Arctera™ Insight Surveillance User Guide

arctera™

Arctera Insight Surveillance: User Guide

Last updated: 2025-07-25

Legal Notice

Arctera US LLC | www.arctera.io

Documentation

Make sure that you have the current version of the documentation. Each document displays the date of the last update on page 2. The latest documentation is available here:

https://sort.veritas.com/arctera/documents

Documentation feedback

Your feedback is important to us. Suggest improvements or report errors or omissions to the documentation. Include the document title, document version, chapter title, and section title of the text on which you are reporting. Send feedback to:

productdocs@arctera.io

You can also see documentation information or ask a question on the Arctera community site:

https://vox.veritas.com/category/arctera-discussions/discussions/infoscale

Technical Support

Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within the company to answer your questions in a timely fashion.

Our support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about our support offerings, you can visit our website at the following URL:

www.arctera.io/support

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.arctera.io/support

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information
- Available memory, disk space, and NIC information

- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Technical Support
  - Recent software configuration changes and network changes

Licensing and registration

If your product requires registration or a license key, access our technical support Web page at the following URL:

www.arctera.io/support

Customer service

Customer service information is available at the following URL:

www.arctera.io/support

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Advice about technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs, DVDs, or manuals

Support agreement resources

If you want to contact us regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Worldwide	CustomerCare@arctera.io

Contents

Chapter 1

Introducing Arctera Insight Surveillance

This chapter includes the following topics:

About Insight Surveillance

Insight Surveillance is a software-as-a-service (SaaS) offering that deals with monitoring, searching, retrieving, and reporting of emails and messages. It is designed to meet a wide variety of regulatory requirements for the supervision of electronic communications.

Insight Surveillance offers a simple and intuitive user experience. It delivers end-to-end supervisory workflow to Arctera Insight Archiving customers, greatly reducing audit review time, minimizing compliance risk and increasing organizational efficiency for today's global enterprises.

This guide describes the procedures involved in configuring and managing Insight Surveillance and ensures that organizations meet electronic communication supervision requirements.

Insight Surveillance multi-tier architecture

Insight Surveillance has a two-tier architecture, which provides the ability to manage and delegate compliance responsibilities across multiple geographical, functional, and departmentally-distributed compliance departments. The following diagram illustrates this architecture:

The mirroring of an organizational department can be accomplished by creating departments and sub-departments in Insight Surveillance. The parent department (top tier) is a Corporate Office tier. The sub-department (bottom tier) is an office tier in which an administrator can create as many sub-departments as necessary. This architecture enables the corporate office to distribute the items monitoring workload to the second-tier offices as required.

Within a department in Insight Surveillance, an administrator or a reviewer can:

- Create another department for monitoring individual compliance and subsequently generate department-specific reports.
- Create, edit, and delete reviewer and escalation reviewer accounts for an office.
- Control whether the reviewers in an office can create hotwords (department-specific keywords or phrases) as per the compliance policy.
- Create compliance-specific searches (immediate, scheduled, and guaranteed sample searches).
- Monitor and review items.
- Reassign items to an escalation reviewer for approval or rejection.
- Export and print search results and reports for offline review or for sharing with an approved third-party organization.

System requirements

Compatibility documentation

For more information on web browser compatibility, supported social media servers and file services, refer to the latest Arctera Insight Archiving Compatibility List document in the Arctera Documentation Library.

Product documentation

Table 1-1 lists the documentation that accompanies Insight Surveillance. Before you start working with Insight Surveillance, you must understand how Insight Surveillance is associated with Arctera Insight Archiving, Arctera Insight Management Console, and Arctera Insight eDiscovery. This documentation is also available in PDF and HTML format in the Arctera Documentation Library.

Table 1-1 Product documentation

Document	Comments
Arctera Insight Archiving : Arctera Insight Management Console Help	Provide information on searching for archive accounts, creating an archive account, deploying users and enabling their access to Insight Surveillance, and removing user access.
Arctera Insight Archiving : Customer Administration Guide	Provide information on viewing your company configuration details and creating the archive instance for a customers.

Sampling support for content sources

Arctera Insight Surveillance supports sampling and capturing of review items from the Arctera Insight Archiving and Insight Capture content sources. The sampled items of the configured and enabled content sources are subsequently included in the review set for reviewers. The currently supported content sources are as follows:

Audio Files	Signal
Avaya	SMS
Blackberry	SMS Collaboration
CellTrust	Symphony
CrowdCompass	TeamsChannel
Domino	TeamsChat
EML	Text-Delimited
EWS	UBS
Exchange	Video Files
FXConnect	Viva Engage
IMessage	WebpageCapture
Collaboration	WeChat
IPC	WhatsApp
LinkedIn Audit	WhatsApp Collaboration
Mobile Phone	Workplace from Facebook
Pivot	XIP
Redtail Speak	XSLT/XML
London Stock Exchange Group (LSEG)	Yammar
Salesforce	Yieldbroker
Chatter	YouTube
ServiceNow	Zoom

While creating a department, in the **Monitoring policies** section, you can specify the sampling percentages for these content sources as shown in the sample image below.

For more information, See "Creating departments" on page 54.

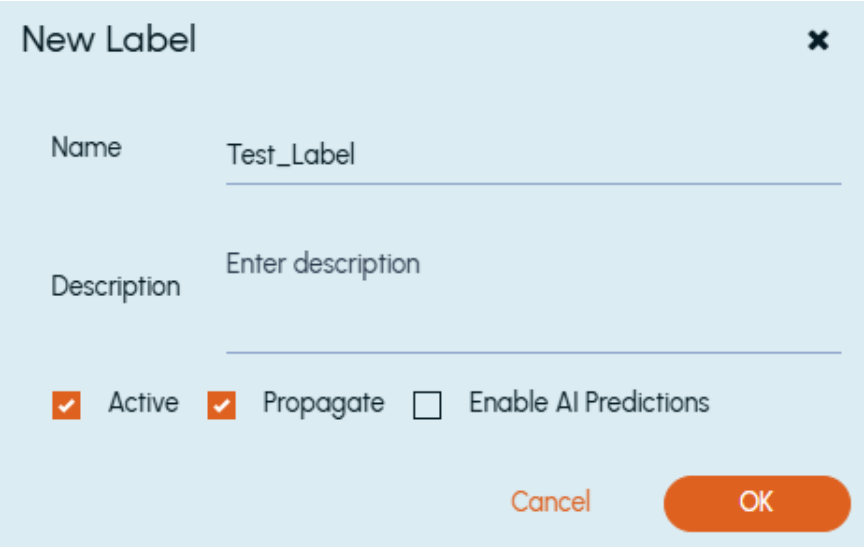
AI-based label predictions support for efficient review process

Arctera Insight Surveillance introduced the **Intelligent Review – Label Predictions** feature that uses Artificial Intelligence (AI) to predict labels for new items by analyzing how reviewers previously assigned labels to their review items.

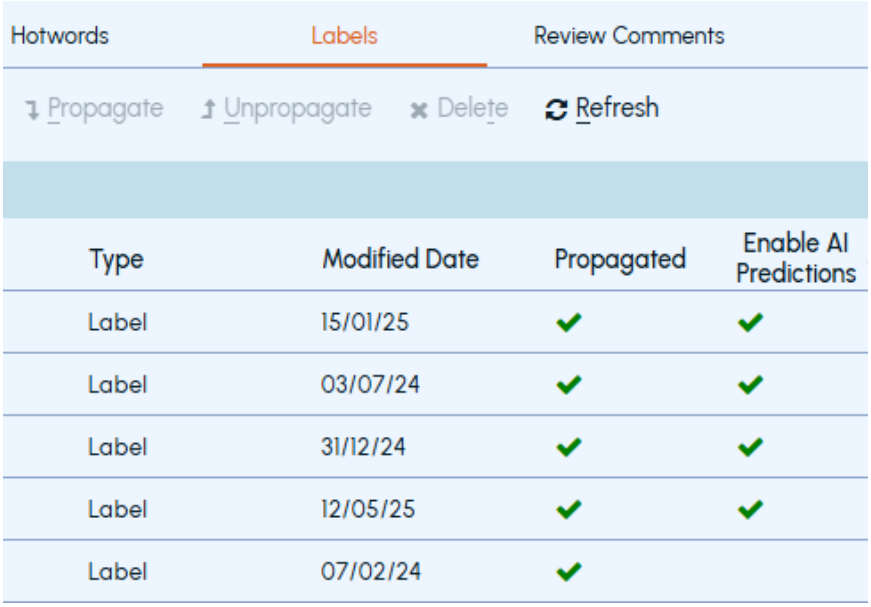
To enable AI-based label predictions at both the department and application levels, labels need to be activated, and the **Enable AI Predictions** option must be

selected. For AI predictions, only 20 active labels (including single choice group labels) can be enabled per department or at application level.

Refer to the sample image below to see where you can enable this feature in the application.



Select a department, go to the **Labels** tab. The **Enable AI Predictions** column displays if the labels, label groups, and a single choice label groups are AI-enabled.



Deactivating a label or label group disables AI predictions for that label or label group.

For more information on enabling AI-based label predictions and viewing predicted labels, refer the below mentioned sections.

See "Managing department-specific labels" on page 115.

See "Managing department-specific single choice label groups" on page 124.

See "Managing application-specific labels" on page 174.

See "Managing application-specific single choice label groups" on page 183.

See "Viewing predicted labels of review items" on page 276.

Date format support in Insight Surveillance

The default date format for the Insight Surveillance application is DD/MM/YYYY, which is also supported in Arctera Insight Management Console and Insight eDiscovery. However, as an administrator, you can opt for any of the available supported date formats based on your organizational needs or regional preferences.

If the tenant/customer modifies the date format in the Arctera Insight Management Console, the change will be reflected in Insight Surveillance after the database synchronization between the Arctera Insight Management Console

and the Insight Surveillance servers is completed successfully. This job runs every 15 minutes.

When any user logs in to the Insight Surveillance application, a user can see the date in the format specified by the tenant/customer.

