents node.

8. Click **Save and Next** to navigate to the **Review** tab.
9. On the **Review** tab, do the following:
    - Check the configuration information to ensure accuracy.
    - To modify configuration information, click the corresponding **Edit** link.

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

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

    > **Note:** If the status of the Microsoft Teams targeted collector is **Archived**, you can expand the targeted collector row to view the **Collection Defensibility Report** of the Teams-specific reactive data. It displays the details like Items Collected, Items Received, Items Archived, Items Duplicate, Items Rejected, and Items Failed. To download the Collection Defensibility Report, click the **Download** icon.

11. 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 collect items properly. User cannot remove the previously selected and saved options.

12. If the status of the targeted collector is **Archived**, and you want to send items to cases, click **Send to case** in the respective row.

    See Sending collected data to cases.

Adding targeted collection for OneDrive for Business

The OneDrive for Business reactive collector lets your organization collect files that are associated with customer's OneDrive cloud storage. After an administrator configures this collector for your organization, the files that match the user source criteria can be collected in Arctera eDiscovery.

You must configure the user source criteria for each OneDrive for Business reactive collector. Based on this user source criteria, the OneDrive reactive collector collects the files in Arctera eDiscovery to perform all eDiscovery operations.

You can configure this targeted collection only if the Arctera eDiscovery primary service and the OneDrive for Business secondary service is enabled for a required customer is enabled in the Arctera Unified Platform Arctera Management Console. You must possess the administrator role to configure the OneDrive for Business reactive collector synchronization in Arctera eDiscovery.

To configure Targeted Collection for OneDrive for Business:

1. On the **Investigations** tab, in the left navigation pane, select **Targeted Collection**.

2. Click **Add** and select the **OneDrive for Business** collector.

> **Note:** At the time of adding the first collector, the **Set up Collection** button appears in the middle of the screen. If one or more collectors are already added, the **Add** option 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 to get data from	Select the OneDrive for Business collector that is already configured in Arctera Unified Platform Management Console.
	Note: If the **EV Folder Target** field is set to **No** while configuring the OneDrive for Business archive collector in the Management Console, the collector does not appear in the drop-down list during targeted collection configuration in Arctera eDiscovery. This is because items from such collectors are not ingested into Arctera Unified Platform - whether through regular, proactive, or cloned targeted collection.

4. Click **Save and Next** to navigate to the **Filter** tab.
5. On the **Filter** tab, specify the following:

USER SOURCE CONFIGURATION	**- 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 COLLECT, AND CLICK CONFIRM.
	SYNCHRONIZING USER ACCOUNTS
	TO GET THE LATEST USER LIST, CLICK SYNC. THIS SYNCHRONIZATION PROCESS MAY TAKE SEVERAL MINUTES AS IT SYNCHRONIZES ALL THE ACCOUNTS FROM THE CONTENT SOURCE.
	RESETTING CURRENT USER SELECTION:
	CLICK THE RESET ICON TO RESET THE LIST OF MONITORED USERS TO THE LASTLY-SAVED SELECTION.
Select matching method for the keyword search	Provide any words contained in the file name or other file metadata. Press ENTER to confirm the word or a phrase.
	You can enter multiple words and phrases.
	Select All to consider all the specified words and phrases you want to search and collect.
	Select Any to consider any of the specified words and phrases you want to search and collect.
Select date range	Specify the date range for collection. The available options are Before, After, and Between.

6. Click **Save and Next** to navigate to the **Send to Cases** tab.
7. On the **Send to Cases** tab, specify the following:

SEND TO EXISTING CASE	**ALTHOUGH THIS FIELD IS OPTIONAL, THE CHECK BOX IS SELECTED BY DEFAULT.**
	- IF YOU WANT TO SEND A SEARCH RESULT TO CASES, SELECT THIS CHECK BOX AND CHOOSE ONE OR MORE CASES FROM THE LIST OF AVAILABLE CASES. NAVIGATE TO THE NEXT AND PREVIOUS PAGES TO ACCESS THE AVAILABLE CASES.
	- IF YOU DO NOT WANT TO SEND A SEARCH RESULT TO CASES, CLEAR THIS CHECK BOX. UPON CLEARING THIS CHECK BOX, THE APPLICATION DISPLAYS A CONFIRMATION PROMPT THAT YOU HAVE NOT SELECTED ANY CASE TO SEND THE COLLECTED ITEMS. DO THE FOLLOWING AS REQUIRED: CLICK NO TO ASSIGN A CASE AND COMPLETE THE SETUP. CLICK YES TO PROCEED WITHOUT SELECTING A CASE. THIS ALLOWS YOU TO ARCHIVE THE ITEMS FIRST AND SEND THEM TO THE REQUIRED CASES LATER.
Collection set name	Enter the collection set name.
	When you select a single or multiple cases in the eDiscovery tab, the node of this name is displayed under the Case Documents node.
	After the targeted collector is configured and the displayed status is Archived, all the items are sent to this Collection Set in the respective cases under the Case Documents node.

8. Click **Save and Next** to navigate to the **Review** tab.
9. On the **Review** tab, do the following:
    - Check the configuration information to ensure accuracy.
    - To modify configuration information, click the corresponding **Edit** link.

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

    The OneDrive for Business archive collector appears in the Targeted Collections page.

    > **Note:** If the status of the OneDrive targeted collector is **Archived**, you can expand the targeted collector row to view the **Collection Defensibility Report** of the OneDrive-specific reactive data. It displays the details like Items Collected, Items Received, Items Archived, Items Duplicate, Items Rejected, and Items Failed. To download the Collection Defensibility Report, click the **Download** icon.

11. 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, items cannot be sent to case. User cannot modify the previously selected and saved options.

12. If the status of the targeted collector is **Archived**, and you want to send items to cases, click **Send to case** in the respective row.

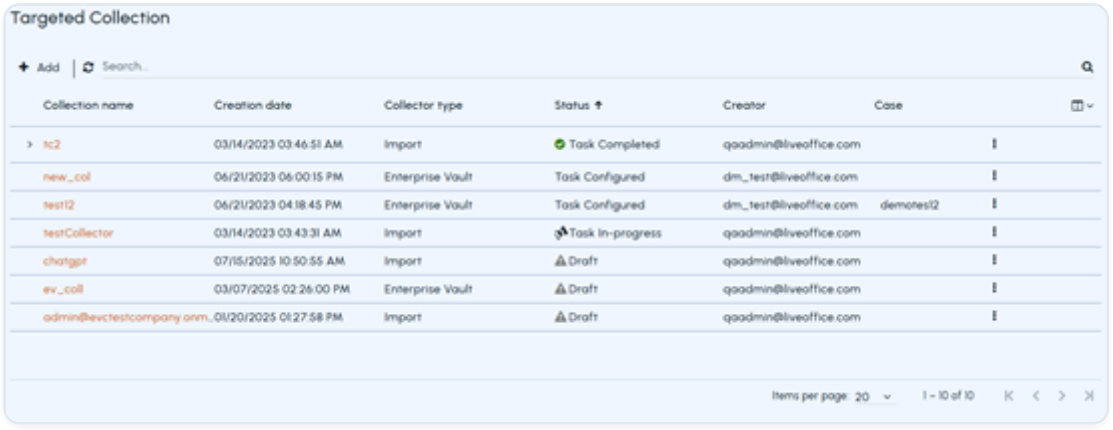
    See Sending collected data to cases.

Managing Arctera Capture collectors from Arctera eDiscovery

To manage Arctera Capture collectors from Arctera eDiscovery:

1. On the **Investigations** tab, select **Targeted Collection**.

   A list of existing collection names are displayed.



2. Search for a collector on which you want to perform a required action.
3. Perform the following actions, as needed:

- **To start a collector**:

Make sure the collection status is shown as *Stopped*. Click the **More actions** icon, and then click **Start**.

The collection status updates to *Task In-progress*.

> **Note:** The **Start** option appears only when the collector is in the **Stopped** state.

- **To stop a collector**:

Make sure the collection status is shown as *Task In-progress*. Click the **More actions** icon, and then click **Stop**.

The collection status updates to *Stopped*.

- **To restart a collector**:

Make sure the *Collection Defensibility Report* is showing *Failed* or *Rejected* items. Click the **More actions** icon, and then click **Restart**.

The restart operation begins the collection process from the start and the collection status gets updated to *Task In-progress*.

> **Note:** The **Restart** option appears only when the **Collection Defensibility Report** shows **Failed** or **Rejected** items. Otherwise, this option remains unavailable in the **More actions** menu.

- **To hide a collector**:

Click the **More options** icon in the corresponding row, and then click **Hide**.

> **Note:** Hidden collectors remain in the system and reappear in the table when you select **Show Hidden**.

- **To view hidden collectors**:

Click the **Select columns to show or hide** icon displayed in the top-right corner of the table, click the **Show Hidden** check box, and then click **Apply**.

- **To unhide (show) a collector**:

Click the **Select columns to show or hide** icon displayed in the top-right corner of the table, click the **Show Hidden** check box, and then click **Apply**. Locate the collector you want to unhide (show) in the main table again. Click the **More actions** icon, and then click **Show**.

Sending collected data to cases

To send collected data to cases:

1. On the **Investigations** tab, select **Targeted Collection**.
2. Search for and select the collection name with the *Task Completed* status.
3. Expand the Collection Name to view the collection details.
4. Click **Send to Case** link from the same row.
5. In the **Send to Cases** dialog box, specify the following:

SEND TO EXISTING CASE	ALTHOUGH THIS FIELD IS OPTIONAL, THE CHECK BOX IS SELECTED BY DEFAULT.
	- IF YOU WANT TO SEND A SEARCH RESULT TO CASES, SELECT THIS CHECK BOX AND CHOOSE ONE OR MORE CASES FROM THE LIST OF AVAILABLE CASES. NAVIGATE TO THE NEXT AND PREVIOUS PAGES TO ACCESS THE AVAILABLE CASES.
	- IF YOU DO NOT WANT TO SEND A SEARCH RESULT TO CASES, CLEAR THIS CHECK BOX. UPON CLEARING THIS CHECK BOX, THE APPLICATION DISPLAYS A CONFIRMATION PROMPT THAT YOU HAVE NOT SELECTED ANY CASE TO SEND THE COLLECTED ITEMS. DO THE FOLLOWING AS REQUIRED: CLICK NO TO ASSIGN A CASE AND COMPLETE THE SETUP. CLICK YES TO PROCEED WITHOUT SELECTING A CASE. THIS ALLOWS YOU TO ARCHIVE THE ITEMS FIRST AND SEND THEM TO THE REQUIRED CASES LATER.
Collection set name	Enter the collection set name.

SEND TO EXISTING CASE	**ALTHOUGH THIS FIELD IS OPTIONAL, THE CHECK BOX IS SELECTED BY DEFAULT.**
	- IF YOU WANT TO SEND A SEARCH RESULT TO CASES, SELECT THIS CHECK BOX AND CHOOSE ONE OR MORE CASES FROM THE LIST OF AVAILABLE CASES. NAVIGATE TO THE NEXT AND PREVIOUS PAGES TO ACCESS THE AVAILABLE CASES.
	- IF YOU DO NOT WANT TO SEND A SEARCH RESULT TO CASES, CLEAR THIS CHECK BOX. UPON CLEARING THIS CHECK BOX, THE APPLICATION DISPLAYS A CONFIRMATION PROMPT THAT YOU HAVE NOT SELECTED ANY CASE TO SEND THE COLLECTED ITEMS. DO THE FOLLOWING AS REQUIRED: CLICK NO TO ASSIGN A CASE AND COMPLETE THE SETUP. CLICK YES TO PROCEED WITHOUT SELECTING A CASE. THIS ALLOWS YOU TO ARCHIVE THE ITEMS FIRST AND SEND THEM TO THE REQUIRED CASES LATER.
	When you select a case in the eDiscovery tab, the node of this name is displayed under the Case Documents node.
	Note: After sending a collection set to the selected case, it is recommended to wait for some time for indexing items of this collection set under the **Case Documents** node. until the indexing is not complete, you may view the partial results. Once the indexing is complete, all the items will be available.

6. Click **Confirm**.

About transcription of media attachments

Arctera eDiscovery supports transcription of media attachments included in emails, collaboration messages, and files. By default, this feature is disabled. To enable it, contact your system administrator or the Arctera Support team.

When the feature is enabled:

1. The media attachments are marked with the Audio Description icon. Clicking the icon displays the media transcription in the preview pane.
2. Upon displaying the transcription, the Smart Transcript icon (media icon) appears on the preview pane toolbar. Clicking the Smart Transcript (media) icon opens the attachment in a new window with playback.
3. Customer can request to enable the required audio/video format. The currently supported media formats are `.mp3, .wav, .ogg, .mp4, .mov, .webm, .mpeg,` and `.opus`.

Viewing transcription of media attachments

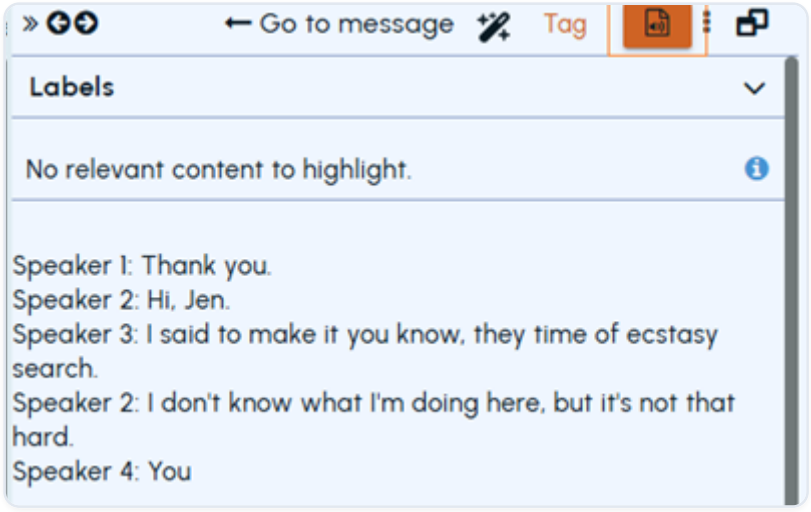
You can start with a new search or access previous, ongoing, standard, or advanced ECA searches as needed.

To view transcription of media attachments:

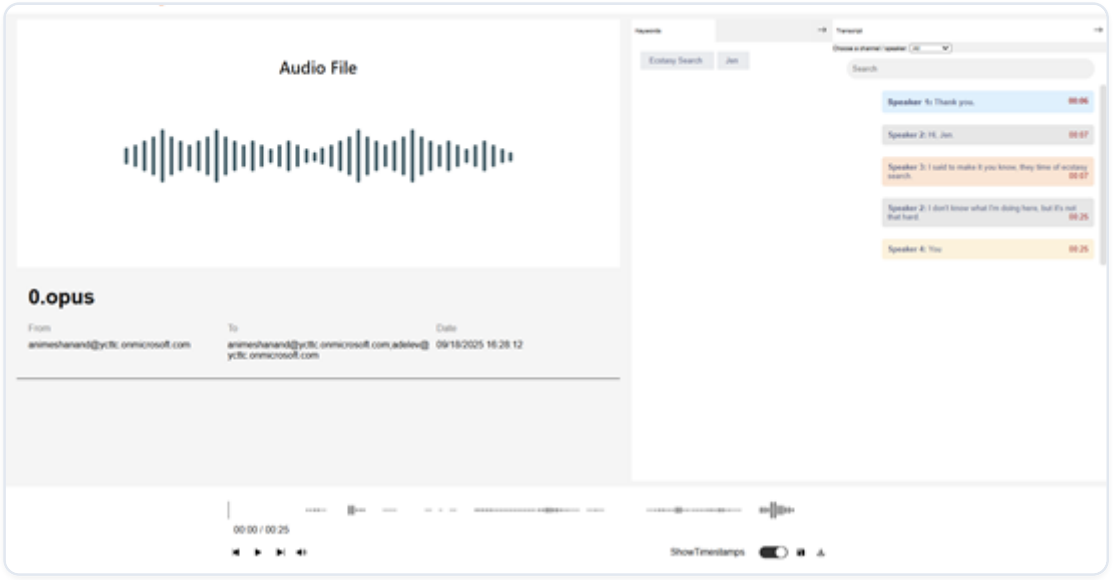
1. Navigate to Emails, Collaboration, or Files tab, and open the search result.
2. Search for and select the review item that contains media attachment (marked with the **Audio Description** icon.). Refer to the sample image below.

3. Click the **Audio Description** icon.

   The application displays the media transcription in the preview pane. At the same moment, the **Smart Transcript** icon (media icon) appears on the preview pane toolbar as shown in the sample image below.



4. Click the **Smart Transcript** (media) icon to opens the attachment in a new window, along with playback. Refer to the sample image below.



   The following functionalities are available for users:

- **Audio File Details**
  - Displays the file name (for example, xyz.opus).
  - Shows sender (From), recipients (To), and the Date/Time of the email.
- **Audio Waveform Panel**
  - Visual representation of the audio file.

    - Helps users see playback position and intensity of sound across the recording.

- **Transcript Panel**
    - Identifies speakers (for example, Speaker 1, Speaker 2) and lists conversation text aligned with timestamps.
    - Highlights each line with the exact time in the audio file.
    - Provides a Search box to locate keywords in the transcript. Allows filtering by channel/ speaker.
- **Keywords Section**
    - Displays matched keywords (for example, Ecstasy Search, Jen).
    - Enables quick navigation to relevant parts of the transcript.
- **Download Option**: Allows downloading of the audio file for offline use.
- **Timestamps Toggle Option**: Show or hide timestamps alongside transcript text.

Working with Advanced ECA searches

The Advanced Early Case Assessment (ECA) Search is a new type of search under the Managed Accounts node you can create for investigation purposes. The application creates this node when you create an Advance ECA search for the first time. You don't need to configure anything in the Arctera Management Console to view this node under Managed Accounts.

Advanced ECA search is different from the on-going and standard search. In on-going and standard searches, you can specify certain criteria based on which the application fetches emails, collaboration messages, and files from archives. In case of on-going and standard searches, after creating a search, you cannot again filter the required records (emails, messages, and files) within the search result. However, in the Advanced ECA search, you can refine your search results based on several filter options. It helps reviewers to filter the records and view the results most easily.

In a single Advanced ECA search, the application can save maximum 1000000 records each for emails, collaboration messages, and files.

Applying labels to the Advanced ECA search items

You can apply new labels to emails, collaboration messages, and files that are filtered during the Advanced ECA search. You can also view the previously applied labels of the items. The following sections explains how to apply labels to these search items.

Applying labels to collaboration messages in Advanced ECA search

To apply labels to collaboration messages in Advanced ECA search:

1. On the **Investigations** tab, select **Managed Accounts**>**Advanced ECA**.
2. Select the Advanced ECA search in which you want to filter the records and apply labels to the required collaboration messages within the search.

   The search result opens in the right pane.
3. Set the filter options and click **Apply** to view the filtered items.
4. On the **Collaboration** pane, select the collaboration messages to which you want to apply labels.

   > **Note:** Before you apply labels to the items, you can view the previously applied labels of the items in the preview pane.

5. On the action menu, click **Label**.
6. In the **Add/Remove Labels** dialog box, select the labels you want to apply to the emails.

   You can clear the labels if these are not required anymore. In case you have selected multiple messages, the **Add/Remove Labels** dialog box shows applied level status as follows:

- The check box that is not selected yet means this label is not at all applied to the selected messages.
- The check box with the dash mark means the label is applied to some of the selected messages, but not applied to all the selected message.
- The check box with the tick mark means the label is applied to all the selected messages.

1. Select the required labels, and click **Apply Changes**.

   After you apply labels to the collaboration messages, these labeled messages are available under the respective labels under the **labels** node.
2. To ensure if the label is applied to the messages, select the message, and expand the **Labels** section to view its details in the right pane.

Applying labels to emails in Advanced ECA search

To apply labels to emails in Advanced ECA search:

1. On the **Investigations** tab, select **Managed Accounts**>**Advanced ECA**.

2. Select the Advanced ECA search in which you want to filter the records and apply labels to the required emails within the search.

   The search result opens in the right pane.

3. Set the filter options and click **Apply** to view the filtered items.
4. On the Emails tab, select the emails to which you want to apply labels.

> **Note:** Before you apply labels to the items, you can view the previously applied labels of the items in the preview pane.

5. On the action menu, click **Label**.
6. In the **Add/Remove Labels** dialog box, select the labels you want to apply to the emails.

   You can clear the labels if these are not required anymore. In case you have selected multiple emails the **Add/Remove Labels** dialog box shows applied level status as follows:

- The check box that is not selected yet means this label is not at all applied to the selected emails.
- The check box with the dash mark means the label is applied to some of the selected emails, but not applied to all the selected emails.
- The check box with the tick mark means the label is applied to all the selected emails.

1. Select the required labels, and click **Apply Changes**.

   After you apply labels to the emails, these labeled emails are available under the respective labels under the **labels** node.

2. To ensure if the label is applied to the emails, select the emails, and expand the **Labels** section to view its details in the right pane.

Applying labels to files in Advanced ECA search

To apply labels to files in Advanced ECA search:

1. On the **Investigations** tab, select **Managed Accounts**>**Advanced ECA**.
2. Select the Advanced ECA search in which you want to filter the records and apply labels to the required files within the search.

   The search result opens in the right pane.

3. Set the filter options and click **Apply** to view the filtered items.

4. On the **Files** pane, select the files to which you want to apply labels.

> **Note:** Before you apply labels to the files, you can view the previously applied labels of the files in the preview pane.

5. In the preview pane, click the **Text View** or **Native View** icon to toggle between the file views.

   Text view displays the file content in the plain text format. Whereas, the native view displays the file content in the original format, for example, MS Word, PDF, and so on.

6. (Optional) In the preview pane, click the download icon to save file on your local computer.
7. On the action menu, click **Label**.
8. In the **Add/Remove Labels** dialog box, select the labels you want to apply to the files.

   You can clear the labels if these are not required anymore. In case you have selected multiple files the **Add/Remove Labels** dialog box shows applied level status as follows:

- The check box that is not selected yet means this label is not at all applied to the selected files.
- The check box with the dash mark means the label is applied to some of the selected files, but not applied to all the selected files.
- The check box with the tick mark means the label is applied to all the selected files.

1. Select the required labels, and click **Apply Changes**.

   After you apply labels to the files, these labeled files are available under the respective labels under the **labels** node.

2. To ensure if the label is applied to the files, select the emails, and expand the **Labels** section to view its details in the right pane.

Applying tags to the Advanced ECA search items

You can apply new tags to emails, collaboration messages, and files that are filtered during the Advanced ECA search. You can also view the previously applied tags and classification tags of the items. The following sections explains how to apply tags to these search items.

Applying tags to collaboration messages in Advanced ECA search

To apply tags to the collaboration messages in Advanced ECA search:

1. On the **Investigations** tab, select **Managed Accounts**>**Advanced ECA**.

2. Select the Advanced ECA search in which you want to tag the records. The search result opens in the right pane.
3. Set the filter options and click **Apply** to view the filtered items.
4. In the right pane, on the **Collaboration** tab, select the collaboration messages to which you want to apply tags.

> **Note:** Before you apply tags to the items, you can view the previously applied tags and classification tags of the message in the preview pane. In the following sample image, you can see the previously applied tags and classification tags of the collaboration messages when you hover over the icons.

5. On the action menu, click **Tag**, and do any of the following as required.
   - To tag all the items in the search, click **Tag all messages**.
   - To tag only the selected items, click **Tag selected messages**.
6. In the **Add Tag** dialog box, specify the following:

TAG NAME	ENTER A NEW UNIQUE TAG NAME.
Comments	Provide a comment or a description for the tag name.
Legal Hold	Select this check box if you want to apply the legal hold on the emails.
Select retention Tag	Instead of applying a new tag, you can apply the retention tags that are created in Arctera Unified Platform. To access and apply those retention tags, select this option, and choose the tags you want to apply.
	After you select this option, the application disables the Tag Name field.

7. Click **Tag**.

   After you apply tags to the emails, these tagged emails are available under the respective tags under the **Tags** node.

Applying tags to emails in Advanced ECA search

To apply tags to emails in Advanced ECA search:

1. On the **Investigations** tab, select **Managed Accounts**>**Advanced ECA**.
2. Select the Advanced ECA search in which you want to tag the records. The search result opens in the right pane.
3. Set the filter options and click **Apply** to view the filtered items.
4. In the right pane, on the **Emails** tab, select one or more emails to which you want to apply tags.

> **Note:** Before you apply tags to the items, you can view the previously applied tags of the items in the preview pane. However, you need to select only one item at a time to view the tags. In the following sample image, you can see the previously applied tags and retention tags to the email in the **Emails** tab.

5. To add a tag to an individual item, click the item to preview its details in the preview pane, and click **Tag** as shown in the image above.
6. To add a tag to multiple items, on the action menu, click **Tag**, and select any of the following options as required.
   - To tag all the items in the search, click **Tag all emails**.
   - To tag all the items in the current page, click **Tag current page**.
   - To tag only the selected items, click **Tag selected emails**.
7. In the **Add Tag** dialog box, specify the following:

TAG NAME	ENTER A NEW UNIQUE TAG NAME.
Comments	Provide a comment or a description for the tag name.
Legal Hold	Select this check box if you want to apply the legal hold on the emails.
Select retention Tag	Instead of applying a new tag, you can apply the retention tags that are created in Arctera Unified Platform. To access and apply those retention tags, select this option, and choose the tags you want to apply.

TAG NAME	ENTER A NEW UNIQUE TAG NAME.
	After you select this option, the application disables the Tag Name field.

8. Click **Tag**.

   After you apply tags to the emails, these tagged emails are available under the respective tags under the **Tags** node.

Applying tags to files in Advanced ECA search

To apply tags to files in Advanced ECA search:

1. On the **Investigations** tab, select **Managed Accounts**>**Advanced ECA**.
2. Select the Advanced ECA search in which you want to tag the records. The search result opens in the right pane.
3. Set the filter options and click **Apply** to view the filtered items.
4. On the **Files** tab, select the files to which you want to apply tags.

> **Note:** Before you apply tags to the items, you can view the previously applied tags of the file in the preview pane. You can see the previously applied tags and retention tags to the file.

5. On the action menu, click **Tag**, and do any of the following as required.
   - To tag all the items in the search, click **Tag all files**.
   - To tag only the selected items, click **Tag selected files**.
6. In the **Add Tag** dialog box, specify the following:

TAG NAME	ENTER A NEW UNIQUE TAG NAME.
Comments	Provide a comment or a description for the tag name.
Legal Hold	Select this check box if you want to apply the legal hold on the emails.

TAG NAME	ENTER A NEW UNIQUE TAG NAME.
Select retention Tag	Instead of applying a new tag, you can apply the retention tags that are created in Arctera Unified Platform. To access and apply those retention tags, select this option, and choose the tags you want to apply.
	After you select this option, the application disables the Tag Name field.

7. Click **Tag**.

   After you apply tags to the emails, these tagged emails are available under the respective tags under the **Tags** node.

Exporting an Advanced ECA search summary report

This section describes the exporting the summary report for emails, collaboration messages, and files.

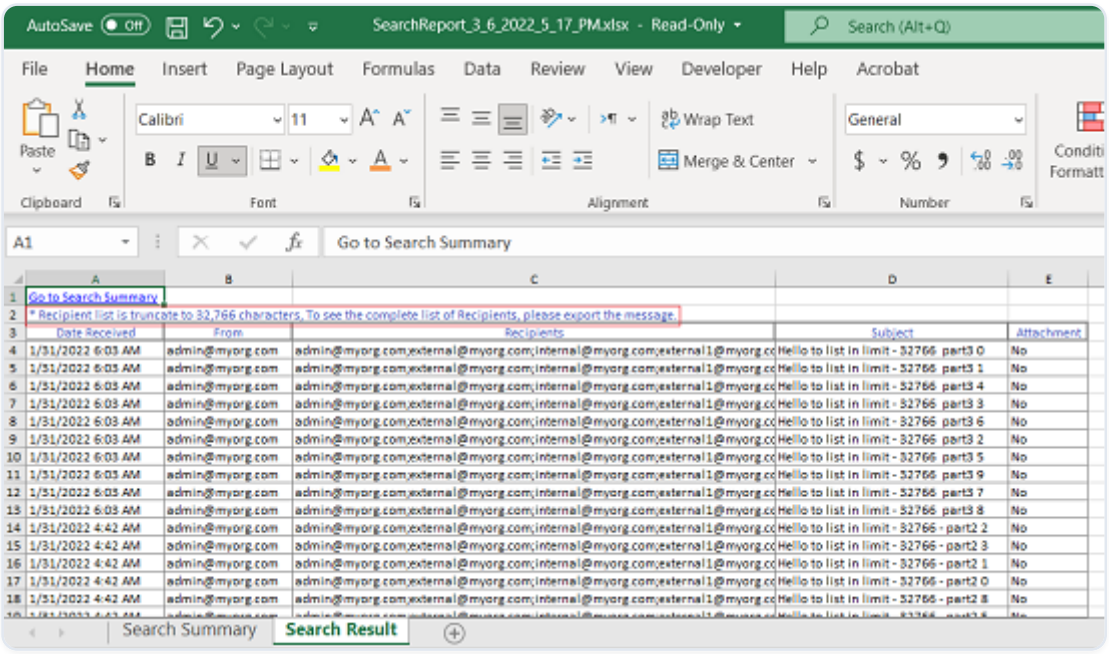
Exporting a search summary report for emails

To export an Advanced ECA search summary report for emails:

1. On the **Investigations** tab, select **Managed Accounts**>**Advanced ECA**.
2. Select the Advanced ECA search for which you want to export the summary report.

   The search result opens in the right pane.
3. On the **Emails** tab, click the **More Actions** icon, and click **Export Report**.

   The application downloads the summary report (.xlsx) of the emails within the Advanced ECA search as a zipped (.zip) folder. A sample report is shown below. The report comprises of two sheets.



> **Note:** TheSearch Summarysheet displays details such as Search Parameters and Custodians. TheSearch Resultsheet displays details such as Date Received, From, Recipients, Subject, and Attachments. The recipient column in this summary report includes recipients mentioned in the To, CC, and BCC fields. If the list of recipients is longer than 32766 characters, the application truncates the list. The report displays a note that -Recipient list is truncate to 32,766 characters, To see the complete list of Recipients, please export the message.In such scenario, to view the complete list of recipients, you need to export the individual message.

Exporting summary report for collaboration messages

To export an Advanced ECA search summary report for collaboration messages:

1. Select the required search under the Research Sets or the Review Sets node.
2. On the **Investigations** tab, select **Managed Accounts**>**Advanced ECA**.
3. Select the search for which you want to export the summary report.

   The search result opens in the right pane.
4. On the **Collaboration** tab, and click **Export Report**.

   The application downloads the summary report (.xlsx) of the collaboration messages within the search as a zipped (.zip) folder.

Exporting summary report for files

To export an Advanced ECA search summary report for files:

1. On the **Investigations** tab, select **Managed Accounts**>**Advanced ECA**.
2. Select the Advanced ECA search for which you want to export the summary report.

   The search result opens in the right pane.
3. On the **Files** tab, and click **Export Report**.

   The application downloads the summary report (.xlsx) of the files within the Advanced ECA search as a zipped (.zip) folder.

Exporting the Advanced ECA search items

You can export maximum 50000 records at a time.

Exporting collaboration messages from Advanced ECA search

To export collaboration messages from Advanced ECA search:

1. On the **Investigations** tab, select **Managed Accounts**>**Advanced ECA**.
2. Select the Advanced ECA search in which you want to filter the records and export the required collaboration messages from the search.

   The search result opens in the right pane.
3. Set the filter options and click **Apply** to view the filtered items.
4. On the **Collaboration** tab, select the check box for one or more messages (conversations) to which you want to apply labels, and click **Export**. Do any of the following:

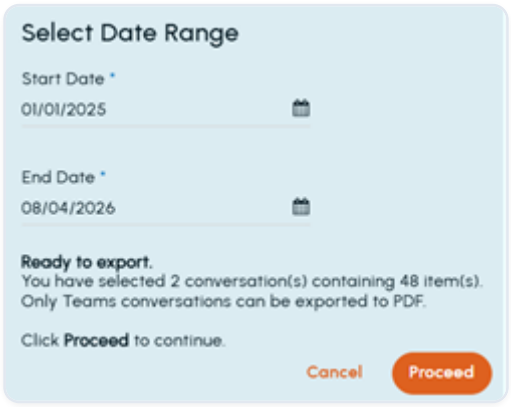
   - Click **Export selected messages** to export only the selected messages.
   - Click **Export all messages** to export all the available collaboration messages within the search.

   In both the scenarios, the **Export Options** dialog box appears with the following fields:

MESSAGE FORMAT	SELECT THE APPROPRIATE MESSAGE FORMAT FOR BATCH EXPORT. OPTIONS INCLUDE\:
	- JSON NOTE: THIS FORMAT IS SELECTED BY DEFAULT. WHEN YOU SELECT JSON FORMAT FOR EXPORT, FILES ARE DOWNLOADED IN THEIR ORIGINAL FORM, AND NOT AS JSON.
	- EDRM ONLY
Enable AES-256 Encryption	Select this check-box if you want to secure the access of the downloaded export batch.
Export Name	Provide the name for the batch you want to export. By default, it takes the Search Name. You can change it if required.
Export Password	Enter the password that you want end user to provide when they access this exported batch of messages.
Confirm Password	Repeat the same password for confirmation.
Generate Azure SAS URL	**Note:** Users can see this button only if the **Export to Azure private storage location** feature in the Arctera Management Console is enabled for them. Users can export items to their private Azure Blob storage location.
	Click Generate Azure SAS URL to get the Azure Blob SAS URL to access the location and save it for future use.
	For security reasons, the application does not show this URL the next time. However, if the SAS URL is misplaced for any reason, click Generate Azure SAS URL again to generate a new SAS URL and save it securely.
	After you click Export on the Export Options dialog box, all the selected items are exported to the Azure private storage location. You can

MESSAGE FORMAT	SELECT THE APPROPRIATE MESSAGE FORMAT FOR BATCH EXPORT. OPTIONS INCLUDE\:
	- JSON NOTE: THIS FORMAT IS SELECTED BY DEFAULT. WHEN YOU SELECT JSON FORMAT FOR EXPORT, FILES ARE DOWNLOADED IN THEIR ORIGINAL FORM, AND NOT AS JSON.
	- EDRM ONLY
	use Microsoft Storage Explorer to access the exported items.
Share Export	Click Select Admin to choose the recipients of this batch export and click Update.
	Note: You need to manually share the Export Password with the administrators and follow all the security specific rules of the organization.

- Click **Print selected conversations** to print the selected conversations. A**Select Date Range **dialog box appears. Specify the **Start Date **and **End Date** to retrieve conversations within the selected date range.



> **Note:**
>
> - The **Print selected conversations** option is visible only when at least one Microsoft Teams collector is configured and applies only to Microsoft Teams conversations.

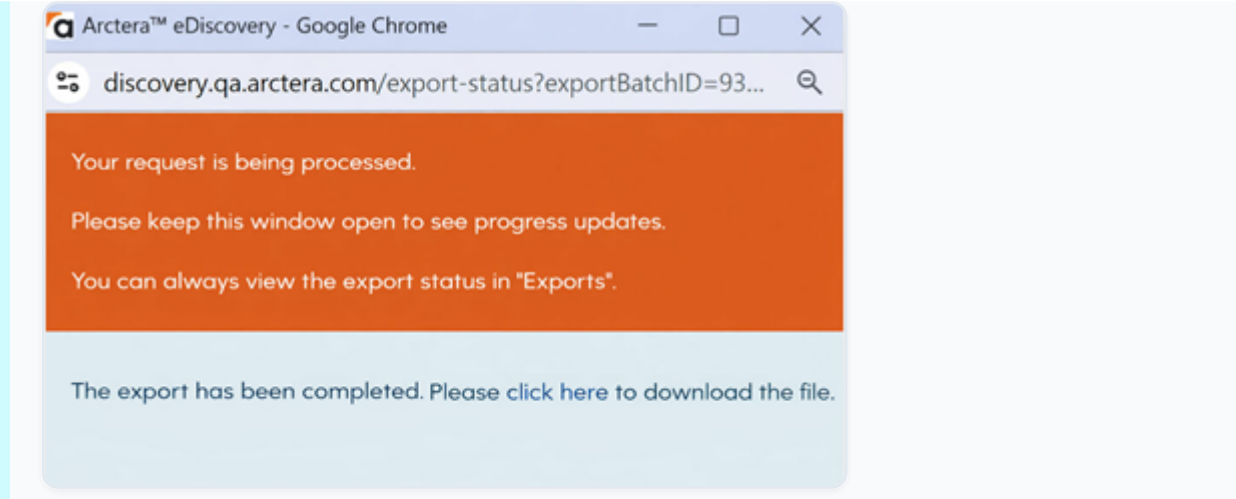
- If conversations are not available for the selected date range, the **Proceed** option remains disabled. Modify the date range to retrieve conversations, and then click **Proceed**.

In this scenarios, the **Export Options** dialog box appears with the following fields:

MESSAGE FORMAT	SELECT THE APPROPRIATE MESSAGE FORMAT FOR BATCH EXPORT.
	CURRENTLY, PDF IS THE DEFAULT AND ONLY AVAILABLE FORMAT FOR BATCH EXPORT.
Enable AES-256 Encryption	Select this check-box if you want to secure the access of the downloaded export batch.
Export Name	Provide the name for the batch you want to export. By default, it takes the Search Name. You can change it if required.
Export Password	Enter the password that you want end user to provide when they access this exported batch of messages.
Confirm Password	Repeat the same password for confirmation.
Share Export	Click Select Admin to choose the recipients of this batch export and click Update.
	Note: You need to manually share the Export Password with the administrators and follow all the security specific rules of the organization.

1. Click **Export**.

Note: The exported batch can either gets downloaded as a single or multiple file segments.



2. Click **Click here** to download the exported batch of messages.
3. To confirm the status of batch export, on the **Investigations** tab, select **Exports**, and search this export batch name.

Exporting emails from Advanced ECA search

To export emails from Advanced ECA search:

1. On the **Investigations** tab, select **Managed Accounts**>**Advanced ECA**.
2. Select the Advanced ECA search in which you want to filter the records and export the required emails from the search.The search result opens in the right pane.
3. Set the filter options and click **Apply** to view the filtered items.
4. In the right pane, select the emails you want to export.
5. Click **Export**, and do any of the following:
   - Click **Export current page** to export emails that are available on the current page.
   - Click **Export selected emails** to export all the selected emails from the search.
   - Click **Export all emails** to export all the emails available in the search.
6. In the **Export Options** dialog box, do the following:

FIELD	DESCRIPTION
Message Format	Select the appropriate message format. By default, the **PST** format is selected. The available message formats are:**•Clearwell•EML•EML with EDRM•PST with EDRM•MSG with EDRM•FTI-RingTail•EDRM Only•PST**When exporting

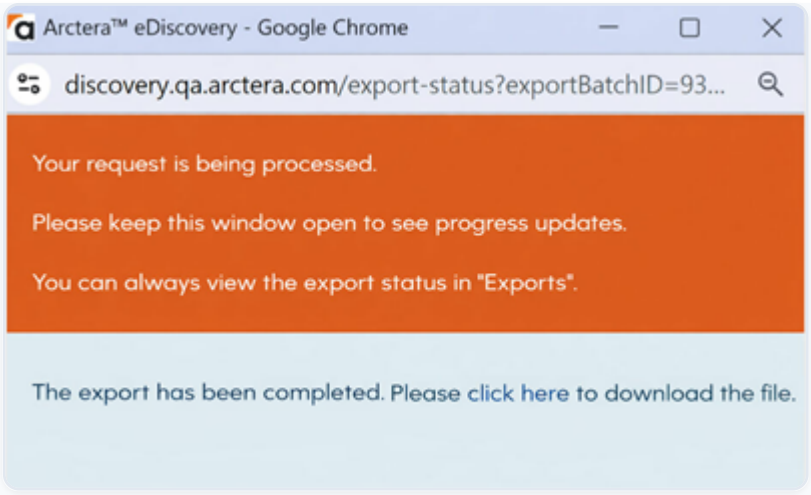
FIELD	DESCRIPTION
	messages to PST, the export may fail or stop responding if the batch contains calendar invitations with very large embedded attachments, such as oversized Base64 files. In such cases, the export may show failed items, and a usable PST file may not be generated. Resubmitting the same failed items may result in the same export failure.To resolve this issue, the Arctera eDiscovery application excludes only the oversized Base64 attachment from the item being exported. The calendar invitation itself is still exported with its key details, such as subject, organizer, attendees, date, time, location, message body, and reminders.During export, if an oversized Base64 embedded attachment is excluded, a **Skipped_Attachments_Report.csv** file is generated in the export output folder. Reviewers can refer to this report to identify the affected items and understand which attachments were excluded from the PST export.•**Original EDRM**If you select this option, the exported file includes emails in both MSG and EML formats, allowing you to work with the emails in the format that best suits your needs. In addition, the exported file includes the **edrmXML.xml** and **HTMLReport.html** files in their original formats. These files facilitate the smooth transfer of electronically stored information (ESI) between different software programs during the electronic discovery process.•**Original**If you select this option, the exported file includes emails in both MSG and EML formats, allowing you to work with the emails in the format that best suits your needs.**Note:** The **Original EDRM** and **Original** message formats are available only to users listed in the **Configuration_Override** table in the Arctera

FIELD	DESCRIPTION
	Unified Platform database. To make these options available in the **Message Format** drop-down field, contact Arctera Support.
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 check box to secure access to the downloaded export batch.
Export Name	Specify a name for the export batch. By default, the search name is used. You can change it if required.
Export Password	Enter the password that users must provide to access the exported batch of messages.
Confirm Password	Re-enter the password for confirmation.
Generate Azure SAS URL	**Note:** This button is available only if the **Export to Azure private storage location** feature is enabled for your account in the Arctera Management Console.Click **Generate Azure SAS URL** to generate the Azure Blob SAS URL for your private storage location and save it for future use.For security reasons, the application does not display the URL the next time. If you lose the URL, click **Generate Azure SAS URL** again to generate a new URL and save it securely.After you click **Export** in the **Export Options** dialog box, the selected items are exported to the Azure private storage location. You can use Microsoft Storage Explorer to access the exported items.
Share Export	Click **Select Admin** to choose the recipients of the export batch, and then click **Update**.**Note:** You must manually share the

FIELD	DESCRIPTION
	export password with the administrators and follow your organization's security policies.