Note: In case the selected date format mentions a single **Y**, it indicates **YYYY** format for the year variable (for example, 2024), and a single **M** indicates **MMM** format for the month variable (for example, Aug).

About Insight Surveillance system security

Insight Surveillance provides several security features that help ensure the integrity of your archived items. These features include:

- **128-bit SSL encryption** - When you log in to Insight Surveillance, SSL is used to encrypt the communication between your browser and our servers.
- **Role-based permissions to users** – As every role has limited permissions, functions like configuration, review, access control, escalation, and export are always performed by an authorized user.
- **Strong passwords** - For security reasons, passwords must be created using suitably complex criteria. The password policy can be configured based on customer needs.

Chapter 2

Getting started

This chapter includes the following topics:

Signing in to Insight Surveillance

To sign in to Insight Surveillance

1 Enter the Insight Surveillance URL in the internet browser.

For the best viewing experience, use Mozilla Firefox or Google Chrome. Insight Surveillance is not supported on Internet Explorer.

Note: Whenever a new version of the Insight Surveillance application is available, the application displays the following alert.

"A new version of this app is available. It is recommended to close all open tabs and reopen application for better experience. Click OK to refresh."

Arctera recommends you to click **OK** and close all the open browser tabs. Open the application again. In case you do not perform this action, the application page gets refreshed automatically and opens the latest version of the application.

---

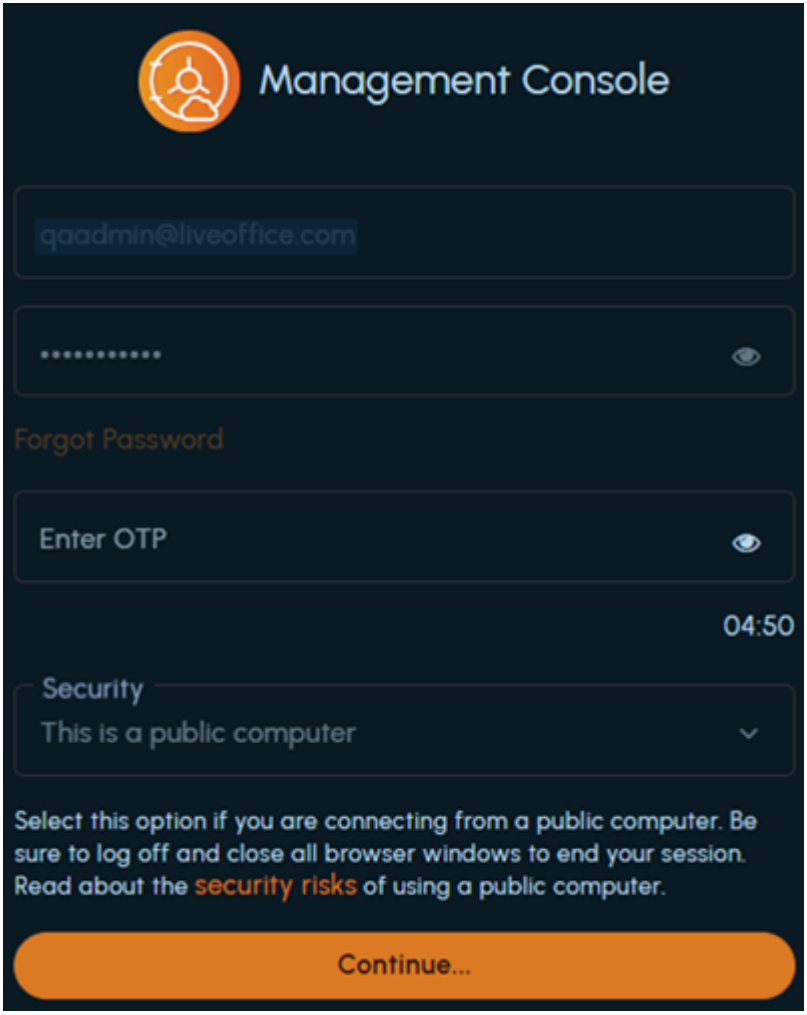
2 (Optional) Bookmark this URL in the Insight Surveillance compatible internet browser.

See "System requirements" on page 16.

3 Enter your user name (format: domain\user name) and password in the authentication screen.

4 Click **Sign In**.

5 If the multi-factor authentication (MFA) is enabled for you, the **OTP** field appears on the authentication screen.



This email-based authentication enhances the access and data security of Insight Surveillance. Management Console administrators have the permission to enable or disable multi-factor authentication at the user and tenant level. If the email-based authentication 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.

6 Click **Continue**.

After successful authentication, the Insight Surveillance dashboard appears.

Signing out from Insight Surveillance

To sign out from Insight Surveillance

1 On the Insight Surveillance user interface, in the upper right-hand corner, click the user profile icon.

2 Click **Log Out**.

Launching Arctera Insight Archiving applications

To launch Arctera Insight Archiving applications

1 On the Insight Surveillance user interface, in the upper right-hand corner, click the user profile icon.

When you hover over this icon, the account user name is displayed. Based on the access granted to the user, any or all of the following options are displayed:

- Arctera Insight eDiscovery
- Arctera Insight Management Console
- Arctera Insight Personal Archive

2 Select the application that you want to launch. The application appears in a new browser window.

3 On the new browser window for the selected application, enter your credentials.

Note: If the user has signed into Insight Surveillance using Single Sign-On and access is allowed using this method, then the sign in for the launched application is automatically authenticated.

Resetting a forgotten password

You can follow the below-mentioned procedure to securely and conveniently regain access to your account and mitigate the risk of unauthorized access and data breaches.

To reset your forgotten password

1 In the authentication screen, click the **Forgot your password?** link.

2 In the **User Name** field, provide your user name (email ID).

3 In the **Validation Code** field, enter the CAPTCHA text without spaces.

Note: The CAPTCHA text is not case-sensitive.

4 Click **Continue**.

Insight Surveillance sends the **Reset Password** link via email notification on your primary email address. The reset password link expires in 30 minutes.

Note: If you have not received any notification, check spam and junk folders, or contact admin if needed.

5 Click the **Reset Password** link and do the following:

- In the **User Name** field, provide your user name (email ID).
- In the **New Password** field, enter your new password.
- In the **Confirm Password** field, enter your new password again.

6 Click **Submit**.

The application redirects you to the login page.

Chapter 3

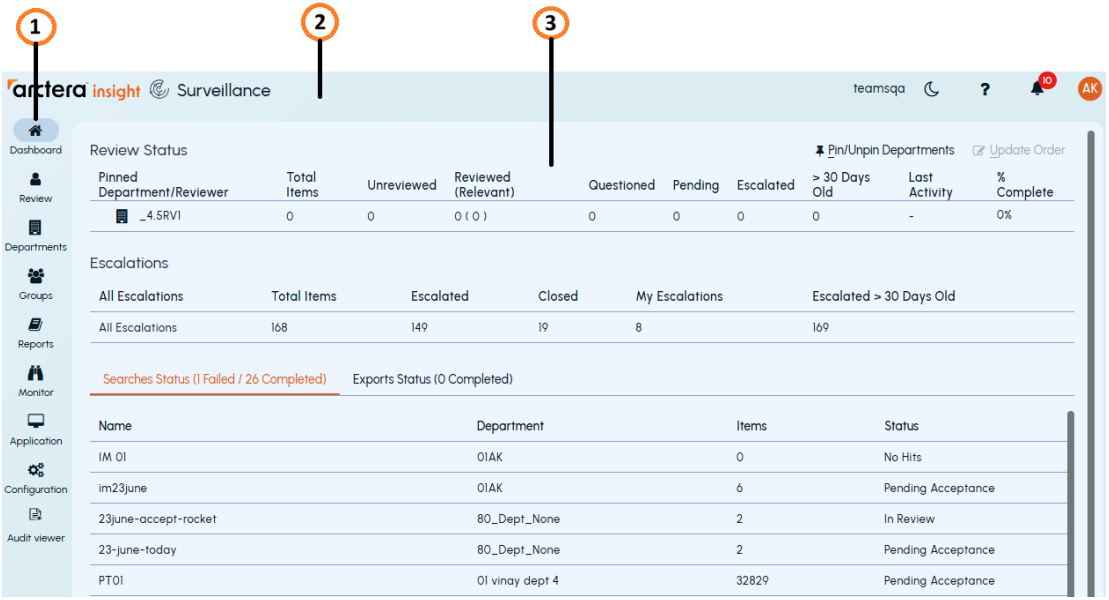
Working with dashboard widgets

This chapter includes the following topics:

Understanding the Dashboard page

After logging in to Insight Surveillance, your dashboard appears by default. If not, you can view it by clicking the **Dashboard** tab. The dashboard page lets you view the status of department reviews, escalations, and tasks. Aggregated statistics are used to report the status of these items.

Figure 3-1 An example of the dashboard that appears to administrators and reviewers upon login



1. Left navigation pane

The left pane provides a navigational menu. When you click on an item in this menu, the corresponding view appears in the right pane. The availability of these menu items and the corresponding views depend on the roles that are assigned to the signed-in user. Therefore, if you are a reviewer, some of these tabs may not be visible, depending on the permissions that your administrator has assigned to you.

You can click the **>>** icon to expand and the **<<** icon to collapse the navigation banner.

Tab	Description
Dashboard	This tab provides an overview of the status of the activities that you can perform in Insight Surveillance. It also gives you quick access to the activities that you are likely to perform frequently with Insight Surveillance.
Review	This tab displays a list of review items. A reviewer can provide comments for them and assign actions like review irrelevant or relevant, pending, question, escalate, and appraise.

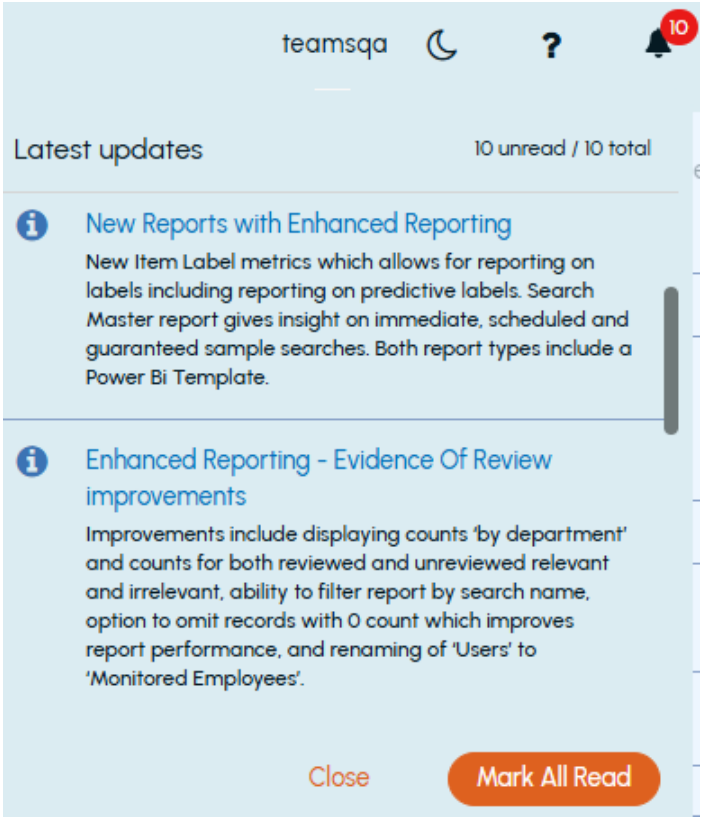
Tab	Description
Departments	This tab lets you manage departments, the monitored employees who belong to them, and reviewers assigned to department and allocate items for review to reviewers, specifying the allocation as a percentage.
Groups	This tab lets you manage employee groups that belongs to departments.
Reports	This tab lets you generate reports about review status for Bloomberg, Domino, Exchange, SMTP, Instant Messaging (IM), Microsoft Teams Chat and Microsoft Teams Channel.
Monitor	This tab lets you monitor and resubmit searches as necessary.
Application	This tab lets you access commonly used administrative facilities. You can manage the following: ■ **Roles** – Set up and amend the roles you can assign to users to manage their access to Insight Surveillance. ■ **Role Assignment** – Assign Insight Surveillance roles to users. ■ **Hotwords** - Set up lists of important words that you may want to search within archived items.
Configuration	This tab lets you: ■ Create schedules at which searches can run across multiple departments. ■ Manage audit settings for the Audit viewer. ■ Configure reporting API endpoints that can be used to generate reports and perform data analytics through custom scripts or templates.
Audit viewer	This tab lets you search and save audit records for various modules and operations at department and application level.

2. Banner

The banner contains the Insight Surveillance logo, company name, user name of the administrator or reviewer who is signed in, the **Switch to dark/light mode** icon, the **Help** icon, the **Notifications** icon, and the **Account Profile** icon.

- Click the **Help** icon to display application help in a separate window, without leaving the application window.

- Click the **Notification** icon to view the most recent updates in the application. Notifications and their summaries are displayed. Click notification titles for corresponding details in user help.



  Click **Mark All Read** to mark them all as read. Click **Close** to exit the notifications panel.

- Click the **Account Profile** icon to open the Arctera Insight eDiscovery, Arctera Insight Management Console, and Arctera Insight Personal Archive applications in new windows if you are authorized to access these applications.
- Click **Log Out** to exit the application.

3. Details pane

The details pane displays summary of the following sections:

- **Review Status:** Provides details of up to five or less pinned departments. If user has not pinned any department, then it presents details of the five departments to which that user has access.

- **Escalations:** Provides details of escalated items.
- **Searches and Export Status:** Displays results of the last few exports and searches run by a user.

Viewing status summary of recently reviewed departments

The **Review Status** widget displays detailed information on review status of your pinned departments. If user has not pinned any departments, then it displays detailed information on review status of 5 departments to which you have access. You can pin (bookmark) up to five departments to quickly view their review status when required. If you try to select the sixth department, a notification appears that you cannot pin more than five departments. If the pinned departments are no longer required, you can unpin them.

When you log out and log in the session again, the pinned departments from the last session are displayed.

If you have permissions to view department reviewers details, click the **>** icon to expand the department row. When department row is expanded, the department reviewer details are displayed. You can drill down for further details in a specific area.

Figure 3-2 An example of a summary of recently reviewed departments

Review Status

Pin/Unpin Departments | Update Order

Pinned Department/Reviewer	Total Items	Unreviewed	Reviewed (Relevant)	Questioned	Pending	Escalated	> 30 Days Old	Last Activity	% Complete
01_KD_Dept	121929	121888	6 (5)	2	33	2	121888	14/01/25	0%
Admin	37	-	2 (2)	2	33	0	0	14/01/25	-
Kanchan Dudhe	4	-	4 (3)	0	0	1	0	04/09/23	-
Aditya Magare	0	-	-	0	0	0	0	-	-
Mandar Nagarkar	0	-	-	0	0	0	0	-	-
Sarita Korake	0	-	-	0	0	0	0	-	-
Tushar Patil	0	-	-	0	0	0	0	-	-
User5	0	-	-	0	0	0	0	-	-
01 vinay dept 1 - Updated	47660	47607	7 (4)	11	35	9	47607	01/05/25	0%
vinay-independent	543	523	17 (14)	2	1	3	523	21/11/23	3%
0001test	25378	25376	1 (1)	1	0	0	25376	09/06/25	0%
01-Karan-Test	43802	43657	117 (116)	1	27	5	43657	01/12/24	0%
Total in this subset	239312	239051	148 (140)	17	96	19	239051	-	0%

It summarizes the departmental details such as:

- Total items presented for review
- Total relevant items reviewed and unreviewed

- Number of pending, questioned, or escalated items
- Items more than 30 days old that are still unreviewed
- Date of the last marking activity performed in the department
- Current review completion status

Pinning and unpinning departments to view review status

You can pin (bookmark) up to five departments to quickly view their review status when required. You can drill down for further details in a specific area. If the pinned departments are no longer required, you can unpin them.

To pin and unpin departments

1 In the left navigation pane, click **Dashboard**.

2 On the **Review Status** wizard, click **Pin/Unpin Departments**.

3 In the **Pin/Unpin Departments** dialog box, search for the department that you want to pin or unpin, then and click the pin icon adjacent to it.

The icon color and direction of the pin icon changes to indicate that the department is selected. Use the navigation arrows to go to the previous and next pages to select departments. The count of the departments selected for pin or unpin is displayed at the bottom of the dialog box.

4 Click **Save**.

If the departments selected for pinning, these departments appear on the **Review Status** wizard. If the departments selected for unpinning, these departments disappear from the **Review Status** wizard.

Changing the order of pinned departments

The **Update Order** button is enabled only if the **Review Status** wizard contains more than one pinned departments.

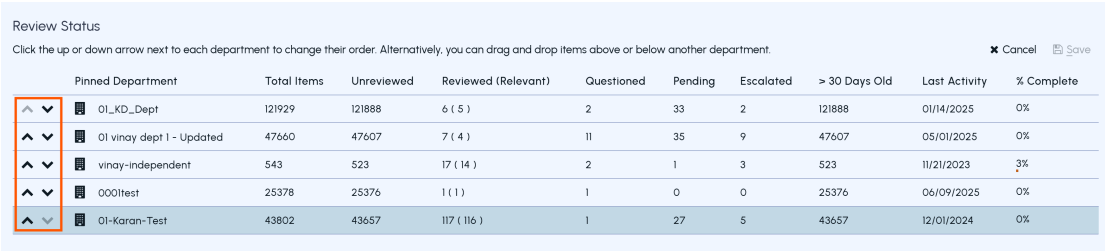
To change the order of pinned departments

1 In the left navigation pane, click **Dashboard**.

2 On the **Review Status** wizard, click **Update Order**.

3 Use the UP and DOWN arrows adjacent to the department name to change order of pinned departments.

Alternatively, drag and drop the department above or below another pinned department.



Note: The **Save** option remains disabled till you change the order of at least one department.

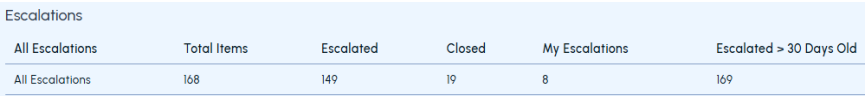
4 After updating the order, click **Save**.

The dashboard refreshes and displays the updated order.

Viewing the review status summary of escalated items

The **Escalations** widget displays the escalation history for specific items.

Figure 3-3 An example of a summary of escalated items



It summarizes the details such as:

- Total items reviewed
- Total items escalated
- Total items closed

- Items more than 30 days old that are still unreviewed

Viewing a summary of searches and exports

This is a read-only function. The **Searches Status** tab is visible only when the user has the *View Task Status* permission in any of the departments and also has any of the *Search capture* or *Application Search* permissions. If the administrator removed the *View Task Status* permission from all departments for a user, the **Searches Status** tab is not displayed to that user.

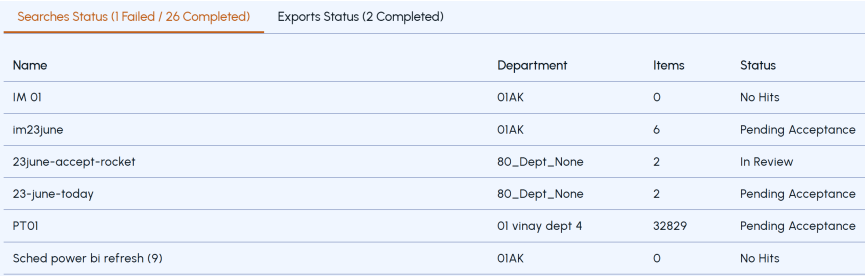
To view a summary of completed searches

1 In the left navigation pane, click **Dashboard**.

2 Click the **Searches Status** tab to view the status of failed and completed searches.

Click the **Exports Status** tab to view the status of failed and completed exports.