7. Click **Export**.

> **Note:** The exported batch can either gets downloaded as a single or multiple file segments.



8. Click **Click here** to download the exported batch of messages.
9. To confirm the status of batch export, on the **Investigations** tab, select **Exports**, and search this export batch name.

Exporting files from Advanced ECA search

To export files from Advanced ECA search:

1. On the **Investigations** tab, select **Managed Accounts**>**Advanced ECA**.
2. Select the Advanced ECA search in which you want to filter the records and export the required files from the search.

   The search result opens in the right pane.
3. Set the filter options and click **Apply** to view the filtered files.
4. Select the files you want to export.
5. Click **Export**, and do any of the following:

   - Click **Export selected files** to export all the selected files from the search.

- Click **Export all files** to export all the files available in the Advanced ECA search.

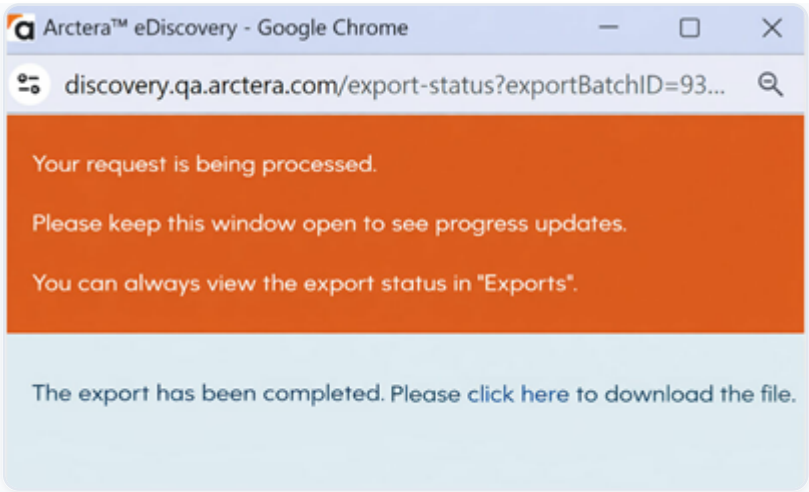
6. In the **Export Options** dialog box, do the following:

MESSAGE FORMAT	SELECT THE APPROPRIATE MESSAGE FORMAT FOR BATCH EXPORT. OPTIONS INCLUDE\:
	- JSON NOTE: THIS FORMAT IS SELECTED BY DEFAULT. WHEN YOU SELECT JSON FORMAT FOR EXPORT, FILES ARE DOWNLOADED IN THEIR ORIGINAL FORM, AND NOT AS JSON.
	- EDRM ONLY
Enable AES-256 Encryption	Select this check-box if you want to secure the access of the downloaded export batch.
Export Name	Provide the name for the batch you want to export. By default, it takes the Search Name. You can change it if required.
Export Password	Enter the password that you want end user to provide when they access this exported batch of messages.
Confirm Password	Repeat the same password for confirmation.
Generate Azure SAS URL	**Note:** Users can see this button only if the **Export to Azure private storage location** feature in the Arctera Management Console is enabled for them. Users can export items to their private Azure Blob storage location.
	Click Generate Azure SAS URL to get the Azure Blob SAS URL to access the location and save it for future use.
	For security reasons, the application does not show this URL the next time. However, if the SAS URL is misplaced for any reason, click Generate Azure SAS URL again to

MESSAGE FORMAT	SELECT THE APPROPRIATE MESSAGE FORMAT FOR BATCH EXPORT. OPTIONS INCLUDE\:
	- JSON NOTE: THIS FORMAT IS SELECTED BY DEFAULT. WHEN YOU SELECT JSON FORMAT FOR EXPORT, FILES ARE DOWNLOADED IN THEIR ORIGINAL FORM, AND NOT AS JSON.
	- EDRM ONLY
	generate a new SAS URL and save it securely.
	After you click Export on the Export Options dialog box, all the selected items are exported to the Azure private storage location. You can use Microsoft Storage Explorer to access the exported items.
Share Export	Click Select Admin to choose the recipients of this batch export and click Update.
	Note: You need to manually share the Export Password with the administrators and follow all the security specific rules of the organization.

7. Click **Export**.

> **Note:** The exported batch can either gets downloaded as a single or multiple file segments.



8. Click **Click here** to download the exported batch of messages.
9. To confirm the status of batch export, on the **Investigations** tab, select **Exports**, and search this export batch name.

Creating an Advanced ECA search

You can create an advanced ECA search in the following ways:

- Create a new search and save it as an Advanced ECA search, as explained in this section.
- Update the existing standard search under the Managed Accounts node. See Updating an on-going or a standard search from Managed Accounts.

To create an Advanced ECA search:

1. On the **Investigations** tab, select **Managed Accounts**>**New Search**.
2. Perform advanced search or query search to get the expected items. See Performing Advanced Search and Query Search.
3. Click **Save Search**.
4. In the **Save Search** dialog box, enter a unique name for the search.
5. Select the **Advanced ECA** check box.

> **Note:** After you select the Advanced ECA check box, the application disables the **Tag name** field, the **On-going** check box, and the **Legal Hold** check box.

6. To send this search to a particular case, select the **Send to Case** check box, and select a valid case from the drop-down list.

> **Note:** The **Keep copy in Investigations** remains selected by default. When you send the Advanced ECA search from the **Investigations** tab to a Case in the **eDiscovery** tab, it gets saved under **Research Sets**. After sending this Advanced ECA search to Case, it may show different result (email count) depending on the custodians selected in the **Case Setup** option. For AI-enabled cases,**Send to Case** supports only email items, and any non-email items (such as files and collaboration messages) are automatically skipped.

7. Click **Save**.

   The search appears under the Advanced ECA node in the left navigation pane.

   After the search is created, you can select the appropriate filter options to refine the search results. For example, under **Filters**, expand **FormatType** and select **MS Teams** to view only MS teams related search results.

   In a single Advanced ECA search, the application can save maximum 1000000 records each for emails, collaboration messages, and files.

> **Note:** If the Advanced ECA search processing fails, you need to click **Please try again** to retry processing. If this search fails consecutively, you need to delete the search and create a new search again.

Deleting an Advanced ECA search

To delete an Advanced ECA search:

1. On the **Investigations** tab, select **Managed Accounts**>**Advanced ECA**.
2. Select the Advanced ECA search that you want to delete.

   The search result opens in the right pane.
3. Click **Delete Saved Search**.

   The application prompts you to confirm that you want to perform the operation.
4. Click **Yes** to complete the operation or click **No** to cancel it.

   The application deletes the search from the Advanced ECA node.

Filtering an Advanced ECA search

To filter an Advanced ECA search:

1. On the **Investigations** tab, select **Managed Accounts**.
2. Select the already existing Advanced ECA search that you want to filter.

   The search opens in the right pane.
3. Expand **Search Criteria** to view the criteria based on which this Advanced ECA search is created. You cannot edit the search criteria of Advanced ECA search.
4. Expand **Filters**, and click **Apply** to view the total number of records captured while saving this Advanced ECA search.

   > **Note:** ClickingApplyis a mandatory action to view correct number of filtered records in the Advanced ECA search. In a single Advanced ECA search, the application can save maximum 1000000 records each for emails, collaboration messages, and files. Out of 1000000 records, the application displays only 50000 email records to users based on the filters applied. Users need to set the filter criteria carefully to filter desired archived items. If number of filtered item messages is greater than 50000, the application displays the following message: Too many items match the filter. The review set is capped at 50000 items.
5. Under **Filters**, select or clear corresponding filter options.

   The **Filters** section provides the following filter options that you can select or clear based on the idea of record analysis. To reset all filter options simultaneously, click **Clear**. You cannot save the filter criteria. After you clear the filter options, you need to set the filter options again.

FILTER NAME	ACTION
Subject	Specify any word or a term that is used in the Subject statement of a Search item.
Author	Specify the author of that email or message.
FormatType	Select this option to filter records based on format type.
SourceType	Select one or more required source types to filter items collected from them.
	For more information, See Performing Advanced Search and Query Search.

FILTER NAME	ACTION
Direction	Selects items that are traveling in a certain direction (incoming, outgoing, or interoffice communications).
MessageDate	Specify the duration of the records you want to search. You can customize the date range.
PolicyAction	Selects items by the policy action with which your policy management software has tagged them. This action can be one of the following\:
	- Inclusion (demands or suggests capture)
	- Exclusion (precludes capture or advocates non-capture)
	- No Action (the item is subject to normal random sampling)
PolicyName	Specify the specific policy with which your policy management software has tagged the items you want to filter.
SentimentScore	Classifies and displays the records based on their sentiment score. Click the displayed options to view those specific records.
TagValue	Select the specific tags to filter items to which these tags are applied.
Label	Select the specific labels to filter items to which these labels are applied.
HasAttachments	Specify if you want to filter records that have or have not the attachments to them.

1. Click **Apply** to view the filtered records from the selected Advanced ECA search.

Printing the selected Advanced ECA searched items

To print the selected Advanced ECA searched items:

1. On the **Investigations** tab, select **Managed Accounts**>**Advanced ECA**.
2. Select the Advanced ECA search in which you want to filter the records for printing.

   The search result opens in the right pane.
3. Set the filter options and click **Apply** to view the filtered items.
4. To print emails, on the **Emails** tab, select the items you want to print. Click the **More Actions** icon, and click **Print**.

   A separate dialog box appears and displays the metadata and the content of the items ready for printing.
5. To print files, on the **Files** tab, select the file you want to print. Click the **Download** icon to save that file on your local computer, and then print it.
6. Ensure that the content is the same you want to print. Click **Print** and save the document as PDF.

Reassigning emails from the Advanced ECA search

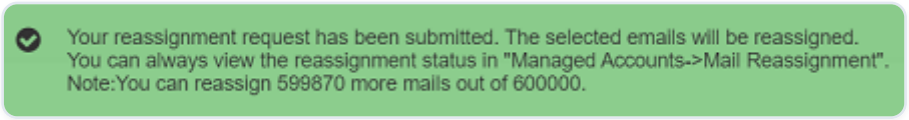
To reassign emails from the Advanced ECA search:

1. On the **Investigations** tab, select **Managed Accounts**>**Advanced ECA**.
2. Select the Advanced ECA search in which you want to filter the records for reassigning to specific accounts.

   The search result opens in the right pane.
3. Set the filter options and click **Apply** to view the filtered items.
4. In the right pane, select the items you want to reassign.
5. Click **Reassign Mails**, and do the following:

   - To reassign selected emails, click **Reassign selected emails**.
   - To reassign emails displayed on one page, click **Reassign emails in current page**.

   The application displays the sample message as follows:



Updating an Advanced ECA search

To update an Advanced ECA search:

1. On the **Investigations** tab, select **Managed Accounts**.
2. Select the Advanced ECA search that you want to update for its name.

   The searched items appear in the details pane.
3. Click **Update Search**.
4. Enter a unique name for the search.
5. Click **Update**.

Working with searched collaboration messages

In Arctera eDiscovery, you can collect the Microsoft Teams data. To view and review the Microsoft Teams specific communication, you can access the Collaboration tab after creating a search. This tab is visible only if -

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

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.

Applying labels to collaboration messages

To help organize your work you can apply labels to the collaboration messages. Labels are applied to collaboration messages typically to mark them as exempt from the review process.

To apply a label to collaboration messages:

1. On the **Investigations** tab, create a new search or select the searches from the On-going searches or Standard searches node.
2. Perform advanced search or query search to get the expected items. See Performing Advanced Search and Query Search.

The application displays result.

3. On the **Collaboration** tab, select the check box for one or more messages (chats) to which you want to apply labels.
4. On the action menu, click **Label**.
5. In the **Add/Remove Labels** dialog box, select the labels you want to apply to the messages.

   You can clear the labels if these are not required anymore. In case you have selected multiple collaboration messages, the **Add/Remove Labels** dialog box shows applied level status as follows:

- The check box that is not selected yet means this label is not at all applied to the selected messages.
- The check box with the dash mark means the label is applied to some of the selected messages, but not applied to all the selected messages.
- The check box with the tick mark means the label is applied to all the selected messages.

1. Select the required labels, and click **Apply Changes**.

   After you apply labels to the collaboration messages, these labeled messages are available under the respective labels under the **labels** node.
2. To ensure if the label is applied to the message, select the message to view its details in the right pane. Hover over the blue Label icon to view all the labeled messages.

   - To view all the applied labels in the **Labels** popup, click the blue-colored Label icon.
   - You can click any label in the **Labels** popup to navigate to the respective label under the **Labels** node.

Applying tags, legal hold tags and retention tags to collaboration messages

To help organize your work you can tag emails with custom tags of your own choice, which are visible only to you. You can also tag messages with a Retention tags (also called as managed tags), if you have any of these available to you. Retention tags are created in the Arctera Management Console, under the My Config > Managed Tags node. For more information on managed tags, see the Arctera Management Console help.

To apply tags, legal hold tags and retention tags to collaboration messages:

1. On the **Investigations** tab, create a new search or select the searches from the On-going searches, Standard searches, or Advanced ECA nodes.

2. Perform advanced search or query search to get the expected items. See Performing Advanced Search and Query Search.

   The application displays result.

3. On the **Collaboration** tab, select the check box for one or more messages (chats) that you want to tag.
4. On the action menu, click **Tag**, and do any of the following as required.

   - To tag only the selected messages, click **Tag selected messages**.
   - To tag all the messages in the search, click **Tag all messages**.

5. In the **Add Tag** dialog box, specify the following:

TAG NAME	ENTER A NEW UNIQUE TAG NAME.
Comments	Provide a comment or a description for the tag name.
Legal Hold	Select this check box if you want to apply the legal hold on the messages.
Select retention Tag	Instead of applying a new tag, you can apply the retention tags that are created in Arctera Unified Platform. To access and apply those retention tags, select this option, and choose the tags you want to apply.

6. Click **Tag**.

   After you apply tags to the collaboration messages, these tagged messages are available under the respective tags under the **Tags** node.

7. To ensure if the tag is applied to the message, select the message to view its details in the right pane. Hover over the black Tag icon to view all the tags applied to this message.

   You can click the black Tag icon to view all the applied tags in the **Tags** popup.

   You can click any tag in the **Tags** popup to navigate to the respective tag under the **Tags** node.

Note

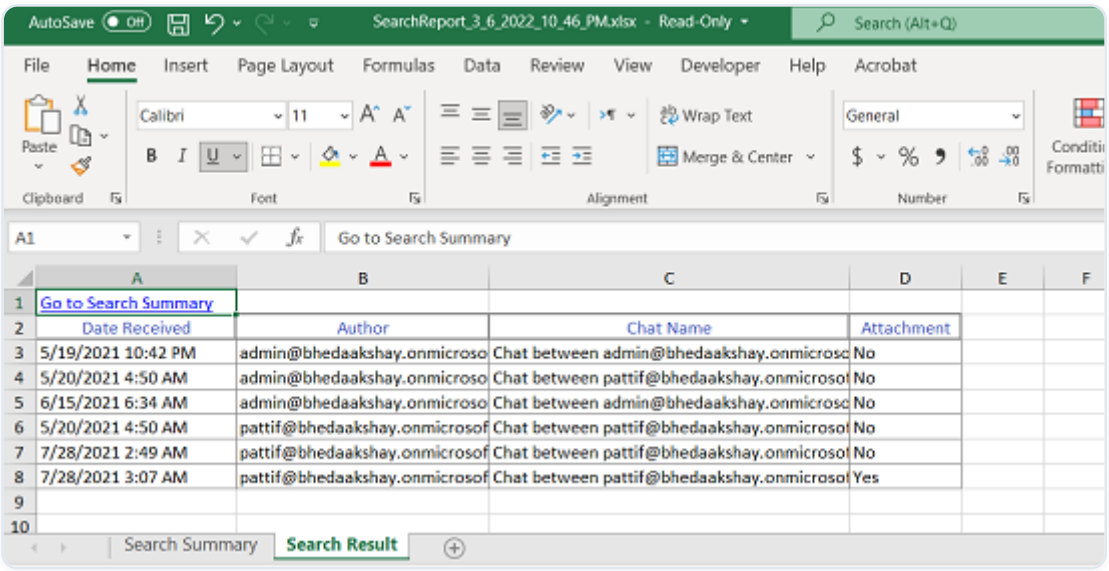
- The default limit for applying tags and legal hold in a search result is 1000000 items, including emails, collaboration messages, and files. For any technical support, contact Arctera Support via your system administrator.
- The application displays a notification indicating that tagging is in progress and may take some time to complete.

Exporting a search summary report for collaboration messages

To export a search summary report for collaboration messages:

1. On the **Investigation** tab, select the search for which you want to export a summary report.
2. Click **New Search** to create a new search. Else, expand **On-going Searches** or **Standard Searches** to select existing search.
3. On the **Collaboration** tab, and click **Export Report**.

   The application downloads the summary report (.xlsx) of the collaboration messages within search as a zipped (.zip) folder. A sample report is shown below. The report comprises of two sheets.



Note

- **Search Summary**: This sheet displays details such as *Search Parameters* and *Custodians*.
- **Search Result**: This sheet displays details such as *Date Received*, *Author*, Chat Names (list of people involved in chat), and *Attachments*.

- The **Chat Name** column displays the email addresses of message recipients involved in a chat. This column supports up to 100 characters; any text beyond this limit is truncated in the exported report.

Exporting collaboration messages

You can export a batch of collaboration messages and share it with the concerned authority for the intended use. To secure the information, you can use the AES-256 encryption while creating a batch of collaboration messages for export. After exporting the batch of messages, you can download and share it with others.

To export a batch of collaboration messages:

1. On the **Investigations** tab, create a new search or select the searches from the On-going searches or Standard searches node.
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.
3. On the **Collaboration** tab, select the check box for one or more messages (conversations) to which you want to apply labels, and click **Export**. Do any of the following:

   - Click **Export selected messages** to export only the selected messages.
   - Click **Export all messages** to export all the available collaboration messages within the search.

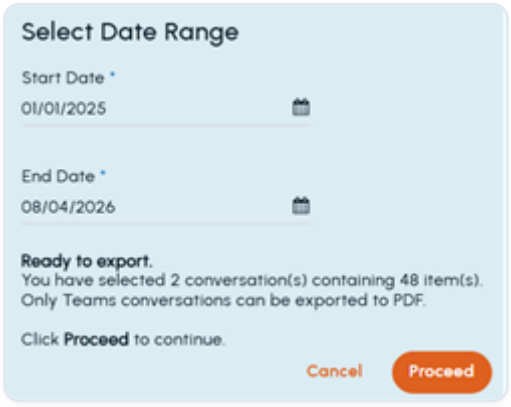
   In both the scenarios, the **Export Options** dialog box appears with the following fields:

MESSAGE FORMAT	SELECT THE APPROPRIATE MESSAGE FORMAT FOR BATCH EXPORT. OPTIONS INCLUDE\:
	- JSON NOTE: THIS FORMAT IS SELECTED BY DEFAULT. WHEN YOU SELECT JSON FORMAT FOR EXPORT, FILES ARE DOWNLOADED IN THEIR ORIGINAL FORM, AND NOT AS JSON.
	- EDRM ONLY
Enable AES-256 Encryption	Select this check-box if you want to secure the access of the downloaded export batch.

MESSAGE FORMAT	SELECT THE APPROPRIATE MESSAGE FORMAT FOR BATCH EXPORT. OPTIONS INCLUDE\:
	- JSON NOTE: THIS FORMAT IS SELECTED BY DEFAULT. WHEN YOU SELECT JSON FORMAT FOR EXPORT, FILES ARE DOWNLOADED IN THEIR ORIGINAL FORM, AND NOT AS JSON.
	- EDRM ONLY
Export Name	Provide the name for the batch you want to export. By default, it takes the Search Name. You can change it if required.
Export Password	Enter the password that you want end user to provide when they access this exported batch of messages.
Confirm Password	Repeat the same password for confirmation.
Generate Azure SAS URL	**Note:** Users can see this button only if the **Export to Azure private storage location** feature in the Arctera Management Console is enabled for them. Users can export items to their private Azure Blob storage location.
	Click Generate Azure SAS URL to get the Azure Blob SAS URL to access the location and save it for future use.
	For security reasons, the application does not show this URL the next time. However, if the SAS URL is misplaced for any reason, click Generate Azure SAS URL again to generate a new SAS URL and save it securely.
	After you click Export on the Export Options dialog box, all the selected items are exported to the Azure private storage location. You can use Microsoft Storage Explorer to access the exported items.

MESSAGE FORMAT	SELECT THE APPROPRIATE MESSAGE FORMAT FOR BATCH EXPORT. OPTIONS INCLUDE\:
	- JSON NOTE: THIS FORMAT IS SELECTED BY DEFAULT. WHEN YOU SELECT JSON FORMAT FOR EXPORT, FILES ARE DOWNLOADED IN THEIR ORIGINAL FORM, AND NOT AS JSON.
	- EDRM ONLY
Share Export	Click Select Admin to choose the recipients of this batch export and click Update.
	Note: You need to manually share the Export Password with the administrators and follow all the security specific rules of the organization.

- Click **Print selected conversations** to print the selected conversations. A**Select Date Range **dialog box appears. Specify the **Start Date **and **End Date** to retrieve conversations within the selected date range.



Note:

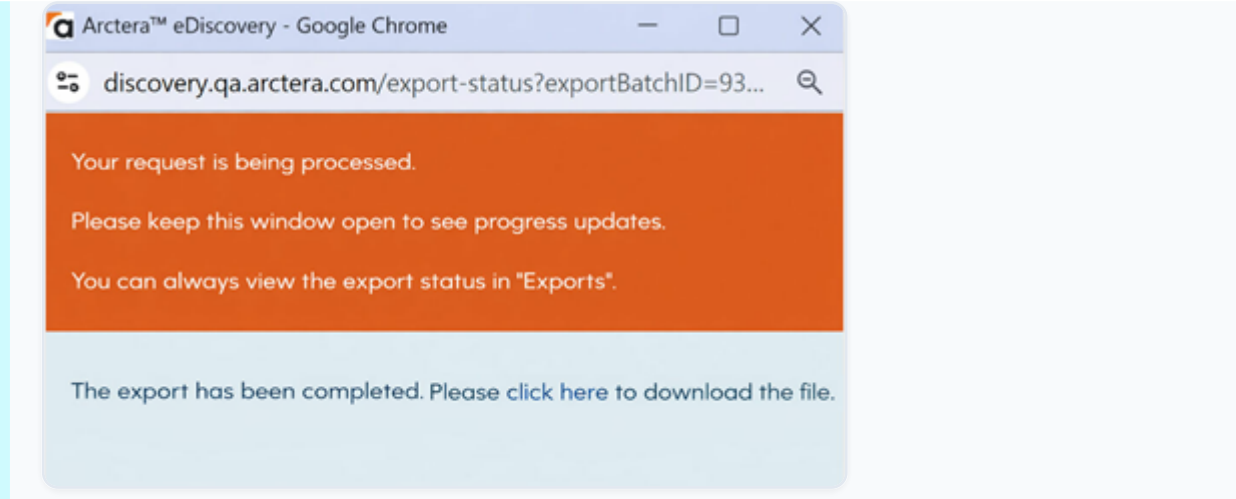
- The **Print selected conversations** option is visible only when at least one Microsoft Teams collector is configured and applies only to Microsoft Teams conversations.
- If conversations are not available for the selected date range, the **Proceed** option remains disabled. Modify the date range to retrieve conversations, and then click **Proceed**.

In this scenarios, the **Export Options** dialog box appears with the following fields:

MESSAGE FORMAT	SELECT THE APPROPRIATE MESSAGE FORMAT FOR BATCH EXPORT.
	CURRENTLY, PDF IS THE DEFAULT AND ONLY AVAILABLE FORMAT FOR BATCH EXPORT.
Enable AES-256 Encryption	Select this check-box if you want to secure the access of the downloaded export batch.
Export Name	Provide the name for the batch you want to export. By default, it takes the Search Name. You can change it if required.
Export Password	Enter the password that you want end user to provide when they access this exported batch of messages.
Confirm Password	Repeat the same password for confirmation.
Share Export	Click Select Admin to choose the recipients of this batch export and click Update.
	Note: You need to manually share the Export Password with the administrators and follow all the security specific rules of the organization.

1. Click **Export**.

Note: The exported batch can either gets downloaded as a single or multiple file segments.



2. Click **Click here** to download the exported batch of messages.
3. To confirm the status of batch export, on the **Investigations** tab, select **Exports** and check the status of your export.

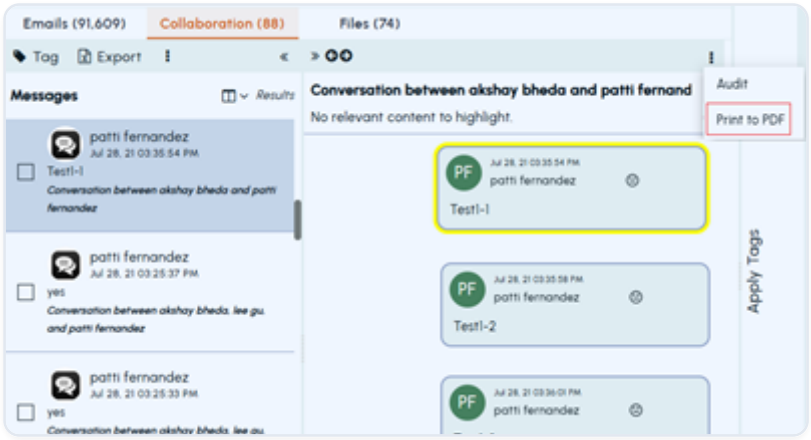
Printing MS Teams messages to PDF during investigation

You can print collaboration messages collected from the *MS Teams* collectors using the Print to PDF feature. This feature is exclusive to *MS Teams* collaboration messages and is not supported for messages collected from other archive collectors. It is available when you select the collected MS Teams item and preview its content no matter the item is collected and accessed from the following nodes:

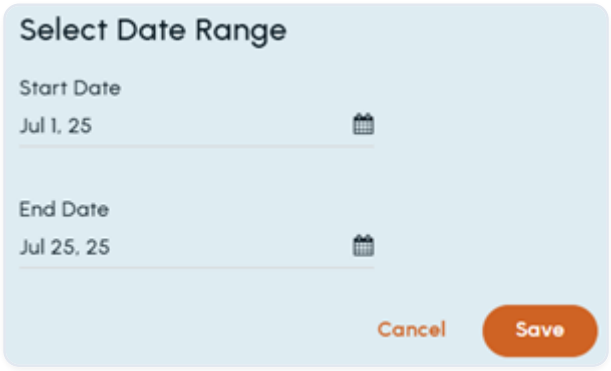
- *Managed Accounts* (MS Teams messages that are collected during new searches, as well as when examining items from previous searches, ongoing searches, standard searches, and advanced ECA searches.)
- *Labels*
- *Legal Holds*
- *Tags*
- *Retention Tags*

To print MS Teams messages to PDF during investigation:

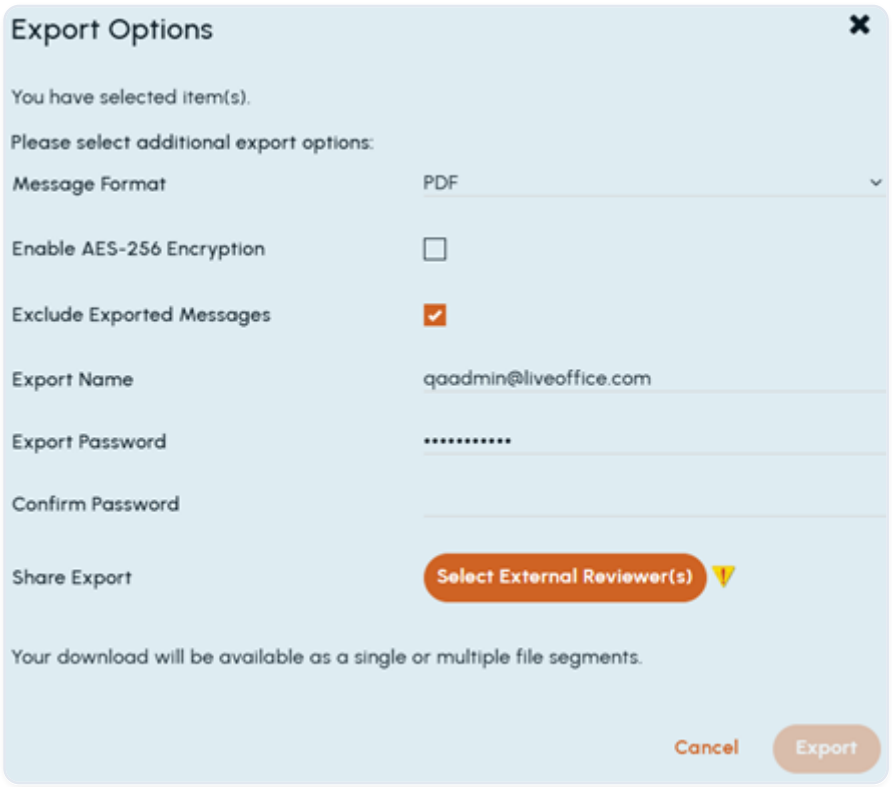
1. From the **Investigations** tab, select the required search or node (Labels, Legal Hold, Tags, or Retention Tags).
2. On the **Collaboration** tab, select the collaboration message you want to print to PDF.
3. Click the **More options** icon and select **Print To PDF**.



The application displays the **Select Date Range** as shown in the following sample image.



4. Specify the date range and click **Save**.
5. In the **Export Options** dialog box, specify the following details:



MESSAGE FORMAT	THE PDF FORMAT IS SELECTED BY DEFAULT.
Enable AES-256 Encryption	Select this check-box if you want to secure the access of the downloaded export batch.
Exclude Exported Messages	Select this option to exclude the exported messages.
Export Name	Provide the name for the batch you want to export. By default, it takes the Search Name. You can change it if required.
Export Password	Enter the password that you want end user to provide when they access this exported batch of messages.
Confirm Password	Repeat the same password for confirmation.
Share Export	Click Select Admin(s) to choose the recipients of this batch export and click Update.
	Note: You need to manually share the Export Password with the administrators and follow all the security specific rules of the organization.

6. Click **Export**.

   A browser appears showing the progress. Upon completion, click the **Click here** link to download the PDF.

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 > New Search**.
- To search a single managed account, select **Managed Accounts > Accounts** and click the required account.
- To search one or more of your managed accounts select **Managed Accounts > New Search**.

2. Perform advanced search or query search to get the expected items. See Performing Advanced Search and Query Search.
3. Click **Search**.

   The search result appears.
4. Click **Save Search**.

   See Saving searches in Review sets and Research sets.

Working with searched emails

This section describes the tasks that a user can perform with the searched emails.

Applying labels to emails

To help organize your work you can apply labels to the emails. Labels are applied to emails typically to mark them as exempt from the review process.

To apply a label to emails:

1. On the **Investigations** tab, create a new search or select the searches from the On-going searches or Standard searches node.
2. Perform advanced search or query search to get the expected items. See Performing Advanced Search and Query Search.

   The application displays result.
3. On the **Emails** tab, select the check box for one or more emails to which you want to apply labels.
4. On the action menu, click **Label**.
5. In the **Add/Remove Labels** dialog box, select the labels you want to apply to the emails.

You can clear the labels if these are not required anymore. In case you have selected multiple emails, the **Add/Remove Labels** dialog box shows applied level status as follows:

- The check box that is not selected yet means this label is not at all applied to the selected emails.
- The check box with the dash mark means the label is applied to some of the selected emails, but not applied to all the selected emails.
- The check box with the tick mark means the label is applied to all the selected emails.

6. Select the required labels, and click **Apply Changes**.

   After you apply labels to the emails, these labeled emails are available under the respective labels under the **Labels** node.

7. To ensure if the label is applied to the email, select the email to view its details in the right pane, and expand **Labels**.

   You can click any label in the **Labels** popup to navigate to the respective label under the **Labels** node. See the sample image below

Applying tags, legal hold tags and retention tags to emails

You can apply tags, legal hold tags and retention tags to the searched emails.

To apply tags, legal hold tags and retention tags to emails:

1. On the **Investigations** tab, navigate to any of the following locations, as required:

   - **Managed Accounts**>**New Search**.
   - **Managed Accounts**>**On-going Searches**.
   - **Managed Accounts**>**Standard Searches**.

2. Create a new search or select the existing search in which you want to tag the items.

   The application displays the searched items in the right pane.

3. Set the filter options and click **Apply** to view the filtered items.
4. In the right pane, on the **Emails** tab, select one or more emails to which you want to apply tags.

> **Note:** Before you apply tags to the items, you can view the previously applied tags of the items in the preview pane. However, you need to select only one item at a time to view

the tags. In the following sample image, you can see the previously applied tags and retention tags to the email in the **Emails** tab.

5. On the action menu, click **Tag**, and do any of the following as required.
   - To tag all the items in the search, click **Tag all emails**.
   - To tag all the items in the current page, click **Tag current page**.
   - To tag only the selected items, click **Tag selected emails**.
6. In the **Add Tag** dialog box, specify the following:

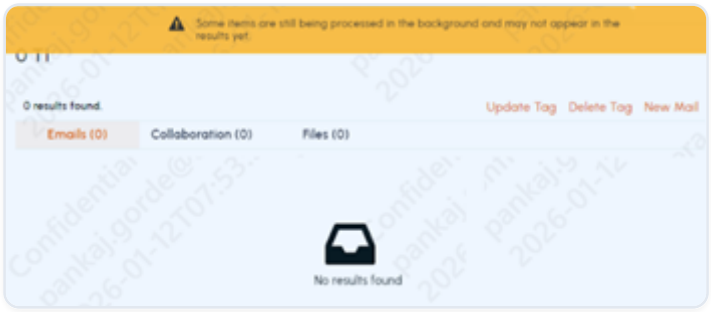
TAG NAME	ENTER A NEW UNIQUE TAG NAME.
Comments	Provide a comment or a description for the tag name.
Legal Hold	Select this check box if you want to apply the legal hold on the emails.
Select retention Tag	Instead of applying a new tag, you can apply the retention tags that are created in Arctera Unified Platform. To access and apply those retention tags, select this option, and choose the tags you want to apply.
	After you select this option, the application disables the Tag Name field.

7. Click **Tag**.

   After you apply tags to the emails, these tagged emails are available under the respective tags under the **Tags** node.

Note

- The default limit for applying tags and legal hold in a search result is 1000000 items, including emails, collaboration messages, and files. For any technical support, contact Arctera Support via your system administrator.
- The application displays a notification indicating that tagging is in progress and may take some time to complete.



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 enable **Privilege Delete** to company level, see **Configuring archive options** in the *Management Console Help*. For information on how to enable **Privilege Delete** to administrators, see **Editing the built-in administrator roles** in the *Management Console Help*.

To delete emails:

1. Under **Managed Accounts**, navigate to **New search**, and then conduct a search.
2. If required, select the check box 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 **Yes**.

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

5. To check the status of the deleted emails, navigate to **Deleted items** under **Managed 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.

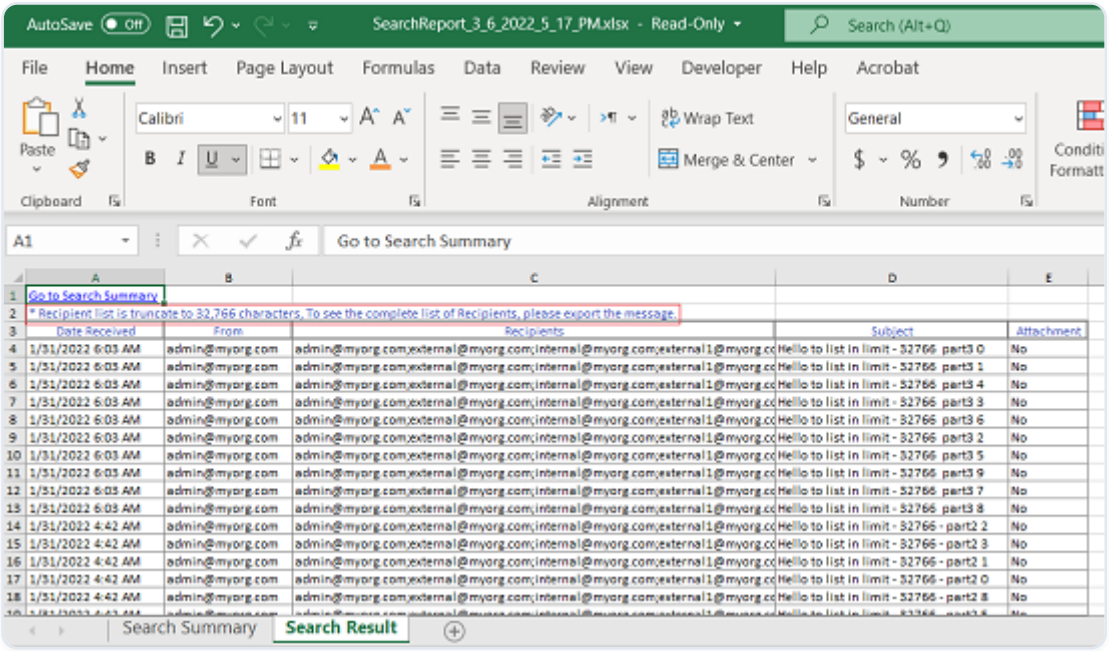
  The email on legal hold has Legal hold tag, Legal hold search, or Legal hold Custodian in a Case applied. To delete an email marked on legal hold, first, remove any applicable legal hold that has been previously applied.

Exporting a search summary report for emails

To export a search summary report for emails:

1. On the **Investigation** tab, select the search for which you want to export a summary report.
2. Click **New Search** to create a new search. Else, expand **On-going Searches** or **Standard Searches** to select existing search.
3. On the **Emails** tab, click the **More Actions** icon, and click **Export Report**.

   The application downloads the summary report (.xlsx) of the emails within the search as a zipped (.zip) folder. A sample report is shown below. The report comprises of two sheets.



> **Note:** TheSearch Summarysheet displays details such as Search Parameters and Custodians. TheSearch Resultsheet displays details such as Date Received, From,

Recipients, Subject, and Attachments. The recipient column in this summary report includes recipients mentioned in the To, CC, and BCC fields. If the list of recipients is longer than 32766 characters, the application truncates the list. The report displays a note that -Recipient list is truncate to 32,766 characters, To see the complete list of Recipients, please export the message.In such scenario, to view the complete list of recipients, you need to export the individual message.

Exporting searched emails

You can export a batch of emails and share it with the concerned authority for the intended use. To secure the information, you can use the AES-256 encryption while creating a batch of emails for export. After exporting the batch of emails, you can download and share it with others.

To export a batch of emails:

1. On the **Investigations** tab, create a new search or select the searches from the On-going searches or Standard searches node.
2. Perform advanced search or query search to get the expected items. See Performing Advanced Search and Query Search.

   The application displays result.
3. On the **Emails** tab, select the check box for one or more emails, and click **Export**. Do any of the following:
   - Click **Export current page** export emails that are available on the current page.
   - Click **Export selected emails** to export only the selected emails.
   - Click **Export all emails** to export all the available emails within the search.
4. In the **Export Options** dialog box, specify the following:

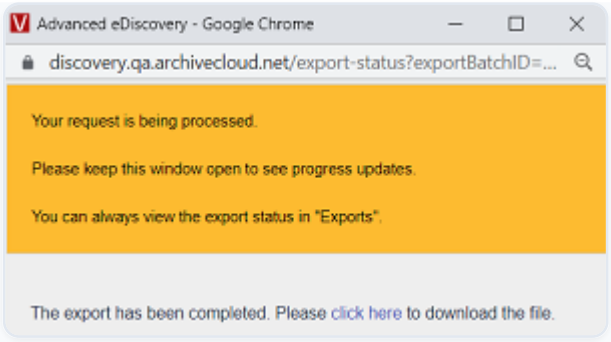
FIELD	DESCRIPTION
Message Format	Select the appropriate message format. By default, the **PST** format is selected. The available message formats are:**•Clearwell•EML•EML with EDRM•PST with EDRM•MSG with EDRM•FTI-RingTail•EDRM Only•PST**When exporting messages to PST, the export may fail or stop responding if the batch contains calendar

FIELD	DESCRIPTION
	invitations with very large embedded attachments, such as oversized Base64 files. In such cases, the export may show failed items, and a usable PST file may not be generated. Resubmitting the same failed items may result in the same export failure.To resolve this issue, the Arctera eDiscovery application excludes only the oversized Base64 attachment from the item being exported. The calendar invitation itself is still exported with its key details, such as subject, organizer, attendees, date, time, location, message body, and reminders.During export, if an oversized Base64 embedded attachment is excluded, a **Skipped_Attachments_Report.csv** file is generated in the export output folder. Reviewers can refer to this report to identify the affected items and understand which attachments were excluded from the PST export.•**Original EDRM**If you select this option, the exported file includes emails in both MSG and EML formats, allowing you to work with the emails in the format that best suits your needs. In addition, the exported file includes the **edrmXML.xml** and **HTMLReport.html** files in their original formats. These files facilitate the smooth transfer of electronically stored information (ESI) between different software programs during the electronic discovery process.•**Original**If you select this option, the exported file includes emails in both MSG and EML formats, allowing you to work with the emails in the format that best suits your needs.**Note:** The **Original EDRM** and **Original** message formats are available only to users listed in the **Configuration_Override** table in the Arctera Unified Platform database. To make these

FIELD	DESCRIPTION
	options available in the **Message Format** drop-down field, contact Arctera Support.
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 check box to secure access to the downloaded export batch.
Export Name	Specify a name for the export batch. By default, the search name is used. You can change it if required.
Export Password	Enter the password that users must provide to access the exported batch of messages.
Confirm Password	Re-enter the password for confirmation.
Generate Azure SAS URL	**Note:** This button is available only if the **Export to Azure private storage location** feature is enabled for your account in the Arctera Management Console.Click **Generate Azure SAS URL** to generate the Azure Blob SAS URL for your private storage location and save it for future use.For security reasons, the application does not display the URL the next time. If you lose the URL, click **Generate Azure SAS URL** again to generate a new URL and save it securely.After you click **Export** in the **Export Options** dialog box, the selected items are exported to the Azure private storage location. You can use Microsoft Storage Explorer to access the exported items.
Share Export	Click **Select Admin** to choose the recipients of the export batch, and then click **Update**.**Note:** You must manually share the export password with the administrators and follow your organization's security policies.