Figure 3-4 An example of Searches and Exports status on dashboard



Chapter 4

Managing employee groups

This chapter includes the following topics:

Creating custom employee group

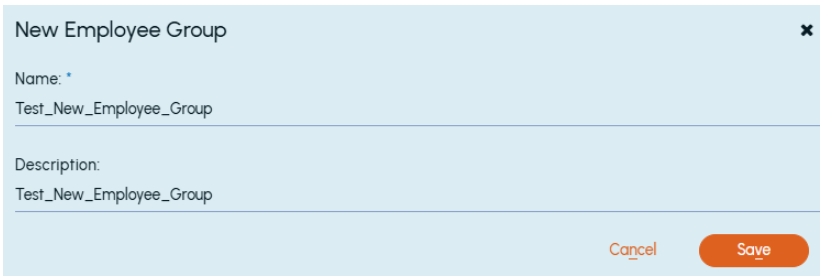
You must have the *Manage Employees* permission to set up an employee group. By default, users with the application-level *App User Admin* role have this permission.

To create a custom employee group

1 In the left navigation pane, click **Groups**.

2 Click on the **Employee Groups** section and expand it.

3 By default, the **General** tab is displayed. If not, select the **General** tab. On the action bar of the tab, click **New Custom Group**. The **New Employee Group** dialog box appears.



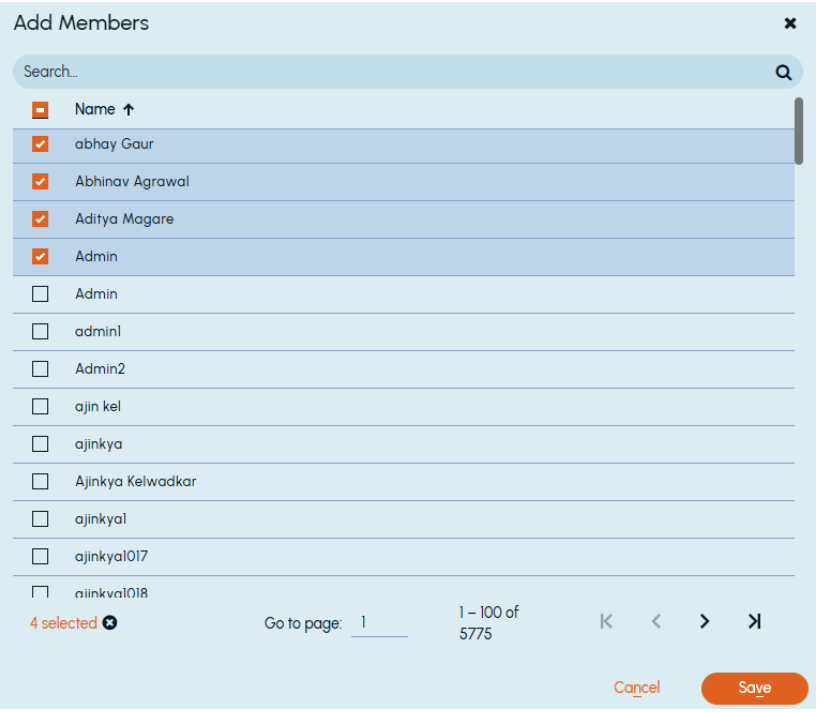
4 Provide the following details:

Name	Specify a name for the employee group.
Description	Specify a description for the employee group.

5 To add employees to the group manually, click the **Members** tab.

6 Click **Add**. *Add Members* window is displayed.

Select the employees from the list as shown in the following sample image:



7 Click **Save**.

Editing custom employee group details

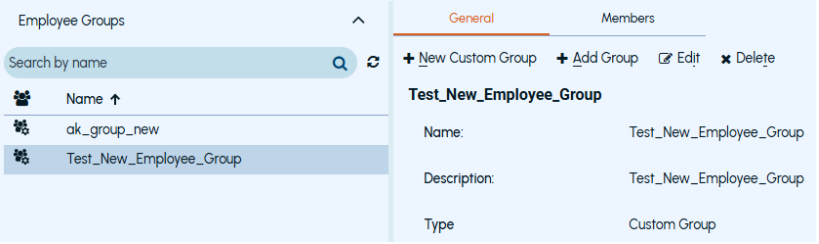
You must have the *Manage Employees* permission to edit an employee profile. By default, users with the application-level *App User Admin* role have this permission.

To edit the details of the custom employee group

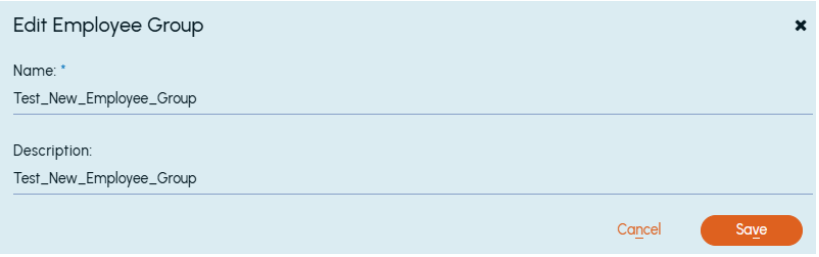
1 In the left navigation pane, click **Groups**.

2 Click on the **Employee groups** section and expand it.

3 Search for and select the employee group you want to edit.



4 By default, the **General** tab is displayed. If not, select the **General** tab. On the action bar of the tab, click **Edit**. The **Edit Employee Group** dialog box appears.

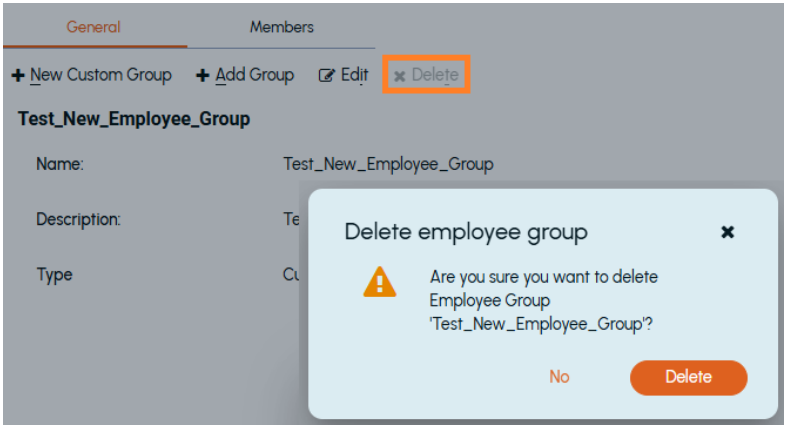


5 Update the employee group details. For more information on the employee group fields and adding members to a group, See "Creating custom employee group" on page 37.

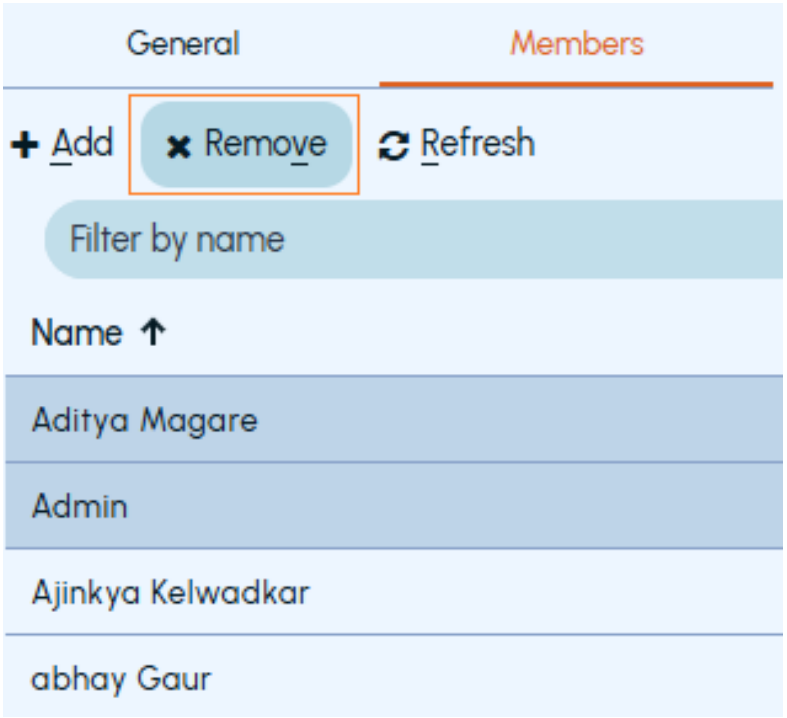
6 Click **Save**.

7 On the action bar of the tab, perform the following actions as required:

- **Deleting an employee group**: If an employee group is no more required, under **General** tab, click **Delete**.



- **Removing an employee from employee group**: If an employee is no longer a part of an employee group, under **Members** tab, select the employee/s, click **Remove**.



Adding employee groups

Like adding users (employees) from Microsoft Azure Active Directory, you can add new employee groups to Insight Surveillance from the Microsoft Azure Active Directory. After the employee groups are successfully added, their records are automatically synchronized to display the corresponding group members. Additionally, you have the option to manually initiate synchronization.

If you no longer need certain employee groups, you can remove them from Insight Surveillance. Note that when you remove employee groups from Insight Surveillance, these groups are not deleted from the Microsoft Azure Active Directory. However, if the employee groups are deleted from the Azure Active Directory, those groups gets deleted from the Insight Surveillance database immediately after successful synchronization. To permanently delete the group, you should delete it from the Azure Active Directory.