5. Click **Export**.

> **Note:** The exported batch can either gets downloaded as a single or multiple file segments.



6. Click **Click here** to download the exported batch of emails.
7. To confirm the status of batch export, on the **Investigations** tab, select **Exports**.

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 Arctera eDiscovery, administrators can search and view these hidden emails.

To hide emails:

1. Under **Managed Accounts**, conduct a **New search**.
2. Perform advanced search or query search to get the expected items. See Performing Advanced Search and Query Search.
3. Select the emails that you want to hide.
4. Click **Hide/Unhide me**, and select an option to specify which emails to hide or unhide.
5. Select the option to **Hide selected emails** or **Hide email in current page**.

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

> **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.

6. Click **Yes**.
7. Execute the same search again.

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

   To unhide emails:
8. Under **Monitored Accounts**, conduct a **New search**.
9. Perform advanced search or query search to get the expected items. See Performing Advanced Search and Query Search.
10. Select the emails that you want to unhide.
11. Click the **Hide/Unhide me** icon, and select the emails that are hidden previously.
12. Select the option to **Unhide selected emails** or **Unhide email in current page**.

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

> **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.

13. Click **Yes**.
14. 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.

Reassigning emails

To understand email reassigning, See About Mail Reassignment.

Working with searched files

In Arctera eDiscovery, you can collect the data from OneDrive for Business and Audio-Video archive collectors. To view and review the files, you can access the Files tab after creating a search. This tab is visible only if -

- The OneDrive for Business service is enabled and the OneDrive for Business collector is configured.
- The Audio-Video service is enabled and the Audio-Video collector is configured.

Applying labels to files

To help organize your work you can apply labels to the files. Labels are applied to files typically to mark them as exempt from the review process.

To apply a label to files:

1. On the **Investigations** tab, create a new search or select the searches from the On-going searches or Standard searches node.
2. Perform advanced search or query search to get the expected items. See Performing Advanced Search and Query Search.

   The application displays result.
3. On the **Files** tab, select the check box for one or more files to which you want to apply labels.
4. On the action menu, click **Label**.
5. In the **Add/Remove Labels** dialog box, select the labels you want to apply to the files.

   You can clear the labels if these are not required anymore. In case you have selected multiple files, the **Add/Remove Labels** dialog box shows applied level status as follows:

- The check box that is not selected yet means this label is not at all applied to the selected files.
- The check box with the dash mark means the label is applied to some of the selected files, but not applied to all the selected files.
- The check box with the tick mark means the label is applied to all the selected files.

1. Select the required labels, and click **Apply Changes**.

   After you apply labels to the files, these labeled files are available under the respective labels under the **Labels** node.

2. To ensure if the label is applied to the files, select the file to view its details in the right pane, and expand **Labels**.

   You can click any label in the **Labels** popup to navigate to the respective label under the **Labels** node.

Applying tags, legal hold tags and retention tags to files

To apply tags, legal hold tags and retention tags to files:

1. On the **Investigations** tab, navigate to any of the following locations, as required:
   - **Managed Accounts**>**New Search**.
   - **Managed Accounts**>**On-going Searches**.
   - **Managed Accounts**>**Standard Searches**.
2. Create a new search or select the existing search in which you want to tag the files.

   The application displays the searched items in the right pane.
3. Set the filter options and click **Apply** to view the filtered files.
4. In the right pane, on the **Files** tab, select one or more files to which you want to apply tags.

   > **Note:** Before you apply tags to the files, you can view the previously applied tags of the files in the preview pane. However, you need to select only one file at a time to view the tags. In the following sample image, you can see the previously applied tags and retention tags to the file in the **Files** tab.

5. On the action menu, click **Tag**, and do any of the following as required.
   - To tag all the files in the search, click **Tag all files**.
   - To tag only the selected items, click **Tag selected files**.
6. In the **Add Tag** dialog box, Specify the following:

TAG NAME	ENTER A NEW UNIQUE TAG NAME.
Comments	Provide a comment or a description for the tag name.

TAG NAME	ENTER A NEW UNIQUE TAG NAME.
Legal Hold	Select this check box if you want to apply the legal hold on the files.
Select retention Tag	Instead of applying a new tag, you can apply the retention tags that are created in Arctera Unified Platform. To access and apply those retention tags, select this option, and choose the tags you want to apply.
	After you select this option, the application disables the Tag Name field.

7. Click **Tag**.

   After you apply tags to the files, these tagged files are available under the respective tags under the **Tags** node.

Note

- The default limit for applying tags and legal hold in a search result is 1000000 items, including emails, collaboration messages, and files. For any technical support, contact Arctera Support via your system administrator.
- The application displays a notification indicating that tagging is in progress and may take some time to complete.

Exporting a search summary report for files

To export a search summary report for files:

1. On the **Investigation** tab, select the search for which you want to export a summary report.
2. Click **New Search** to create a new search. Else, expand **On-going Searches** or **Standard Searches** to select existing search.
3. On the **Files** tab, and click **Export Report**.

   The application downloads the summary report (.xlsx) of the files within the search as a zipped (.zip) folder. The report comprises of two sheets.

   The **Search Summary** sheet displays details such as Search Parameters and Custodians.

The **Search Result** sheet displays details such as Date Received, list of people involved, and Attachments.

Exporting searched files

You can export a batch of files and share it with the concerned authority for the intended use. To secure the information, you can use the AES-256 encryption while creating a batch of files for export. After exporting the batch of files, you can download and share it with others.

To export a batch of files:

1. On the **Investigations** tab, create a new search or select the searches from the On-going searches or Standard searches node.
2. Perform advanced search or query search to get the expected items. See Performing Advanced Search and Query Search.

   The application displays result.
3. On the **Files** tab, select the check box for one or more files, and click **Export**. Do any of the following:

   - Click **Export selected files** to export only the selected files.
   - Click **Export all files** to export all the available files within the search.
4. In the **Export Options** dialog box, specify the following:

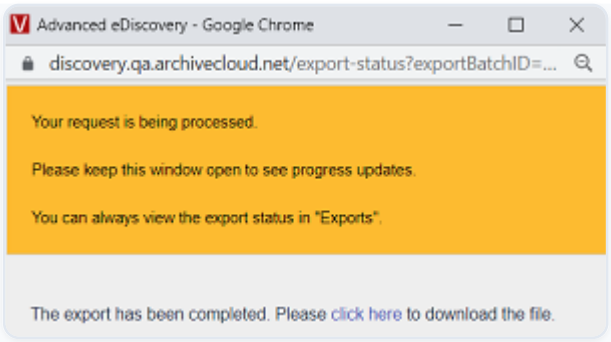
MESSAGE FORMAT	SELECT THE APPROPRIATE MESSAGE FORMAT FOR BATCH EXPORT. OPTIONS INCLUDE\:
	- JSON NOTE: THIS FORMAT IS SELECTED BY DEFAULT. WHEN YOU SELECT JSON FORMAT FOR EXPORT, FILES ARE DOWNLOADED IN THEIR ORIGINAL FORM, AND NOT AS JSON.
	- EDRM ONLY
Enable AES-256 Encryption	Select this check-box if you want to secure the access of the downloaded export batch.
Export Name	Provide the name for the batch you want to export. By default, it takes the Search Name. You can change it if required.

MESSAGE FORMAT	SELECT THE APPROPRIATE MESSAGE FORMAT FOR BATCH EXPORT. OPTIONS INCLUDE\:
	- JSON NOTE: THIS FORMAT IS SELECTED BY DEFAULT. WHEN YOU SELECT JSON FORMAT FOR EXPORT, FILES ARE DOWNLOADED IN THEIR ORIGINAL FORM, AND NOT AS JSON.
	- EDRM ONLY
Export Password	Enter the password that you want end user to provide when they access this exported batch of files.
Confirm Password	Repeat the same password for confirmation.
Generate Azure SAS URL	**Note:** Users can see this button only if the **Export to Azure private storage location** feature in the Arctera Management Console is enabled for them. Users can export items to their private Azure Blob storage location.
	Click Generate Azure SAS URL to get the Azure Blob SAS URL to access the location and save it for future use.
	For security reasons, the application does not show this URL the next time. However, if the SAS URL is misplaced for any reason, click Generate Azure SAS URL again to generate a new SAS URL and save it securely.
	After you click Export on the Export Options dialog box, all the selected items are exported to the Azure private storage location. You can use Microsoft Storage Explorer to access the exported items.
Share Export	Click Select Admin to choose the recipients of this batch export and click Update.

MESSAGE FORMAT	SELECT THE APPROPRIATE MESSAGE FORMAT FOR BATCH EXPORT. OPTIONS INCLUDE\:
	- JSON NOTE: THIS FORMAT IS SELECTED BY DEFAULT. WHEN YOU SELECT JSON FORMAT FOR EXPORT, FILES ARE DOWNLOADED IN THEIR ORIGINAL FORM, AND NOT AS JSON.
	- EDRM ONLY
	Note: You need to manually share the Export Password with the administrators and follow all the security specific rules of the organization.

5. Click **Export**.

> **Note:** The exported batch can either gets downloaded as a single or multiple file segments.



6. Click **Click here** to download the exported batch of files.
7. To confirm the status of batch export, on the **Investigations** tab, select **Exports**. The application displays status of performed exports.

Working with Audio-Video files

Arctera eDiscovery supports managing the archived audio-video files. The audio-video files can be collected from the Audio-Video collectors if these services are enabled for you.

The currently supported formats are as follows:

- Video Formats: MP4, MOV, WebM, MPEG-4, and OGG

- Audio Formats: MP3, WAV, OGG, AAC, and WebM

After executing a search, the audio-video files are listed under the Files tab. When you select the audio-video file, its details are displayed in the File Metadata pane.

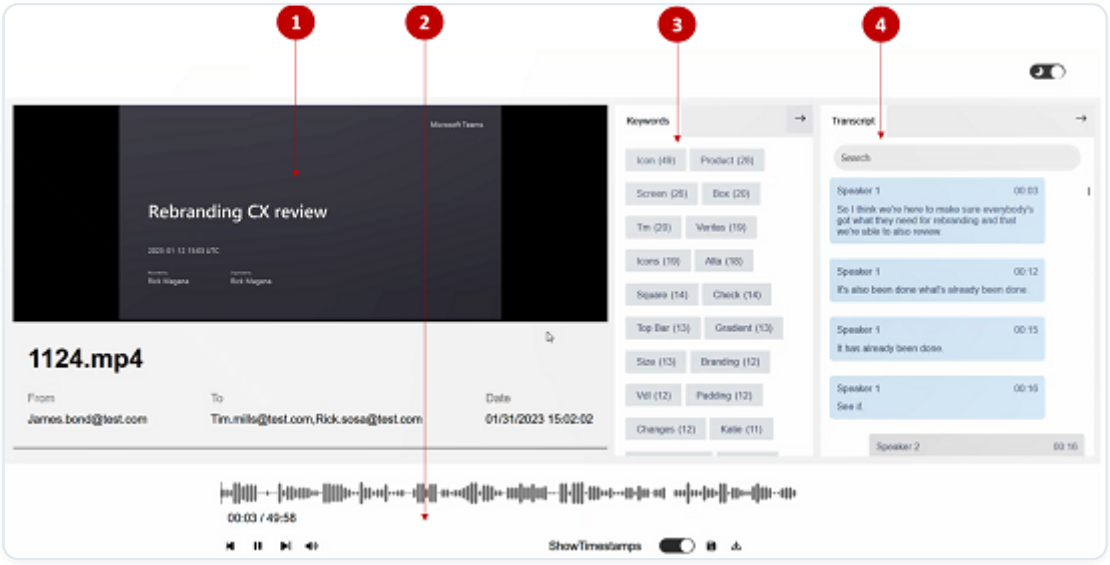
The AI Transcription of the audio-video content appears. Unlike other file formats, you cannot directly view the audio or video files in the native format in the File Metadata pane.

Expand the Labels section to view the labels applied to the file.

To view the audio-video file in its native format:

- Search for and select the file, and do any of the following:
  - Click the **Download** icon to save the file on your local computer.
  - Click the **Native viewer** icon available in the top-right corner of the **File Metadata** pane.

The selected file opens in a separate window in its native format.



1\. Native view

This panel displays the audio-video file in its original format.

2\. Control panel

This panel provides options to rewind, forward, pause, and control audio level of the file. In addition, it provides options to download, save, and view/hide time stamps.

3\. Keywords

This panel lists the keywords and the exact count of those keywords in the audio-video content. Click the keyword to navigate to the respective content in the audio-video file and play from that point onwards.

4\. AI Transcript

This panel displays the AI transcript of the audio-video content. to navigate to the respective content in the audio-video file and play from that point onwards.

Like other files, you can apply tags and labels to the audio-video files. You can move these files to production sets and export to the intended user. Only the AI transcripts of these files are exportable in PDF format. You can apply annotations and redactions to these PDF files for review purposes. Refer to the sample image of exported AI transcript file.

About Hit Highlighting

Hit highlighting visually marks important terms within the item preview pane to quickly identify relevant content. These terms include the terms matched by your search criteria as well as terms in any associated tags.

Highlighting applies to the subject line, message body, attachment names, and the text or HTML preview of attachments. Search terms are highlighted in *orange*, while tags are highlighted in *green*. You can hover over a highlighted term to identify whether it originated from a query or a tag.

To help you review content efficiently, the preview pane includes a drop-down list showing all matched terms along with their occurrence counts. You can select *All* to view every highlighted term or choose a specific term to focus only on its instances. This targeted highlighting enables faster review of search results, especially when navigating through large message bodies or attachments.

To understand hit highlighting precisely, refer to the following scenario.

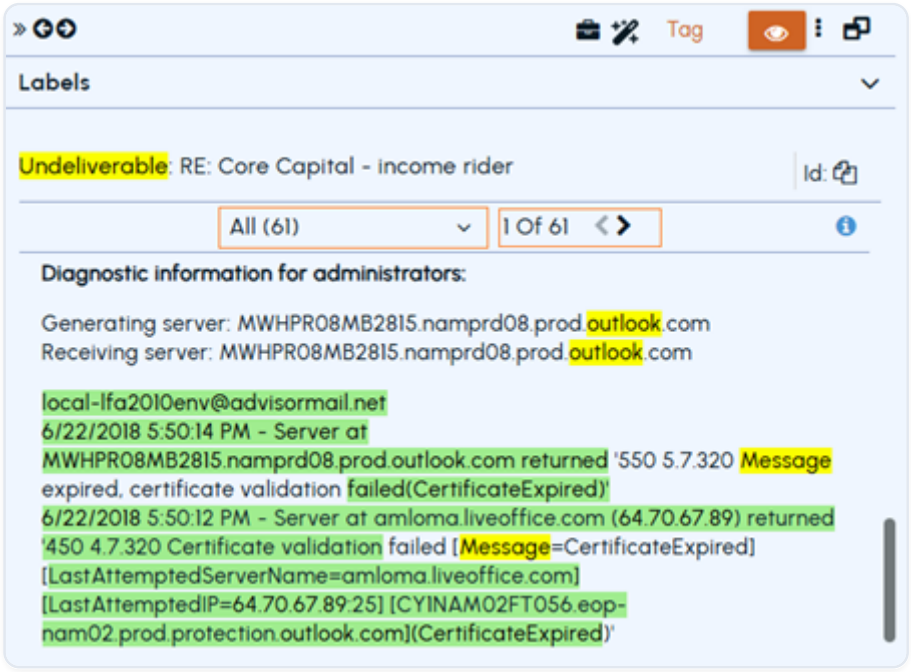
1. Create a new search or open an existing one by performing one of the following actions:
    - On the **Investigation** tab, expand **Managed Accounts** and click **New Search**; or select an existing search from previously created searches, *ongoing searches, standard searches, or advanced ECA searches*.

- On the **eDiscovery** tab, click **Cases**, search for and select a case. The selected case appears under Cases. Click **New Search** to create a new one, or expand *Research Sets* or *Review Sets* to select an existing search.

2. Use *Advanced Search* or *Query Search* to define your criteria for filtering relevant emails, collaboration content, or files. Click **Search**.

   The filtered items (emails, collaboration messages, and files) in the items grid.

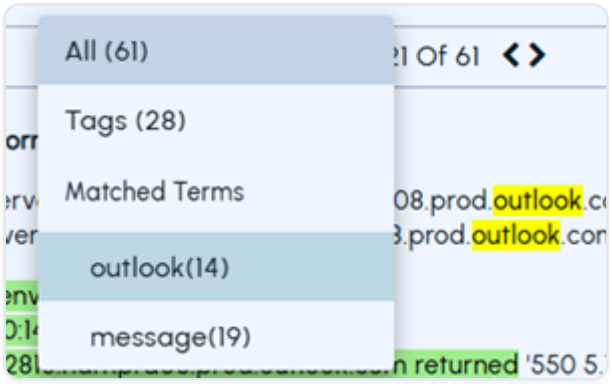
3. From the items grid, click the item you want to review. The selected item opens in the preview pane on the right.
4. In the preview pane, click the drop-down arrow to view a list of matched terms and the number of occurrences for each term.



- Use the previous and next arrows to navigate between term hits in the message body.

> **Note:** Though highlighting applies to the subject line, message body, attachment name, and the text or HTML preview of attachments, navigation is only available within the message body content.

- Select *All* to view all highlighted terms, or select a specific term to highlight only its occurrences.



Capabilities

- Supports stop words and special characters
- Handles multi-byte characters
- Highlights terms across line breaks
- Applies highlighting in Native Viewer
- Works with tenants where stop word indexing is enabled
- Supports proximity-based searches
- Provides navigation between highlighted terms

Known Limitations

- Does not highlight search terms with leading or trailing special characters
- Counts/includes stop words in highlights within Native Viewer
- Does not support highlighting in Query Search
- Cannot highlight non-visible metadata such as image information or indexed item metadata

About Investigations

From the Arctera eDiscovery Investigations tab, administrators or reviewers can conduct initial, probative, or Active Directory 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 items 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 items of interest as in the eDiscovery tab. The difference is that in the Investigations tab the search and the work that you do with the items is not tracked as part of a case. Also in investigations the review status tags are not available.

In investigations, permission to view the items 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 Managed Accounts

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 Active Directory 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 eDiscovery tab to track these searches.

Creating archive sets during investigation

To create an archive set during investigation:

1. On the **Investigations** tab, select **Managed Accounts**. and do any of the following:
    - Select **New Search** to execute a search.
    - Expand **On-going Searches** or **Standard Searches** as required, and select the required saved search.
2. To send all the items of the search to a collection set, click **Send to Case**.

    To send specific items of the search to a collection set, search for and select them, and then click **Send to Case**. For AI-enabled cases,**Send to Case** supports only email items, and any non-email items (such as files and collaboration messages) are automatically skipped.
3. In the **Send to Case - Create Archive Set** dialog box, specify the following:

CASES	SEARCH AND SELECT THE CASE IN WHICH YOU WANT TO CREATE AN ARCHIVE SET AND DOCUMENTS ACCORDINGLY.
Archive Set name	To create a new Archive Set, select New and provide a unique name for the archive set you want to create.
	To send the items in the existing Archive Set, select Existing. The application displays a list of existing archive sets, then select the required archive set.
	Sending this search result from Investigations to a Case in eDiscovery ignores the custodian(s) selected in the Case setup.

> **Note:** The default limit for sending search results to an archive set is 1000000 items, including emails, collaboration messages, and files. This limit can be adjusted based on customer requirements, but customers cannot modify it themselves. They can contact Arctera Support for assistance.

4. Click **Save**.

Managing cases

This section includes the following topics:

About AI-Enabled Cases

Arctera eDiscovery supports AI-powered data mining at the eDiscovery case level to make case review quicker and more efficient. When a case is created with the AI Feature enabled, the AI module scans case-level items and documents, looks for useful information, patterns, and signals, and transforms raw information into actionable intelligence.

AI-powered data mining identifies document details such as main topics, tone (sentiment), language, and relevance. This helps reviewers identify critical information faster, reduce noise, and focus on what truly matters.

This AI enablement enables you to do the following:

- Creating AI-enabled cases See Creating cases.
- Viewing AI feature summary of a case See Viewing AI Feature Summary of cases.
- Viewing AI Status and configuration of cases See Viewing AI status and configuration of cases.
- Viewing AI Analytics of cases See Viewing AI Analytics of Cases.

- Viewing audit log and history of AI enabled cases See Viewing audit log and history of AI enabled cases.
- Tracking AI Usage via AI wallet statement.

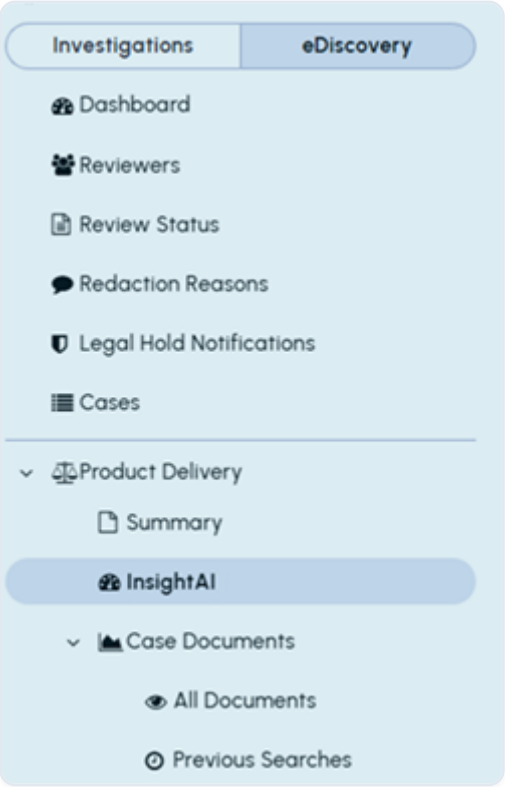
The Management Console administrator can track the AI units usage in Arctera Management Console.

Viewing AI Analytics of Cases

You can view AI analytics for a case only if the case is AI-enabled.

To view AI analytics of a case:

1. On the **eDiscovery** tab, search for and select the required case. The case-specific nodes appear in the left navigation pane.

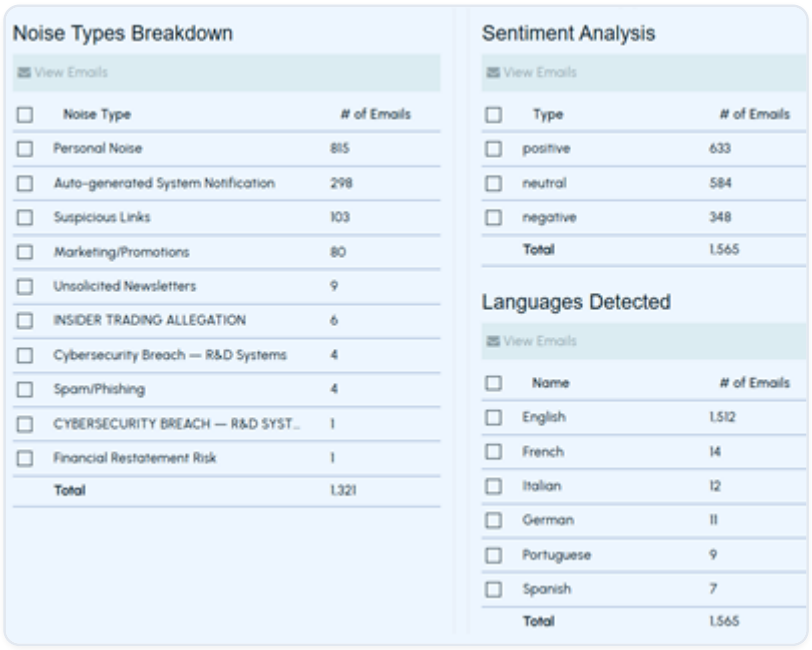


2. Select the **InsightAI** node to view **InsightAI Dashboard**. The dashboard displays case-level metrics as follow:

   - **AI analytics summary:** Displays the number of emails scanned, topics mined, emails identified as noise, and AI units consumed for the selected case.

- **Topic cloud:** Displays a visual representation of the human-defined topics and AI-extracted topics identified in the case. The human-defined topics appear in blue color, and the AI-extracted topics appear in yellow color.

- **AI analytics tables:** Display case-level breakdowns of the extracted information, including the number of emails by noise type, sentiment, and language.



Noise Types Breakdown

View Emails

Noise Type	# of Emails
Personal Noise	815
Auto-generated System Notification	298
Suspicious Links	103
Marketing/Promotions	80
Unsolicited Newsletters	9
INSIDER TRADING ALLEGATION	6
Cybersecurity Breach — R&D Systems	4
Spam/Phishing	4
CYBERSECURITY BREACH — R&D SYST...	1
Financial Restatement Risk	1
Total	1,321

Sentiment Analysis

View Emails

Type	# of Emails
positive	633
neutral	584
negative	348
Total	1,565

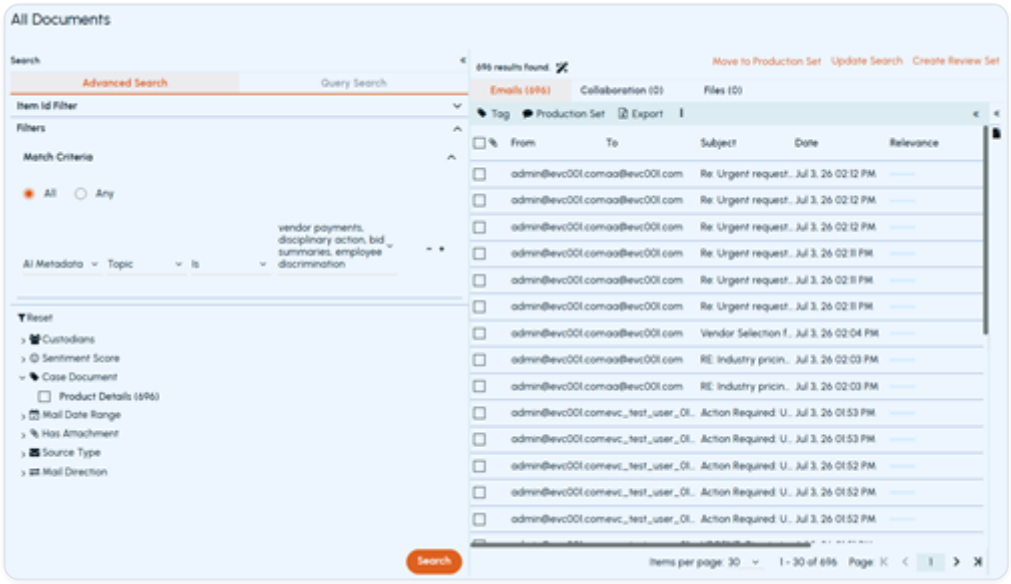
Languages Detected

View Emails

Name	# of Emails
English	1,512
French	14
Italian	12
German	11
Portuguese	9
Spanish	7
Total	1,565

3. Review analytics available on single-click:

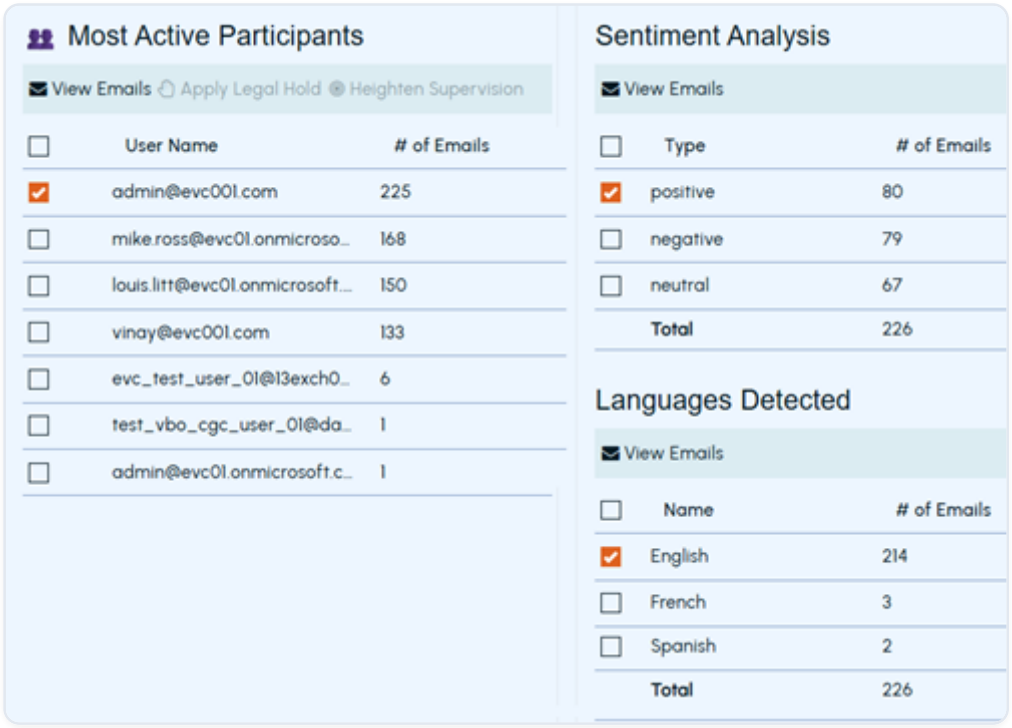
- Hover over the topic to know its relative frequency or prominence.
- Single-click the topic to enable the **View Emails** option.
- Click **View Emails** to view emails associated with the selected topic to view all emails.



4. Review analytics available on double-click:

   - Double-click the topic to display a visual representation of the **User Communication**.

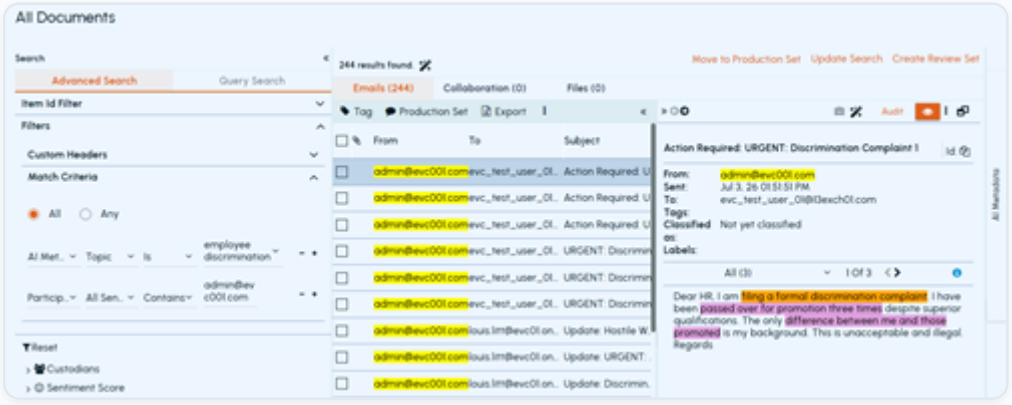
   - Hover over a spike to view communication details between the sender and recipient.
   - Click **View Emails** to view emails associated with the selected spike. Each spike represents the communication between specific email senders and receivers.
   - Click **View Summary** to view an AI-generated summary of the email content associated with the selected topic.
   - Review information in the following tables:
     - **Most Active Participants:** Displays the users who exchanged the highest number of emails in the selected topic, along with the number of emails associated with each user.
     - **Sentiment Analysis:** Displays the number of emails identified for various sentiments for the selected topic, along with the total number of emails.
     - **Languages Detected:** Displays the number of emails identified in each language for the selected topic, along with the total number of emails.



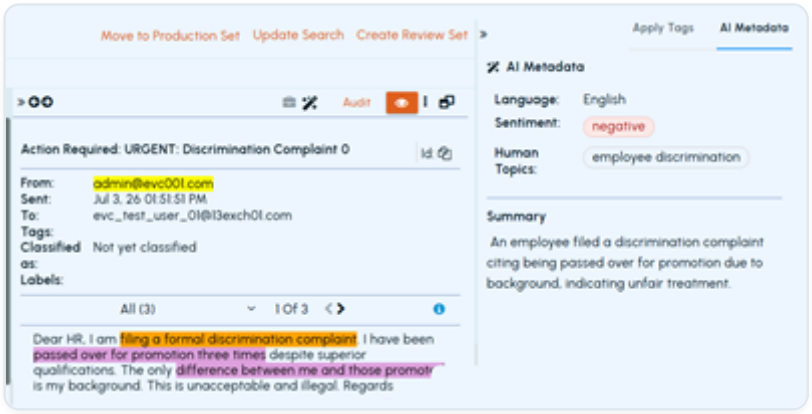
- Select the required entry in an analytics table, and then click **View Emails** in that table to view the associated emails.

> **Note:** The **Apply Legal Hold** and **Heighten Supervision** options appear on the table but are not functional in this release.

The email preview supports hithighlighting of relevant content in the preview pane.



- Click the **AI Metadata** pane on the right side of the email preview to view sentiment analysis information.



After reviewing the required AI analytics, you can use the available insights to identify relevant topics, communication patterns, participants, sentiments, languages, and associated emails for further case review.

Viewing AI Feature Summary of cases

To view AI Feature summary of a case:

1. On the **eDiscovery** tab, click **Cases**.

   A list of cases is displayed.
2. Search for and select the case. The case-specific nodes appears in the left navigation pane.
3. Click **Summary** to open the Case Summary page.
4. Scroll down to the AI Features Summary section.

   Refer to the sample image below.

The details about enabled and disabled content sources, AI capabilities, and the topics used for the case.

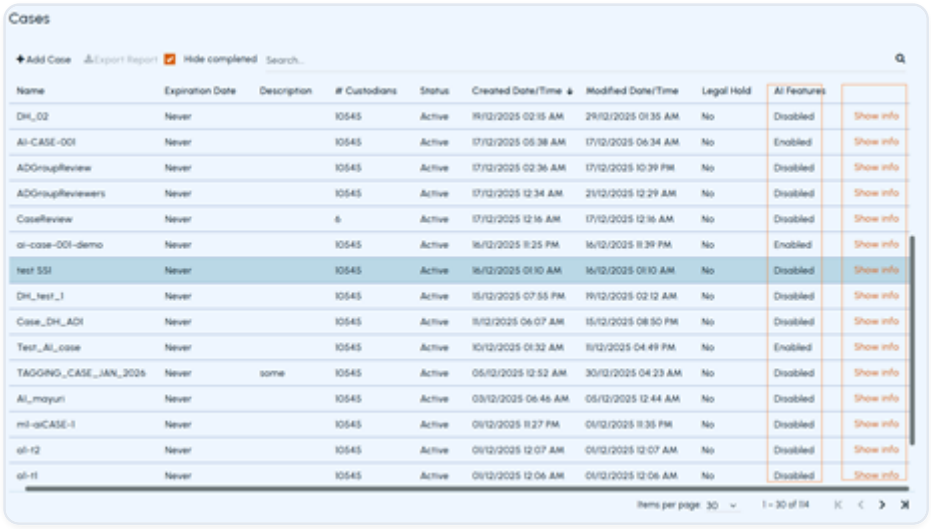
Viewing AI status and configuration of cases

You can verify whether a case is AI-enabled and view its AI configuration without opening the case.

To view AI status and configuration of cases:

1. In the left navigation pane, on the **eDiscovery** tab, select **Cases**.

   A list of available cases appears.



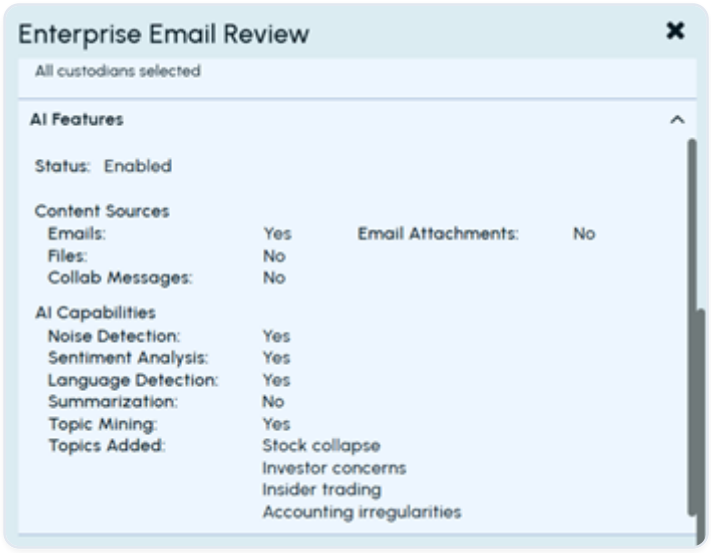
2. Refer to the **AI Features** column.

   - If the AI Feature was enabled during case creation, the case is marked as **Enabled** in the column.
   - If the AI Feature was disabled during case creation, the case is marked as **Disabled** in the column.

3. To view the detailed AI configuration of an AI-enabled case, click **Show info** in the row for the case.

   A detailed view opens and displays the following information:

- AI Feature status
- Selected content sources
- Enabled AI capabilities
- Topics configured for the case



Viewing audit log and history of AI enabled cases

You can use the audit log to review changes made to AI features for the selected case and export the results for further analysis or record keeping.

To view the audit log and history of AI-enabled cases:

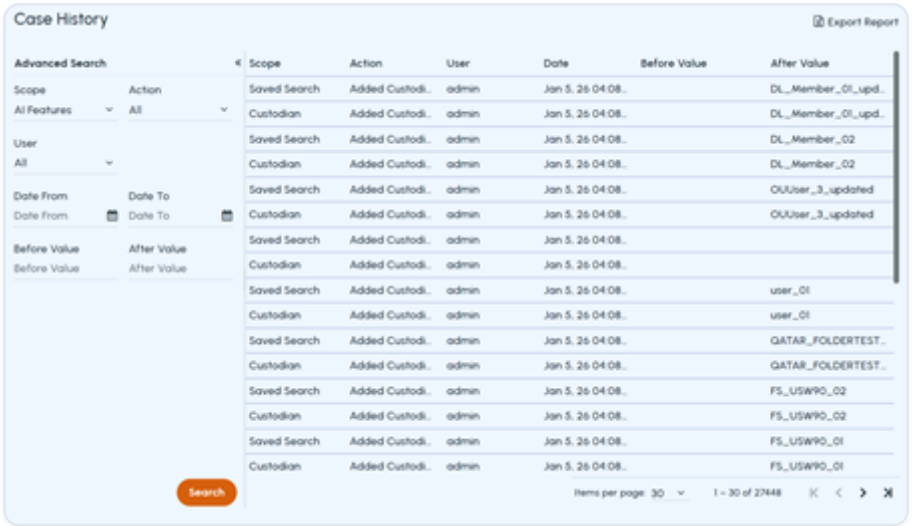
1. In the left navigation pane, on the **eDiscovery** tab, select **Cases**.

   A list of available cases appears.

2. Search for and select the AI-enabled case.

   The case-specific nodes appear in the left navigation pane.

3. Select the **Case History** node.



4. Under **Advanced Search**, specify the following criteria:

FIELD	DESCRIPTION
Scope	Select **AI Features**.
Action	Select **All** or a specific action. The currently available actions are:- Added Topics- Changed AI Features Status- Changed Language Detection Status- Changed Sentiment Analysis Status- Changed Noise Detection Status- Changed Topic Mining Status- Included Emails as Content Source
User	Select **All** or a specific user.
Date From/To	Specify the period for which you want to view the case history.
Before Value/After Value	Enter the value.

5. Click **Search** to view the audit log.
6. Click **Export Report** to download the audit log report.

About searches in eDiscovery

This section helps you understand seaches-specific tasks within the cases.

Applying a search-level legal hold

Accounts with the appropriate permissions can place items from a search on legal hold. Applying a search-level hold ensures that specific items 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:

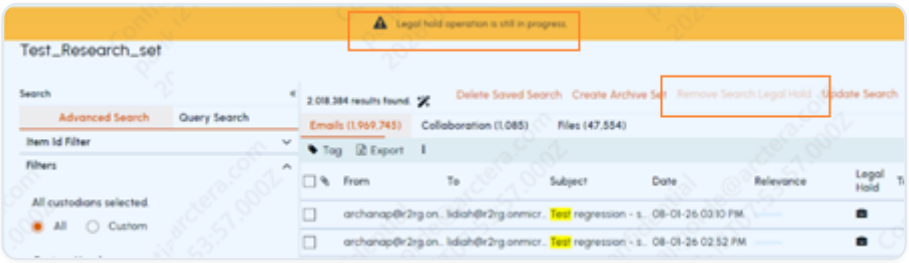
1. On the **eDiscovery** tab, select **Cases** to view a list of cases.
2. Search for and select the required case from the list of cases.
3. Under the **Cases** node, in the left pane, a***case_name*** node appears for the selected case.
4. Select the ***case_name***>**Research Sets** or **Review Sets**
5. Select the required search under the Research Sets or the Review Sets node or the node.

The search displays its results.

6. In the top-right corner, click **Apply Search Legal Hold**.

Note

- The default limit for applying search-level legal hold in a search result is 1000000 items, including emails, collaboration messages, and files. For any technical support, contact Arctera Support via your system administrator.
- The application displays a notification indicating that applying search-level legal hold is in progress and may take some time to complete.



- To remove a legal hold after it has been applied, select the same search, and click **Remove Search Legal Hold**. However, if the applying search-level legal hold operation is in progress, the **Remove Search Legal Hold** option remains disable as shown in the sample image above.

Assigning review 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.

> **Note:** After assigning a search 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.

> **Note:** You can create a Review Set only if the total number of items is 1000000 or less. If your current search result or Archive Set has more than 1000000 items, the **Create Review Set** button will be disabled.

3. Select one of the following options to assign items to reviewers.

NO ASSIGNMENT	NO SPECIFIC PERCENTAGE OF ITEMS 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 items to reviewers.
	The total allocation percentage must be 100 percent. If the case has only one reviewer, Arctera eDiscovery automatically assigns all items to the reviewer.
Assign equally to all reviewers	The application equally distributes percentage of items among reviewers.
Allow shared reviews	Select this check box to allow reviewers to access and review items 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 items 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**.

   Arctera eDiscovery automatically moves the search to the **Review Sets** node.

Generating a search summary report

Any user who has access to the New Searches node, the On-going Searches node, the Standard Searches node, and the Advanced ECA node on the Investigations tab can generate a printable report of searches.

Any user who has access to the New Searches node, the Research Set node, and the Review Set node on the eDiscovery tab can generate a printable report of searches.

To generate a printable report for searches on the Investigations tab:

1. On the **Investigations** tab, expand the New Searches node, the On-going Searches node, the Standard Searches node, and the Advanced ECA node as required.
2. Select the search for which you want to export the printable report.
3. On the action menu bar, click the *More Options* icon, and click **Export Report**.

   The application generates a report with the information about custodians, the parameters, and the results.

   To generate a printable report for searches on the eDiscovery tab:
4. On the **eDiscovery** tab, expand the **New Searches** node, the **Research Sets** node, or the **Review Sets** node.
5. Select the search for which you want to export the printable report.
6. On the action menu bar, click the *More Options* icon, and click **Export Report**.

   The application generates a report with the information about custodians, the parameters, and the results.

Modifying saved searches of cases

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. On the **eDiscovery** tab, select **Cases** to view a list of cases.
2. Search for and select the required case from the list of cases.
3. Under the **Cases** node, in the left pane, a***case_name*** node appears for the selected case.
4. Select the ***case_name***>**Research Sets** or **Review Sets**
5. Select the required search under the Research Sets or the Review Sets node or the node.

   The search displays its results.

6. 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.

7. 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.

Performing searches within cases

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, attachments, collaboration chats, and files that include a classification tag. The Arctera Classification assigns classification tags to emails, attachments, collaboration chats, and files that match an enabled classification policy. The built-in Arctera Classification policies help you to locate any emails that may infringe your corporate policies or regulations.

> **To perform a new search of a case**:

1. On the **eDiscovery** tab, select **Cases** to view a list of cases.
2. Search for and select the required case from the list of cases.

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

3. Select the ***case_name*** node >**New Search**.
4. Perform advanced search or query search to get the expected items. See Performing Advanced Search and Query Search.
5. Click **Search**.

> **Note:** The results of an Advanced Search include a **Relevance** column. The length of the bar in this column represents how closely the item matches the search criteria, relevant to the other items in the results.

6. Click **Save Search**.

   See Saving searches in Review sets and Research sets.

Saving searches in Review sets and Research sets

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 and collaboration messages and files 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 zero percentage to all reviewers. In this case, items are not assigned to any single reviewer. Any reviewer can again review and tag the items that are reviewed and tagged before. The review tag can be changed by another reviewer.

To save a search of a case:

1. Perform a new search on the case.

   See Performing searches within cases.
2. Click **Save Search**.
3. In the **Save Search** dialog box, provide the following information:

ENTER SAVED SEARCH NAME	ENTER A NAME FOR THE SAVED SEARCH.
Legal hold	Select to place all items in the saved search on legal hold. Items that are on legal hold cannot be 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 items to reviewers.
	- No assignment: No specific percentage of items are assigned to any single reviewer. Items 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 items to reviewers. The total allocation percentage must be 100 percent. If the case has only one reviewer, Arctera eDiscovery automatically assigns all items to the reviewer.
	- Assign equally to all reviewers: The application equally distributes percentage of items among reviewers.
	- Allow shared reviews: Select this check box to allow reviewers to access and review items 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 items assigned to other reviewers. If you have selected the No Assignment option, this check box is selected by default. You cannot clear it.

ENTER SAVED SEARCH NAME	ENTER A NAME FOR THE SAVED SEARCH.
	Note: If you do not select **Create Review Set**, the search is saved as a Research Set. Items continue to be added to a Research Set until it is assigned to the reviewers and so becomes an Assigned Search.

4. Click **Save** to save the search.
    - If you selected the **Create Review Set** check box, the search is saved under the **Review Sets** node.
    - Otherwise the search is saved under the **Research Sets** node.

Viewing previously executed but unsaved searches in cases

While working with cases, you may often run a search and retrieve the data, but knowingly or unknowingly do not save it. In such scenarios, the application logs the search under *eDiscovery* > *Case Name* > *Case Documents* > *Previous Searches* node. This allows you to refer to your previously executed but unsaved searches within cases when needed. You can rerun the same search and save it for future investigative purposes.

To view previously executed but unsaved searches in a case:

1. In the left navigation pane, select **eDiscovery**> *Case Name* >**Case Documents**>**Previous Searches** node.

    A list of previously executed but unsaved searches within the selected case. Use the page navigation arrows to access cases displayed on other pages.
2. To view the search-specific details, click **Show info** in the row corresponding to the search.
3. If needed, select the search and do the following:
    - Click **Export Report** to share with the concerned people.
    - Select the **Hide Completed** check box to list only the active cases.

> **Note:** This checkbox is visible only to users with the necessary permissions. Please contact your administrator if you require this permission.

> **Note:** Department Reviewers may encounter certain role-specific limitations. For details, these are known, low-impact issues targeted for resolution in the next release.

About case workflow summary- eDiscovery Administrator

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

Table: Process for an eDiscovery Administrator to set up a new case

PHASE	ACTION	DESCRIPTION
Phase 1	Prepare the reviewers, labels, review status tags, and redaction reasons for the cases.	- Prepare the reviewers. The System Administrator can assign Arctera Unified Platform accounts to the Reviewer and Administrator roles as required. See About account roles and Arctera eDiscovery. **Note:** Take care in selecting users for the **Reviewer** role, since reviewers can see other employees' emails, messages, and files.
		- 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 items 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

PHASE	ACTION	DESCRIPTION
		Investigations > Labels node. See Creating a label.
		- Prepare the review status tags. You can create review status tags and choose which are available when creating new cases. See Creating case review statuses.
		- Prepare the redaction reasons. You can create redaction reasons and choose which are available when creating cases. See Adding redaction reasons.
Phase 2	In eDiscovery > 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.
		- Select redaction reasons to use with the case.
		- Use AI feature to create cases efficiently.

PHASE	ACTION	DESCRIPTION
		See Creating cases.
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 items that the reviewers can process further. Typically, the reviewers do not see any other items than these.
		See Performing searches within cases.
Phase 4	Apply tags and notes to the search items.	Apply tags to items as required.
		See Applying tags to emails.
		See Adding 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 searches in Review sets and Research sets.
		See Assigning review sets to reviewers.
		See Applying a search-level legal hold.

About cases

In Arctera eDiscovery, an eDiscovery administrator creates a case as a container that contains emails, collaboration messages, and files related to the case. Administrators and reviewers can perform a traceable examination on these items. Administrators can view all the cases in Arctera eDiscovery, whereas reviewers can only view the cases to which they are assigned.

Cases are created and managed in the eDiscovery tab. AI-enabled case creation is also available to help administrators create cases more efficiently. However, to view and configure AI features during case creation, AI capabilities must be enabled at the group level. For more details, contact Arctera Support or your system administrator.

When creating a case, the eDiscovery administrator selects the user accounts (custodians) that the eDiscovery has to include. Within the case, the eDiscovery administrator can create and save the searches that find the custodian emails, messages, and files that may be pertinent to the case. The searches and review actions within a case are traceable.

> **Note:** Cases can never be deleted from Arctera 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 a legal hold on all the emails, messages, and files that are associated with it. The legal hold ensures that these items are retained in Arctera Unified Platform, regardless of the company's email retention policies. These items remain on a legal hold until the reviewer or administrator removes the legal hold. Normally, the legal hold is removed for an item 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 reviewers of that 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.

Adding parent tags and their child tags

Adding case tags to individual cases helps you categorize, organize, and analyze them during the review process. You can customize new parent and child tags.

Under the parent tag, you can add a maximum of 10 child tags up to three levels in the hierarchy. Adding tags with same names under different parent is permitted. However, you cannot save a new tag with a duplicate name in the same window; you must save other identical tags individually first.

To add new parent tags and their child tags:

1. On the **eDiscovery** tab, click **Cases**.
2. Click **Add Case**.
3. In the **Add New Case** dialog box, under **Case Tags**, specify the following:

NONE	BY DEFAULT, THE NONE OPTION IS SELECTED DURING CREATING A CASE, INDICATING NO TAG APPLIED TO THE CASE.
	SELECT THIS OPTION IF YOU DO NOT WANT TO ADD PARENT AND CHILD TAGS TO THE CASE.
Custom	Select this option to customize new parent and child tags for the case. Upon selecting this option, the Customize Case Tags option appears. Click this option to open the New Case Tag dialog box.
View	While editing the case, click this option to view the previously applied tags.
	This option remains disabled if you are creating a new case.

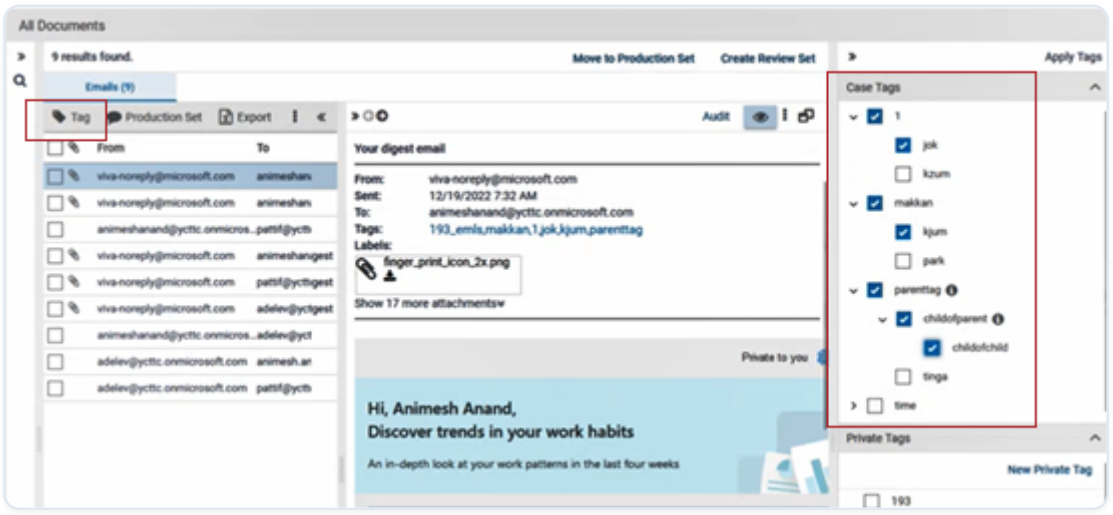
4. In the **New Case Tag** dialog box, specify the following:

TAG NAME	ENTER A UNIQUE TAG NAME, LIMITED TO A MAXIMUM OF 50 CHARACTERS.
Comments	Enter a description or comment to the parent tag to clarify its role.

TAG NAME	ENTER A UNIQUE TAG NAME, LIMITED TO A MAXIMUM OF 50 CHARACTERS.
Child Tag Selection Required	Select this check box to enforce including at least one of its child tags when applying this parent tag to a case.
Add Child > Tag Name	Enter a unique child tag name, limited to a maximum of 50 characters.
Add Child > Comments	Enter a description or comment to the child tag to clarify its role.
Children > Comments	Displays the child tags (a maximum of 10 child tags) added under this parent tag.

5. Click **Done**.

Apply this parent tag and its child tags to cases as needed as shown in the sample image below. See Applying tags to the searched items in cases.



Note: Before applying tags to the review items, it is essential to understand the following facts: While creating a parent tag, if you have not selected the **Child Tag Selection Required** option, you can apply the parent tag to selected items from cases with or without selecting its child tag. While creating a parent tag, if you have selected the **Child Tag Selection Required** option, you cannot apply that tag to selected items from cases without selecting at least one child tag. The **Info** icon appears alongside for easy identification of such parent tags. If you attempt to apply such parent tags without selecting a child tag, an **Error** icon appears next to the parent tag, instructing you to

> select at least one child tag. If you attempt to remove preselected child tags, a **Caution** icon appears, indicating you cannot remove them. Therefore, before applying such parent tags, ensure that you have selected at least one child tag of that parent.

Applying tags to the searched items in cases

To apply tags to the searched items in a case:

1. From the **eDiscovery** tab, select the **Cases** node to display the cases list.
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.
3. Click the ***case_name*** node to display the case details such as summary, case documents, research set, review set, and so on.
4. Select **Archive Search > New Search** to execute a new search, or select case documents, research set, or other nodes to get the items in the item grid.
5. From the **Email**,**Collaboration**, or **Files** tab, select one or more items to which you want to apply tags, and do any of the following:

   - Click **Tag** from the action bar and select the option as required.

   For example, upon selecting items from the Emails tab, you can select any of the following options:

   - To tag all the items in the search, click **Tag all emails**.
   - To tag all the items in the current page, click **Tag current page**.
   - To tag only the selected items, click **Tag selected emails**.
   - Select the **Apply Tags** panel provided in the right side.

   The application displays the **Apply Tags** panel as shown in the sample image below. Expand **Case Tags**/**Private Tags** and select the multiple relevant tags.

> **Note:** Before applying tags to the review items, it is essential to understand the following facts: While creating a parent tag, if you have not selected the **Child Tag Selection Required** option, you can apply the parent tag to selected items from cases with or without selecting its child tag. While creating a parent tag, if you have selected the **Child Tag Selection Required** option, you cannot apply that tag to selected items from cases without selecting at least one child tag. The **Info** icon appears alongside for easy

> identification of such parent tags. If you attempt to apply such parent tags without selecting a child tag, an **Error** icon appears next to the parent tag, instructing you to select at least one child tag. If you attempt to remove preselected child tags, a **Caution** icon appears, indicating you cannot remove them. Therefore, before applying such parent tags, ensure that you have selected at least one child tag of that parent.

6. Click **Apply**.

Note

- The default limit for applying tags in a search result is 1000000 items, including emails, collaboration messages, and files. For any technical support, contact Arctera Support via your system administrator.
- The application displays a notification indicating that tagging is in progress and may take some time to complete.

Creating case review statuses

The eDiscovery 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 create the case review status:

1. On the **eDiscovery** tab, select **Review Status**.
2. Click **Add Row**.
3. To customize a new status tag, do the following:
    - Provide a unique name and the description for the review status tag.
    - Select the **Is Active** check box for the status tags you want to display when creating a new case.
    - To hide the review status tag, clear the **Is Active** check boxes for respective statues.
    - Select the **Is Default** column to indicate the tag status as default.

    > **Note:** You must specify at least two review status tags as default.

4. Click **Save**.

Creating cases

The eDiscovery administrators can create cases and select which custodians to associate with the case. Once a case is created, all items (emails, collaboration messages, and files) for the case can be placed on legal hold to ensure that the items are retained.

AI-enabled case creation is also available to help administrators create cases more efficiently. However, to view and configure AI features during case creation, AI capabilities must be enabled at the group level. For more details, contact Arctera Support or your system administrator.

To create a case:

1. On the **eDiscovery** tab, click **Cases**.
2. Click **Add Case**.

   The **Add New Case** dialog box appears.
3. Under **Case Status**, specify the following details:

CASE STATUS	SELECT THE ACTIVE OPTION.
Legal Hold	By default, this option is set to OFF.
	Switch this field to ON or OFF to toggle the options whether to apply a case-level legal hold to case items.
Number of custodians	Displays number of custodians associated with the case.
Number of Items	Displays the total count of items associated with the custodians selected for the case.
	Note: Items collected during the investigation may include items associated with custodians who are not part of the case. Thus, if not all custodians associated with the case are selected, the item count may differ.
Expiration Date	Displays case expiration date.

CASE STATUS	SELECT THE ACTIVE OPTION.
Number of Items on Legal Hold	Displays number of items in a case that are on legal hold.

4. Under **Case Details**, specify the following details:

APPLY LEGAL HOLD	CLICK YES TO TOGGLE THE OPTION BETWEEN YES AND NO. THE YES OPTION APPLIES A CASE-LEVEL LEGAL HOLD TO ITEMS, AND IS THE DEFAULT VALUE.
	NOTE: THIS OPTION KEEPS ALL ITEMS 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 becomes read-only for reviewers, but all its associated data and any hold remains intact. The eDiscovery administrator can revert an inactive case back to active status.
Filing date	Specify the case filing date.
Case Type	Specify the type of case.
Department	Provide the department details.
Matter Number	Provide the matter number.
Court/Docket	Provide the court and docket number.
Additional Staff Members	Provide the additional staff member names involved in the case.

APPLY LEGAL HOLD	**CLICK YES TO TOGGLE THE OPTION BETWEEN YES AND NO. THE YES OPTION APPLIES A CASE-LEVEL LEGAL HOLD TO ITEMS, AND IS THE DEFAULT VALUE.**
	NOTE: THIS OPTION KEEPS ALL ITEMS FOR THE CASE ON LEGAL HOLD UNTIL THE ADMINISTRATOR REMOVES THE LEGAL HOLD.
Case Notes	Provide a note for a case, if required.

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.

     > **Note:** If under **Case Status**, the **Legal Hold** option is set to **ON**, and under **Custodians for Case**, you select the **All Custodians** option, the application displays the following message:

   This alert message recommends you to select specific custodians instead of all custodians to avoid performance issues. However, if you are sure about selecting the **All Custodians** option, click **Yes**. Else, click **No** and select the **Select Custodians** option.

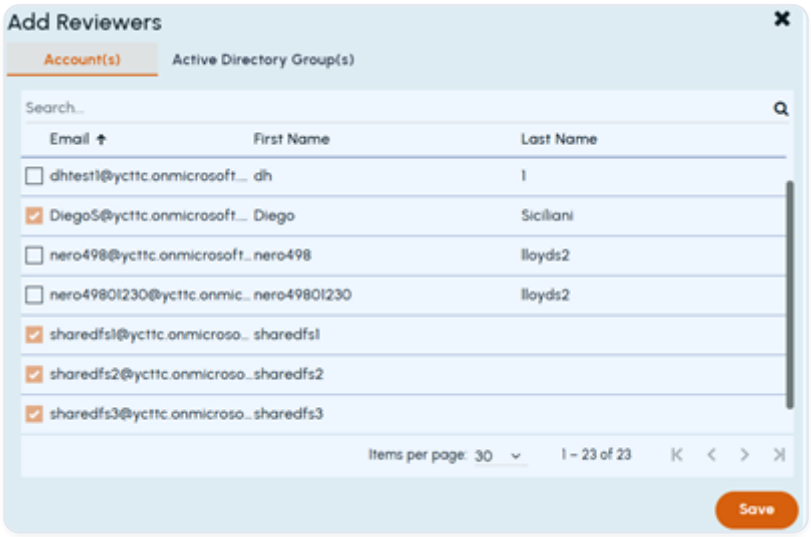
   When you select the **All Custodians** option, the **Add Custodians** option remains disabled.

   - Select **Select Custodians** to choose the archive accounts that you want to include for search. The **Add Custodians** option gets enabled. Click **Add Custodians** and select the required custodians, then click **Save**. The **Add/Remove Custodians** dialog box appears.

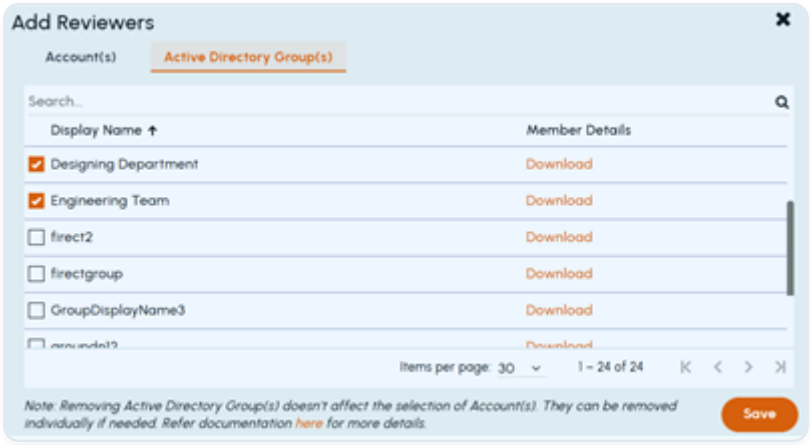
     - (Optional) Select **Search Between Custodians** at the bottom of the pop-up to retrieve emails exchanged exclusively among the selected custodians. For details, See Searching emails exchanged among specific custodians.
     - Expand the **Manage Custodians** to search and select the available custodians across the pages and click **Update**.
     - Expand the **Selected Custodians** to view your selection. To remove the selected custodian, click the **Delete** icon beside it and then click **Update**.

6. Under **Reviewers for Case**, click **Add Reviewers** and do the following as required:

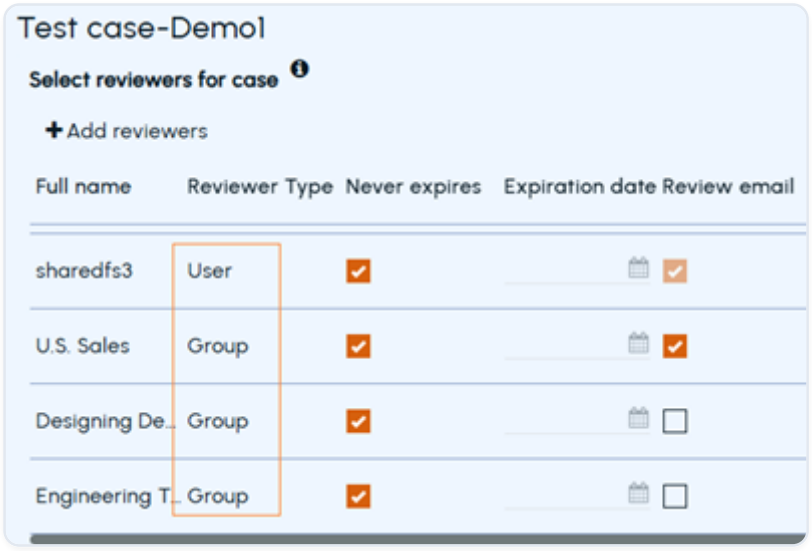
- On the **Account(s)** tab, select one or more individual reviewers for the case, and then click **Save**.



- On the **Active Directory Group(s)** tab, select one or more Active Directory groups for the case. To view group members, click **Download** next to the group name and review the downloaded file, which displays names of direct members of the corresponding Active Directory group. Then click **Save**.



The assigned Accounts and Active Directory groups are displayed on the case details page as shown in the sample image below.



Note:

- When you add one or more Active Directory group reviewers to a case, the application displays a notification indicating that the selected reviewers do not have access to Arctera eDiscovery. However, after you save the case, the notification is cleared and Arctera eDiscovery access is automatically enabled for the members of such groups when they log in to Arctera eDiscovery.
- The assigned Active Directory Groups appear as reviewers at the following spaces on the **eDiscovery** tab:
  - Select the **Reviewers** node and search for newly added Active Directory group(s).
  - Select the case > **Case Documents** >**Create Review Set**. The system lists case-specific reviewers, where you are required to assign a review share percentage to each reviewer.
  - Select the case > **Case History**.

7. Under **Customizations**, select the review statuses that need be available to the reviewers when they review each message.

   Under **Set Review Status to**, do any of the following:

   - Select **Default** and click **View** to use the default list of review statuses in their default order.
   - Select **Custom** and click **Choose Review Status Tags** to choose which review statuses are to be used with this case.

8. Under **Redaction Reasons**, select the redaction reasons that need to be available to the reviewers when they review each message.

   Under **Set Redaction Reasons to**, do any of the following:

   - Select **Default** and click **View** to preview the by default selected redaction reasons.
   - Select **Custom** and click **Choose Redaction Reasons Status** to choose the redaction reasons to be used with this case. Then, click **View** to preview the selected redaction reasons.

9. Under **Case Tags**, add parent tags and their child tags.

   Before you add parent tags and their child tags, See Adding parent tags and their child tags.

   By default, it is set to **None**.

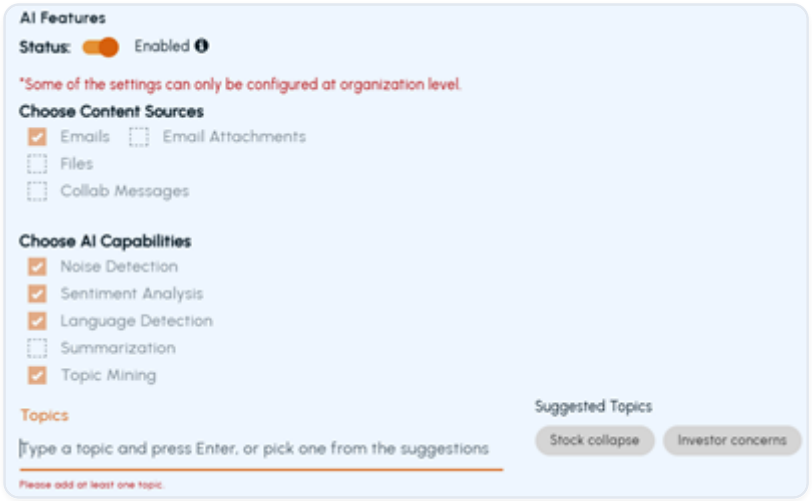
   Select **Custom**>**Customize Case Tags** to add a case-specific tags.

   Click **New Case Tag** to create a new parent tag. Provide a unique tag name and comments for this parent tag.

   If required, add child tags, and click **Done**.

   > **Note:** Under the parent tag, you can add a maximum of 10 child tags up to three levels in the hierarchy. Adding tags with same names under different parent is permitted. However, you cannot save a new tag with a duplicate name in the same window; you must save other identical tags individually first. The **New Case Tag** functionality lets you create multiple tags simultaneously. While applying tags to the searched items, you can select multiple tags.

10. Under **AI Features**, do the following:



Note: The **AI Features** section appears on the **Add New Case** page only when AI capabilities are enabled at the group level. To enable this option, contact your system administrator or Arctera Support.

STATUS	USE THIS SWITCH TO ENABLE OR DISABLE AI-ENABLED CASE CREATION. BY DEFAULT, THIS OPTION IS SET TO OFF.
	SWITCH THIS FIELD TO ON TO ENABLE AI-ENABLED CASE CREATION, OR TO OFF TO DISABLE THE FEATURE.
Choose Content Sources	Emails is selected by default as the content source for AI-enabled case creation.
	Other content sources, such as Email Attachments, Files, and Collaboration Messages, are not included in AI-enabled case creation at this time.
Choose AI Capabilities	The following capabilities are enabled by default\:
	- Noise Detection
	- Sentiment Analysis

STATUS	USE THIS SWITCH TO ENABLE OR DISABLE AI-ENABLED CASE CREATION. BY DEFAULT, THIS OPTION IS SET TO OFF.
	SWITCH THIS FIELD TO ON TO ENABLE AI-ENABLED CASE CREATION, OR TO OFF TO DISABLE THE FEATURE.
	- Language Detection
	- Topic Mining
Topics	Enter a topic and press ENTER. Alternatively, select one or more topics from the Suggested Topics list.

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

Editing cases

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 **eDiscovery** 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.
3. In the left navigation pane, click the ***case_name*** node to display the case details pane.
4. 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.

CASE STATUS	YOU CAN EDIT THE CASE-LEVEL LEGAL HOLD STATUS.
	YOU CAN ALSO SET THE CASE STATUS TO INACTIVE OR COMPLETED. SETTING THE STATUS TO INACTIVE DISABLES ALL FUNCTIONALITY FOR WORKING WITH THE CASE.
Case Details	You can edit the case name, description, case filing date, case expiration date, case type, department, matter number, docket number, and notes. You can add additional staff members to 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 Items	You can reassign items from one reviewer to another reviewer.
Customizations	You can change the Review Status available for the case.
Redaction Reasons	You can change the redaction reasons available for the reviewers of the case.

Note: Click **Refresh** to update the number of items that are included in the selected case and the number of items on legal hold.

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

Removing tags of the searched items in cases

To remove tags of the searched items in a case:

1. From the **eDiscovery** tab, select the **Cases** node to display the cases list.

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.
3. Click the ***case_name*** node to display the case details such as summary, case documents, research set, review set, and so on.
4. Execute a new search or select case documents, research set, or other nodes to get the items in the item grid.
5. Select one or more items of which you want to remove tags.
6. Click **Tag** from the action bar and select **Remove from Tag**.

   The **Remove Tags** panel appears.
7. Select the parent and child tags that you want to remove, and click **Remove**.

> **Note:** If the **Child Tag Selection Required** option is selected for a parent tag, the **Info** icon appears alongside for easy identification. The application does not allow you to remove the child tags. If necessary, you can remove the entire parent tag. To understand the facts about such parent tags, See Applying tags to the searched items in cases.

Viewing case details

To view the details of a case:

1. On the **eDiscovery** tab, select the **Cases** node to display a list of cases.

   If you are a reviewer, Arctera eDiscovery lists only those cases to which you have been assigned.
2. 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.
3. 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 cases.

- **Summary**: Click this node to view a Case Information Summary table. It provides a summary about case description, custodian information, reviewer information, and AI Features summary
- **AI Analytics**: Upon selecting the AI-enabled case, select **AI Analytics** in the left navigation pane. The AI Analytics dashboard displays case-specific AI insights (key metrics and topics) to help users quickly know the selected case. For more information, See About AI-Enabled Cases.
- **Case Documents**: Click this node to view Collection Sets and Archive Sets created for the corresponding case. You can easily differentiate these sets as the icons are different for them.
    - **Collection Set**: When you collect the items from Targeted Collectors, the document set is called an **Collection Set**.
    - **Archive Set**: When you collect the items from Archives, the document set is called an **Archive Set**.
    - **All Documents**: When you want to see documents from collection sets and archive sets of a case, click this node.
- **New Search**: From this node you can perform new searches. or run any saved searches that are related to the case.

  See Performing searches within cases.
- **Research Set**: A Research Set is a collection of searches saved in a particular case. These searches are not assigned to reviewers. Emails continue to be added to Research Sets until a reviewer is assigned. Click this node to view the case-specific searches saved for preliminary research.
- **Review Set**: A Review Set is collection of searches saved for a particular case. Searches are assigned to the reviewers of the case. You can allocate a percentage of the search results to each reviewer. Click this node to view the case-specific searches saved for review.
- **Tags**: Click this node to view all of the tag assignments for the case.
- **Production Sets**: Click this node to view all the production sets created within a case.
- **Exports**: Click this node to view the exports-specific details of the selected case.
- **Case History**: Click this node to view a table of actions that were performed on this case.

Managing case documents

This section includes the following topics:

Understanding Archive Search

This section explains what archive search is and how you can create a Research Set and Archive Set.

About Archive Searches

During case management, the Archive Search feature lets you:

- Create new searches

  You can use *Advanced Search* and *Query Search* to refine the data collected by archive collectors, and then save the search for further research.

- View previous unsaved searches

  You can access previously executed but unsaved searches.

- Save searches under Research Set for further research

  Upon saving the search, it appears under Research Set. You can update or delete these saved searches anytime as needed. If you are satisfied with the searched data and want to move this data to any case, create a new Archive Set. This archive set appears under Case Documents.

Next steps

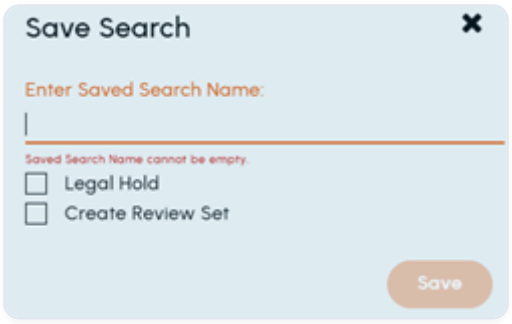
The Archive Sets can be updated or deleted from the Case Documents as needed. From the Archive Set, a new Review Set can be created and assigned to corresponding reviewers to expedite the discovery process or can be moved to the Production Set.

Creating research sets and archive sets

Note: You may encounter certain minor limitation. For details, these are known, low-impact issues targeted for resolution in the next release.

To create research set and archive set:

1. On the **eDiscovery** tab, select a case you want to work on from the list of cases.
2. In the left navigation pane, select **Archive Search** and perform any of the following as required.
   - Select **New Search** and do the following:
     - Use *Advanced Search* and *Query Search* to refine the data collected by archive collectors.
     - If you are satisfied with the resulted data and want to save it, click **Save Search**. The **Save Search** dialog box appears.



   Provide the following details and click **Save**.

   - Enter a unique search name.
   - To apply a legal hold to this search, select the **Legal Hold** check box.
   - To create a review set of the searched items, select the **Create Review Set** check box.

     Note: You can create a Review Set only if the total number of items is 1000000 or less. If your current search result or Archive Set has more than 1000000 items, the **Create Review Set** check box will be disabled.

   - To save the search as **Research Set**, do not select the **Create Review Set** check box.
   - If you are confident that the data can be moved directly to the case without saving it as Research Set, click **Create Archive Set**. In the *Create Archive Set* dialog box, specify the following fields, and click **Save**.

CASES	SEARCH AND SELECT THE CASE IN WHICH YOU WANT TO CREATE AN ARCHIVE SET AND DOCUMENTS ACCORDINGLY.
Archive Set name	To create a new Archive Set, select New and provide a unique name for the archive set you want to create.
	To send the items in the existing Archive Set, select Existing. The application displays a list of existing archive sets, then select the required archive set.
	Sending this search result from Investigations to a Case in eDiscovery ignores the custodian(s) selected in the Case setup.

> **Note:** The default limit for sending search results to an archive set is 1000000 items, including emails, collaboration messages, and files.

Upon saving, it appears under the **Case Documents** node.

- Select **Previous Searches** to access previously executed but unsaved searches.
    - Identify the search you want to run again and click **Rerun Search** in the *Action* column of the corresponding row to retrieve the search result.
    - Use *Advanced Search* and *Query Search* to refine the data collected by archive collectors.
    - If you are satisfied with the searched data and want to save it, click **Save Search**. Upon saving the search, it appears under **Research Set**.
    - If you are confident that the data can be moved directly to the case without saving it as Research Set, click **Create Archive Set**.
    - In the *Create Archive Set* dialog box, specify the fields mentioned in the table above, and click **Save**.

Upon saving, it appears under the **Case Documents** node.

- Expand **Research Set** and select a required research set for further action.

> **Note:** If the research set contains 1000000 or more items, the **Create Review Set** button remains disabled.

- If you are confident that the data can be moved to the case, click **Create Archive Set**.
- In the *Create Archive Set* dialog box, specify the fields mentioned in the table above, and click **Save**.

Upon saving, it appears under the **Case Documents** node.

Moving case documents to production sets

You can move emails, collaboration messages, and files from the case documents to the unlocked production sets only, and not to the locked production sets. You need to unlock the production sets before moving these items to the locked production sets.

To move case documents to production sets:

1. On the **eDiscovery** tab, click **Cases**.
2. Search for and select the case in which you want to search emails.

   The selected ***Case_Name*** node appears below **Cases**.
3. Click **Case Documents** and select a set of documents from which you want to move items to document set.

   The available emails, collaboration messages, and files are displayed.
4. To further filter the items from the case document set, use the **Advanced Search** or the **Query Search** tabs.

   If you are performing the Advanced Search in Case Documents node, a new filter attribute - **Custodians** — is available along with other attributes under the **Filter** facet. This filter attribute is available only for the Case Documents node.

   > **Note:** The **Custodians** filter attribute is not available in the **Advanced Search** tab of any other node. When you expand the **Custodians** attribute, the application displays a top few custodians and a **Show more** option. Click **Show more** to open the **Select Custodians** dialog box.

5. Set the filter criteria to further refine your items search, and click **Search**.

The filtered emails, collaboration messages, and files are displayed.

6. To move all the emails, collaboration messages, and files from the result, click **Move to Production Set**.
7. To move emails only, on the **Emails** tab, select the emails you want to include in the production set. Click **Production Set**, and do any of the following:
   - Click **Move all emails** to include all the emails available in the search.
   - Click **Move current page** to include all the emails displayed on the selected page.
   - Click **Move selected emails** to include all the selected emails from the search.
8. To move collaboration messages, on the **Collaboration** tab, select the emails you want to include in the production set. Click **Production Set**, and do any of the following:
   - Click **Move all messages** to include all the collaboration messages available in the search.
   - Click **Move selected messages** to include all the selected collaboration messages from the search.
9. To move files, on the **Files** tab, select the files you want to include in the production set. Click **Production Set**, and do any of the following:
   - Click **Move all files** to include all the files available in the search.
   - Click **Move selected files** to include all the selected files from the search.
10. In the **Production Set** dialog box, specify the following:

NEW PRODUCTION SET	SELECT THIS OPTION IF YOU WANT TO MOVE THE SELECTED EMAILS IN A NEW PRODUCTION SET. THIS OPTION IS SELECTED BY DEFAULT.
	IN THE PRODUCTION SET NAME FIELD, ENTER A UNIQUE NAME FOR THIS PRODUCTION SET.
	IN THE DESCRIPTION FIELD, ENTER A BRIEF DESCRIPTION OF THE PRODUCTION SET.
Existing Production Set	In the Production Set Name drop-down list, you can view only the unlocked production

NEW PRODUCTION SET	**SELECT THIS OPTION IF YOU WANT TO MOVE THE SELECTED EMAILS IN A NEW PRODUCTION SET. THIS OPTION IS SELECTED BY DEFAULT.**
	IN THE PRODUCTION SET NAME FIELD, ENTER A UNIQUE NAME FOR THIS PRODUCTION SET.
	IN THE DESCRIPTION FIELD, ENTER A BRIEF DESCRIPTION OF THE PRODUCTION SET.
	sets. You can not move emails to the locked production set.
	In the Production Set Name drop-down list, select a set to which you want to move (add) the selected emails.
	The description of the selected production set appears for your reference.

11. Click **Submit**.

    If you have created a new production set, the application displays the *Production set created successfully* message. This newly created production set gets listed under **eDiscovery** tab >**Cases**> *Case_Name* >**Production Set**.

    If you have moved the items to an existing production set, the application displays the *Production set updated successfully* message.

Understanding document sets in cases

For cases, you can collect documents from Targeted Collectors and Archives (new searches, saved On-going/Standard searches, and saved research sets).

When you collect the items from targeted collections, the document set is called an Collection Set.When you collect the items from archives, the document set is called an Archive Set. You can create new Collection and Archive Sets while sending the search results from the Investigation tab to cases under the eDiscovery tab. These sets are saved and displayed in the eDiscovery tab. After you select the case, you can view such Collection and Archive Sets under Case Documents.

Use Advance Search to filter the result. The Query Search is not supported for case documents.

Case Documents support tagging, creating production sets, exporting, and exporting report. Tagging and exporting by custodians is not supported.

Managing redaction reasons

This section includes the following topics:

About redaction reasons

Redaction reasons are the reason codes that lets reviewers justify a reason of redaction in the document. You can create, edit, and delete redaction reasons. Redaction reasons can be applied on the documents while adding redactions. Redactions and redaction reasons can be applied to the document from the Native view of the document.

Adding redaction reasons

To add a redaction reason:

1. On the **eDiscovery** tab, select **Review Status**.
2. Click **Add Row**.
3. In the newly added row, do the following:
    - In the **Name** column, enter a unique reason name in brief.
    - In the **Description** column, describe the reason in detail.
    - Select the **Active** column to keep this reason available in the system.

    Clear the check box if you want to deactivate this reason.
4. Click **Save**.

Deleting redaction reasons

You cannot delete a redaction reason if that reason is applied to any of the redactions marked in any of the documents. The reasons that are not applied to any redaction can be deleted any time.

To delete a redaction reason:

1. On the **eDiscovery** tab, select **Review Status**.
2. Search for and select the reason that you want to delete.
3. Click **Delete Row**.

Editing redaction reasons

You cannot edit a redaction reason if that reason is applied to any of the redactions marked in any of the documents. Such redaction reasons remain disabled for editing. The reasons that are not applied to any redaction can be edited any time.

To edit a redaction reason:

1. On the **eDiscovery** tab, select **Review Status**.
2. Search for and select the reason that you want to modify.
3. In the **Name** column, click the redaction reason name. The field becomes editable. Modify the reason name in brief, if required.
4. In the **Description** column, click the redaction reason name. The field becomes editable. Modify the reason description, if required.
5. Select or clear the **Active** column to keep this reason active or inactive respectively.
6. Click **Save**.

Managing reviews

This section includes the following topics:

About reviewing cases

As a reviewer assigned to a case, you can see only the search results assigned to you. It includes emails, collaboration chats, and files, along with their associated attachments. You can preview this content and attachments to identify the information of interest.

> **Note:** In Arctera eDiscovery, previewing Microsoft Excel files may occasionally take longer to load or fail. This issue is specific to Microsoft Excel files and does not affect other Microsoft formats, such as Word, PowerPoint, or Notepad. The preview issue may occur when:

> - The Excel file contains significant data, complex formatting, or processing overhead by the application.
> - A high volume of classification tags and search terms to be highlighted.
> - Increased browser memory usage leads to unresponsiveness.
> - The generated preview content exceeds supported size limits.

> Arctera eDiscovery provides review status tags, custom tags, and labels, all of which you can apply to emails, attachments, collaboration chats, and files to help you manage the review process. You can then discover the emails, attachments, collaboration chats, and files by tag name.

You can 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 email, attachment, collaboration chat, and file or for the history of an entire case.

Reviewing emails

The Emails tab appears only if the Exchange Online service is enabled and the archive collector is configured for you. You can review all the emails that are coming from the Exchange Online. While reviewing the emails, you can perform the following actions:

- Applying tags
- Creating and exporting production sets
- Copying Arctera Surveillance Id to search exact item for review
- Exporting emails
- Exporting summary report
- Viewing audit history
- Adding notes
- Applying review status
- Printing emails
- Restoring emails
- Forwarding emails

Accessing emails for review

To access emails for review:

1. On the **eDiscovery** tab, click **Cases**.
2. Search for and select the case in which you want to search emails.
3. The selected ***Case_Name*** node appears below **Cases**.
4. Click **New Search** to create a new search. Else, expand **Research Sets** or **Review Sets** to select existing search.