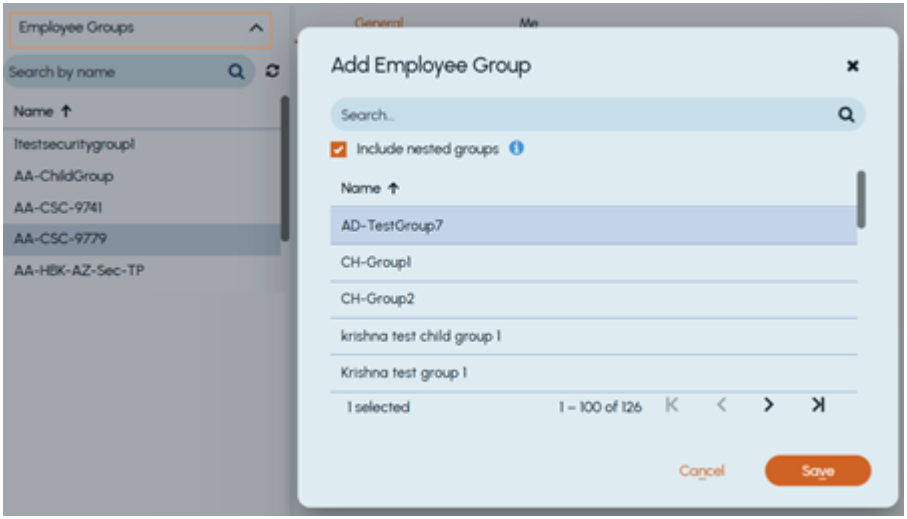
You must have the *Manage Employee Groups* permission to add employee groups from Microsoft Azure Active Directory. By default, users with the application role of *App User Admin* have this permission.

To add employees and employee groups

1 In the left navigation pane, click **Groups**.

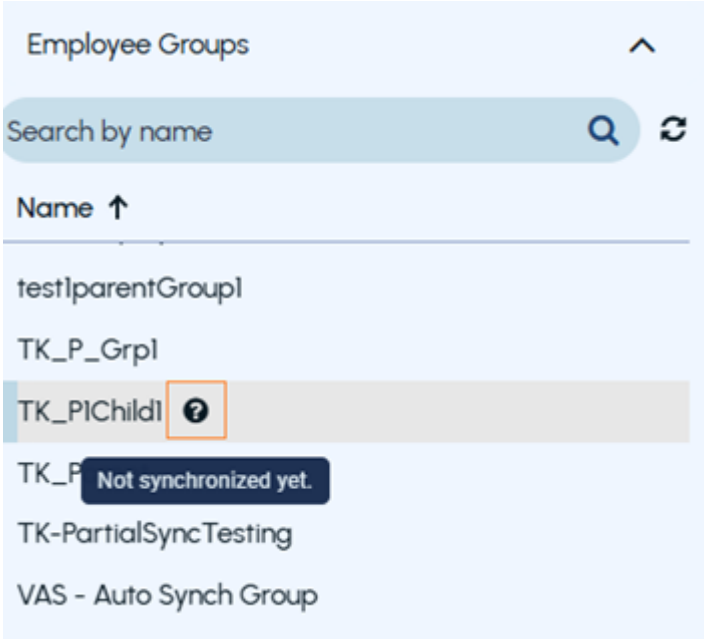
2 Expand the **Employee Groups** section, if not expanded by default.

The application displays the currently available employee groups in Insight Surveillance as shown in the sample image below. To sort employee groups in either ascending or descending alphabetical order, click on the **Name** column heading.

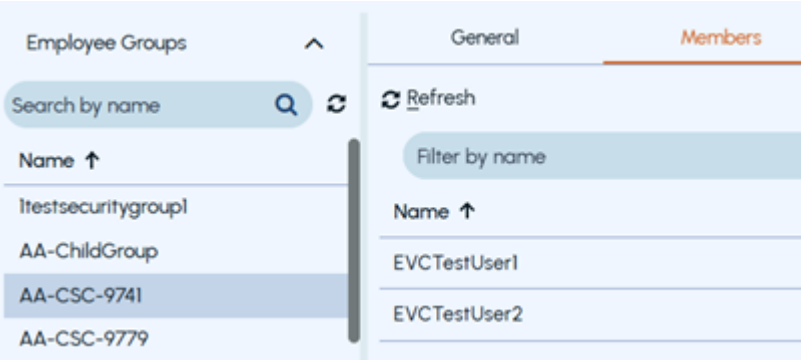


3 To view the employee group details, select the group.

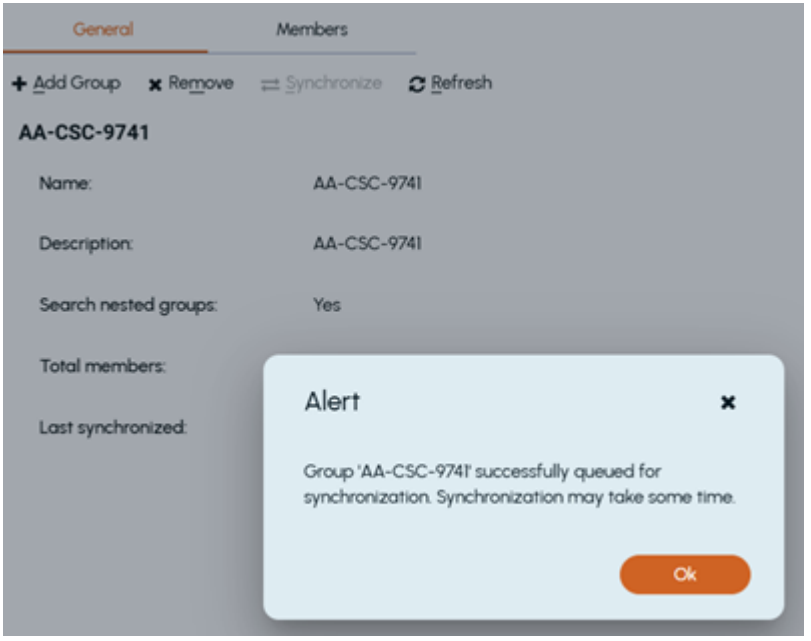
- Hover over the status icon adjacent to the employee group name to view the status of synchronization with the Azure Active Directory.



- On the right side, the **General** tab is displayed by default. It provides the name and description of the group, total members in the group, status to search the nested groups, and the date when this group record is lately synchronized with the Azure Active Directory.
- Click the **Members** tab to view the details of group members. This is a read-only information. After group record synchronization, addition or deletion of members is updated on this tab.
  To sort member names in either ascending or descending alphabetical order, click on the **Name** column heading.
  To search members by name, specify a few characters of member name, and click the filter icon or press ENTER.
  To view members from other pages, use navigation arrows in the bottom of the dialog box to go to the next or previous pages.



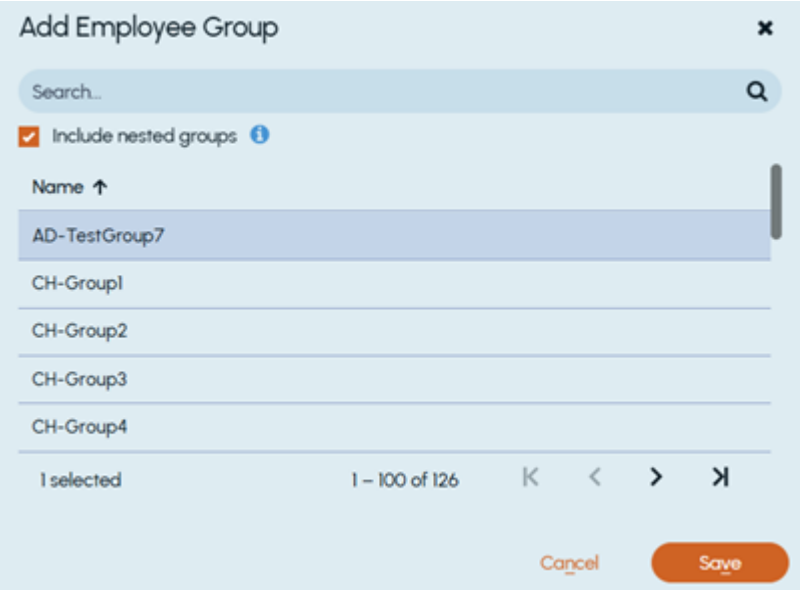
4 To manually synchronize the group record across departments, click **Synchronize**. The application displays an alert as shown in the sample image below.



Note: The application takes some time to update the record. Besides that, the application automatically synchronizes the record with the Azure Active Directory every 15 minutes. Click **Refresh** to view the updated details.

---

5 To add a new employee group, click **Add Group**. In the **Add Employee Group** dialog box, do the following:



- To sort employee groups in either ascending or descending alphabetical order, click on the **Name** column heading.
- To search a group, in the **Search** field, specify the group name characters, and click the search icon.
- To manually search a group, use navigation arrows in the bottom of the dialog box to go to the next or previous pages.
- To include all the members from the nested groups, select the **Include nested groups** check box.
- To add the selected employee group to Insight Surveillance, click **Save**. Wait for some time for record synchronization.

6 To remove the existing employee group, search for and select the group you want to remove, and click **Remove**.

Chapter 5

Managing departments

This chapter includes the following topics:

About departments

The mirroring of organizational department can be accomplished by creating departments and sub-departments in Insight Surveillance. The parent department (top tier) is a Corporate Office tier. The sub-department (bottom tier) is an office tier in which, an administrator can create as many sub-departments as necessary.

This architecture enables the corporate office to distribute the items monitoring workload to the second-tier offices as required.

Figure 5-1 A sample departmental structure in Insight Surveillance

Departments allow for the organization of monitored employees, the configuration of department-wide monitoring policies, and capture and review of monitored employees' archived communication items via random sampling and searches. Administrators can configure individual monitoring policies for each department and sub-department. Insight Surveillance lets you organize monitored employees into departments that reflect the structure of your company. For example, an administrator can create departments that are called Marketing, Sales, Engineering and so on. Employees can be added to the appropriate departments. Reviewers can review items of these departments and the nested departments.

Understanding the Departments page

The following images highlight the standard features of the **Departments** page.