   You can access existing saved searches of the selected case from the **Review Set** and **Research Set** nodes. Alternatively, Perform advanced search or query search to get the expected items. See Performing Advanced Search and Query Search.

After performing a new search or accessing the existing searches from review set and research sets, the application displays the filtered emails, collaboration messages, and files in the details pane.

5. Click the **Emails** tab.
6. Select the email to view its details in the **Preview** pane.

> **Note:** Arctera eDiscovery does not support previewing certain file types, such as .dll and .exe and large files (over 30 MB to maintain browser responsiveness). For compressed files, Arctera eDiscovery supports previewing only the .zip file format and does not support other formats like .7z, .tar, and so on. If you cannot preview a specific file type, simply download it and use the appropriate tools to view its content.

Adding notes to emails

Reviewers can add notes to emails that are visible to other reviewers of that case. Notes are case-specific, therefore, a note that is applied to an email in one case does not appear for the same email in a different case. Notes can be provided to emails that are from the Review Sets only. You cannot provide notes to the emails that are from the Research Set.

To add a note to an email:

1. From the **eDiscovery** 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.
3. Click the ***case_name***>**Review Sets**.
4. Select the required search under the Review Sets node.
5. On the **Emails** tab, select the email to view its details in the preview pane.
6. Click the **More options** icon and select **Notes**.
7. In the **Add Notes** dialog box, specify the note about this message.
8. Click **Add** to save the note.

> **Note:** Different reviewers can add and save their notes for the same email. The application displays all the notes applied to the email that can be used for a collaborative reviews.

Applying review status to emails

Case reviewers can apply one of the following default review status to emails to indicate its status in the eDiscovery review process:

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

In addition, the eDiscovery Administrators can customize the available review status options.

To apply review status to emails:

1. Under the associated case, select **Review Set**, and open the corresponding review set node.
2. To apply review status 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** on the action bar.
    - Then select the required review status.
3. To apply a review status to an email while you view its details:
    - Select the email from the **Review Set** list to display its details in the preview pane.

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

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

> **Note:** To view emails based on their review status, you can filter the required review status 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 Arctera Management Console, under the My Config >

Managed Tags node. For more information on managed tags, see the Arctera Management Console help.

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. Click on emails to view its details in the preview pane.
3. Select the emails you want to tag, and click **Tag**.
   - To tag only the selected emails, click **Tag selected emails**.
   - To tag all the emails displayed on the page, click **Tag current page**.
   - To tag all the emails in the search, click **Tag all emails**.
4. In the **Add Tag** dialog box, do the following:

TAG NAME	ENTER A NEW UNIQUE TAG NAME.
Comments	Provide a comment or a description for the tag name.
Legal Hold	Select this check box if you want to apply the legal hold on the emails.
Select retention Tag	Instead of applying a new tag, you can apply the retention tags that are created in Arctera Unified Platform. To access and apply those retention tags, select this option, and choose the tags you want to apply.

5. Enter a tag name and description for the custom tag. Alternatively, you can select the a retention tag, if any are available to you.
6. Click **Tag**.

> **Note:** In the eDiscovery tab, any custom tags you create are listed in the Tags node of the selected case.

Exporting a search summary report for emails

To export a search summary report for emails during case review:

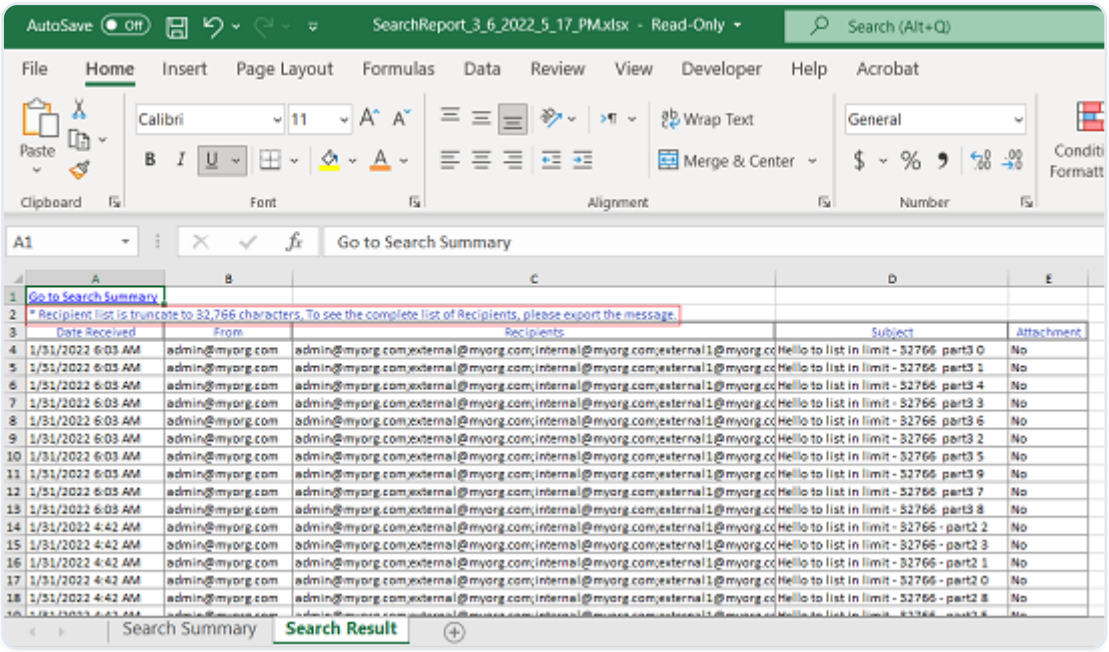
1. On the **eDiscovery** tab, click **Cases**.
2. Search for and select the case in which you want to search emails.
3. The selected ***Case_Name*** node appears below **Cases**.
4. Click **New Search** to create a new search. Else, expand **Research Sets** or **Review Sets** to select existing search.

   You can access existing saved searches of the selected case from the **Review Set** and **Research Set** nodes. Alternatively, you can click **New Search**, specify a new criteria in the *Advanced Search* or the *Query Search* option to search for new emails for review.

   After performing a new search or accessing the existing searches from review set and research sets, the application displays the filtered emails, collaboration messages, and files in the details pane.
5. On the **Emails** tab, click the **More Actions** icon, and click **Export Report**.

> **Note:** The following sample image is specific to a search in **Review Sets**. If you select the search from **Research Sets**, the application do not show the **Review Status** and the **Message Legal Hold** options on the action bar.

> The application downloads the summary report (.xlsx) of the emails within the search as a zipped (.zip) folder. A sample report is shown below. The report comprises of two sheets.



The **Search Summary** sheet displays details such as Search Parameters and Custodians.

The **Search Result** sheet displays details such as Date Received, From, Recipients, Subject, and Attachments. The recipient column in this summary report includes recipients mentioned in the To, CC, and BCC fields. If the list of recipients is longer than 32766 characters, the application truncates the list. The report displays a note that - *Recipient list is truncate to 32,766 characters, To see the complete list of Recipients, please export the message.* In such scenario, to view the complete list of recipients, you need to export the individual message.

> **Note:** If you select a search from **Review Sets**, and select any filter option and click **Apply**, the **Export Report** option remains disabled.

Exporting emails

To export emails:

1. On the **eDiscovery** tab, click **Cases**.
2. Search for and select the case in which you want to search emails. The selected ***Case_Name*** node appears below **Cases**.
3. Click **New Search** to create a new search. Else, expand **Research Sets** or **Review Sets** to select existing search.

> **Note:** You can access existing saved searches of the selected case from the **Review Set** and **Research Set** nodes. Alternatively, you can click **New Search**, perform advanced search or query search to get the expected items. See Performing Advanced Search and Query Search. After performing a new search or accessing the existing searches from review set and research sets, the application displays the filtered emails, collaboration messages, and files in the details pane.

4. On the **Emails** tab, select the emails you want to export. Click **Export**, and do any of the following:
   - Click **Export current page** to export all the emails displayed on the selected page.
   - Click **Export selected emails** to export all the selected emails from the search.
   - Click **Export all emails** to export all the emails available search.
   - Click **Export by custodians** to export all the emails from the selected custodians.
5. Click **Export**, and do any of the following:

6. If you are exporting all emails in the search, all emails displayed on the page, or selected emails, in the **Export Options** dialog box, do the following:

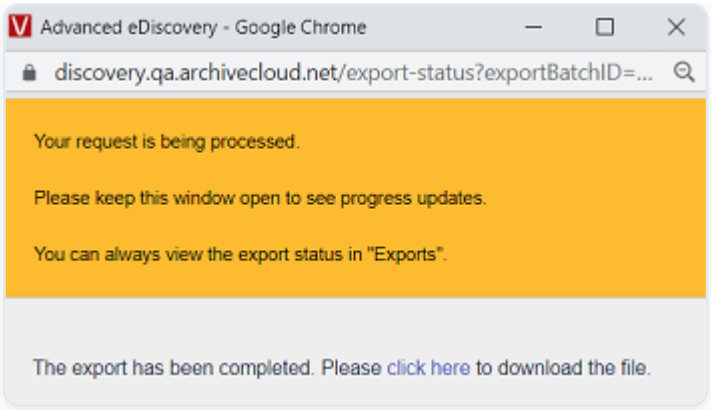
FIELD	DESCRIPTION
Message Format	Select the appropriate message format. By default, the **PST** format is selected. The available message formats are:**•Clearwell•EML•EML with EDRM•PST with EDRM•MSG with EDRM•FTI-RingTail•EDRM Only•PST**When exporting messages to PST, the export may fail or stop responding if the batch contains calendar invitations with very large embedded attachments, such as oversized Base64 files. In such cases, the export may show failed items, and a usable PST file may not be generated. Resubmitting the same failed items may result in the same export failure.To resolve this issue, the Arctera eDiscovery application excludes only the oversized Base64 attachment from the item being exported. The calendar invitation itself is still exported with its key details, such as subject, organizer, attendees, date, time, location, message body, and reminders.During export, if an oversized Base64 embedded attachment is excluded, a **Skipped_Attachments_Report.csv** file is generated in the export output folder. Reviewers can refer to this report to identify the affected items and understand which attachments were excluded from the PST export.**•Original EDRM**If you select this option, the exported file includes emails in both MSG and EML formats, allowing you to work with the emails in the format that best suits your needs. In addition, the exported file includes the **edrmXML.xml** and **HTMLReport.html** files in their original formats. These files facilitate the smooth transfer of electronically stored information (ESI) between different software programs

FIELD	DESCRIPTION
	during the electronic discovery process.•**Original**If you select this option, the exported file includes emails in both MSG and EML formats, allowing you to work with the emails in the format that best suits your needs.**Note:** The **Original EDRM** and **Original** message formats are available only to users listed in the **Configuration_Override** table in the Arctera Unified Platform database. To make these options available in the **Message Format** drop-down field, contact Arctera Support.
Include Journaling Envelope	Select this option to include journaling envelopes, which contain information about email recipients, such as distribution lists.
Exclude Exported Messages	Select this option to exclude the exported messages.
Enable AES-256 Encryption	Select this check box to secure access to the downloaded export batch.
Export Name	Specify a name for the export batch. By default, the search name is used. You can change it if required.
Export Password	Enter the password that users must provide to access the exported batch of messages.
Confirm Password	Re-enter the password for confirmation.
Generate Azure SAS URL	**Note:** This button is available only if the **Export to Azure private storage location** feature is enabled for your account in the Arctera Management Console.Click **Generate Azure SAS URL** to generate the Azure Blob SAS URL for your private storage location and save it for future use.For security reasons, the application does not display the URL the next time. If you lose the URL, click **Generate Azure SAS URL** again

FIELD	DESCRIPTION
	to generate a new URL and save it securely.After you click **Export** in the **Export Options** dialog box, the selected items are exported to the Azure private storage location. You can use Microsoft Storage Explorer to access the exported items.
Share Export	Click **Select Admin** to choose the recipients of the export batch, and then click **Update**.**Note:** You must manually share the export password with the administrators and follow your organization's security policies.

7. If you are exporting emails by custodians, in the **Add/Remove Custodians** dialog box, search for and select the custodians.
8. Click **Export**.

> **Note:** The exported batch can either gets downloaded as a single or multiple file segments.



9. Click **Click here** to download the exported batch of emails.
10. To confirm the status of batch export, on the **eDiscovery** tab, under the selected case node, select **Exports**, and search this export batch name.

Forwarding emails

To forward an email:

1. On the **eDiscovery** tab, click **Cases**.

2. Search for and select the case in which you want to search emails.
3. The selected ***Case_Name*** node appears below **Cases**.
4. Click **New Search** to create a new search. Else, expand **Research Sets** or **Review Sets** to select existing search.

   You can access existing saved searches of the selected case from the **Review Set** and **Research Set** nodes. Alternatively, you can click **New Search**, specify a new criteria in the *Advanced Search* or the *Query Search* option to search for new emails for review. After performing a new search or accessing the existing searches from review set and research sets, the application displays the filtered emails, collaboration messages, and files in the details pane.
5. Click the **Emails** tab.
6. Select the email to view its details in the Preview pane.
7. Click the **More options** icon and select **Forward**.
8. In the **Mail Composer** window, draft the email content, and click **Send** to send the original email content to a recipient.

Printing emails

To print emails:

1. On the **eDiscovery** tab, click **Cases**.
2. Search for and select the case in which you want to search emails.
3. The selected ***Case_Name*** node appears below **Cases**.
4. Click **New Search** to create a new search. Else, expand **Research Sets** or **Review Sets** to select existing search.

   You can access existing saved searches of the selected case from the **Review Set** and **Research Set** nodes. Alternatively, you can click **New Search**, specify a new criteria in the *Advanced Search* or the *Query Search* option to search for new emails for review. After performing a new search or accessing the existing searches from review set and research sets, the application displays the filtered emails, collaboration messages, and files in the details pane.
5. Click the **Emails** tab.
6. Select the email to view its details in the Preview pane.
7. Click the **More options** icon and select **Print**.

The entire email content appears on a browser.

8. Click **Print** to save the email on your local computer.

Restoring emails

To restore an email:

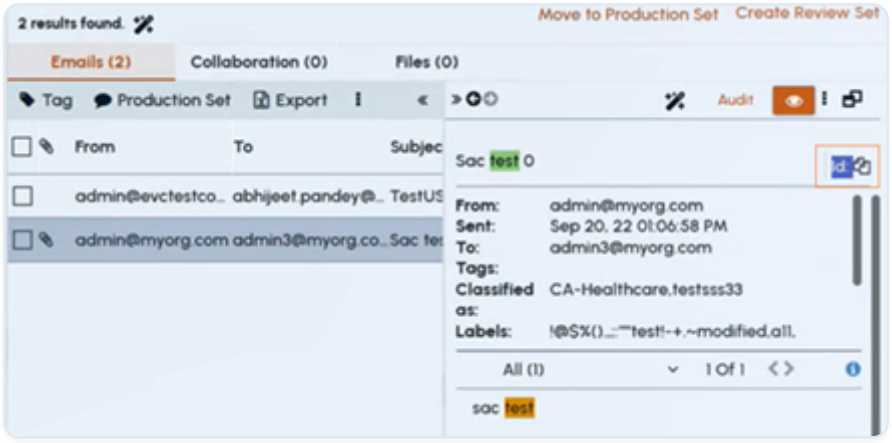
1. On the **eDiscovery** tab, click **Cases**.
2. Search for and select the case in which you want to search emails.
3. The selected ***Case_Name*** node appears below **Cases**.
4. Click **New Search** to create a new search. Else, expand **Research Sets** or **Review Sets** to select existing search.

   You can access existing saved searches of the selected case from the **Review Set** and **Research Set** nodes. Alternatively, you can click **New Search**, specify a new criteria in the *Advanced Search* or the *Query Search* option to search for new emails for review. After performing a new search or accessing the existing searches from review set and research sets, the application displays the filtered emails, collaboration messages, and files in the details pane.
5. Click the **Emails** tab.
6. Select the email to view its details in the Preview pane.
7. Click the **More options** icon and select **Restore**.
8. Search for and select the account for which you want to restore the email, and click **Restore**.

Searching for the exact Arctera Surveillance item for review

To search for the exact Arctera Surveillance item:

1. Browse the archives of accounts that are assigned to you. Conduct a search to filter the required items.
2. Select the item to preview its content.
3. If the item originates from Arctera Surveillance, its document ID appears in the preview pane, as shown in the example below.



4. Click the **Id** icon to copy the item ID.
5. In the Advanced Filter pane, expand the **Item Id Filter**, and paste the copied item Id.

> **Note:** When the **Item ID Filter** facet is used, all other filter facets are cleared to allow searching for only the exact matching Item ID in the archive.

6. Click **Search** to view the exact item in the preview pane.

Viewing audit history of emails

To view the audit history of a emails:

1. From the **eDiscovery** 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.
3. Click the ***case_name***>**Research Sets** or **Review Sets**.
4. Select the required search under the Research Sets or the Review Sets node.
5. On the **Emails** tab, select the emails to view its content in the preview pane.
6. On the Preview pane, click **Audit**.

   The application displays the audit history.
7. If required, use the navigation icons to go to the next page, previous page, the first page, and the last page.

Reviewing collaboration messages

The Collaboration tab appears only if the MS Teams service is enabled and the archive collector is configured for you. You can review all the files that are coming from the MS Teams. While reviewing the messages, you can perform the following actions:

- Applying tags
- Applying legal hold
- Applying review status
- Exporting collaboration messages
- Exporting search summary report
- Adding notes
- Viewing audit history

Accessing collaboration messages for review

To search Collaboration messages during investigation:

1. On the **eDiscovery** tab, click **Cases**.
2. Search for and select the case in which you want to search Collaboration messages.

   The selected ***Case_Name*** node appears below **Cases**.
3. Click **New Search** to create a new search. Else, expand **Research Sets** or **Review Sets** to select existing search.

   You can access existing saved searches of the selected case from the **Review Set** and **Research Set** nodes. Alternatively, you can click **New Search**, specify a new criteria in the *Advanced Search* or the *Query Search* option to search for new collaboration messages for review.

   After performing a new search or accessing the existing searches from review set and research sets, the application displays the filtered emails, collaboration messages, and files in the details pane.
4. Click the **Collaboration** tab to view the Chat and Channel messages for your review.
5. Select the collaboration message to view its details in the Preview pane.

> **Note:** Arctera eDiscovery does not support previewing certain file types, such as .dll and .exe and large files (over 30 MB to maintain browser responsiveness). For

> compressed files, Arctera eDiscovery supports previewing only the .zip file format and does not support other formats like .7z, .tar, and so on. If you cannot preview a specific file type, simply download it and use the appropriate tools to view its content.

Adding notes to collaborative messages

Reviewers can add notes to collaborative messages that are visible to other reviewers of that case. Notes are case-specific, therefore, a note that is applied to a collaborative messages in one case does not appear for the same collaborative messages in a different case. Notes can be provided to collaborative messages that are from the Review Sets only. You cannot provide notes to the collaborative messages that are from the Research Set.

To add a note to a collaborative message:

1. From the **eDiscovery** 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.
3. Click the ***case_name***>**Review Sets**.
4. Select the required search under the Research Sets or the Review Sets node.
5. On the **Collaboration** tab, select the collaboration message to view its content in the message preview pane.
6. Click the **More options** icon and select **Notes**.
7. In the **Add Notes** dialog box, specify the note about this message.
8. Click **Add** to save the note.

> **Note:** Different reviewers can add and save their notes for the same message. The application displays all the notes applied to the message that can be used for a collaborative reviews.

Applying and removing review status to collaboration message

Case reviewers can apply one of the following default review status to collaboration message to indicate its status in the eDiscovery review process:

- Not reviewed
- Escalate

- Irrelevant
- Privileged
- Redact
- Relevant

In addition, the eDiscovery Administrators can customize the available review status options.

To apply and remove review status to collaboration messages:

1. Under the associated case, select **Review Set**, and open the corresponding review set node.
2. To apply a review status to one or more collaboration messages directly from the **Review Set**:
   - Select the check box for one or more collaboration messages in the list, and click **Review Status**.
   - Then select the required review status.

   To remove the applied review status, click the selected review status again.
3. To apply a review status to an collaboration message while you view its details:
   - Select the message from the **Review Set** list to display its details.

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

- Select the required review status from the available options.

> **Note:** To view collaboration messages based on their review status, you can filter the required review status node under the **Filter** section.

Applying legal hold to collaboration messages

To apply legal hold to the collaboration messages during case review:

1. From the **eDiscovery** 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.
3. Click the ***case_name***>**Research Sets** or **Review Sets**.
4. Select the required search under the Research Sets or the Review Sets node.

5. On the **Collaboration** tab, select the collaboration messages to which you want to apply legal hold.

> **Note:** Before you apply legal hold to the collaboration messages, you can view the previously applied tags, labels, and classification tags of the message in the preview pane. In the following sample image, you can see the previously applied tags, labels, and classification tags of the collaboration messages when you hover over the icons.

6. On the action menu, click **Message Legal Hold**, and do any of the following as required.
   - To apply legal hold to the selected message, click **Message Legal Hold**.
   - To remove previously applied legal hold, click **Remove Message Legal Hold**.

Applying tags to collaboration messages

To apply tags to the collaboration messages during case review:

1. From the **eDiscovery** 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.
3. Click the ***case_name***>**Research Sets** or **Review Sets**.
4. Select the required search under the Research Sets or the Review Sets node.
5. In the right pane, on the **Collaboration** tab, select the collaboration messages to which you want to apply tags.

> **Note:** Before you apply tags to the items, you can view the previously applied tags and classification tags of the message in the preview pane. In the following sample image, you can see the previously applied tags and classification tags of the collaboration messages when you hover over the icons.

6. On the action menu, click **Tag**, and do any of the following as required.
   - To tag all the items in the search, click **Tag all messages**.
   - To tag only the selected items, click **Tag selected messages**.
7. In the **Add Tag** dialog box, do the following:

TAG NAME	ENTER A NEW UNIQUE TAG NAME.
Comments	Provide a comment or a description for the tag name.
Legal Hold	Select this check box if you want to apply the legal hold on the emails.
Select retention Tag	Instead of applying a new tag, you can apply the retention tags that are created in Arctera Unified Platform. To access and apply those retention tags, select this option, and choose the tags you want to apply.
	After you select this option, the application disables the Tag Name field.

8. Click **Tag**.

   After you apply tags to the emails, these tagged emails are available under the respective tags under the **Tags** node.

Exporting a search summary report for collaboration messages

To export a search summary report for messages during case review:

1. On the **eDiscovery** tab, click **Cases**.
2. Search for and select the case in which you want to search emails.
3. The selected ***Case_Name*** node appears below **Cases**.
4. Click **New Search** to create a new search. Else, expand **Research Sets** or **Review Sets** to select existing search.

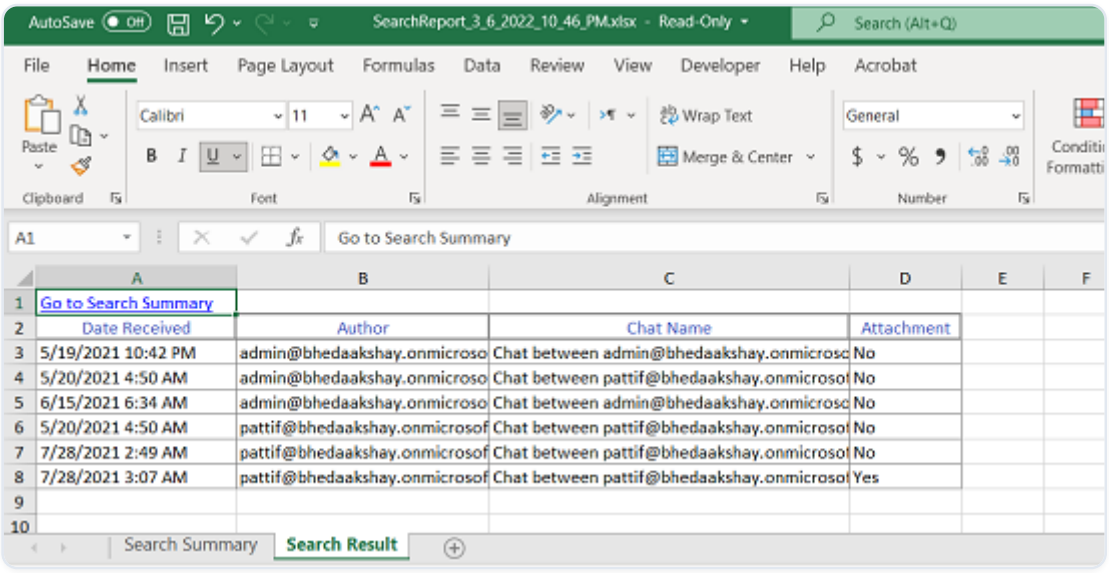
   You can access existing saved searches of the selected case from the **Review Set** and **Research Set** nodes. Alternatively, you can click **New Search**, specify a new criteria in the *Advanced Search* or the *Query Search* option to search for new emails for review.

- If you select the search from **Research Sets**, the application do not show the **Review Status** option on the action bar.
- If you select a search from **Review Sets**, choose any filter option, and click **Apply**, the **Export Report** button remains disabled.

After performing a new search or accessing the existing searches from review set and research sets, the application displays the filtered emails, collaboration messages, and files in the details pane.

1. On the **Collaboration** tab, click the Ellipsis icon (more actions) and click **Export Report**.

   The application downloads the summary report (.xlsx) of the emails within search as a zipped (.zip) folder. A sample report is shown below. The report comprises of two sheets.



Note

- **Search Summary**: This sheet displays details such as *Search Parameters* and *Custodians*.
- **Search Result**: This sheet displays details such as *Date Received*, *Author*, Chat Names (list of people involved in chat), and *Attachments*.
- The **Chat Name** column displays the email addresses of message recipients involved in a chat. This column supports up to 100 characters; any text beyond this limit is truncated in the exported report.

Exporting collaboration messages

To export collaboration messages:

1. On the **eDiscovery** tab, click **Cases**.
2. Search for and select the case in which you want to search collaboration messages.

   The selected ***Case_Name*** node appears below **Cases**.
3. Click **New Search** to create a new search. Else, expand **Research Sets** or **Review Sets** to select existing search.

> **Note:** You can access existing saved searches of the selected case from the **Review Set** and **Research Set** nodes. Alternatively, you can click **New Search**, specify a new criteria in the **Advanced Search** or the **Query Search** option to search for new collaboration messages for review. After performing a new search or accessing the existing searches from review set and research sets, the application displays the filtered emails, collaboration messages, and files in the details pane.

4. In the right pane, on the **Collaboration** tab, select the messages you want to export.
5. Click **Export**, and do any of the following:
   - Click **Export selected messages** to export all the selected messages from the search.
   - Click **Export all messages** to export all the messages available search.
   - Click **Export by custodians** to export all the messages from the selected custodians.
6. If you are exporting all or selected messages, in the **Export Options** dialog box, do the following:

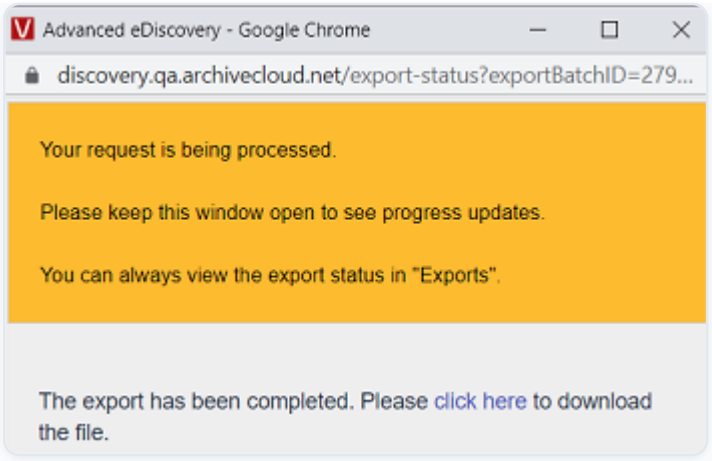
MESSAGE FORMAT	SELECT THE APPROPRIATE MESSAGE FORMAT FOR BATCH EXPORT. OPTIONS INCLUDE\:
	- JSON NOTE: THIS FORMAT IS SELECTED BY DEFAULT. WHEN YOU SELECT JSON FORMAT FOR EXPORT, FILES ARE DOWNLOADED IN THEIR ORIGINAL FORM, AND NOT AS JSON.
	- EDRM ONLY
Exclude Exported Messages	Select this option to exclude the exported messages.
Enable AES-256 Encryption	Select this check-box if you want to secure the access of the downloaded export batch.
Export Name	Provide the name for the batch you want to export. By default, it takes the Search Name. You can change it if required.

MESSAGE FORMAT	SELECT THE APPROPRIATE MESSAGE FORMAT FOR BATCH EXPORT. OPTIONS INCLUDE\:
	- JSON NOTE: THIS FORMAT IS SELECTED BY DEFAULT. WHEN YOU SELECT JSON FORMAT FOR EXPORT, FILES ARE DOWNLOADED IN THEIR ORIGINAL FORM, AND NOT AS JSON.
	- EDRM ONLY
Export Password	Enter the password that you want end user to provide when they access this exported batch of messages.
Confirm Password	Repeat the same password for confirmation.
Generate Azure SAS URL	**Note:** Users can see this button only if the **Export to Azure private storage location** feature in the Arctera Management Console is enabled for them. Users can export items to their private Azure Blob storage location.
	Click Generate Azure SAS URL to get the Azure Blob SAS URL to access the location and save it for future use.
	For security reasons, the application does not show this URL the next time. However, if the SAS URL is misplaced for any reason, click Generate Azure SAS URL again to generate a new SAS URL and save it securely.
	After you click Export on the Export Options dialog box, all the selected items are exported to the Azure private storage location. You can use Microsoft Storage Explorer to access the exported items.
Share Export	Click Select Admin to choose the recipients of this batch export and click Update.

MESSAGE FORMAT	SELECT THE APPROPRIATE MESSAGE FORMAT FOR BATCH EXPORT. OPTIONS INCLUDE\:
	- JSON NOTE: THIS FORMAT IS SELECTED BY DEFAULT. WHEN YOU SELECT JSON FORMAT FOR EXPORT, FILES ARE DOWNLOADED IN THEIR ORIGINAL FORM, AND NOT AS JSON.
	- EDRM ONLY
	Note: You need to manually share the Export Password with the administrators and follow all the security specific rules of the organization.

7. If you are exporting messages by custodians, in the **Add/Remove Custodians** dialog box, search for and select the custodians.
8. Click **Export**.

> **Note:** The exported batch can either gets downloaded as a single or multiple file segments.



9. Click **Click here** to download the exported batch of messages.
10. To confirm the status of batch export, on the **eDiscovery** tab, under the selected case node, select **Exports**, and search this export batch name.

Printing MS Teams messages to PDF during eDiscovery

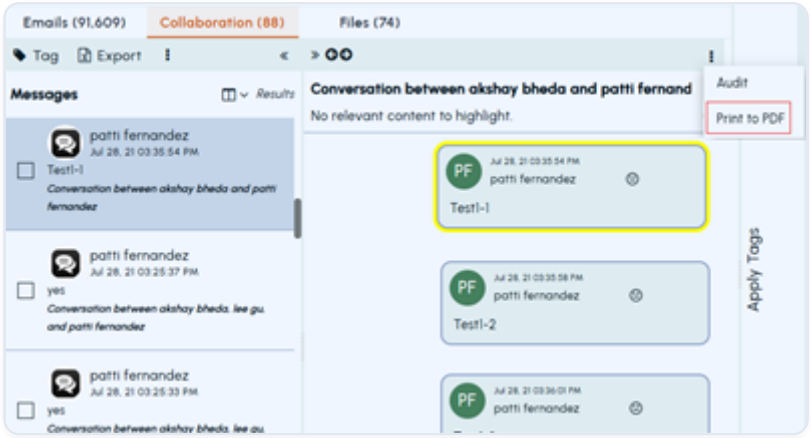
You can print collaboration messages collected from the *MS Teams* collectors using the Print to PDF feature. This feature is exclusive to *MS Teams* collaboration messages and is not supported for messages collected from other archive collectors.

> **Note:** This feature is not available for *Production Sets*, as it is not applicable in that context.

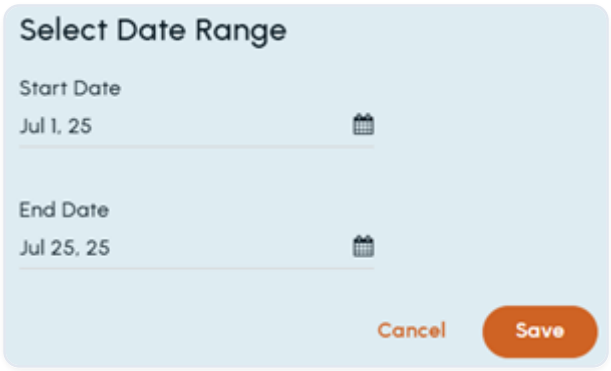
> **To print MS Teams messages to PDF during eDiscovery**:

1. From the **eDiscovery** 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.
3. Click the ***case_name***.
4. Access a required search result.
5. On the **Collaboration** tab, select the collaboration message.
6. Click the **More options** icon and select **Print To PDF**.

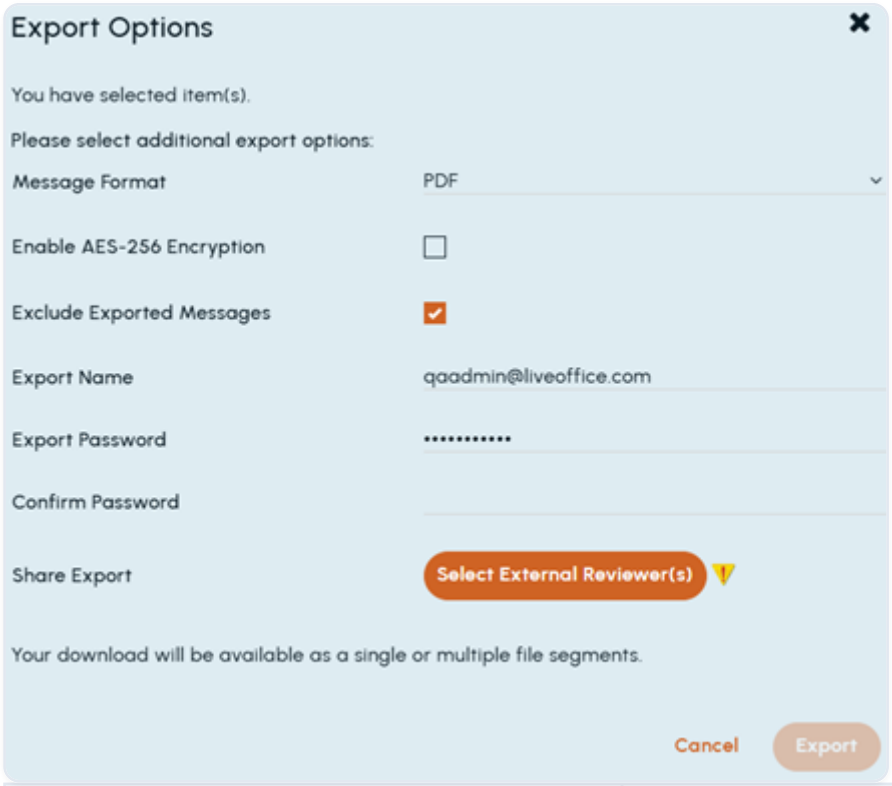


The application displays the **Select Date Range** as shown in the following sample image.



7. Specify the date range and click **Save**.

8. In the **Export Options** dialog box, specify the following details:



MESSAGE FORMAT	THE PDF FORMAT IS SELECTED BY DEFAULT.
Enable AES-256 Encryption	Select this check-box if you want to secure the access of the downloaded export batch.
Exclude Exported Messages	Select this option to exclude the exported messages.
Export Name	Provide the name for the batch you want to export. By default, it takes the Search Name. You can change it if required.
Export Password	Enter the password that you want end user to provide when they access this exported batch of messages.
Confirm Password	Repeat the same password for confirmation.
Share Export	Click Select Admin(s) to choose the recipients of this batch export and click Update.

MESSAGE FORMAT	THE PDF FORMAT IS SELECTED BY DEFAULT.
	Note: You need to manually share the Export Password with the administrators and follow all the security specific rules of the organization.

9. Click **Export**.

   A browser appears showing the progress. Upon completion, Click the **Click here** link to download the PDF.

Viewing audit history of collaboration messages

To view the audit history of a collaboration message:

1. From the **eDiscovery** 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.
3. Click the ***case_name***>**Research Sets** or **Review Sets**.
4. Select the required search under the Research Sets or the Review Sets node.
5. On the **Collaboration** tab, select the collaboration message to view its content in the message preview pane.
6. Click the **More options** icon and select **Audit**.

   The application displays the audit history as shown in the following sample image.
7. If required, use the navigation icons to go to the next page, previous page, the first page, and the last page.

Reviewing files

The Files tab appears only if the OneDrive for Business service is enabled and the archive collector is configured for you. You can review all the files that are coming from the OneDrive for Business. While reviewing the messages, you can perform the following actions:

- Toggle between the original format and the plain text format of the file
- Applying tags

- Applying Legal hold
- Applying review status
- Exporting files
- Adding notes
- Viewing audit history
- Downloading messages

Accessing files for review

To access files for review:

1. On the **eDiscovery** tab, click **Cases**.
2. Search for and select the case in which you want to search files.
3. The selected ***Case_Name*** node appears below **Cases**.
4. Click **New Search** to create a new search. Else, expand **Research Sets** or **Review Sets** to select existing search.

   You can access existing saved searches of the selected case from the **Review Set** and **Research Set** nodes. Alternatively, you can click **New Search**, specify a new criteria in the *Advanced Search* or the *Query Search* option to search for new files for review.

   After performing a new search or accessing the existing searches from Review set and Research sets, the application displays the filtered emails, collaboration messages, and files in the details pane.
5. Click the **Files** tab to view the files for your review.
6. Select a file to view its details in the native view in the **Preview** pane.

   > **Note:** Arctera eDiscovery does not support previewing certain file types, such as .dll and .exe and large files (over 30 MB to maintain browser responsiveness). For compressed files, Arctera eDiscovery supports previewing only the .zip file format and does not support other formats like .7z, .tar, and so on. If you cannot preview a specific file type, simply download it and use the appropriate tools to view its content.

7. Click **Native View** and **Text View** to toggle between the original file format and the plain text format respectively.

Adding notes to files

Reviewers can add notes to files that are visible to other reviewers of that case. Notes are case-specific, therefore, a note that is applied to a files in one case does not appear for the same file in a another case. Notes can be provided to files that are from the Review Sets only. You cannot provide notes to the files that are from the Research Set.

To add a note to a file:

1. From the **eDiscovery** 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.
3. Click the ***case_name***>**Review Sets**.
4. Select the required search under the Review Sets node.
5. On the **Files** tab, select the file to view its content in the preview pane.
6. Click the **More options** icon and select **Notes**.
7. In the **Add Notes** dialog box, specify the note about this file.
8. Click **Add** to save the note.

Applying and removing review status to files

Case reviewers can apply one of the following default review status to files to indicate its status in the eDiscovery review process:

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

In addition, the eDiscovery Administrators can customize the available review status.

To apply and remove review status to a file:

1. Under the associated case, select **Review Set**, and open the corresponding review set node.
2. To apply a review status to one or more files directly from the **Review Set**:

- Select the check box for one or more files in the list. In the preview pane, click **Review Status**.
- Then select the required review status.

To remove the applied review status, click the selected review status again.

3. To apply a review status to a file while you view its details:
   - Select the file from the **Review Set** list to display its details.

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

- Select the required review status from the available options.

  To remove the applied review status, click the selected review status again.

> **Note:** To view collaboration messages based on their review status, you can filter the required review status node under the **Filter** section.

Applying or removing legal hold to files

To apply or remove legal hold to the files during case review:

1. From the **eDiscovery** 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.
3. Click the ***case_name***>**Research Sets** or **Review Sets**.
4. Select the required search under the Research Sets or the Review Sets node.
5. In the right pane, on the **Files** tab, select the files to which you want to apply legal hold.
6. On the action menu, click **File Legal Hold**, and do any of the following as required.
   - To apply legal hold to the selected files, click **File Legal Hold**.
   - To remove previously applied legal hold, click **Remove File Legal Hold**.

Applying tags to Files

To apply tags to the files during case review:

1. From the **eDiscovery** 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.

3. Click the ***case_name***>**Research Sets** or **Review Sets**.
4. Select the required search under the Research Sets or the Review Sets node.
5. On the **Files** tab, select the files to which you want to apply tags.

   > **Note:** Before you apply tags to the files, you can view the previously applied tags and classification tags of the files in the preview pane.

6. On the action menu, click **Tag**, and do any of the following as required.

   - To tag all the files in the search, click **Tag all files**.
   - To tag only the selected files, click **Tag selected files**.

7. In the **Add Tag** dialog box, do the following:

TAG NAME	ENTER A NEW UNIQUE TAG NAME.
Comments	Provide a comment or a description for the tag name.
Legal Hold	Select this check box if you want to apply the legal hold on the files.
Select retention Tag	Instead of applying a new tag, you can apply the retention tags that are created in Arctera Unified Platform. To access and apply those retention tags, select this option, and choose the tags you want to apply.
	After you select this option, the application disables the Tag Name field.

8. Click **Tag**.

   After you apply tags to the files, these tagged files are available under the respective tags under the **Tags** node.

Downloading files

To download a file:

1. On the **eDiscovery** tab, click **Cases**.
2. Search for and select the case in which you want to search files.
3. The selected ***Case_Name*** node appears below **Cases**.
4. Click **New Search** to create a new search. Else, expand **Research Sets** or **Review Sets** to select existing search.