Figure 5-2 A sample page showing summary of departments

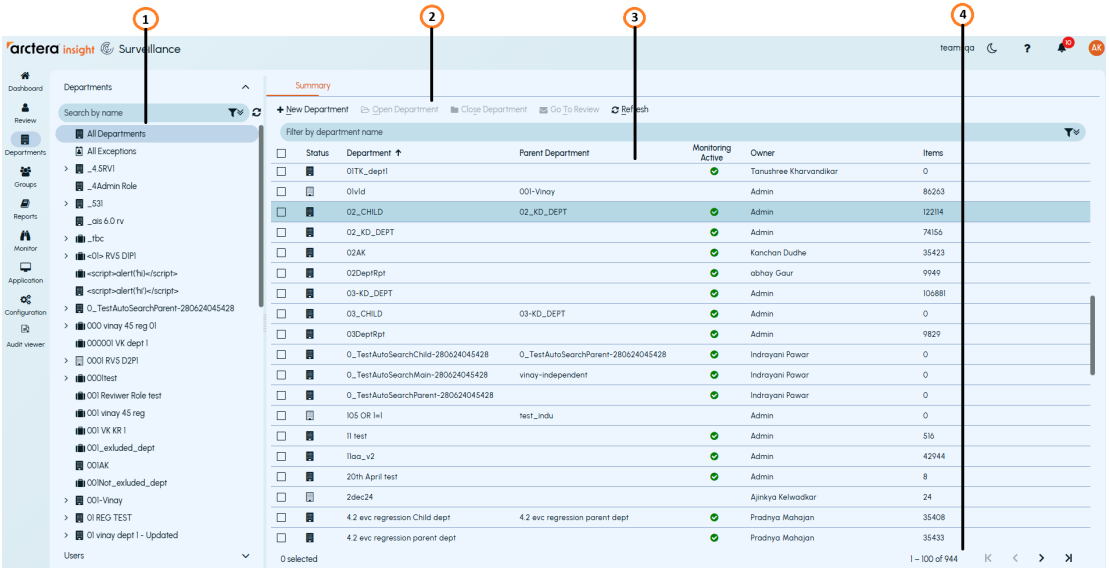
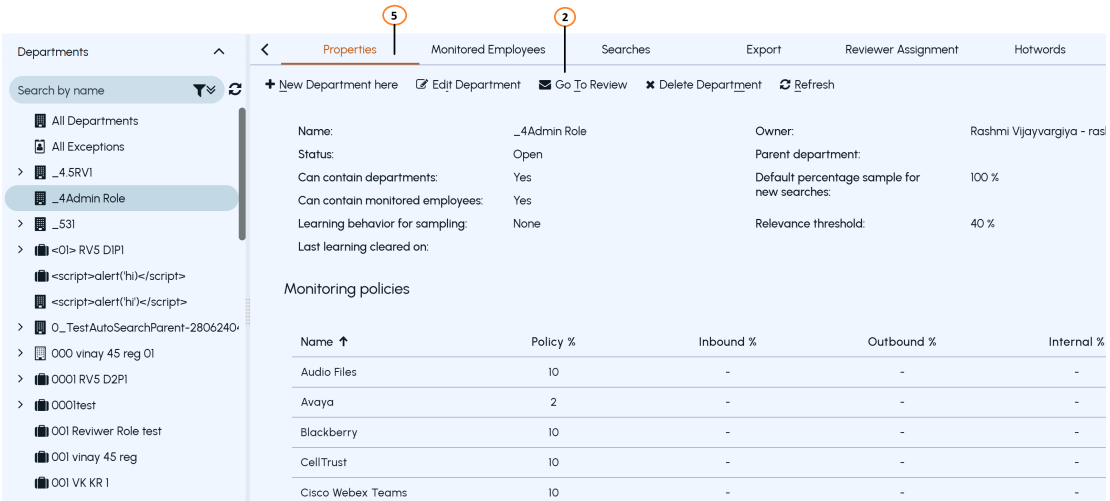


Figure 5-3 A sample page after selecting a single department



1. Search and filter pane

Insight Surveillance lists all the available departments. After you create a search, the application searches for the items based on the search criteria. You can use the filters to narrow down the search results. You can use the filtering options

to search the required department. Options include filtering by department name, exception employees, and reviewers associated with the department.

You can select a single or multiple departments just by selecting the corresponding check boxes. You can select the departments from multiple pages. For better performance, it is recommended to select maximum 200 records. To clear the entire selection, click the **Clear selection** icon on the bottom pagination pane.

2. Action bar

Functions of the action bar vary with the menus you have selected. The available action buttons are mentioned below.

Table 5-1 Department view action buttons and their function

Action button		Function
When the **All Departments** node is selected:		
	New Department	Opens a **New Department** page to create a new department.
	Open Department	Opens a closed department for monitoring .
	Close Department	Closes an open department and restricts monitoring of employees in the department.
	Go to Review	Navigates you to the **Review** tab of the current department.
	Refresh	Refreshes the page information.
	Filter by department name	Allows you to narrow down the results by specifying a department name.
	When an individual department node is selected:	
	New Department here	Opens a **New Department** page to create a new department.
	Edit Department	Opens an **Edit Department** page to let you to modify department configuration/details.
	Go To Review	Opens the selected department in the review pane to access items for review.
	Refresh	Refreshes the page information.

3. Details pane

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

or more columns on the selected page. The sorting is case insensitive. After performing a sort action, users land on the first page, by default.

You can change the size and order of the columns on this pane. This change persists till the time you are signed in. After you log out from the application, the default column size and the order is retained.

4. Bottom navigation bar

This bar displays total number of records, total number of records on page, and total number of the selected records if you have selected these records. The navigation options are supported for multi-page lists.

- Click the **Clear selection** icon to clear the selection of records in the table.
- 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.

5. Menu bar

The Title bar appears directly underneath the upper banner. The left side of the title bar always displays the name of the current page. This bar also displays menus based on the permissions you have to work within departments.

Table 5-2 Department view menu bar tabs and their function

Menu	Function
Properties	Displays department-level properties. You must have the *Configure Department Properties* permission in a department to edit its properties. Users with the *User Admin* role have this permission by default. You can filter the departments by name and choose whether to list any exception employees and reviewers that are associated with them. Using the **Properties** tab, you can perform the following: ■ rename a department ■ change monitoring policy ■ close and reopen the department ■ nominate a new owner Note: Even if you nominate a new owner, the original owner still retains all the administrative permissions. You can use the **Role Assignment** feature to remove these permissions.

Table 5-2 Department view menu bar tabs and their function *(continued)*

Menu	Function
Monitored Employees	Allows you to manage the configuration activities for department-specific searches.
Searches	Allows you to manage the configuration activities for department-specific searches.
Export	Allows you to manage the export activities for department-specific data.
Role Assignment	Allows you to manage department-specific roles and responsibilities.
Hotwords	Allows you to manage department-specific hotwords and hotword sets.
Labels	Allows you to manage department-specific labels.
Review Comments	Allows you to manage department-specific review comments.
Trash	Allows you to manage department-specific trash rules.
Allowlist	Allows you to manage department-specific allowlist rules.
History	Displays start and end dates for employees added to the department.

Searching departments

Upon accessing the **Department** page, a list of all the available departments appears.

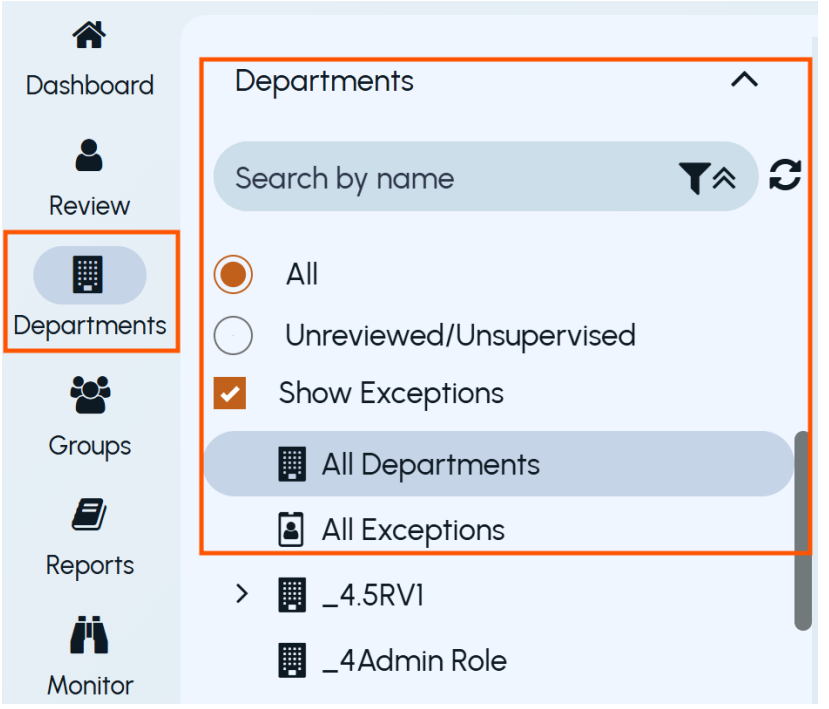
To quickly search a required department

1 In the left navigation pane, click **Departments**.

2 Expand the **Departments** section if it is not expanded by default, and click the **Apply filter** icon to view the filtering options.

Note: Insight Surveillance lists all departments. Use the provided filtering options to search the required department. Options include filtering by department name, exception employees, and reviewers associated with the department.

A closed department will only be visible if any of its child department is open.



3 Perform the following steps as required:

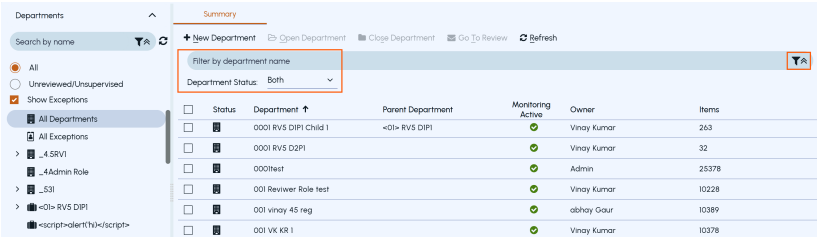
- In the **Search by name** field, type name of a department or department owner containing items you want to search.
  Click **Show extra filtering options** to see the following filters:
- Select **All** to search a department within all departments.

- Select **Unreviewed/Unsupervised** to search a department where no department reviewer or compliance supervisor is assigned.
- Select **Show Exceptions** to search for exception employees. Type a name of exception employee.
- Select **Show Reviewers** to search for the specific reviewers. Type a name of a reviewer.

4 Click the **Apply Filters** icon to apply the search criterion.

The application displays a summary of your search result.

5 Alternatively, select the **All Departments** node to obtain a summary of all the available departments. To view the departments based on their *closed* or *open* status, expand the filter section and choose the respective option from the **Department Status** drop-down list as shown in the sample image below:



The application displays the summary of departments based on their status.

Creating departments

The minimum information needed to create a department is its name and an owner. The owner can be any employee that you have added to the system but is typically the main system administrator for Insight Surveillance. You can add either a new department or a nested department (a child department of an existing department).

Note: You must have the *Create Departments* permission to add a new department. By default, users with the *App User Admin* role have this permission.

To create a department

1 In the left navigation pane, click **Departments**.

2 On the action bar, click **New Department** or press **Alt + N**.

The **New Department** dialog box appears.

3 In the **Department** section, specify the relevant information in the respective fields.

Name	Type a unique name for the department. The name can contain spaces, all the special, and the text characters.
Status	Choose **Open** to make the department open for monitoring. Choose **Closed** to restrict monitoring of employees in the department. The closed department name appears on the start page of the application only when any of its child department is open. Employees who are also monitored in other departments continue to be monitored in the closed departments.
Owner	Select the name of the principal administrator for the department. Note: Each department has an owner, who must have a logon but does not need any special privileges assigned. By default, Insight Surveillance grants the permissions associated with the *Admin* role to department owners. These permissions are as follows: ■ Grant access to users ■ Add monitored employees ■ Configure department properties ■ View reports
Parent department	If the department itself is a parent department, do not select any previous department in this field. If you want to create this department under any existing department, click the search icon to select the parent department.

4 In the **Options** section, specify the relevant information in the respective fields.

Can contain departments	Click the slider switch to turn it ON to allow creating nested departments under this department. Click the slider switch to turn it OFF to restrict creating nested departments under this department.
Can contain monitored employees	Click the slider switch to turn it ON to allow adding monitored employees to this department. Click the slider switch to turn it OFF to restrict adding monitored employees to this department. Note: You may want to clear this option in cases where you need to set up a department hierarchy, where the top-level department do not contain any monitored employees, but the nested departments do.

5 In the **Search details** section, specify the policy that Insight Surveillance must follow when it adds the results of a search to the department review set.

Default percentage sample for new searches	Specifies the minimum percentage of the items that a search returns to add to the review set. When you create a search, you can qualify this option further by specifying the minimum number of items that are required per employee.
Lock	Click the slider switch to turn it OFF to allow department administrators to change the sample rate for new searches. Click the slider switch to turn it ON to restrict department administrators from changing the sample rate for new searches.

6 In the **Intelligent review** section, specify a sampling method and relevancy threshold.

Note: To use the Intelligent Review feature efficiently, ensure that the *Add or remove content snippets* permission is enabled for the departments in which you will be creating Searches. Else, you will not be able to capture or remove text for machine learning in Arctera Insight Surveillance. After you capture a sample text, Insight Surveillance adds it to the machine learning model.

When you execute a search in the same department, based on the actions that reviewers have taken on earlier items, Insight Surveillance quickly retrieves and categorizes other items as relevant or irrelevant for your review. Intelligent Review is not applicable in the case of *Immediate* searches, if Intelligent Review is not enabled at department level. To determine the relevance of an item for review, Insight Surveillance checks email metadata, classification tagging, the content of the items, and its route from sender to recipients. However, the Intelligent Review feature does not consider the Microsoft Teams items for machine learning, and always mark them as *Relevant*, by default.

Learning behavior for sampling

The options that are available depend on whether you use guaranteed sampling, which is the default sampling mode, or statistical sampling.

None: Insight Surveillance samples items in the normal way, without implementing Intelligent Review.

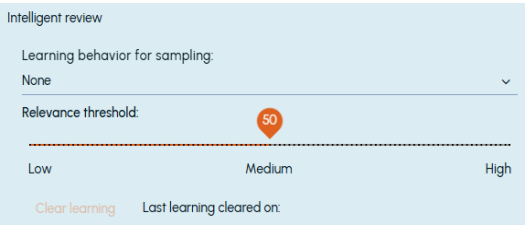
Sample exact percentage and prioritize: Sample exact percentage and prioritize for guaranteed sampling. Insight Surveillance samples both relevant items and irrelevant items without favoring one over the other. So, if your monitoring policy requires that you capture and review 10% of items, Insight Surveillance captures 10% - but a substantial number of the items may be irrelevant. With this option, however, Insight Surveillance does give the items a status of either Unreviewed (Irrelevant) or Unreviewed (Relevant) as it adds them to the review set. When you later review the items in the Review pane, you can filter them by their Unreviewed status to distinguish between the relevant and irrelevant items.

Sample exact percentage of relevant content in addition to current sample: Sample exact percentage of relevant content in addition to current sample (guaranteed sampling only). Insight Surveillance adds both relevant items and irrelevant items to the review set until it has captured the required percentage of relevant items. With this option, therefore, Insight Surveillance may capture more items for review than your monitoring policy demands. For example, suppose that your policy requires you to review 10% of items. To achieve the required number of items, you may need to capture 20% of items, only half of which are relevant.

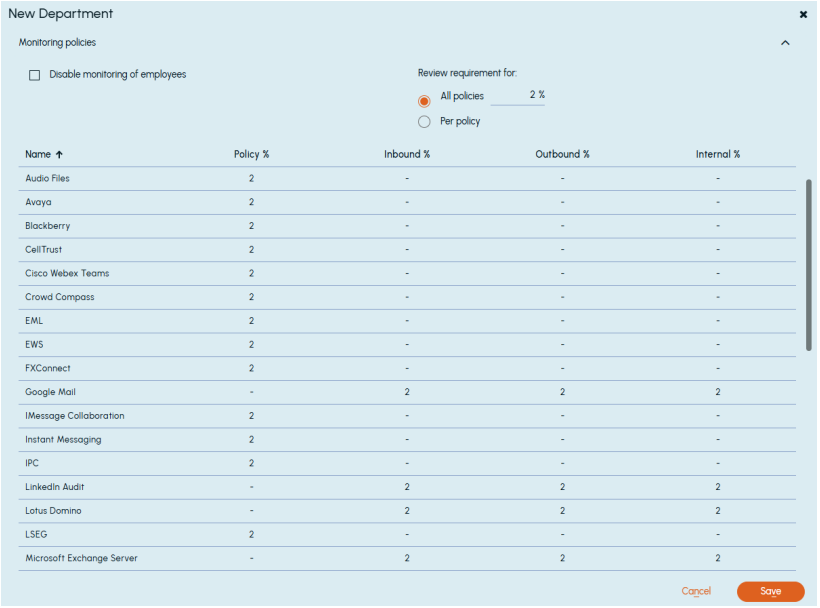
Sample exact percentage of available relevant content: Sample exact percentage of available relevant content (guaranteed sampling).Insight Surveillance discards all content that it considers irrelevant and samples relevant content only, until it has captured the required percentage. So, if your monitoring policy requires that you capture and review 10% of items, Insight Surveillance captures precisely 10%.

In the case of guaranteed sampling only, if there are too few relevant items to fulfil the monitoring policy then Insight Surveillance supplements them with irrelevant items. For example, suppose that 100 items are available for sampling, and your monitoring policy requires you to capture 10% of them.

If only seven items are relevant, Insight Surveillance adds three irrelevant items to achieve the required number of 10 items.

Relevance threshold	Relevance Threshold specifies the level of confidence that Insight Surveillance must have in the accuracy of its prediction before it marks the item as Unreviewed Relevant. Depending on the relevance threshold value, Insight Surveillance determines whether the item is relevant or irrelevant for review and accordingly marks the item as *Unreviewed relevant* or *Unreviewed irrelevant*. On a scale of 0 to 100, the default threshold value is 40, with a recommended range of 20 to 80. Though it is recommended to set the relevance threshold value between 20 and 80, depending on the requirement, it can still be set to a lower or higher value by adjusting the slider as shown in the sample image below.  An item with a relevance score greater than or equal to the set relevance threshold is classified as *Relevant*, or otherwise *Irrelevant*.
Clear learning	Discards all the accumulated learning behavior for this department.
Last learning cleared on	Specifies the date when the accumulated learning behavior for this department was discarded.

7 In the **Monitoring policies** section, specify the sampling percentages for the configured and enabled content sources as shown in the sample image below.



The administrator or compliance supervisor can -

- View the content sources that are configured and enabled for customers. The list of content sources updates when new content sources are configured and enabled for the customer. For detailed list of supported content sources, See "Sampling support for content sources" on page 17.

  Note: If the content source is no longer required, it is recommended to disable it, as valuable data may be retained for potential future use. The list of content sources does not update when a content source is disabled.

- Set the monitoring policy at the department, child department, and the user level.
- Create a monitoring policy by setting sampling percentages for the items from these content sources, with the option to specify different percentages for each individual service.

Perform the following actions:

Disable monitoring of employees

This option controls if the employees of the department will be eligible for random sampling.

Do not select this check box if you want to allow employee monitoring in this department.

Select this check box to disable monitoring of employees in the department. If you select this option, you disable all the other options on this tab. However, the reviewers and department administrator can still access the department. Employees who are also monitored in other departments continue to be monitored in those departments.

Review requirement for

- Select **All policies** and specify the percentage of items to set the same monitoring policy for all the configured and enabled content sources (message types). For example, if you set the sampling percentage value as 5%, then 5% items of all these services will be captured and provided for review.