   You can access existing saved searches of the selected case from the **Review Set** and **Research Set** nodes. Alternatively, you can click **New Search**, specify a new criteria in the *Advanced Search* or the *Query Search* option to search for new files for review. After performing a new search or accessing the existing searches from Review set and Research sets, the application displays the filtered emails, collaboration messages, and files in the details pane.
5. Click the **Files** tab to view the files for your review.
6. Select the file to view its details in the **Preview** pane.
7. Click **Native View** and **Text View** to toggle between the original file format and the plain text format respectively.
8. Click the **Download** icon to save copy of a file on your local computer.

Exporting a search summary report for files

To export a search summary report for files during case review:

1. On the **eDiscovery** tab, click **Cases**.
2. Search for and select the case in which you want to search emails.
3. The selected ***Case_Name*** node appears below **Cases**.
4. Expand **Research Sets** or **Review Sets** to select existing search.
5. Select the filter options and click **Apply**.
6. On the **Files** tab, and click **Export Report**.

> **Note:** The following sample image is specific to a search in **Review Sets**. If you select the search from **Research Sets**, the application do not show the **Review Status** option on the action bar.

> The application downloads the summary report (.xlsx) of the emails within the search as a zipped (.zip) folder.

> **Note:** If you select a search from **Review Sets**, and select any filter option and click **Apply**, the **Export Report** option is not displayed. The **Export Report** functionality is not available for the searches in **New Search**.

Exporting files

To export files:

1. On the **eDiscovery** tab, click **Cases**.
2. Search for and select the case in which you want to search files.

   The selected ***Case_Name*** node appears below **Cases**.
3. Click **New Search** to create a new search. Else, expand **Research Sets** or **Review Sets** to select existing search.

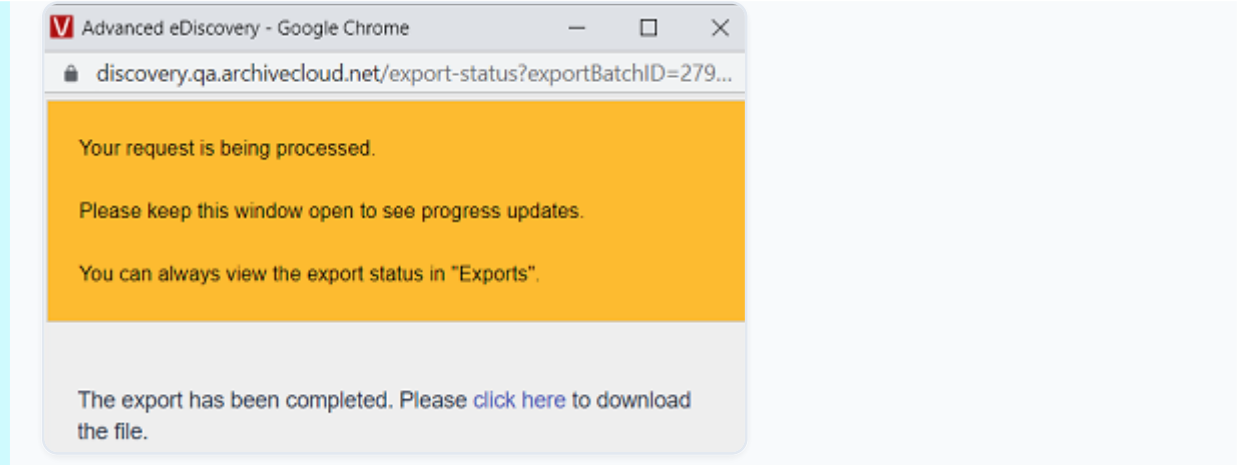
   > **Note:** You can access existing saved searches of the selected case from the **Review Set** and **Research Set** nodes. Alternatively, you can click **New Search**, specify a new criteria in the **Advanced Search** or the **Query Search** option to search for new files for review. After performing a new search or accessing the existing searches from review set and research sets, the application displays the filtered emails, collaboration messages, and files in the details pane.
4. In the right pane, on the **Files** tab, select the files you want to export.
5. Click **Export**, and do any of the following:
   - Click **Export all files** to export all the files available search.
   - Click **Export selected files** to export all the selected files from the search.
   - Click **Export by custodians** to export all the files from the selected custodians.
6. If you are exporting all or selected files, in the **Export Options** dialog box, do the following:

MESSAGE FORMAT	SELECT THE APPROPRIATE MESSAGE FORMAT FOR BATCH EXPORT. OPTIONS INCLUDE\:
	- JSON NOTE: THIS FORMAT IS SELECTED BY DEFAULT. WHEN YOU SELECT JSON FORMAT FOR EXPORT, FILES ARE DOWNLOADED IN THEIR ORIGINAL FORM, AND NOT AS JSON.
	- EDRM ONLY
Exclude Exported Messages	Select this option to exclude the exported messages.
Enable AES-256 Encryption	Select this check-box if you want to secure the access of the downloaded export batch.
Export Name	Provide the name for the batch you want to export. By default, it takes the Search Name. You can change it if required.
Export Password	Enter the password that you want end user to provide when they access this exported batch of messages.
Confirm Password	Repeat the same password for confirmation.
Generate Azure SAS URL	**Note:** Users can see this button only if the **Export to Azure private storage location** feature in the Arctera Management Console is enabled for them. Users can export items to their private Azure Blob storage location.
	Click Generate Azure SAS URL to get the Azure Blob SAS URL to access the location and save it for future use.
	For security reasons, the application does not show this URL the next time. However, if the SAS URL is misplaced for any reason, click Generate Azure SAS URL again to generate a new SAS URL and save it securely.

MESSAGE FORMAT	SELECT THE APPROPRIATE MESSAGE FORMAT FOR BATCH EXPORT. OPTIONS INCLUDE\:
	- JSON NOTE: THIS FORMAT IS SELECTED BY DEFAULT. WHEN YOU SELECT JSON FORMAT FOR EXPORT, FILES ARE DOWNLOADED IN THEIR ORIGINAL FORM, AND NOT AS JSON.
	- EDRM ONLY
	After you click Export on the Export Options dialog box, all the selected items are exported to the Azure private storage location. You can use Microsoft Storage Explorer to access the exported items.
Share Export	Click Select Admin to choose the recipients of this batch export and click Update.
	Note: You need to manually share the Export Password with the administrators and follow all the security specific rules of the organization.

7. If you are exporting files by custodians, in the **Add/Remove Custodians** dialog box, search for and select the custodians.
8. Click **Export**.

> **Note:** The exported batch can either gets downloaded as a single or multiple file segments.



9. Click **Click here** to download the exported batch of files.
10. To confirm the status of batch export, on the **eDiscovery** tab, under the selected case node, select **Exports**, and search this export batch name.

Viewing audit history of files

To view the audit history of a file:

1. From the **eDiscovery** 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.
3. Click the ***case_name***>**Research Sets** or **Review Sets**.
4. On the **Files** tab, select the file to view its content in the preview pane.
5. Click the **More options** icon and select **Audit**.
6. The application displays the audit history as shown in the following sample image.
7. If required, use the navigation icons to go to the next page, previous page, the first page, and the last page.

Translating email, collaboration message, and file content

The translation feature enables eDiscovery reviewers to translate non-English content directly in the item preview without downloading the item or using an external translation tool.

As a reviewer, you can translate complete or partial (selected portion) content of an email or collaboration message. However, for files and attachments, only the selected portion of the content can be translated.

When you translate the complete content, the English translation replaces the original content in the preview. The **Translate** icon changes to **Revert**, which you can use to restore the original content.

The **Translate selected text to English** icon becomes available only after you select text in the item body. Existing search-term highlights remain visible in the translated text.

> **Note:** Full-item translations of emails and collaboration messages are cached for seven days. If you translate the same item again during this period, eDiscovery retrieves the cached translation instead of submitting another translation request. This reduces the associated AI usage.

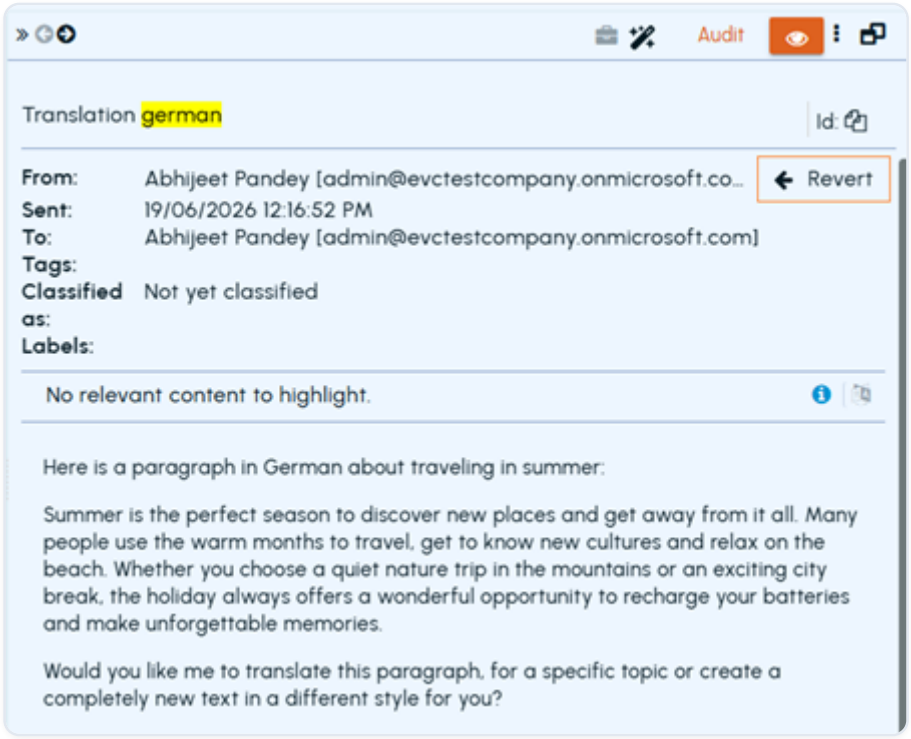
Prerequisites

Ensure that the Translation feature is enabled for you or your group. If the feature is unavailable, contact your system administrator.

To translate the complete content of email or collaboration message:

1. On the **Emails** or **Collaboration** tab, select an item to preview its content.Refer to the sample image below.

2. Click the **Translate** icon provided in the Preview pane.The application translates the content into English, and the **Translate** icon changes to **Revert** as shown in the sample image below. (The same options are available when you open the item in full-screen view.)

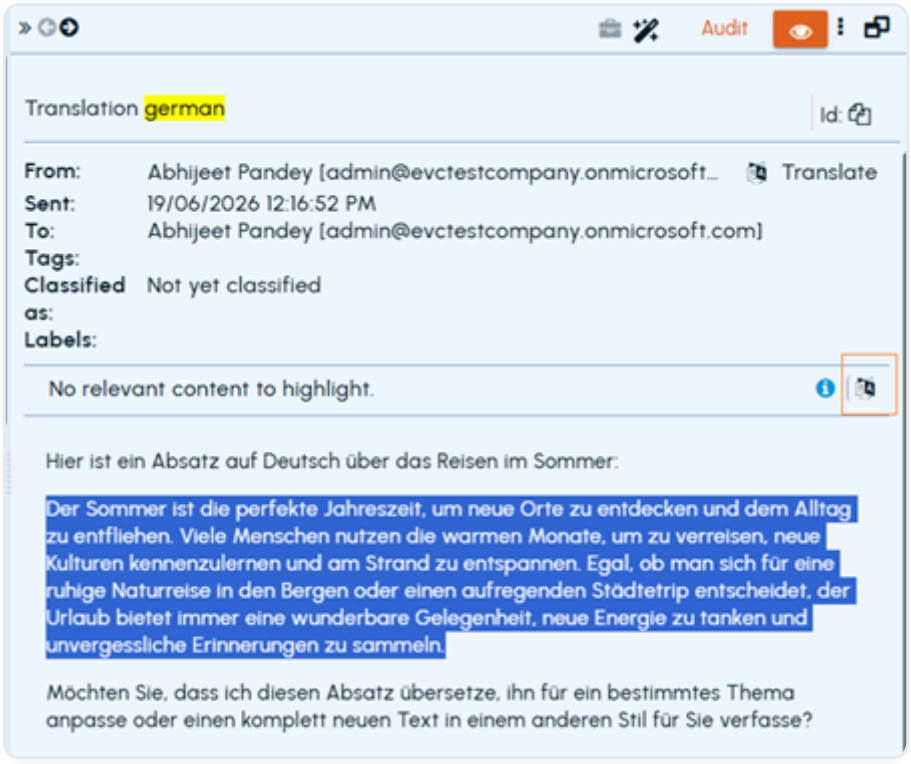


3. Click **Revert** to return to the original language.

To translate the selected text in email, collaboration message, or file attachment:

4. On the **Emails**,**Collaboration **or **Files** tab, select an item to preview its content and attachments. The item and its available attachments open in the Preview pane.
5. Select the text that you want to translate.

   The **Translate selected text to English** icon becomes available. Refer to the sample image below.



6. Click **Translate selected text to English**.

   The application translates the selected text and highlights the translated section. Existing search-term highlights remain visible.

> **Note:** A selected-text translation is temporary. The **Revert** option is not available. When you navigate away from the item, the translation is discarded. When you return to the item, the original content is displayed.

Annotating and redacting email and file content in native viewer

Annotations

Depending on your review requirements, you can add text and shape annotations to a document. For example, you can annotate the text or area with arrows, lines, boxes, stamps and then customize the line size, color, and fill color. You can also add comments for other users of the document. These annotations can be viewed and edited by other users for which you might need appropriate permissions. You can print and download such annotations for further use.

Redactions

Depending on your review requirements, you can draw dark rectangles to hide sensitive information within a document to avoid a confidentiality breach. You can determine the

transparency level of such dark rectangles as required. When you print the document, you can permanently add these redactions over the content or entire page, and provide reasons for redactions. You can print and download such redactions for further use.

See About annotations and redactions.

Managing legal hold notifications

This section includes the following topics:

About legal hold notifications

A legal hold is a process used to preserve information that may be required for legal proceedings, investigations, or regulatory matters. When a legal hold is issued, custodians are notified to preserve the relevant information until the hold is released.

The **Legal Hold Notifications** feature in Arctera eDiscovery provides a centralized workflow to manage the complete legal hold lifecycle, from creating legal holds and sending preservation notices to tracking notice delivery, acknowledgments, reminders, escalations, survey responses, and notice events. This workflow replaces manual email and spreadsheet-based legal hold processes. Each legal hold progresses through the **Active**,**Released**, and **Archived** stages of its lifecycle.

Access to this feature is restricted to **eDiscovery Administrators**. Users with this role can access the **Legal Hold Notifications** node under the **eDiscovery** tab.

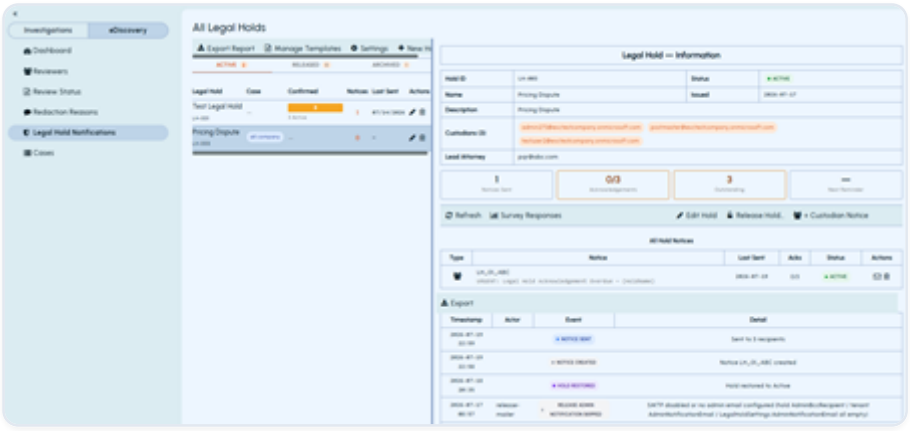
Using this feature, eDiscovery Administrators can:

- Configuring legal hold notification settings
- Managing legal hold notice templates
- Creating legal holds
- Accessing legal holds
- Editing legal holds
    - Include survey or questionnaire questions in custodian notices.
    - Track notice delivery and custodian acknowledgments.
    - View and export survey responses and notice events.
    - Resend notices to custodians who have not acknowledged them.
- Sending a legal hold notice to custodians
- Releasing a legal hold
- Archiving and deleting legal holds
- Restoring a released or archived legal hold
- Deleting legal holds

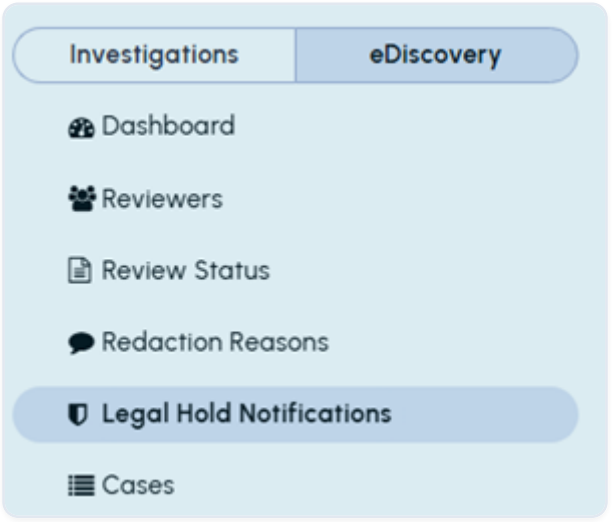
This feature uses **OTP-protected acknowledgment links** to help verify that custodians have acknowledged their legal hold notices. Custodian acknowledgment helps confirm that the preservation instruction was received and understood. If a notice is not acknowledged, administrators can identify outstanding responses and follow up with custodians before the acknowledgment link expires. Each acknowledgment link remains valid for 30 days from the time the notification is sent.

The Legal Hold Notifications workspace includes the navigation pane, the All Legal Holds page, and the Legal Hold — Information pane. The following sample images show the main areas of the Legal Hold Notifications workspace, including where to access the feature, view legal holds, and review details for a selected legal hold and available actions.

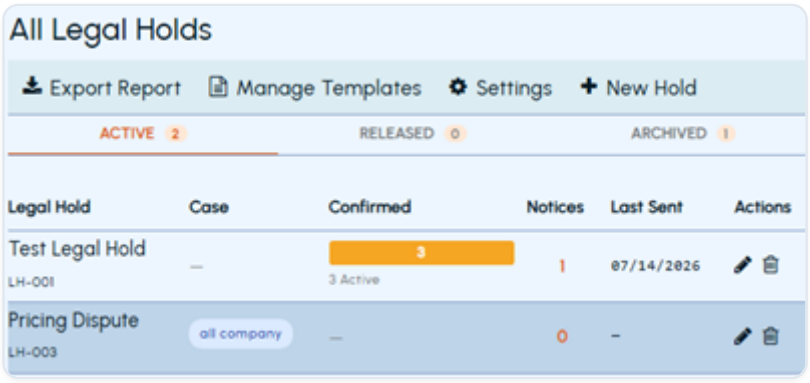
Entire workspace:



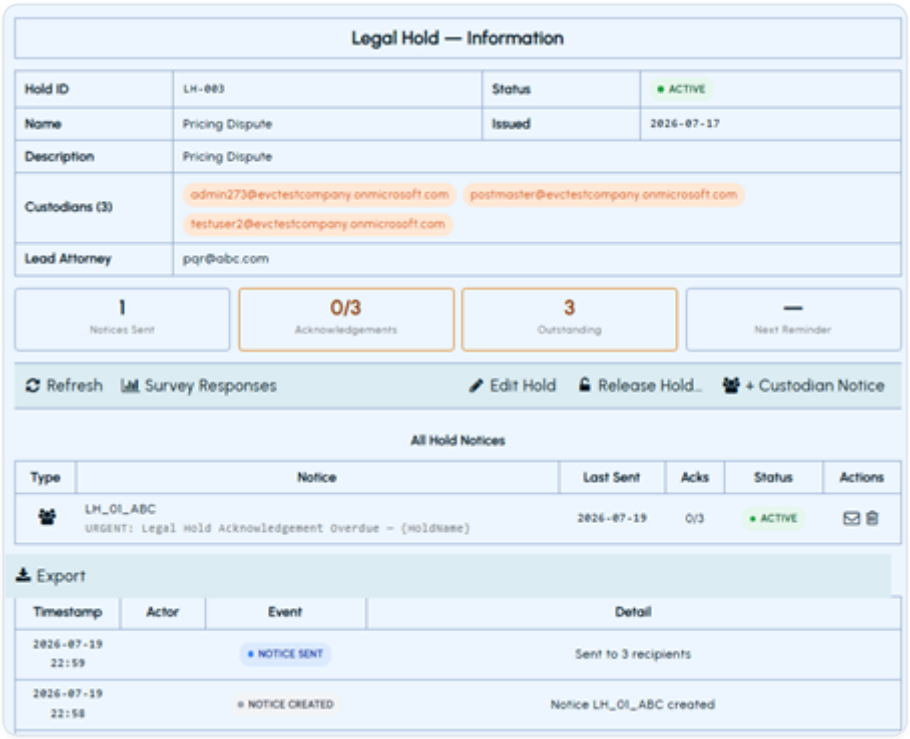
Legal Hold Notifications option in the eDiscovery navigation pane:



All Legal Holds page showing legal holds by status:



Legal Hold — Information pane showing details and actions for the selected legal hold:



Configuring legal hold notification settings

As an eDiscovery Administrator, you can use the **Legal Hold Settings** page to define:

- default administrative recipients who receive summary emails or hidden copies of legal hold notices sent to custodians.
- default notice content and footer text for reminder notices, escalation notices, hold release notices, and status reminder notices.

When a legal hold is created, these defaults prepopulate the notice fields. You can override the defaults to personalize the notice for a specific legal matter.

To configure legal hold notification settings:

1. On the **eDiscovery** tab, select **Legal Hold Notifications**.

   The **All Legal Holds** page appears.

2. Click **Settings**.

   The **Legal Hold Settings** page appears.

3. In the **General** section, do the following:

   - In the **Admin Notification Email** field, enter one or more email addresses who should receive summary emails when a legal hold notice is created or updated and the Send a copy to admin option is selected while sending the notice.

Separate multiple email addresses with semicolons.

- In the **Admin Bcc Recipient** field, enter one or more email addresses to receive hidden copies of summary emails when a legal hold notice is created or updated and the Send a copy to admin option is selected while sending the notice.

  Separate multiple email addresses with semicolons.

4. In the **Default Custodian Notices** section, specify the email subject line and the email body content for the following:

   - Default Reminder Notice
   - Default Escalation Notice
   - Default Hold Release Notice
   - Default Repeating Status Reminder Notice

   This subject line and content will appear while creating a legal hold.
5. In the **Default Footer Text** section, specify the default footer text for the following:

   - Initial, Reminder, and Escalation notice
   - Hold Release and Repeating Status Reminder notice
6. Click **Save Settings**.

Managing legal hold notice templates

As an eDiscovery Administrator, you can use the **Legal Hold Notice Templates** page to define reusable content for custodian and administrator notices. Templates help standardize notice content and reduce the effort required to create similar notices for different legal holds.

You can use templates to:

- Create templates for custodian and administrator notices.
- Add merge tokens to personalize notice content.

> **Note:** Merge tokens are replaced with actual values when a notice is created from a template. For example, tokens such as `{HoldName}`, `{CustodianName}`, `{AcknowledgeLink}`, `{AcknowledgeBy}`, `{ReleaseDate}`, and `{CaseID}` can be used to personalize the notice subject and body.

- Edit template information.
- Reuse standard notice content when creating a legal hold notice.

To create a new notice template:

1. On the **eDiscovery** tab, select **Legal Hold Notifications**.

   The **All Legal Holds** page appears.

2. Click **Manage Templates**.

   The **Notice Templates** page appears.

3. Click **New Template**, and specify the following details:

OPTION	DESCRIPTION
Template Name	Enter a unique name for the notice template that clearly identifies the purpose of the template.
Audience	Select the intended audience for the template. You can create templates for custodian notices or administrator notices.
Subject Line	Enter the subject line for the notice.
Body	Enter the notice content.To reuse content from an existing active template, identify the template under **Active Templates**, and click the **Edit** icon in the corresponding row.The content from the selected template is populated in the **Body** field. You can review and modify the content as required.
Insert	Use merge tokens to personalize the notice subject and body.The available tokens are {HoldName}, {CustodianName}, {AcknowledgeLink}, {AcknowledgeBy}, {ReleaseDate}, and {CaseID}.To insert a token, place the cursor where you want the token to appear in the notice content, and then select the required token.When a notice is created from the template, these tokens are replaced with the corresponding legal

OPTION	DESCRIPTION
	hold, custodian, acknowledgment, release, or case values.

4. Click **Create Template**.

   The newly created legal hold notice template appears on the **Notice Templates** page.

Creating legal holds

As an eDiscovery Administrator, you can create a legal hold to define the preservation matter, associate it with a case, and configure default notice details for the hold. After the legal hold is created, you can create a custodian notice, add recipients, review or update the notice content, and configure the confirmation questionnaire. You can save the notice as a draft or send it immediately to the selected custodians.

To create a new legal hold:

1. On the **eDiscovery** tab, select **Legal Hold Notifications**.

   The **All Legal Holds** page appears.
2. Click **New Hold**.

   The **New Legal Hold** page appears. Specify the following details:

OPTION	DESCRIPTION
Legal Hold Name	Enter a unique name for the legal hold that clearly identifies the purpose of the legal hold notice.
Description	Describe the purpose of this legal hold notice.
Case	Select a case from the drop-down list to identify the legal matter for which the legal hold is being created. The selected case provides context for the hold and helps organize the related notices, custodians, acknowledgments, and audit

OPTION	DESCRIPTION
	information.Legal holds that are linked to a case also appear inside that case.
Admin Bcc Recipient	Enter one or more email addresses to receive an email for this outgoing legal hold notice. Separate multiple email addresses with semicolons.**Note:** These recipients are not visible to custodians.
Lead Attorney (Email)	Enter one or more email addresses of the attorneys associated with the legal hold. Separate multiple email addresses with semicolons. These recipients receive the outgoing legal hold notice and serve as legal contacts for questions or follow-up related to the hold.
Default Custodian Notices	Use this section to define default custodian-facing notice content and footer text for legal hold notifications. These defaults prepopulate the notice fields when a new legal hold is created and can be overridden for an individual hold.• Default Reminder Notice: Defines the default content for reminder notices sent to custodians.• Default Escalation Notice: Defines the default content for escalation notices.• Default Hold Release Notice: Defines the default content for notices sent when a legal hold is released.• Default Repeating Status Reminder Notice: Defines the default content for repeating status reminder notices.• Default Footer Text — Initial, Reminder & Escalation Notices: Defines the footer text for initial notices, reminder notices, and escalation notices.• Default Footer Text — Hold Release & Repeating Status Reminder: Defines the footer text for hold release notices and repeating status reminder notices.

3. Click **Create Hold**.

   The new legal hold appears on the **All Legal Holds** page, and the **Legal Hold — Information** page opens.

4. To add custodians to this legal hold, click Custodian Notice.

   The **New Custodian Notice** page appears. Specify the following details:

OPTION	DESCRIPTION
Name of Notice	Enter a unique name for the legal hold notice that clearly identifies the purpose.
Internal Notes (not sent)	Enter any internal notes about the legal hold notice. These notes are for administrative reference only and are not included in legal hold notices sent to custodians.
Load from Template	Select a template from the drop-down list to populate the notice content. You can review and edit the populated content before sending the notice.**Note:** Merge tokens in the template are not replaced when the template is loaded. They are resolved when the notice is sent and are replaced with values specific to each recipient.
From Name/From Email	Enter the name and email address of the notice issuer. This information appears as the sender on legal hold notices sent to custodians.
To — Custodians / Recipient	Specify the custodians who must receive the legal hold notice. You can enter one or more email addresses manually, separated by semicolons, or select **Browse Custodians** to choose custodians from the list.When you select **Browse Custodians**, the **Add/ Remove Custodians** window appears. Select the required custodians, and then select **Update**. The selected custodians appear in the **To — Custodians / Recipient** section.To add custodians manually, enter

OPTION	DESCRIPTION
	one or more email addresses, and then click **Add**.To add all browsed custodians, click **Select All**.To remove selected custodians, click **Remove Selected**. The count of selected custodians is displayed on the **Remove Selected** option.To deselect selected custodians, clear the corresponding check boxes, or select **Deselect All**.
Cc (comma-separated)	This read-only field displays other recipients included in the notice.
Subject	Review the subject line that is populated automatically. If the subject is relevant to the notice, keep it as is. Otherwise, enter a new subject line for the notice.
Body	Review the prepopulated notice content and update it as required for the legal matter. Use merge tokens if necessary. Use this field to provide the preservation instructions, acknowledgment details, and any additional information that custodians must know before acknowledging the notice.
Confirmation Page (Questionnaire) >	**Page Heading:** Enter the heading that appears on the custodian confirmation page.**Instruction text:** Enter instructions for custodians before they answer the questionnaire. Use this text to explain what custodians must review or complete before acknowledging the notice.**Question prompt:** Enter the question that the custodian must answer as part of the acknowledgment process. Click Add Question to enter a new question.**Type:** Select the response type for the question, such as Yes / No, freeform text, single choice, or multiple choice, depending on the available options.**Require Answer to Question:** Select this option to make the question mandatory. Custodians must

OPTION	DESCRIPTION
	answer required questions before they can complete the acknowledgment.**Add Question:** Select this option to add another question to the questionnaire.
Send a copy of changes to admin	Select this check box to send a notice summary email when the legal hold notice is created or updated. The summary is sent to the email address shown next to this option.

5. To save the notice without sending it, click **Save as Draft**. You can edit and send the draft later.
6. To send the legal hold notice to the selected custodians, click **Send Now**.
7. To discard the current changes and abort changes, click **Cancel**.

Accessing legal holds

As an eDiscovery Administrator, you can access legal holds according to their lifecycle status: **Active**,**Released**, or **Archived**. These views help you quickly identify legal holds that are active, released, or archived.

Use the **All Legal Holds** pane to review legal hold details, such as the legal hold name, associated case, confirmation progress, number of notices, and last sent date. Depending on the legal hold status, the **Actions** column displays the actions that you can perform on the legal hold.

To access legal holds status wise:

1. On the **eDiscovery** tab, select **Legal Hold Notifications**.

   The **All Legal Holds** page appears.
2. To view active legal holds, select the **Active** tab.

   The **Active** tab displays legal holds that are currently in progress. From this tab, you can review the legal hold details and use the icons in the **Actions** column to edit, archive, or delete a legal hold.
3. To view released legal holds, select the **Released** tab.

   The **Released** tab displays legal holds that have been released. From this tab, you can review the legal hold details and use the icons in the **Actions** column to edit, restore, archive, or delete a legal hold.

4. To view archived legal holds, select the **Archived** tab.

   The **Archived** tab displays legal holds that have been archived. From this tab, you can review the legal hold details and use the icons in the **Actions** column to edit or delete a legal hold.

Editing legal holds

As an eDiscovery Administrator, you can edit legal holds that are Active. You cannot edit legal holds that are either in a Released or Archived state.

To edit a legal hold:

1. On the **eDiscovery** tab, select **Legal Hold Notifications**.

   The **All Legal Holds** page appears.

2. On the **Active** tab, select the legal hold that you want to edit.

   The **Legal Hold — Information** page appears.

FIELD	DESCRIPTION
Hold ID	Displays the unique identifier of the legal hold.
Status	Displays the **Active** status of the legal hold. Remember, you can edit legal holds that are **Active**.
Name	Displays the name of the legal hold.
Issued	Displays the date on which the legal hold was issued.
Description	Displays the description provided for the legal hold.
Custodians	Displays the custodians associated with the legal hold. The number indicates the total custodians added to the hold.
Lead Attorney	Displays the **Lead Attorney** associated with the legal hold. The number indicates the total custodians added to the hold.

FIELD	DESCRIPTION
Notices Sent	Displays the number of legal hold notices sent for the hold.
Acknowledgements	Displays the number of acknowledgments received against the total number of custodians.
Outstanding	Displays the number of custodians who have not acknowledged the notice.
Next Reminder	Displays the next scheduled reminder, if available.
Refresh	Click to refresh the legal hold information displayed on the page.
Survey Responses	Click to view responses submitted by custodians for the legal hold.The **Survey Responses** page appears, where you can review the acknowledgment status and questionnaire responses of custodians who received the legal hold notice. The page shows the total number of recipients, the number of custodians who have acknowledged the notice, and the number of custodians whose acknowledgment is pending.You can search for a recipient, review the recipient's response details.Click **Export CSV** to export the responses to a CSV file.
Edit Hold	Opens the legal hold information for editing.
Release Hold	Click to release the selected legal hold. Releasing a hold changes its status from **Active** to **Released** and indicates that custodians are no longer required to preserve information for this hold. If a hold release notice is configured, it can be sent to custodians to inform them that the hold has been released.

FIELD	DESCRIPTION
Custodian Notice	Click to create a notice for the selected legal hold. You can add custodians who must receive this notice, update the notice content if required, and add questions for custodians to answer. For more information, see Sending a legal hold notice to custodians.
All Hold Notices	Lists the notices associated with this legal hold.
Type	Displays the notice type, such as custodian notice or administrator notice. Each notice type can be identified by a different icon.
Notice	Displays the notice name and subject line.
Last Sent	Displays the date on which the notice was last sent.
Acks	Displays the number of recipients who have acknowledged the notice.
Status	Displays the status of the notice.
Actions	Displays the actions available for the notice.• Click the **Resend to Unacknowledged** icon to resend the notice to recipients who have not acknowledged it.• Click the **Delete or Archive** icon to delete or archive the notice, as required.
Export	Click to export the legal hold event information. The exported information includes the event date and time, the user or system that performed the event, the event type, and additional event details.

3. Click **Edit Hold**.
4. In the **Edit Legal Hold** window, you can do the following as required:

    - Revise legal hold name and description

- Add one or more email addresses of lead attorney and Admin BCC Recipient. Separate multiple email addresses with semicolons.

5. Click **Save**.

   The changes reflect on the **Legal Hold — Information** page.

6. Else, click **Refresh** to update the modified details on the page.

Sending a legal hold notice to custodians

As an eDiscovery Administrator, you can send a legal hold notice to custodians to inform them about the preservation requirements for a legal hold and request their acknowledgment.

Before sending the notice, review the recipients, sender details, subject, notice body, and confirmation questionnaire; after the notice is sent, custodians can acknowledge it through the OTP-protected acknowledgment link.

To send a legal hold notice to custodians:

1. On the **eDiscovery** tab, select **Legal Hold Notifications**.

   The **All Legal Holds** page appears.

2. On the **Active** tab, select the legal hold that you want to edit.

   The **Legal Hold — Information** page appears. For more information about fields available on this page, see Editing legal holds.

3. Click **Custodian Notice**, and specify the following:

FIELD	DESCRIPTION
Name of Notice	Enter a unique name for the legal hold notice. Use a name that clearly identifies the purpose of the notice.
Internal Notes (not sent)	Enter internal notes about the notice. These notes are for administrative reference only and are not included in notices sent to custodians.
Load from Template	Select a template to populate the notice content. Review and edit the populated content before sending the notice.If the

FIELD	DESCRIPTION
	template includes merge tokens, keep the tokens where recipient-specific information is required. The system replaces these placeholders with actual values when the notice is sent.For example, {CustodianName} is replaced with the name of each custodian, and {HoldName} is replaced with the name of the legal hold. This helps personalize the same notice for different recipients.
From Name	Enter the name of the notice issuer. This name appears as the sender on the legal hold notice.
From Email	Enter the email address of the notice issuer. Custodians see this email address as the sender of the legal hold notice.
To — Custodians / Recipients	Specify the custodians who must receive the legal hold notice. You can enter one or more email addresses manually, separated by semicolons, or select **Browse Custodians** to choose custodians from the list.When you select **Browse Custodians**, the **Add/ Remove Custodians** window appears. Select the required custodians, and then select **Update**. The selected custodians appear in the **To — Custodians / Recipient** section.To add custodians manually, enter one or more email addresses, and then click **Add**.To add all browsed custodians, click **Select All**.To remove selected custodians, click **Remove Selected**. The count of selected custodians is displayed on the **Remove Selected** option.To deselect selected custodians, clear the corresponding check boxes, or select **Deselect All**.
Cc (comma-separated)	Enter one or more email addresses of additional recipients to include in the notice.

FIELD	DESCRIPTION
	Separate multiple email addresses with semicolons.
Subject	Review the subject line that is populated automatically. Keep it if it is relevant to the notice, or enter a new subject line.
Insert variable	Select a merge token to insert a dynamic value in the subject. The token is replaced with the corresponding value when the notice is sent.
Body	Review the prepopulated notice content and update it as required for the legal matter. Use this field to provide preservation instructions, acknowledgment details, and other information that custodians must know before acknowledging the notice.
Insert variable	Select a merge token to insert a dynamic value in the email content. The token is replaced with the corresponding value when the notice is sent.
Page Heading	Enter the heading that is required to appear on the custodian confirmation page.
Instruction text	Enter instructions that custodians must review before answering the questionnaire.
Question prompt/Type	Enter the question that the custodian must answer as part of the acknowledgment process.Select the response type for the question, such as **Yes / No**, freeform text, single choice, or multiple choice.
Add Question	Adds another question to the questionnaire.
Require Answer to Question	Select this option to make the question mandatory. Custodians must answer

FIELD	DESCRIPTION
	required questions before they can complete the acknowledgment.
Send a copy of changes to admin	Select this option to send a notice summary email to the configured administrator email address.
Cancel	Click to discard the current changes and close the notice page without sending the notice.
Save as Draft	Click to save the notice without sending it. You can edit and send the draft later.

4. Click **Send Now**.

Releasing a legal hold

As an eDiscovery Administrator, you can release an active legal hold when the preservation requirement for the legal matter no longer applies. Releasing a legal hold moves it from the **Active** tab to the **Released** tab.

When a legal hold is released, custodians who are active on the hold are released from the hold and receive a release notice.

To release a legal hold:

1. On the **eDiscovery** tab, select **Legal Hold Notifications**.

   The **All Legal Holds** page appears.
2. On the **Active** tab, select the legal hold that you want to edit.

   The **Legal Hold — Information** page appears.
3. Review the legal hold details before releasing the legal hold.
4. On the **Legal Hold — Information** page, click **Release Hold**.
5. Ensure that the Active legal hold is released and displayed on the **Released** tab.

Archiving and deleting legal holds

As an eDiscovery Administrator, you can archive or delete a legal hold when you no longer need to track custodians, send follow-up notices, or manage acknowledgments for the hold. Before you choose an action, understand the difference between archiving and deleting a legal hold.

- Archive a legal hold when you want to remove it from the current legal hold workflow but retain it for later viewing or further action. You can archive only active and released legal holds. When you archive a legal hold, it is moved from its current status view to the **Archived** tab. If custodians are active on any notice, they are released from the hold and receive a release notice. Archived legal holds remain available on the **Archived** tab, where you can view the hold details and perform the available actions.
- Delete a legal hold only when the hold and its notices are no longer required for viewing or further action. You can delete active, released, or archived legal holds. Deleted legal holds and notices are removed from the legal hold views and are not shown on any tab. After a legal hold is deleted, it cannot be viewed or restored.

To archive or delete a legal hold:

1. On the **eDiscovery** tab, select **Legal Hold Notifications**.

   The **All Legal Holds** page appears.
2. Do one of the following as needed:
   - To archive a legal hold, select the **Active** or **Released** tab.
   - To delete a legal hold, select the **Active**,**Released**, or **Archived** tab.
3. Identify and review the legal hold that you want to archive or delete.
4. In the **Actions** column, select the **Delete or Archive** icon.

   The **Delete Confirmation** dialog box appears.
5. Perform one of the following actions:
   - To archive the legal hold, select **Archive**.

     The legal hold is archived and appears on the **Archived** tab. Custodians who are active on any notice are released from the hold and receive a release notice.
   - To delete the legal hold, select **Delete**.

     The legal hold and its notices are removed from the legal hold views and are no longer available for viewing or further action.

Restoring a released or archived legal hold

As an eDiscovery Administrator, you can restore a released or archived legal hold when the hold must be made active again for further management. For example, you may restore a hold if it was released or archived by mistake or if the preservation requirement still applies. However, after a legal hold is deleted, it cannot be viewed or restored.

Restoring a legal hold moves it from the **Released** tab or the **Archived** tab back to the **Active** tab. After the hold is restored, you can continue managing the hold and its related notices.

To restore released or archived legal hold:

1. On the **eDiscovery** tab, select **Legal Hold Notifications**.

   The **All Legal Holds** page appears.
2. Select the **Released** tab or the **Archived** tab, as necessary.
3. Review the legal hold details, such as the legal hold name, case, confirmation progress, notices, and last sent date.
4. Click the **Restore** icon.
5. Ensure that the released legal hold is restored and displayed on the **Active** tab.

Deleting legal holds

As an eDiscovery Administrator, you can delete a legal hold when the hold and its notices are no longer required for viewing, tracking, or further action.

Delete a legal hold only when you do not need to retain it in the legal hold views. Deleted legal holds and notices are removed from the legal hold views and are not shown on the **Active**,**Released**, or **Archived** tabs. After a legal hold is deleted, it cannot be viewed or restored.

To delete a legal hold:

1. On the **eDiscovery** tab, select **Legal Hold Notifications**.

   The **All Legal Holds** page appears.
2. Select the tab that contains the legal hold that you want to delete.

   You can delete a legal hold from the **Active**,**Released**, or **Archived** tab, depending on the actions available for the legal hold.
3. Identify and review the legal hold that you want to delete.

4. In the **Actions** column, select the **Delete** icon.

   The **Delete Confirmation** dialog box appears.

5. Click the **Delete** icon.

   The legal hold and its notices are removed from the legal hold views.

6. Ensure that the deleted legal hold is not displayed on the **Active**,**Released**, or **Archived** tab.

Exporting a legal hold report

This legal hold report can be downloaded as a CSV file for reference or other purpose. **To export report of all legal holds**:

1. On the **eDiscovery** tab, select **Legal Hold Notifications**.

   The **All Legal Holds** page appears.

2. Click **Export CSV** to download the report as a CSV file.

   The report includes details such as the legal hold name, associated case, confirmation progress, number of notices, and last sent date.

Managing production sets

This section includes the following topics:

Exporting production sets

Arctera eDiscovery allows you to efficiently export content in a variety of formats so that it can be presented to legal parties or ingested by other third party legal applications. Flexible export options make it easy to prepare, process and customize your documents and export options as a single production set.

The production set export is a system-generated file that contains several documents related to the case. You can add emails, collaboration messages, and files to a production set at any time until the production set is locked. After you lock the production set, to add new emails, collaboration messages, and files to this set, you need to first unlock the production set and then lock it again manually. When you click Export without locking the production set, the application automatically locks the production set to be exported.

> **Note:** If the production set includes audio-video files and you intend to export it, these audio-video files cannot be exported in their original format. Only the AI transcripts of these files are exportable in PDF format. However, you can apply annotations and redactions to these PDF files for review purposes.

> You can create individual production sets for emails, collaboration messages, and files. You can also export a collective production set that includes emails, collaboration messages, and files. After the export is successfully completed, you can download the exported zip file. The zip file consists of imaged files of the items, native files, metadata in the CSV format.

The metadata file in the exported zip file captures the details like Bates Number, Document Type, subjects, sender and receiver, attachments if any, and image/native/text file paths. For a collective production set, the sequence of the document type is emails first, then collaboration messages, and lastly files.

Exporting a collective production set for emails, collaboration messages, and files

To export a collective production set for emails, collaboration messages, and files:

1. On the **eDiscovery** tab, select the case under which the production set is created.

   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:

2. Expand **Production Sets** and select the set you want to export.

   The emails, collaboration messages, and files are displayed under respective tabs.

3. Click **Export Production Set**.

   The export file includes all emails, collaboration messages, and files in this production set.

4. Configure the production options before you export the production set. See Configuring production set export options.

5. Click **Export**.

6. In the **Production Set Export Options** dialog box, specify the following details, and click **Export**.

EXPORT NAME	BY DEFAULT, THIS FIELD DISPLAYS THE NAME OF THE SELECTED PRODUCTION SET. HOWEVER, YOU CAN CHANGE THIS NAME AND PROVIDE ANOTHER UNIQUE NAME.
	YOU CAN SEARCH THIS NAME UNDER EXPORTS > PRODUCTION SETS AFTER SUCCESSFUL EXPORT.
Export Password	Enter the strong password to protect the export file.
Confirm Password	Retype the same password for confirmation.

EXPORT NAME	BY DEFAULT, THIS FIELD DISPLAYS THE NAME OF THE SELECTED PRODUCTION SET. HOWEVER, YOU CAN CHANGE THIS NAME AND PROVIDE ANOTHER UNIQUE NAME.
	YOU CAN SEARCH THIS NAME UNDER EXPORTS > PRODUCTION SETS AFTER SUCCESSFUL EXPORT.
Image Format	Select this option to choose output format of the documents. For now, you can publish the document in PDF and TIFF formats.
Markup Type	Select this option to include redactions and annotations during export.
	Select the Redactions checkbox to include the redactions in the export document. You can export the redacted area as an Opaque or a Transparent area.
	Select the Annotations checkbox to include the annotations in the export document.
Include Extracted Text	Select this option to include the actual text of the documents in a text file. For redacted documents, only non-redacted text will be included in the extracted text.
Include EDRM Metadata File	Select this option to preserve and export the EDRM XML output file.
Include Natives	Select this option if you want to export all supported files in their native format.

7. Click **Export**.
8. To view the status of exported production set, in the left navigation, select **Exports**>**Production Sets**.

Exporting an individual production set for emails, collaboration messages, or files

To export an individual production set for emails, collaboration messages, or files:

1. On the **eDiscovery** tab, select the case under which the production set is created.

   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:

2. Expand **Production Sets** and select the set you want to export.

   The emails, collaboration messages, and files are displayed under respective tabs.

3. Based on your requirement, select the **Emails**,**Collaboration**, or **Files** tab.

   > **Note:** On the **Files** tab, the application does not display a preview of file content if the file type of the selected file is not supported by the native viewer. In such scenarios, the application notifies that the PrizmDoc tool does not support the specific file type.

4. Configure the production options before you export the production set. See Configuring production set export options.

5. Click **Export**.

6. In the **Production Set Export Options** dialog box, specify the following details, and click **Export**.

EXPORT NAME	BY DEFAULT, THIS FIELD DISPLAYS THE NAME OF THE SELECTED PRODUCTION SET. HOWEVER, YOU CAN CHANGE THIS NAME AND PROVIDE ANOTHER UNIQUE NAME.
	YOU CAN SEARCH THIS NAME UNDER EXPORTS > PRODUCTION SETS AFTER SUCCESSFUL EXPORT.
Export Password	Enter the strong password to protect the export file.
Confirm Password	Retype the same password for confirmation.

EXPORT NAME	BY DEFAULT, THIS FIELD DISPLAYS THE NAME OF THE SELECTED PRODUCTION SET. HOWEVER, YOU CAN CHANGE THIS NAME AND PROVIDE ANOTHER UNIQUE NAME.
	YOU CAN SEARCH THIS NAME UNDER EXPORTS > PRODUCTION SETS AFTER SUCCESSFUL EXPORT.
Image Format	Select this option to choose output format of the documents. You can publish the document in PDF and TIFF formats.
	The PDF option is selected by default.
TIFF Options	This field becomes enabled when you select the TIFF option in the Image Format field and provides the following options\:
	- Each file on a single page: If a document has multiple pages, a separate TIFF file will be generated for each page. For example, when exporting a production set, three TIFF files will be generated for a three-page email. In the image below, the pre00002suff.xlsx file has two pages. After selecting this option, while exporting the production set from the native folder to the image folder, the application generated two separate TIFF files for the two pages.
	- Each file on multiple pages: If a document has multiple pages, a single TIFF file will be generated for all pages. For example, when exporting a production set, only one TIFF file will be generated for a three-page email. In the image below, the pre00002suff.xlsx file has two pages. After selecting this option, while exporting the production set from the native folder to the image folder, the application generated a single TIFF file for the two pages.

EXPORT NAME	BY DEFAULT, THIS FIELD DISPLAYS THE NAME OF THE SELECTED PRODUCTION SET. HOWEVER, YOU CAN CHANGE THIS NAME AND PROVIDE ANOTHER UNIQUE NAME.
	YOU CAN SEARCH THIS NAME UNDER EXPORTS > PRODUCTION SETS AFTER SUCCESSFUL EXPORT.
Markup Type	Select this option to include redactions and annotations during export.
	Select the Redactions checkbox to include the redactions in the export document. You can export the redacted area as an Opaque or a Transparent area.
	Select the Annotations checkbox to include the annotations in the export document.
Include Extracted Text	Select this option to include the actual text of the documents in a text file. For redacted documents, only non-redacted text will be included in the extracted text.
Include EDRM Metadata File	Select this option to preserve and export the EDRM XML output file.
Include Natives	Select this option if you want to export all supported files in their native format.

7. Click **Export**.
8. To view the status of exported production set and download the zip file, in the left navigation, select **Exports**>**Production Sets**. After the export is completed, do the following:
    - Expand the production set row to view its details.
    - Click the **Download** icon to download the zip file that contains exported emails, collaboration messages, or files.

About Production Sets

The Production Set feature in Arctera eDiscovery supports legally defensible Productions. Users can perform the following activities while managing the production sets:

- Creating production sets
- Adding items to new and existing production sets
- Removing the items from production sets
- Reviewing the items of the production sets
- Annotating and redacting the content and attachments
- Applying redaction reasons to the annotated and redacted content/area
- Locking the production sets
- Exporting Production Set documents with specified templates

In nutshell, the production sets assume that all reviewed, tagged, and relevant documents will be produced and shared for legal defense.

Configuring production set export options

You can specify the production set export options in the tabbed area at any time before running the production set export. This section also explains how can you create and apply the templates for productions sets.

To configure the export options before exporting the production set:

1. On the **eDiscovery** tab, click **Cases**.
2. Search for and select the case in which you want to configure a production set export options before exporting it.

   The selected ***Case_Name*** node appears below **Cases**.
3. From the displayed case nodes, select **Production Sets**.

   A list of available production sets of this case are displayed.
4. Select the production set for which you want to configure the export options before export.

   The application displays the following configuration options:

- General
- Numbering

- Header/Footer
- Imaging
- Slip Sheet

1. Under **General**, specify the following:

LOAD FROM	FROM THE DROP-DOWN LIST, SELECT A PREVIOUSLY CREATED EXPORT TEMPLATE FORMAT.
	IF YOU SELECT THE PREVIOUSLY CREATED TEMPLATE, ALL THE PREVIOUSLY CONFIGURED FIELDS APPEAR AUTOMATICALLY.
Name	If you want to create a new setting, that can be later used as template, provide a name for the current setting. Till the time you do not create a template of this setting, this setting remains intact. When you open the production set, the application displays the lastly saved setting.
	If you save this setting as a template, this name is considered as a new template name, and this template name is listed under the Load from drop-down options.
Description	Provide a brief description for the current setting.
Production Type	Select this option to produce all documents as image files.

2. Under **Numbering**, specify the following values:

   The following example shows the specified format.

   The sample ITEM-0000012-001 shows the prefix ITEM-, numbering that includes 7 digits starting with the number 12, and a suffix of -001.

PREFIX	THE SETTINGS ON THIS TAB ASSOCIATE A PRODUCTION NUMBER WITH A CORRESPONDING DOCUMENT WHEN THE PRODUCTION IS RUN. SPECIFY THE DOCUMENT NUMBERING FOR THE PRODUCTION. IF REQUIRED, INCLUDE A DELIMITER AT THE END.
Minimum number of digits	Specify the minimum number of digits for numbering the documents. The number is padded with zeros, if needed to match the minimum.
Starting number	Specify the starting number for the numbered list of documents.
	Note: The product ensures that the same production number (combination of prefix and number) is not used multiple times on the same case. If the number you specify is below the minimum allowed number for that prefix, the next valid number is displayed.
Suffix	Specify a suffix for the numbered list with a delimiter, if required.

1. Under **Header/Footer**, specify the following:

HEADER	CHOOSE THE INFORMATION TO PRESENT FOR THE LEFT, CENTER, AND RIGHT HEADERS. SELECT FROM THE FOLLOWING ITEMS\:
	- NONE (NO ENTRY)
	- BATES NUMBER
	- AUTHOR
	- DATE PRODUCED
	- DOCUMENT ID
	- FREE TEXT
	- FILENAME
	- PAGE NUMBER
	- PAGE X OF Y
Footer	Choose the information to present for the left, center, and right headers. All the options are same as options in the header field.
Watermark	Type the word or words you want to appear as a watermark on the pages of the production.

2. Under **Imaging**, specify the following:

SLIP SHEET BY MAXIMUM LIMITS	ITEMS THAT EXCEED THESE MAXIMUM LIMITS PRODUCE A SLIP SHEET AND ARE NOT
	IMAGED.
	- PAGE COUNT: SPECIFY NUMBER OF PAGES AFTER WHICH A SLIP SHEET WILL BE PRODUCED.
	- FILE SIZE: SPECIFY MAXIMUM SIZE OF THE FILE (IN MB) AFTER WHICH A SLIP SHEET WILL BE PRODUCED.

3. Under **Slip Sheet**, specify the following:

CUSTOMIZABLE SLIP	THIS OPTION ALLOWS YOU TO CUSTOMIZE SLIP SHEETS WITH VARIOUS FIELDS WHICH CAN
SHEET TEXT	ASSIST IN IDENTIFYING EXCEPTIONS.
	EACH SLIP SHEET WILL RECEIVE A BATES NUMBER AND THE SPECIFIED TEXT WILL BE
	PRINTED IN THE CENTER OF THE SLIP SHEET (WHICH IS CREATED FOR ALL ITEMS THAT ARE
	NOT IMAGED). THE MAXIMUM LENGTH ALLOWED FOR THIS FIELD IS 1,024 CHARACTERS.
	- %DOCID: DOCUMENT ID.
	- %FILENAME: FILE NAME OF THE ITEM
	- %FILEEXTENSION: FILE EXTENSION OF THE ITEM
	- %BATESSTART: STARTING BATES NUMBER
	WHEN PRODUCED, A SLIP SHEET IS A PLACEHOLDER FOR ANY ITEM NOT RENDERED FOR
	ONE OF THE REASONS BELOW.
	- FULLY REDACTED - ITEM WAS REDACTED COMPLETELY
	- IMAGING ERROR - UNABLE TO CREATE IMAGE OF ITEM DURING PRODUCTION
	- CONVERSION ERROR - IMAGE FAILED TO CONVERT TO PDF
	- NATIVE PLACEHOLDER - BATES STAMPED NATIVE PLACEHOLDER
	YOU CAN APPLY YOUR CUSTOMIZED SLIP SHEET SETTINGS EITHER BY CHANGING THE
	TEXT WHILE CREATING THE PRODUCTION

4. Click **Save**, and do any of the following options as required.
    - If, under **General**, you have not selected the previously saved template in the **Load from** field, the application displays the confirmation message:
        - Click **Cancel** to save the settings without creating a new template. The application saves and displays this setting whenever you access the production set. You can modify this setting whenever required, and save it as a template for further use.
        - Click **Create New Template** to save the current setting as a new template. This template name is then displayed under the **Load from** field.
    - If, under **General**, you have selected the previously saved template in the **Load from** field, the application displays the confirmation message:
        - Click **Override** to update the selected template for the current settings
        - Click **Create New Template** to save the current setting as a new template. This template name is then displayed under the **Load from** field.

Locking and unlocking production sets

You can lock production sets to disable some of the features such as add or remove items, add or remove annotations and redactions, and update production export options. To perform all these actions, you must unlock these production sets.

To lock a production set:

1. On the **eDiscovery** tab, click **Cases**.
2. Search for and select the case in which you want to lock the production set before exporting it.

   The selected ***Case_Name*** node appears below **Cases**.
3. From the displayed case nodes, select **Production Sets**.

   A list of available production sets of this case are displayed.
4. Select the unlocked production set that you want to lock.
5. Click **Lock Production Set**.

   The application displays the **Production Set Locked** message.

   To unlock a production set:
6. On the **eDiscovery** tab, click **Cases**.

7. Search for and select the case in which you want to lock the production set before exporting it.

   The selected ***Case_Name*** node appears below **Cases**.

8. From the displayed case nodes, select **Production Sets**.

   A list of available production sets of this case are displayed.

9. Select the locked production set that you want to unlock.
10. Click **Unlock Production Set**.

    The application displays the **Production Set Unlocked** message.

Moving items to production sets

You can move emails, collaboration messages, and files to the unlocked production sets only, and not to the locked production sets. You need to unlock the production sets before moving these items to the locked production sets.

To move items to production sets:

1. On the **eDiscovery** tab, click **Cases**.
2. Search for and select the case in which you want to search items.

   The selected ***Case_Name*** node appears below **Cases**.

3. Click **New Search** to create a new search. To select existing saved searches, expand **Research Sets** or **Review Sets** and select a required search.
4. Perform advanced search or query search to get the expected items. See Performing Advanced Search and Query Search.
5. To move all the emails, collaboration messages, and files from the result, click **Move to Production Set**.
6. To move emails only, on the **Emails** tab, select the emails you want to include in the production set. Click **Production Set**, and do any of the following as required:

   - Click **Move all emails** to include all the emails available in the search.
   - Click **Move current page** to include all the emails displayed on the selected page.
   - Click **Move selected emails** to include all the selected emails from the search.

7. To move collaboration messages only, on the **Collaboration** tab, select the messages you want to include in the production set.

Click **Production Set**, and do any of the following:

- Click **Move all messages** to include all the collaboration messages available in the search.
- Click **Move selected messages** to include all the selected collaboration messages from the search.

8. To move files only, on the **Files** tab, select the files you want to include in the production set.
   - Click **Move all files** to include all the files available in the search.
   - Click **Move selected files** to include all the selected files from the search.
9. In the **Production Set** dialog box, do the following:

NEW PRODUCTION SET	SELECT THIS OPTION IF YOU WANT TO MOVE THE SELECTED EMAILS IN A NEW PRODUCTION SET. THIS OPTION IS SELECTED BY DEFAULT.
	IN THE PRODUCTION SET NAME FIELD, ENTER A UNIQUE NAME FOR THIS PRODUCTION SET.
	IN THE DESCRIPTION FIELD, ENTER A BRIEF DESCRIPTION OF THE PRODUCTION SET.
Existing Production Set	In the Production Set Name drop-down list, you can view only the unlocked production sets. You can not move emails to the locked production set.
	In the Production Set Name drop-down list, select a set to which you want to move (add) the selected emails.
	The description of the selected production set appears for your reference.

10. Click **Submit**.

    If you have created a new production set, the application displays the *Production set created successfully* message. This newly created production set gets listed under **eDiscovery** tab >**Cases**> *Case_Name* >**Production Set**.

If you have moved the items to an existing production set, the application displays the *Production set updated successfully* message.

Removing items from a production set

You can remove items from the unlocked production sets only, and not from the locked production sets. You need to unlock the production sets before removing items from the locked production sets.

To remove items from a production set:

1. On the **eDiscovery** tab, click **Cases**.
2. Search for and select the case from which you want to add or remove items.

   The selected ***Case_Name*** node appears below **Cases**.
3. From the displayed case nodes, select **Production Sets**.

   A list of available production sets of this case are displayed.
4. Select the unlocked production set from which you want to remove items.
5. Select items you want to remove, and click **Remove from Production Set**.

   The application prompts you to confirm that you want to perform the operation.
6. Click **Yes**.

   The application displays the **Email(s) removed from Production Set successfully** message.

Annotating and redacting content in native viewer

This section includes the following topics:

About annotations and redactions

Annotations

Depending on your review requirements, you can add text and shape annotations to a document. For example, you can annotate the text or area with arrows, lines, boxes, stamps and then customize the line size, color, and fill color. You can also add comments for other users of the document. These annotations can be viewed and edited by other users for which you might need appropriate permissions. You can print and download such annotations for further use.

Redactions

Depending on your review requirements, you can draw dark rectangles to hide sensitive information within a document to avoid a confidentiality breach. You can determine the transparency level of such dark rectangles as required. When you print the document, you can permanently add these redactions over the content or entire page, and provide reasons for redactions. You can print and download such redactions for further use.

Before you annotate or redact items, it is recommended to read the following sections.

More Information

Understanding the native viewer interface

Annotating email and file content

You can add annotations to documents to further explain, analyze or illustrate a certain point, or encourage collaboration and communication among a reviewing team. The various editing tools are useful for calling reviewers attention to certain parts of the document. For example, you may want to give a reason for a particular markup to help speed the review or comply with organizational guidelines and regulatory mandates. Or perhaps you need to mark a document for later action such as Redaction.

Annotations are visible on produced documents. This means that emails and files can be annotated with any of the edit tools. After annotating, the item can be reviewed by another reviewer who can also add annotations.

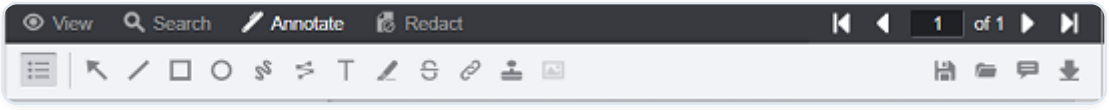
You can consider using different colors and other formatting styles to differentiate reviewers.

To annotate email and file content:

1. Select an email of a file, which you want to annotate, from your search result to view its content in the preview pane.
2. Click the **Native View** icon to view its content in a native viewer.
3. In the native viewer, to search a specific text or a phrase in the document, select the **Search** tab. In the search tool, enter the text or the phrase you want to search in the document, and click the **Search** icon.

   > **Note:** You can use the search tools such as Match exact word or phrase, Match case, Match whole word, Begins with, Ends with, Wildcard search, or Proximity search to make the search more precise.

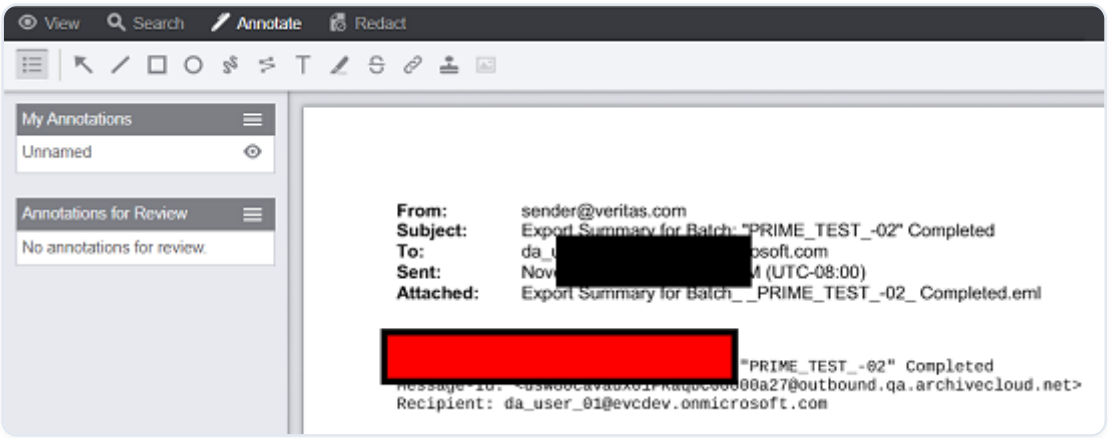
4. Select the text or area in the document and use the redaction tools as described below:



The following annotation tools are available:

- **Arrow**: Enables to draw an arrow. You can select color, opacity, and border width.
- **Line**: Enables to draw a line. You can select color, opacity, and border width.
- **Rectangle**: Enables to draw a rectangle. You can select fill color, opacity, border color, border width, and layer order.
- **Ellipse**: Enables to draw an ellipse. You can select fill color, opacity, border color, border width, and layer order.
- **Freehand**: Enables you to apply a freehand annotation. You can select color, opacity, and border width.
- **Polyline**: Enable to draw a custom polygon. You can select fill color, opacity, border width, and layer order.
- **Text**: Enable to write text within an annotation. You can select fill color, opacity, border color, border width, layer order, and several font options.
- **Highlight**: Enables to highlight the select text highlight annotation.
- **Strikethrough**: Enables to mark text that is mistaken or to be remove. You can select color and border width.
- **Text Hyperlink**: You can give a custom link to the selected text. To change the hyperlink, you can directly click on the text or make selection using the pan tool and change the link using the context menu.
- **Stamp**: User can give stamp of Approved, Rejected or Reviewed using this annotation. As of now, user can only apply one of these thee stamp annotations. Any other customized text is not possible.
- **Image Stamp**: You can apply any of the two pre-existing image stamps, cross or tick mark, on the document.

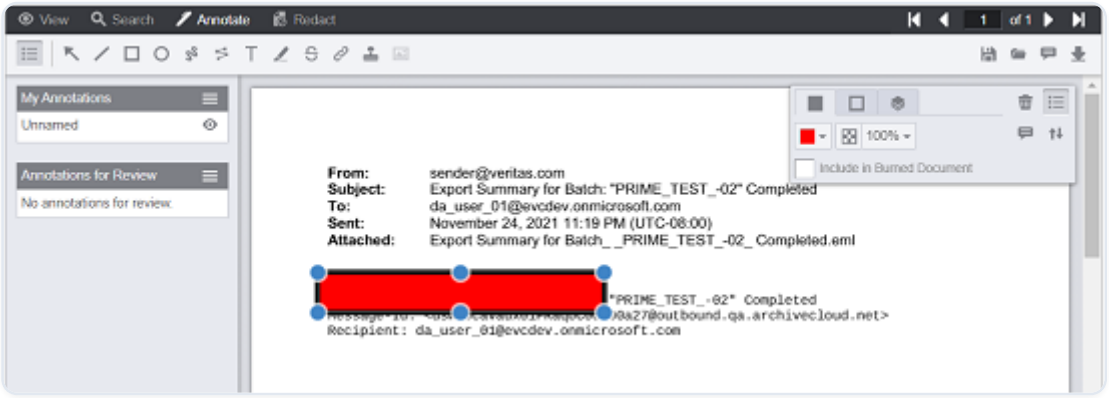
5. (Optional) Select the **Annotation Layers** icon to view the annotations layers in the left pane.



To create a layer, select the redacted text or area. Under **My Annotations**, click the **More Options** icon and do the following:

- Click **Edit Name** to name the selected redaction text or area.
- Select one or more annotations that you want to edit from the drop-down and another reviewer's annotations. Click **Load Annotations** to add these annotations under the selected annotation layer.
- Click **Save Annotations** to save the redaction text or area. A green notification bar displays that mentions the annotation and redaction are now saved in that layer.

6. Navigate to the text or area where you want to apply annotation
7. Select any of the annotation tools, and then draw the annotation.
8. Select the annotation to open the **Annotation Options** pane, and do the following as required. See the following sample image for annotation actions.



- Click the **Fill Color** icon to choose color of redacted area.
- Click the **Border Color** icon to set border color and width.
- Click the **Layer Order** icon to select the layer pattern.
- Select the transparency percentage for the annotation color.

- Select the **Include in burned document** check box to include this annotation when document is printed.
- Click the **Delete** icon to delete the redaction of selected area.
- Click the **Add Comment** icon to add a comment for selected area redaction.
- Click the **Move Menu** icon to shift the **Annotation Options** pane to top or bottom of the native view pane.

9. On the Action Tools bar, do the following as required:
   - Click the **Save** icon to save the redacted text and areas.
   - Select multiple annotations and click the **Load Annotations** icon to create a set of annotations within a document.
   - Click the **Comments Panel** icon to view or hide the comments panel in the viewer.
10. If required, click the **Download** icon, and specify what to include during download in the document.

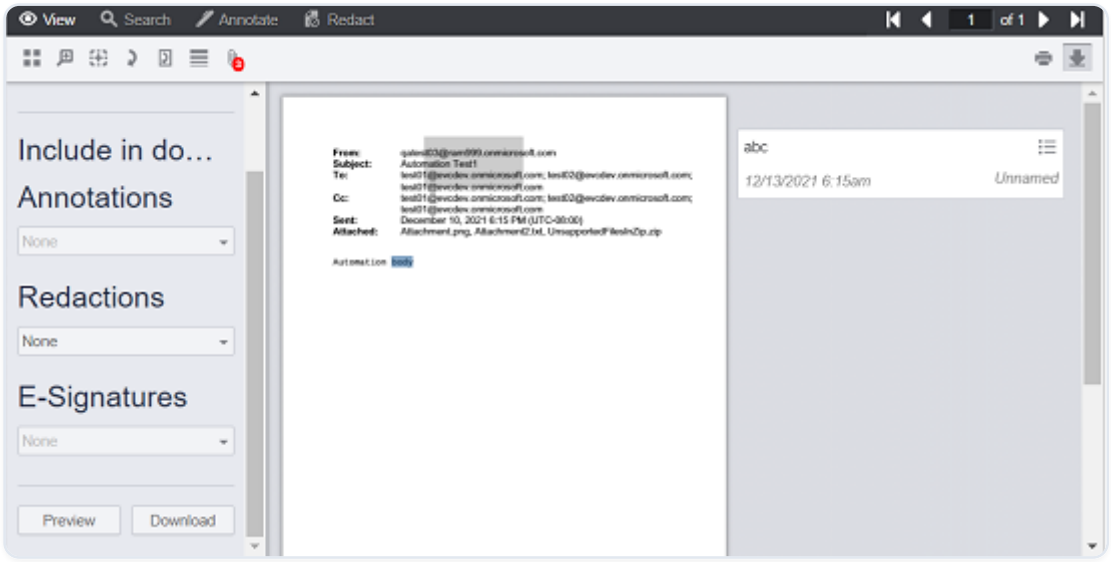
    See Downloading the annotated and redacted document.

Downloading the annotated and redacted document

After annotation or redaction, you can download document in either original format (native) or PDF format. You can choose to include or exclude annotations and redaction while downloading PDF.

To download the annotated and redacted document:

1. After you annotate or redact the content or document, select the **View** tab.
2. Click **Download**. The application displays the following dialog box.



3. Under **Annotation**, select **None** to exclude annotation downloads or select **All** to include all annotations while document downloading.
4. Under **Redaction**, select **None** to exclude redaction downloads or select **All** to include all redactions while document downloading.
5. To preview the document before downloading it, click **Preview**. After preview, you can end preview by clicking the **End Preview** button.
6. Click **Download** to save the document on your computer.

Native viewer capabilities

Arctera eDiscovery uses Native Viewer that provides a powerful document viewing and document conversion functionality. Native Viewer includes an advanced HTML Viewer control which allows users to view, search, annotate, redact, print, and download documents right in their HTML5 browser. It does not require to install any custom software, such as Active-X.

Native view provides the ability to review documents in their native format without requiring each application to be loaded on a reviewer's workstation. Both text search and hit highlighting are available within the native view that increases reviewer productivity.

Persistent Hit Highlighting highlights search terms in email and file content within the native viewer, allowing reviewers to simultaneously view highlighted search terms from the most recently performed searches.

Annotation and redaction functionalities enable reviewers to annotate and redact documents in multiple colors, apply reason codes, and verify redactions prior to production quickly and easily.

Reviewers can redact specific text, pages, or areas within a document. Reviewers can leverage reason codes to quickly perform checks and verify the accuracy of all redactions.

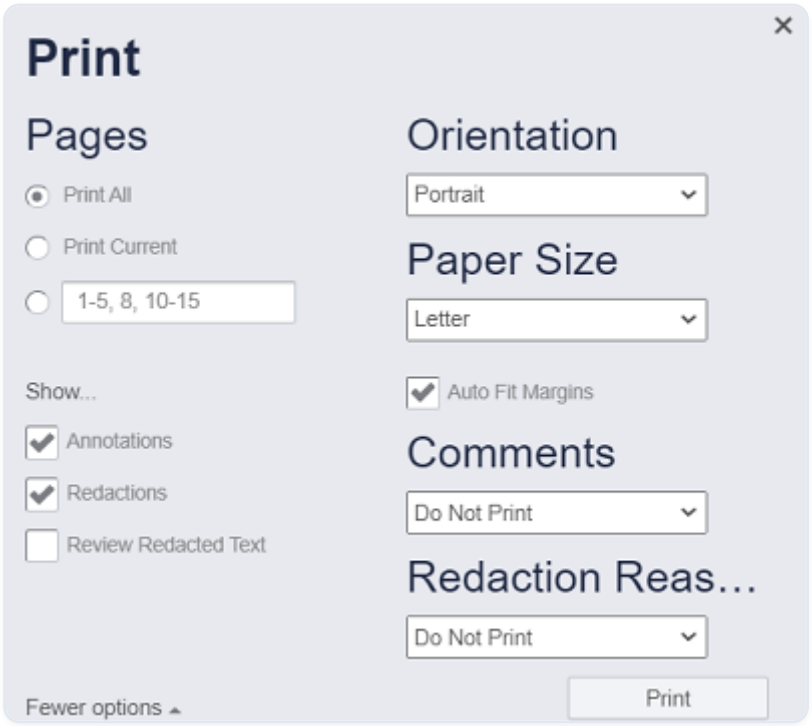
Redaction verification enables reviewers to rapidly navigate through each redaction within a document as part of the quality control process. Reviewers can simultaneously redact all the searched terms in the document.

Printing the annotated and redacted document

After annotation or redaction, you can print the document with these redacted areas burned into the printed image thereby permanently hiding privileged or confidential information.

To print the annotated and redacted document:

1. After you annotate or redact the content or document, select the **View** tab.
2. Click **Print**. The application displays the following dialog box.



3. Under **Pages**, select the options for the pages you want to print. Select the Annotation, Redaction, Review Redacted Text check-boxes if you want to print the document with all annotations, redactions, and review text.
4. Under **Orientation**, select the required page orientation.
5. Under **Paper Size**, select the paper size for the printed document.
6. Under **Comments**, do the following:

- Select **Do Not Print** to exclude printing of comments.
- Select **After Each Page** to print comments after each page.
- Select **At End of Document** to print all comments at the end of the printed document.

7. Under **Redaction Reasons**, do the following:

   - Select **Do Not Print** to exclude printing of redaction reasons.
   - Select **After Each Page** to print redaction reasons after each page.
   - Select **At End of Document** to print all redaction reasons at the end of the printed document.

Redacting email and file content

In case of redacting emails in native view, attachments are linked to the original message (not the parent message with the attachment). The regular fields such as TO and CC are merged with the corresponding Journal fields.

You can redact these fields as well. In case of files, no such metadata is merged with the document. You can directly work on the document content.

To redact email and file content:

1. Select an email of a file, which you want to redact, from your search result to view its content in the preview pane.
2. Click the **Native View** icon to view its content in a native viewer.
3. In the native viewer, do the following:

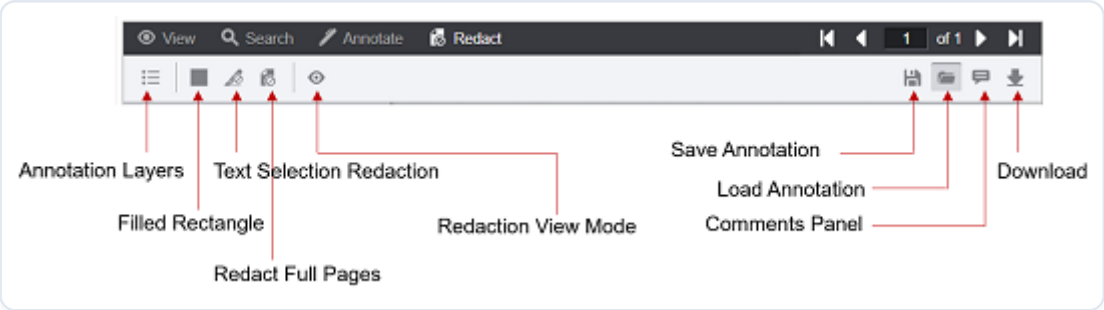
   - To search a specific text or a phrase in the document, select the **Search** tab. In the search tool, enter the text or the phrase you want to search in the document, and click the **Search** icon.

     > **Note:** You can use the search tools such as Match exact word or phrase, Match case, Match whole word, Begins with, Ends with, Wildcard search, or Proximity search to make the search more precise. While using the proximity search, the searched terms in the results are highlighted in the Preview pane and Native views of the attachments. The exact number of words between the search keywords or the order of the keywords does not matter.

- To redact the area, select the **Redact** tab.

> **Note:** You can use the redaction tools like rectangle selection, text selection, and full-page redaction to redact content.

4. Select the text or area in the document and use the redaction tools as described below:

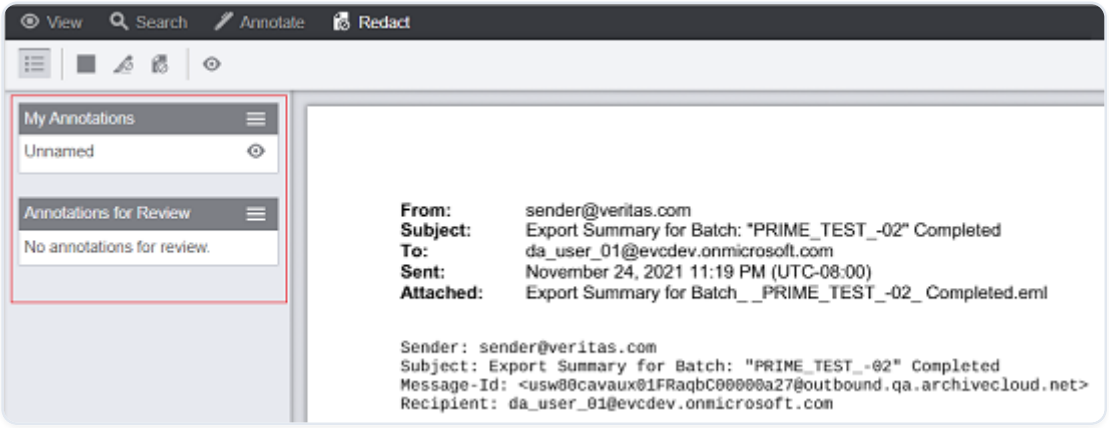


ANNOTATION LAYERS	THE ANNOTATION LAYER ICON IS LOCATED UNDER BOTH THE ANNOTATE AND THE REDACT TABS.
	THE ANNOTATION LAYER FUNCTIONALITY HELPS YOU TO CREATE, VIEW AND MANAGE MULTIPLE SETS OF ANNOTATIONS WITHIN A DOCUMENT AND IMPROVES COLLABORATION DURING DOCUMENT REVIEWING. THE NAME OF THE LAYER THAT A COMMENT BELONGS TO IS DISPLAYED NEXT TO THE DATE AND TIME IN THE COMMENT.
	BEFORE YOU SAVE OR LOAD THE ANNOTATIONS, ENSURE THAT YOUR SESSION IS NOT EXPIRED. ELSE, YOU CANNOT SAVE OR LOAD ANNOTATIONS IF THE SESSION IS EXPIRED.
Filled Rectangle	Redact area option enables you to create a redaction on any part of the viewable document. You can draw redaction boxes over any part of a document.
(Redact Area)	Click the Filled Rectangle icon and then hold down your mouse and drag to select an area to redact. Type a reason in the pop-up

ANNOTATION LAYERS	THE ANNOTATION LAYER ICON IS LOCATED UNDER BOTH THE ANNOTATE AND THE REDACT TABS.
	THE ANNOTATION LAYER FUNCTIONALITY HELPS YOU TO CREATE, VIEW AND MANAGE MULTIPLE SETS OF ANNOTATIONS WITHIN A DOCUMENT AND IMPROVES COLLABORATION DURING DOCUMENT REVIEWING. THE NAME OF THE LAYER THAT A COMMENT BELONGS TO IS DISPLAYED NEXT TO THE DATE AND TIME IN THE COMMENT.
	BEFORE YOU SAVE OR LOAD THE ANNOTATIONS, ENSURE THAT YOUR SESSION IS NOT EXPIRED. ELSE, YOU CANNOT SAVE OR LOAD ANNOTATIONS IF THE SESSION IS EXPIRED.
	window, if prompted to do so, and click OK. The reason is displayed in the redacted area.
	When you hover over the redacted area, the details such as author name of the logged-in user and time of redaction are displayed.
	Redactions in different colors can be done for area redactions.
Text Selection Redaction	Redact text option enables you to select text and apply redaction. Only black color is available for text redactions.
(Redact Text)	Select the text you want to redact, and click the Text Selection Redaction icon.
Redact Full Pages	Redact page option enables you to redact the current page or a page range. Choose a redaction reason, and click Redact. In production, all pages print with black redaction fields.
Redaction View Mode	Redaction View mode allows to make redacted area translucent or opaque. By

ANNOTATION LAYERS	**THE ANNOTATION LAYER ICON IS LOCATED UNDER BOTH THE ANNOTATE AND THE REDACT TABS.**
	THE ANNOTATION LAYER FUNCTIONALITY HELPS YOU TO CREATE, VIEW AND MANAGE MULTIPLE SETS OF ANNOTATIONS WITHIN A DOCUMENT AND IMPROVES COLLABORATION DURING DOCUMENT REVIEWING. THE NAME OF THE LAYER THAT A COMMENT BELONGS TO IS DISPLAYED NEXT TO THE DATE AND TIME IN THE COMMENT.
	BEFORE YOU SAVE OR LOAD THE ANNOTATIONS, ENSURE THAT YOUR SESSION IS NOT EXPIRED. ELSE, YOU CANNOT SAVE OR LOAD ANNOTATIONS IF THE SESSION IS EXPIRED.
	default, the redacted area or text will be displayed in translucent mode.
	If you want the default redaction view mode to be opaque, please contact your case administrator.
	Click the Redaction View Mode icon to view or redact the text or area.

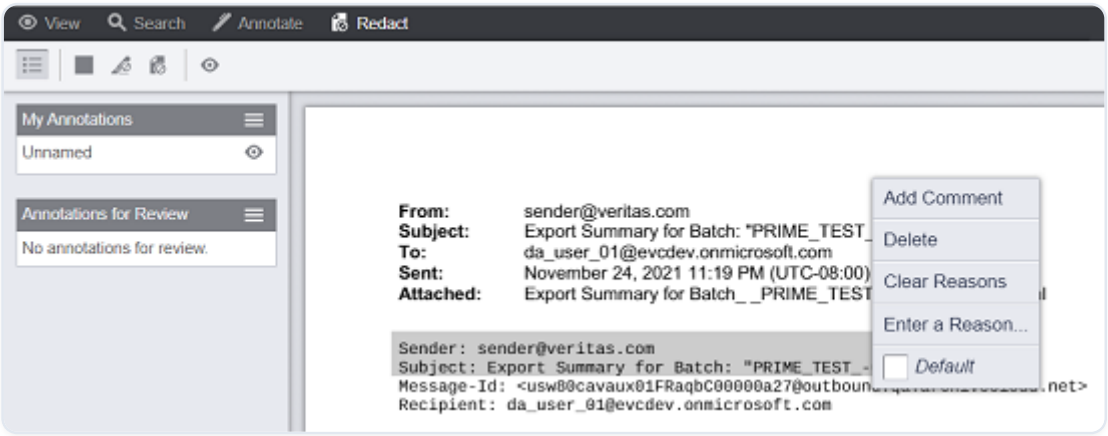
5. (Optional) Select the **Annotation Layers** icon to view the annotations layers in the left pane.



To create a layer, select the redacted text or area. Under **My Annotations**, click the **More Options** icon and do the following:

- Click **Edit Name** to name the selected redaction text or area.
- Select one or more annotations that you want to edit from the drop-down and another reviewer's annotations. Click **Load Annotations** to add these annotations under the selected annotation layer.
- Click **Save Annotations** to save the redaction text or area. A green notification bar displays that mentions the annotation and redaction are now saved in that layer.

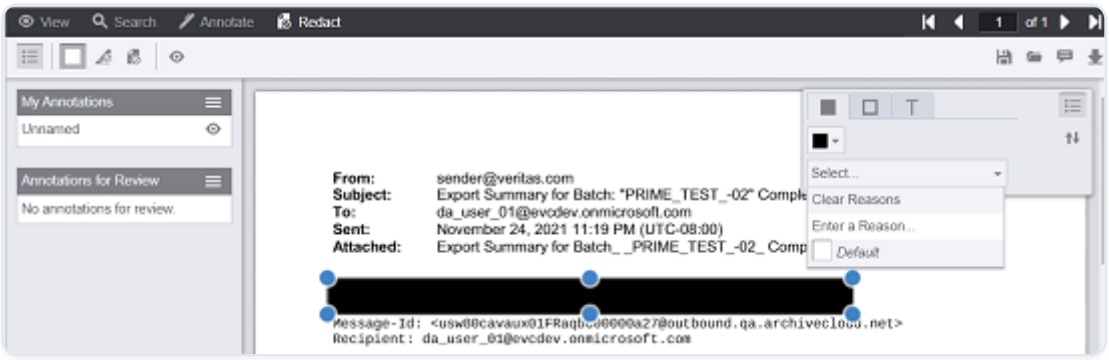
6. Select the redacted text to open the **Annotation Options** pane, and do the following as required. See the following sample image for annotation actions.



- Click the **Add Comment** icon to add a comment for selected text redaction.
- Click the **Delete** icon to delete the redaction of selected text.
- Select **Clear Reasons** to remove the previously implemented redaction reasons.
- Select **Enter Reasons** to provide a new reason for redaction. Select the predefined reasons, if available.

> **Note:** After associating reasons, if you hover over the redacted area, a tooltip appears. The tooltip convention is as below: \<username of the user who applied the redaction reasons\> : \<applied redaction reasons separated by comma\> For example, if the user name is abc@xyz.com, and the applied reasons are RR1 and RR2, then the tooltip will appear asabc@xyz.com:RR1,RR2 If multiple users apply redaction reasons to the same redacted area, then the tooltip displays all users in stack. For example, another user pqr@xyz.com apply AB1 and AB2 redaction reasons to the above-mentioned redacted area, the tooltip appears as below: abc@xyz.com:RR1,RR2 pqr@xyz.com:AB1,AB2

7. Select the redacted area to open the **Annotation Options** pane, and do the following as required:



- Click the **Fill Color** icon to choose color of redacted area.
- In the drop-down list:
  - Select **Clear Reasons** to remove the previously implemented redaction reasons.
  - Select **Enter Reasons** to provide a new reason for redaction.
  - Select the predefined reasons, if available.
- Click the **Delete** icon to delete the redaction of selected area.
- Click the **Add Comment** icon to add a comment for selected area redaction.
- Click the **Move Menu** icon to shift the **Annotation Options** pane to top or bottom of the native view pane.

8. On the Action Tools bar, do the following as required:
   - Click the **Save** icon to save the redacted text and areas.
   - Select multiple annotations and click the **Load Annotations** icon to create a set of annotations within a document.
   - Click the **Comments Panel** icon to view or hide the comments panel in the viewer.
9. If required, click the **Download** icon, and specify what to include during download in the document.

   See Downloading the annotated and redacted document.

Understanding the native viewer interface

The native view provides various document viewing option.

- Action Tabs: You can use these tabs to view, search, annotate, and redact the content.
- Action Tools: When you select any action tab, the corresponding action tools are available for you.

- Display Tabs: You can use various document display options, such as text selection, pan tool, zoom in and out, and full screen mode.
- Print/Download: You can use these tools to print and download the document.
- Page Navigation: You can use these options to navigate across the document pages.

Managing exports

This section includes the following topics:

About exports

During investigation or a case review process, any user who has access to searches can do the following:

- Export the printable summary reports of a search for emails, collaboration messages, and files.
- Export actual emails, collaboration messages, and files.

It is important to understand the difference between exporting summary reports and exporting item records. When you export summary reports, the metadata displayed on the details pane is shown in the excel file. However, when you export items, the actual item files are downloaded.

- Download the exported items locally or to the private Azure Blob storage location.

  Users can see this button only if the Export to Azure private storage location feature in the Arctera Management Console is enabled for them.

  While exporting items, in the Export Options dialog box, users can click Generate Azure SAS URL to get the Azure Blob SAS URL to access the location and save it for future use.

  For security reasons, the application does not show this URL the next time. However, if the SAS URL is misplaced for any reason, click Generate Azure SAS URL again to generate a new SAS URL and save it securely.

After you click Export in the Export Options dialog box, all the selected items are exported to the Azure private storage location. You can use Microsoft Storage Explorer to access the exported items.

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. On the **Investigation** tab, in the left navigation pane, click **Exports**.

   The batch export records appears.
2. Search for and select an export batch in the table of exports.
3. Click the corresponding arrow icon adjacent to the **Batch ID** column to expand and view the export batch details.
4. To download a zip file of the export batch, click **Download**.
5. To cancel the export, click **Cancel Batch** before the export is completed.

Email export FAQ

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

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.

Performing exports in Investigation and eDiscovery

This section provides export-specific links to different sections. You can easily navigate to the export-specific sections of your interest.

- Investigation
  - Exporting items from searches
    - Batch export - Emails: See Exporting searched emails.
    - Summary report - Emails: See Exporting a search summary report for emails.
    - Batch export - Collaboration messages: See Exporting collaboration messages.
    - Summary report - Collaboration messages: See Exporting a search summary report for collaboration messages.
    - Batch export - Files: See Exporting searched files.
    - Summary report - Files: See Exporting a search summary report for files.
    - Summary report export: See Exporting a summary report of searched items.
  - Exporting items from Advance ECA searches
    - Batch export - Emails: See Exporting emails from Advanced ECA search.
    - Summary report export - Emails: See Exporting a search summary report for emails.
    - Batch export - Collaboration messages: See Exporting collaboration messages from Advanced ECA search.
    - Summary report export - Collaboration messages: See Exporting summary report for collaboration messages.
    - Batch export - Files: See Exporting files from Advanced ECA search.
    - Summary report export - Files: See Exporting summary report for files.
- eDiscovery
  - Batch export - Emails from cases: See Exporting emails.

- Summary report - Emails from cases: See Exporting a search summary report for emails.
- Batch export - Collaboration messages from cases: See Exporting collaboration messages.
- Summary report - Collaboration messages from cases: See Exporting a search summary report for collaboration messages.
- Batch export - Files from cases: See Exporting files.
- Summary report - Files from cases: See Exporting a search summary report for files.

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. Arctera 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. On the **Investigation** tab, in the left navigation pane, select **Exports**.

   Or, on the **eDiscovery** tab, select the case, and then in the left navigation pane, select **Exports**.
2. Select the failed export batch you want to resubmit.
3. In the Resubmit Failed Items section, click **Go**.

   > **Note:** The **Resubmit Failed Items** section appears only when the selected batch contains failed export items. The batch contains failed items when **Completed with Errors** or **Error** is listed in the **Step** field.
4. 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.

5. 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.

Viewing export details of native documents

The Export node lets you view the export-specific details of the native documents. The Native page provides a list of export batches. Arctera eDiscovery splits large exports into 2-gigabyte batches. Therefore, multiple export batches can be associated with one export. You can expand the rows to view the export details and export download link. The details include information such as export file type, download size of the file, export start and completion dates, expiration date for download link, output file type, export status, and so on.

The page displays the Resubmit Failed Items section only when the selected export batch contains failed export items. Exports contain failed items when the *Completed with Errors* or *Error* is listed in the Step field.

To review export status of the native documents:

1. On the **eDiscovery** tab, click **Cases**.
2. Search for and select the case.

   The selected ***Case_Name*** node appears below **Cases**.
3. From the displayed case nodes, select **Exports**>**Native**.

   The application displays a list of the native exports.

4. If required, click the **Refresh** icon in the top-right corner of the **Native** page to get the latest available records.

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

5. Search for and select the export batch to view export details on native email exports.

   - When you expand an individual export batch (one without associated export batches), the **Export Details** section displays key information such as priority, export status, output file name, file size, created by, creation date, start and completion dates, file download expiry date, and more.
   - When you expand an export batch that contains associated export batches, the **Export Details** section displays a list of these associated batches. To view the details of each associated batch, you must expand them individually.

6. Download the export summary reports.

    - If it is an individual export batch (one without associated export batches), click the **Download** icon provided in the Download column of the item grid. The export summary of that individual batch will be downloaded for your review.
    - If it is an export batch that contains associated export batches, click the **Download** icon provided in the Download column of the item grid. A new browser window appears.

    When you expand an export batch that contains associated export batches, the **Export Details** section displays a list of these associated batches. To view the details of each associated batch, you must expand them individually.

    Click any of the following as needed:

    - **Download All Batches**: Downloads all batches. Irrespective of the download status, all completed, failed, and unexported batches will begin downloading. The user will see a confirmation box to proceed or not, as the existing download status and download date columns will be reset to their default values.

      To avoid performance issues and potential browser crashes, files will be downloaded in chunks of 10 batches at a time. Once the first chunk of 10 batches/files is downloaded, the next chunk will begin automatically.
    - **Download selected Batches**: Select one or multiple batches to download exported results.
    - **Pause/Resume**: Pause puts ongoing downloads on hold till you click **Resume**. Upon resuming, the paused batches' start downloading. Resume works for remaining batches if the window is reopened.
    - **Cancel**: Stops ongoing downloads, saves status, and shows it upon reopening.

    The downloaded zip file is password protected. Enter the appropriate password to view the report.

Viewing export details of production sets

The Export node lets you view the export-specific details of the production sets.

To view export details of the production set:

1. On the **eDiscovery** tab, click **Cases**.
2. Search for and select the case in which you want to configure a production set metadata before exporting it.

The selected ***Case_Name*** node appears below **Cases**.

3. From the displayed case nodes, select **Exports**>**Production Sets**.

   The application displays a list of the production set export batches.

4. If required, click the **Refresh** icon in the top-right corner of the **Production Sets** page to get the latest available records.

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

5. Search for and select the export batch to view export details on production exports.

   - When you expand an individual export batch (one without associated export batches), the **Export Details** section displays key information such as priority, export status, output file name, file size, created by, creation date, start and completion dates, file download expiry date, and more.

- When you expand an export batch that contains associated export batches, the **Export Details** section displays a list of these associated batches. To view the details of each associated batch, you must expand them individually.

6. Download the export summary reports.

   - If it is an individual export batch (one without associated export batches), click the **Download** icon provided in the Download column of the item grid. The export summary of that individual batch will be downloaded for your review.
   - If it is an export batch that contains associated export batches, click the **Download** icon provided in the Download column of the item grid. A new browser window appears.

     > **Note:** When you expand an export batch that contains associated export batches, the **Export Details** section displays a list of these associated batches. To view the details of each associated batch, you must expand them individually.

   Click any of the following as needed:

   - **Download All Batches**: Downloads all batches. Irrespective of the download status, all completed, failed, and unexported batches will begin downloading. The user will see a confirmation box to proceed or not, as the existing download status and download date columns will be reset to their default values.

     To avoid performance issues and potential browser crashes, files will be downloaded in chunks of 10 batches at a time. Once the first chunk of 10 batches/files is downloaded, the next chunk will begin automatically.
   - **Download selected Batches**: Select one or multiple batches to download exported results.
   - **Pause/Resume**: Pause puts ongoing downloads on hold till you click **Resume**. Upon resuming, the paused batches' start downloading. Resume works for remaining batches if the window is reopened.
   - **Cancel**: Stops ongoing downloads, saves status, and shows it upon reopening.

   The downloaded zip file is password protected. Enter the appropriate password to view the report.

Collaborative reports

This section includes the following topics:

About collaborative eDiscovery reporting

The eDiscovery 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 Archive- eDiscovery dashboard

The eDiscovery 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. On the eDiscovery tab, click Dashboard node.
2. Review the information.
3. If required, click **Export Report** to export the report for review whenever required.

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 the eDiscovery Administrators or reviewers with the **View Case Logs/Reports** permission 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.
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

The eDiscovery 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 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.

Arctera eDiscovery alerts

This section includes the following topics:

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 option on the Profile icon in the top-right corner of the application page.
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

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 Arctera Personal Archive 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 ARCTERA PERSONAL ARCHIVE 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.

4. 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:

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.

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.

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 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.

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:** Arctera Personal Archive treats a space between two search terms as an AND operator.

> The following searches are treated identically:

```
cloud computing
```

```
cloud AND computing
```

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`

Arctera Unified Platform 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.

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.

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 Arctera Unified Platform supports enhanced searches in Japanese, ask your Arctera Unified Platform administrator.

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

> If your company's Arctera Unified Platform 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.
- Arctera 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.

About Hit-highlighting and navigating to searched terms

Hit highlighting visually marks important terms within the item preview pane to quickly identify relevant content. These terms include the terms matched by your search criteria as well as terms in any associated tags.

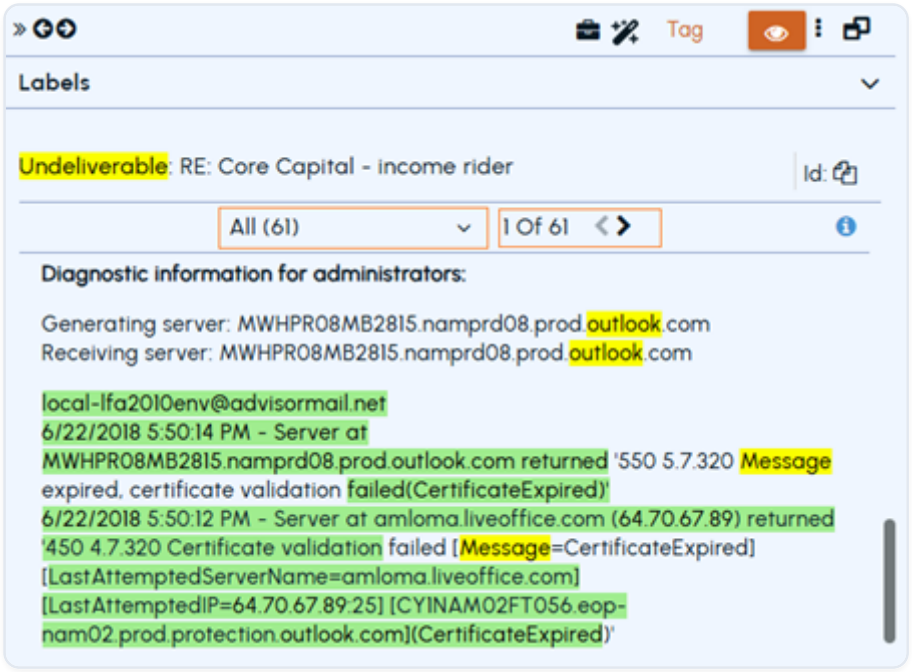
Highlighting applies to the subject line, message body, attachment names, and the text or HTML preview of attachments. Search terms are highlighted in *orange*, while tags are highlighted in *green*. You can hover over a highlighted term to identify whether it originated from a query or a tag.

To help you review content efficiently, the preview pane includes a drop-down list showing all matched terms along with their occurrence counts. You can select *All* to view every highlighted term or choose a specific term to focus only on its instances. This targeted highlighting enables faster review of search results, especially when navigating through large message bodies or attachments.

To understand hit highlighting precisely, refer to the following scenario.

1. Create a new search or open an existing one by performing one of the following actions:
    - On the **Investigation** tab, expand **Managed Accounts** and click **New Search**; or select an existing search from previously created searches, *ongoing searches, standard searches, or advanced ECA searches*.
    - On the **eDiscovery** tab, click **Cases**, search for and select a case. The selected case appears under Cases. Click **New Search** to create a new one, or expand *Research Sets* or *Review Sets* to select an existing search.
2. Use *Advanced Search* or *Query Search* to define your criteria for filtering relevant emails, collaboration content, or files. Click **Search**.

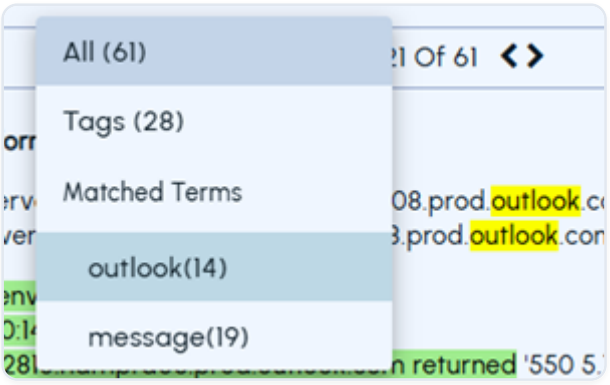
    The filtered items (emails, collaboration messages, and files) in the items grid.
3. From the items grid, click the item you want to review. The selected item opens in the preview pane on the right.
4. In the preview pane, click the drop-down arrow to view a list of matched terms and the number of occurrences for each term.



- Use the previous and next arrows to navigate between term hits in the message body.

> **Note:** Though highlighting applies to the subject line, message body, attachment name, and the text or HTML preview of attachments, navigation is only available within the message body content.

- Select *All* to view all highlighted terms, or select a specific term to highlight only its occurrences.



Capabilities

- Supports stop words and special characters
- Handles multi-byte characters
- Highlights terms across line breaks
- Applies highlighting in Native Viewer
- Works with tenants where stop word indexing is enabled

- Supports proximity-based searches
- Provides navigation between highlighted terms

Known Limitations

- Does not highlight search terms with leading or trailing special characters
- Counts/includes stop words in highlights within Native Viewer
- Does not support highlighting in Query Search
- Cannot highlight non-visible metadata such as image information or indexed item metadata

About stop words and special characters

Stop words

Stop words are a set of commonly used words that Arctera Personal Archive ignores when it performs a Search or Advanced Search. Arctera Personal Archive 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 About Hit-highlighting and navigating to searched terms.

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

See Boolean operator searches.

Special characters

Arctera Personal Archive omits the following special characters from searches:

`* @ # $ % ^ & - + = _ { } [ ], < > ; : / \ ?` **Arctera 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 About Hit-highlighting and navigating to searched terms.

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

See Wildcard searches.

Double-byte character set searches

Arctera Unified Platform 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

Performing Advanced Search and Query Search

Arctera eDiscovery provides the Advanced Search and the Query Search features to search the content within archived accounts and cases. Both the search features are available in the Investigations tab (where you can search your own account or the accounts that you manage) and the eDiscovery tab (where 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.

Performing an advanced search

To perform an advanced search:

1. Access the **Advanced Search** tab from the **Investigation** or the **eDiscovery** tab.
2. Specify the following inputs:

CUSTODIANS	**- SELECT ALL TO SEARCH ARCHIVES OF ALL OF THE CUSTODIANS THAT ARE ASSOCIATED WITH THE CASE.**
	- SELECT CUSTOM TO SEARCH ARCHIVES OF THE PARTICULAR CUSTODIANS.
	1. THE MANAGE BUTTON APPEARS. CLICK MANAGE TO OPEN THE ADD/ REMOVE CUSTODIANS.
	2. EXPAND SELECTED CUSTODIANS TO VIEW THE CUSTODIANS SELECTED FOR THIS SEARCH.
	3. EXPAND MANAGE CUSTODIANS AND SELECT THE CUSTODIANS REQUIRED FOR THIS SEARCH.
	4. (OPTIONAL) SELECT SEARCH BETWEEN CUSTODIANS AT THE BOTTOM OF THE POP-UP TO RETRIEVE EMAILS EXCHANGED EXCLUSIVELY AMONG THE SELECTED CUSTODIANS. FOR DETAILS, SEE SEARCHING EMAILS EXCHANGED AMONG SPECIFIC CUSTODIANS**.**
	5. CLICK UPDATE TO ADD THESE SELECTED CUSTODIANS AS A SEARCH INPUT. THESE CUSTODIANS ARE LISTED UNDER THE SELECTED CUSTODIANS SECTION.
Custom Headers	**Note:** TheCustom Headersoption does not appear if there is no entry for a custom header for a particular group or tenant in database. Custom header does not work independently. You need to use the filter criteria to search the required items.
	Expand Custom Headers and set the header operator values.
	- Click + to add new search clauses.

CUSTODIANS	**- SELECT ALL TO SEARCH ARCHIVES OF ALL OF THE CUSTODIANS THAT ARE ASSOCIATED WITH THE CASE.**
	- SELECT CUSTOM TO SEARCH ARCHIVES OF THE PARTICULAR CUSTODIANS.
	1. THE MANAGE BUTTON APPEARS. CLICK MANAGE TO OPEN THE ADD/ REMOVE CUSTODIANS.
	2. EXPAND SELECTED CUSTODIANS TO VIEW THE CUSTODIANS SELECTED FOR THIS SEARCH.
	3. EXPAND MANAGE CUSTODIANS AND SELECT THE CUSTODIANS REQUIRED FOR THIS SEARCH.
	4. (OPTIONAL) SELECT SEARCH BETWEEN CUSTODIANS AT THE BOTTOM OF THE POP-UP TO RETRIEVE EMAILS EXCHANGED EXCLUSIVELY AMONG THE SELECTED CUSTODIANS. FOR DETAILS, SEE SEARCHING EMAILS EXCHANGED AMONG SPECIFIC CUSTODIANS**.**
	5. CLICK UPDATE TO ADD THESE SELECTED CUSTODIANS AS A SEARCH INPUT. THESE CUSTODIANS ARE LISTED UNDER THE SELECTED CUSTODIANS SECTION.
	- Click - to remove search clauses that are not required.
	- In the first column, select the required header you want to search for. Based on the data type you have selected, the operator changes. For example, if you have selected the receiver date in header, the operator values can be Between, Before inclusive and After inclusive. For a numeric or integer header value, the operator values can be Is equal to, Less than, and Greater than. If you

CUSTODIANS	**- SELECT ALL TO SEARCH ARCHIVES OF ALL OF THE CUSTODIANS THAT ARE ASSOCIATED WITH THE CASE.**
	- SELECT CUSTOM TO SEARCH ARCHIVES OF THE PARTICULAR CUSTODIANS.
	1. THE MANAGE BUTTON APPEARS. CLICK MANAGE TO OPEN THE ADD/ REMOVE CUSTODIANS.
	2. EXPAND SELECTED CUSTODIANS TO VIEW THE CUSTODIANS SELECTED FOR THIS SEARCH.
	3. EXPAND MANAGE CUSTODIANS AND SELECT THE CUSTODIANS REQUIRED FOR THIS SEARCH.
	4. (OPTIONAL) SELECT SEARCH BETWEEN CUSTODIANS AT THE BOTTOM OF THE POP-UP TO RETRIEVE EMAILS EXCHANGED EXCLUSIVELY AMONG THE SELECTED CUSTODIANS. FOR DETAILS, SEE SEARCHING EMAILS EXCHANGED AMONG SPECIFIC CUSTODIANS**.**
	5. CLICK UPDATE TO ADD THESE SELECTED CUSTODIANS AS A SEARCH INPUT. THESE CUSTODIANS ARE LISTED UNDER THE SELECTED CUSTODIANS SECTION.
	have selected a string value in header, then the operator will be Contains.
	- In the second column, select the available operator.
	- In the third column, specify the text, phrase, or date that you want to search for.
Filters	Expand Filters and set the filter operator values. The operators are explained in a table below.

CUSTODIANS	**- SELECT ALL TO SEARCH ARCHIVES OF ALL OF THE CUSTODIANS THAT ARE ASSOCIATED WITH THE CASE.**
	- SELECT CUSTOM TO SEARCH ARCHIVES OF THE PARTICULAR CUSTODIANS.
	1. THE MANAGE BUTTON APPEARS. CLICK MANAGE TO OPEN THE ADD/ REMOVE CUSTODIANS.
	2. EXPAND SELECTED CUSTODIANS TO VIEW THE CUSTODIANS SELECTED FOR THIS SEARCH.
	3. EXPAND MANAGE CUSTODIANS AND SELECT THE CUSTODIANS REQUIRED FOR THIS SEARCH.
	4. (OPTIONAL) SELECT SEARCH BETWEEN CUSTODIANS AT THE BOTTOM OF THE POP-UP TO RETRIEVE EMAILS EXCHANGED EXCLUSIVELY AMONG THE SELECTED CUSTODIANS. FOR DETAILS, SEE SEARCHING EMAILS EXCHANGED AMONG SPECIFIC CUSTODIANS**.**
	5. CLICK UPDATE TO ADD THESE SELECTED CUSTODIANS AS A SEARCH INPUT. THESE CUSTODIANS ARE LISTED UNDER THE SELECTED CUSTODIANS SECTION.
	- 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.

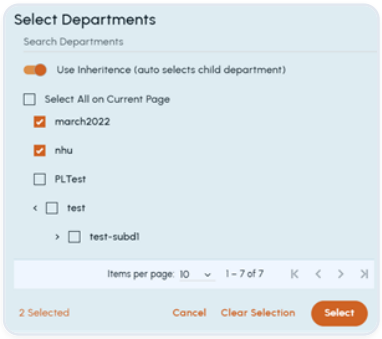
CUSTODIANS	**- SELECT ALL TO SEARCH ARCHIVES OF ALL OF THE CUSTODIANS THAT ARE ASSOCIATED WITH THE CASE.**
	- SELECT CUSTOM TO SEARCH ARCHIVES OF THE PARTICULAR CUSTODIANS.
	1. THE MANAGE BUTTON APPEARS. CLICK MANAGE TO OPEN THE ADD/ REMOVE CUSTODIANS.
	2. EXPAND SELECTED CUSTODIANS TO VIEW THE CUSTODIANS SELECTED FOR THIS SEARCH.
	3. EXPAND MANAGE CUSTODIANS AND SELECT THE CUSTODIANS REQUIRED FOR THIS SEARCH.
	4. (OPTIONAL) SELECT SEARCH BETWEEN CUSTODIANS AT THE BOTTOM OF THE POP-UP TO RETRIEVE EMAILS EXCHANGED EXCLUSIVELY AMONG THE SELECTED CUSTODIANS. FOR DETAILS, SEE SEARCHING EMAILS EXCHANGED AMONG SPECIFIC CUSTODIANS**.**
	5. CLICK UPDATE TO ADD THESE SELECTED CUSTODIANS AS A SEARCH INPUT. THESE CUSTODIANS ARE LISTED UNDER THE SELECTED CUSTODIANS SECTION.
	- Searches are not case-sensitive. The search supports phrase search, Boolean operators, proximity search, and wildcard search. See Search syntax for Advanced Search.

The **Filter** operators are listed below:

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

MESSAGE	ENTIRE MESSAGE	CONTAINS / DOESN'T CONTAIN
Subject	Contains / Doesn't Contain	-
Body	Contains / Doesn't Contain	-
Inbound Message (AND)	Yes / No	-
Outbound Message (AND)	Yes / No	-
Internal Message (AND)	Yes / No	-
	Note: In Advanced Search, this option filters and retrieves only internal messages exchanged within the same organization.	
Is Hidden	Yes / No	-
IP Header	Contains / Doesn't Contain	-
Date Sent/Modified(AND)	Is Equal To	Select a date
Date Sent/Modified(AND)	Before	Select a date
Date Sent/Modified(AND)	After	Select a date
Date Sent/Modified(AND)	Within Range	Select a date range
Participants	All Senders and Recipients	Contains / Doesn't Contain
Participants	Senders Only	Contains / Doesn't Contain
Participants	Recipients Only	Contains / Doesn't Contain
Participants	To/Cc	Contains / Doesn't Contain
Participants	To	Contains / Doesn't Contain
Participants	Bcc	Contains / Doesn't Contain
Classification	Classified As	Contains / Doesn't Contain

MESSAGE	ENTIRE MESSAGE	CONTAINS / DOESN'T CONTAIN
Note: This option is available if the Arctera Classification service is enabled for a user.		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 Arctera Unified Platform.
		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.
Classification	Sentiment Score	Is Equal To / Below (Inc.) / Above (Inc.)
Note: This option is available if the Arctera Classification service is enabled for a user.		
Attachment	Has Attachment	Yes / No
Attachment	File/Attachment Name	Contains / Doesn't Contain
Attachment	File Attachment Type	Contains / Doesn't Contain
		See Searchable attachment types.
Archive Date	Is Equal To: Finds items archived on a specific date.	Select date.
Filter archived data based on the date when emails, collaboration items, or files were archived.	Before: Finds items archived before a certain date.	**Note:** Use this filter only for the data archived after January 2021. Data before January 2021 will not appear in filtered results.

MESSAGE	ENTIRE MESSAGE	CONTAINS / DOESN'T CONTAIN
	After: Finds items archived after a certain date.	Tip: If you want to use Query Search instead of Advanced Search, use the ArchiveDate: term and then build the search criteria.
	Within Range: Finds items archived between two chosen dates.	
Source Type	Is: Filters results that match the selected source type(s)	Select one or more sources as needed.
	Is Not: Excludes results that match the selected source type(s).	
Department	All Senders & Recipients: Filters data where both the sender and recipient belong to the selected department(s).	 Select Any or All operator and then click Select Department.
Note: This option is available if the Arctera Surveillance service is enabled for a user.	Senders Only: Filters data where only the sender belongs to the selected department(s).	A dialog box opens where you can choose one or more departments to apply as a filter.
	Recipients Only: Filters data where only the recipient belongs to the selected department(s).	1. Use the Search Departments field to quickly locate a department by name.
		2. Toggle the Use Inheritance to include child departments

MESSAGE	ENTIRE MESSAGE	CONTAINS / DOESN'T CONTAIN
		of a selected parent department.
		3. Click Select All on Current Page to select every department visible on the current page. Else, select the required departments individually. The count of selected departments appears in the bottom of the dialog box.
		4. Click Select to confirm and apply them as a filter.
		If you want to reset your choices, click Clear Selection. If you want to close the dialog without saving changes, click Cancel.

1. Click **Search**.

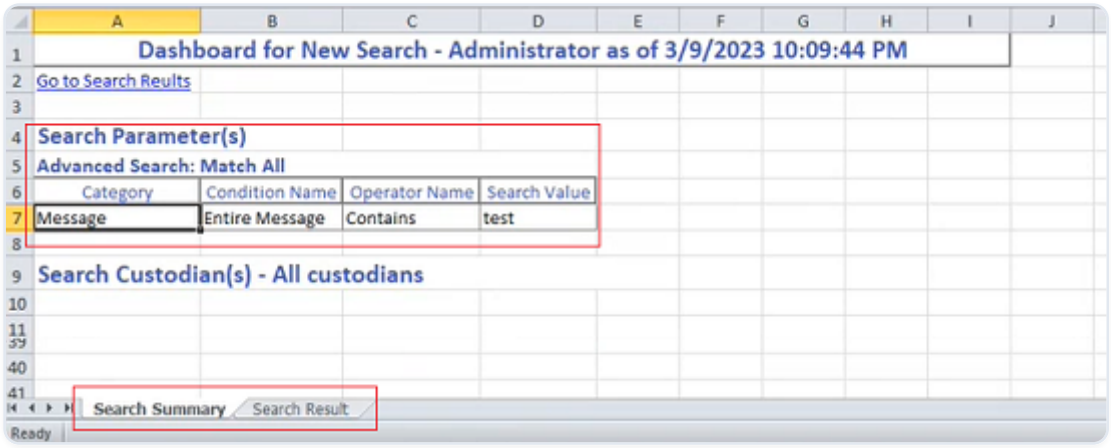
   You can perform a new search and optionally save it, or you can view the results of a previously saved search.

   Important!

- In Advanced Search, the search text input functionality is updated. In previous releases, when users were providing multiple text input with space, the default logical operator "AND" was getting applied. From now onwards, the default logical operator "OR" is getting applied to get user records.

  This operator change from "AND" to "OR" is applied to all kind of searches. If users have previously used spaces while providing the search text inputs, their saved records (saved searches/standard searches/Ongoing searches) will be impacted as the operator is changed from "AND" to "OR".

- Based on the selected attributes, when you export the search report, the Search Summary and Search Report is generated as shown in the sample image below.



Performing a query search

To perform query search:

1. Access the **Query Search** tab from the **Investigation** or the **eDiscovery** tab.
2. Specify the following inputs:

CUSTODIANS	**- SELECT ALL TO SEARCH ARCHIVES OF ALL OF THE CUSTODIANS THAT ARE ASSOCIATED WITH THE CASE.**
	- SELECT CUSTOM TO SEARCH ARCHIVES OF THE PARTICULAR CUSTODIANS.
	1. THE MANAGE BUTTON APPEARS. CLICK MANAGE TO OPEN THE ADD/ REMOVE CUSTODIANS.
	2. EXPAND SELECTED CUSTODIANS TO VIEW THE CUSTODIANS SELECTED FOR THIS SEARCH.
	3. EXPAND MANAGE CUSTODIANS AND SELECT THE CUSTODIANS REQUIRED FOR THIS SEARCH.
	4. (OPTIONAL) SELECT SEARCH BETWEEN CUSTODIANS AT THE BOTTOM OF THE POP-UP TO RETRIEVE EMAILS EXCHANGED EXCLUSIVELY AMONG THE SELECTED CUSTODIANS. FOR DETAILS, SEE SEARCHING EMAILS EXCHANGED AMONG SPECIFIC CUSTODIANS**.**
	5. CLICK UPDATE TO ADD THESE SELECTED CUSTODIANS AS A SEARCH INPUT. THESE CUSTODIANS ARE LISTED UNDER THE SELECTED CUSTODIANS SECTION.
Query Search	Specify the search query by providing keywords.
	For example, if you are using the Source Type filter option, do the following as required:
	- To filter items from one source type, type a query as `SourceType: ""` . Example: `SourceType: "Exchange"`

CUSTODIANS	**- SELECT ALL TO SEARCH ARCHIVES OF ALL OF THE CUSTODIANS THAT ARE ASSOCIATED WITH THE CASE.**
	- SELECT CUSTOM TO SEARCH ARCHIVES OF THE PARTICULAR CUSTODIANS.
	1. THE MANAGE BUTTON APPEARS. CLICK MANAGE TO OPEN THE ADD/ REMOVE CUSTODIANS.
	2. EXPAND SELECTED CUSTODIANS TO VIEW THE CUSTODIANS SELECTED FOR THIS SEARCH.
	3. EXPAND MANAGE CUSTODIANS AND SELECT THE CUSTODIANS REQUIRED FOR THIS SEARCH.
	4. (OPTIONAL) SELECT SEARCH BETWEEN CUSTODIANS AT THE BOTTOM OF THE POP-UP TO RETRIEVE EMAILS EXCHANGED EXCLUSIVELY AMONG THE SELECTED CUSTODIANS. FOR DETAILS, SEE SEARCHING EMAILS EXCHANGED AMONG SPECIFIC CUSTODIANS**.**
	5. CLICK UPDATE TO ADD THESE SELECTED CUSTODIANS AS A SEARCH INPUT. THESE CUSTODIANS ARE LISTED UNDER THE SELECTED CUSTODIANS SECTION.
	- To filter items from multiple source types, type a query as `SourceType: ("" and "")` . Example, `SourceType: ("Exchange" OR "Citrix")`

Guidelines for specifying queries

The application supports query searches only if the following necessary conditions are followed. Else, the application displays corresponding errors.

CONDITIONS	EXAMPLES
-	**The search criteria must be used after the operator and before the query text.**
-	**The AND/OR/NOT operators must be written in capital letters.**
-	**The AND/OR logical operator is missing.**
-	**The extra space(s) between operators is not allowed.**
-	**The space after bracket is not allowed.**
-	The space before colon is not allowed.

> Operator-specific conditions Spaces-specific conditions

1. Click **Search**.

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

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" (with quotes) returns items that include results for the exact phrase as well as for "test not verification". It does not return results for test and verification and test verification (without quotes).
- 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.

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 search terms in the proximity search results are highlighted in the Preview pane and Native views of the attachments. The exact number of words between the search keywords or the order of the keywords does not matter.
- Arctera Personal Archive limits the proximity word count to a maximum of 49 words.
- Using wildcard characters in proximity searches is not recommended. When a proximity search includes wildcard characters, the application limits the search proximity value to a maximum of 10 to prevent performance degradation.

- The results from a proximity search can contain stop words, but the stop words are excluded from the proximity word count.

Search examples and tips

Examples of using Basic, Advanced, and Query Searches

Suppose 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 search. The search returns any items that do not contain *Box* but that contain the exact phrase *password reset*.

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. Add search criterion before query text/ value.	_All:(test or test2)
			"hello world"
			Entiremessage:test

SEARCH TERM	DATA TYPE	DESCRIPTION	EXAMPLE
`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
		Note: This query search term does not support the Searches for the Microsoft Teams messages.	
`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
Bcc	Text	Search by blind carbon copy recipients.	Bcc:JoeBlogs@example.com
			Sender:*@example.com
`Cc`	Text	Search by carbon copy recipients.	Cc:JoeBlogs@example.com

SEARCH TERM	DATA TYPE	DESCRIPTION	EXAMPLE
		Note: This query search term does not support the Searches for the Microsoft Teams messages.	Sender:*@example.com
`Classification.tags`	Text	Search by classification tags.	Classification.tags:PII
		Note: This query search term does not support the Searches for the Microsoft Teams messages.	
`FromOrTo`	Text	Search the text in the From and/or To fields of the email.	FromOrTo:JoeBlogs@example.com
`Hidden`	Boolean	Search whether email is visible to end user or not.	Email Hidden\:
		Note: This query search term does not support the Searches for the Microsoft Teams messages.	Hidden:(1)
			Email Visible:
			NOT Hidden:(1)
`Inbound`	Boolean	Search inbound emails.	Inbound:false
		Note: This query search term does not support the	

SEARCH TERM	DATA TYPE	DESCRIPTION	EXAMPLE
		Searches for the Microsoft Teams messages.	
`Internal`	-	Search and retrieves only internal messages exchanged within the same organization.	To include internal emails, use: `Internal:(3)` .
		Note: This query search term does not support the Searches for the Microsoft Teams messages.	To exclude internal emails, use: `NOT Internal:(3)` .
`Ipheader`	IP Address	Search by the IP header of the email.	Specific IP Address\:
		Note: This query search term does not support the Searches for the Microsoft Teams messages.	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

SEARCH TERM	DATA TYPE	DESCRIPTION	EXAMPLE
			2019-12-31T23:59:59]
			Open Range:
			MailDate: {2018-01-01T00:00:00 TO 2019-12-31T23:59:59}
`Messagesizeinkb`	Floating Point Number	Search by total size of the email.	Messagesizeinkb: \[2.5 TO 5\]
		Note: This query search term does not support the Searches for the Microsoft Teams messages.	
`Outbound`	Boolean	Search whether a user sent the email.	Outbound:true
		Note: This query search term does not support the Searches for the Microsoft Teams messages.	
`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
`SubjectBody`	Text	Search the text in the subject of emails and/or in the content of the email.	SubjectBody:Test

SEARCH TERM	DATA TYPE	DESCRIPTION	EXAMPLE
`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:

- Sourcetype:"Exchange"
- SourceType:{"Exchange" OR "Citrix"}
- 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*.

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 About Hit-highlighting and navigating to searched terms.
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 exclude specific search terms.	cloud NOT computing finds archived messages with the search term cloud but not the search term computing.
		See Boolean operator searches.

SEARCH METHOD	SYNTAX	EXAMPLE AND MORE DETAILS
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: Arctera Personal Archive 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.

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 Arctera Unified Platform 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)
.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

FILE EXTENSION	SEARCHABLE ATTACHMENT TYPES
.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)
.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

FILE EXTENSION	SEARCHABLE ATTACHMENT TYPES
	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
	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

FILE EXTENSION	SEARCHABLE ATTACHMENT TYPES
.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
	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

FILE EXTENSION	SEARCHABLE ATTACHMENT TYPES
	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
	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

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.

Methods for searching tables and reports

This section includes the following topics:

About Quick Search and Criteria Search

The following search interfaces are provided for searching the lists or tables that Arctera 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 Arctera eDiscovery pages. The pages that also have Criteria Search are indicated in brackets.

Investigations tab

- Managed Accounts > Accounts (Criteria Search also available)
- Managed Accounts > Mail reassignment
- Batch Processes > Exports

eDiscovery tab

- Reviewers (Criteria Search also available)
- Cases
- *Case Name* > Exports
- *Case Name* > Case History (Criteria Search also available)

Alerts option

- 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 Arctera 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.

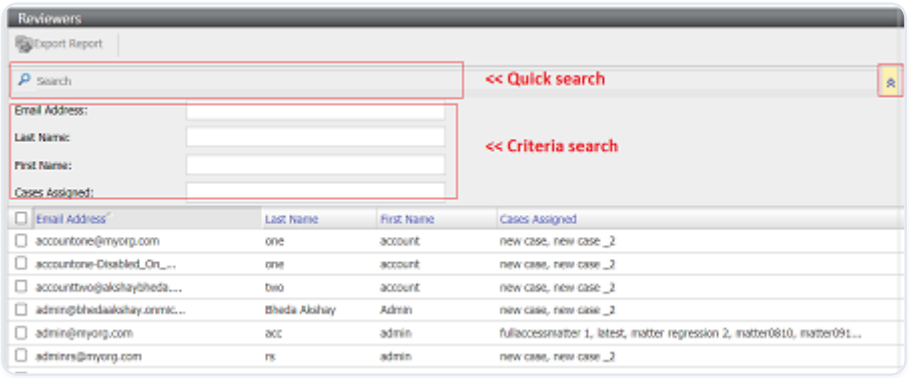
> **Note:** Quick Search and Criteria Search do not support phrase search, Boolean operators, proximity search, or wildcard search. Searches are not case-sensitive.

> **To search tables, lists, and reports**:

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

   The Quick Search interface is visible.

   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:



2. 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.

3. 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
   - eDiscovery tab > Administration > Reviewers
   - eDiscovery 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 option is displayed.

   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.

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

Arctera eDiscovery Frequently Asked Questions

Best practices, limitations, and known issues

This section includes the following topics:

Best practices and limitations with Arctera eDiscovery

General

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

Search

- Search times improve after a user performs their first search during each session because Arctera 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 node, 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 Arctera 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 Arctera eDiscovery.

  Workaround - close the security error message window and retry the download.
- Bcc recipients are currently not searchable in Arctera 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

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 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