  Note: When new message types are added to the list, the existing monitoring policy automatically apply to them.

- Select **Per policy** and specify the percentage of items to set different percentages for each individual content source (message type). For example, if you set the sampling percentage for one service as 5%, you can set different sampling percentage values for other services.

  Note: When new message types are added to the list, the default sampling percentage for these types will be set to 2%.

For some message types, such as Exchange and Domino, you can also set percentages on the items that travel in a particular direction. Refer to the above-mentioned image.

- **Internal**. Selects the items where the author and all recipients are internal to your organization.
- **Inbound**. Selects the items where the author is external to your organization and at least one recipient is internal.
- **Outbound**. Selects the items where the author is internal to your organization and at least one recipient is external.

8 Click **Save**.

Moving existing departments under other departments

When you move a department to a different place in the department hierarchy, its child departments move with it. The monitored employees within the

department, exceptions reviewers, and supervisors also remain assigned to the department in its new position in the hierarchy.

Note: You must have the *Create Departments* permission to move departments. By default, users that have the *App User Admin* role have this permission.

To move a department under another department

1 In the left navigation pane, click **Departments**.

2 Search for and select the department you want to move.

Note: Insight Surveillance lists all departments. You can use the filtering options to search the required department. Options include filtering by department name, exception employees, and reviewers associated with the department.

---

3 Click **Edit Department**.

4 In the **Parent Department** field, search for and select the department to which you want to move the department.

5 Click **Save**.

Note: The reviewers and supervisors of the parent department automatically have access to the moved department.

Adding monitored employees and employee groups to departments

You can add monitored employees and employee groups to the Insight Surveillance departments in the following ways:

- While creating a department in Insight Surveillance (described below)
- While creating an archive account in the Arctera Insight Management Console Insight Surveillance administrators do not need to create employee profiles separately in Insight Surveillance. Instead, Insight Surveillance receives employee profiles from Arctera Insight Archiving. However, for this synchronization, the SQL Server and the Audit server must communicate with each other and the Auditing service should be enabled for the selected department.

Note: Insight Surveillance audits the activity of assigning monitored employees to departments and generates a log file for your reference.

An important activity in Insight Surveillance is to add employees and employee groups to the departments in which you want to monitor them. You can add new employee groups to Insight Surveillance from the Microsoft Azure Active Directory. See "Adding employee groups" on page 42.

Note: You must have the *Add Monitored Employees* and *Grant Users Access* permissions to add employees to a department. By default, users that have the *User Admin* role have these permissions.

For more information on searching for archive accounts, creating an archive account, deploying users and enabling their access to Insight Surveillance, and removing user access, see the Arctera Insight Management Console User Guide.

To add monitored employees to a department

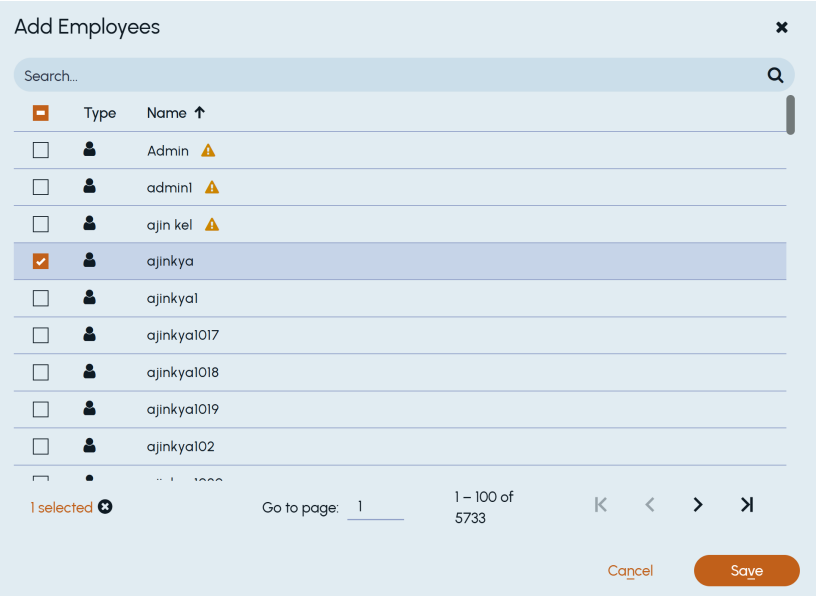
1 In the left navigation pane, click **Departments**.

2 Search for and select the department to which the monitored employees will be added.

Note: Insight Surveillance lists all departments. You can use the filtering options to search the required department. Options include filtering by department name, exception employees, and reviewers associated with the department.

3 In the **Monitored Employees** tab, click **Add Employees**.

The **Add Employees** dialog box appears and displays the available employees and employee groups.



4 Search for and select one or more employees and employee groups.

Note: Remember the following:

- Individual employees and employee group are distinguished using the different icons.

- If the selected employee and employee group are already monitored in other departments, an exclamation icon is displayed besides the names of those employees and employee groups. You can still add such employees to the department for monitoring purposes. The system displays a prompt listing the first ten departments and the number of the remaining departments in which the employee or employee groups being monitored.

To select multiple employees and employee groups from multiple pages, select the corresponding check boxes. Click the navigation arrows to go to the next or the previous pages.

5 Click **Save**.

Editing monitoring policies

You can define the percentage of items that Insight Surveillance should capture for a monitored employee. You must have the *Assign % Review Requirement* permission to edit the monitoring policy for an employee. By default, users that have the *Rule Admin* role have this permission.

By default, employee level sampling is enabled. So, you can only edit the monitoring policies at employee level. If you want to edit monitoring policies at department level, please contact Arctera Technical Support.

Note: When the department level sampling is enabled, the option to edit monitoring policies is disabled. In this case, Insight Surveillance honors the monitoring percentage of the department mentioned on the **Department** tab for sampling and not the employees monitoring percentage mentioned on the **Monitored Employee** tab.

To edit monitoring policies at employee level

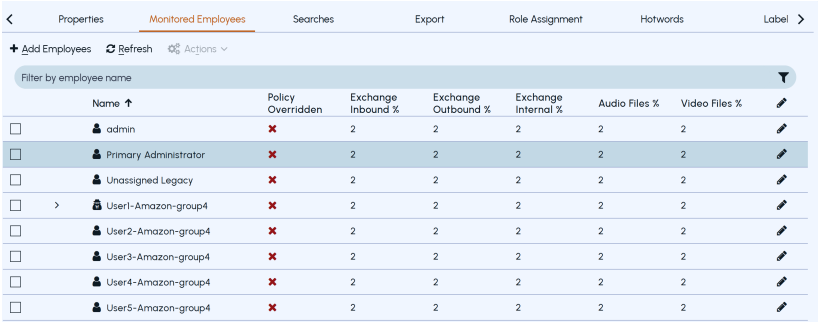
1. In the left navigation pane, click **Departments**.
2. Search for and select the department you want to edit.

   Note: Insight Surveillance lists all departments. You can use the filtering options to search the required department. Options include filtering by department name, exception employees, and reviewers associated with the department.

   ---

3 Click the **Monitored Employees** tab.

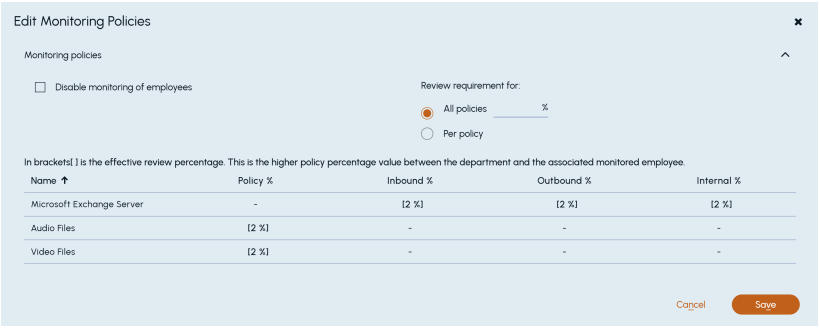
A list appears, showing all monitored employees along with their configured and enabled content sources. as shown in the sample image below.



To search for employees by name, in the **Filter by Employee Name** field, enter keywords that characterize employee names or construct a query. Press ENTER or click the filter icon to view the filtered names. Avoid using wildcard characters (asterisk or question mark) for partial searching, as they do not yield results.

If the employee level sampling is enabled, the option to edit monitoring policies is enabled.

4 Click the *Edit Monitoring Policies* icon for the employee whose monitoring policies you want to edit.



5 Under **Review requirement for**, select one of the following option:

- Select **All policies** and specify the percentage of items to set the same monitoring policy for all the configured and enabled content sources (message types). For example, if you set the sampling percentage value

as 5%, then 5% items of all these services will be captured and provided for review.

Note: When new message types are added to the list, the existing monitoring policy automatically apply to them.

- Select **Per policy** and specify the percentage of items to set different percentages for each individual content sources (message type). For example, if you set the sampling percentage for one service as 5%, you can set different sampling percentage values for other services.

Note: When new message types are added to the list, the default sampling percentage for these types will be set to 2%.

For some types of items, such as Exchange and Domino, you can also set percentages on the items that travel in a particular direction:

- **Internal**. Selects the items where the author and all recipients are internal to your organization.
- **Inbound**. Selects the items where the author is external to your organization and at least one recipient is internal.
- **Outbound**. Selects the items where the author is internal to your organization and at least one recipient is external.

6 Click **Save**.

Editing department details and monitoring policy

You can define the percentage of items that Insight Surveillance should capture for each employee and add to the review set at decided schedules. If you monitor items from different types of content sources, you can set a percentage for each type. For some types of items, such as Exchange and Domino, you can also set percentages on the items that travel in a specific direction (internal, external outbound, or external inbound).

Note: You must have the *Assign % Review Requirement* permission to edit the monitoring policy for an employee. By default, users that have the *Rule Admin* role have this permission.

To edit department details and the monitoring policy for employees

1 In the left navigation pane, click **Departments**.

2 Search for and select the department you want to edit.

Note: Insight Surveillance lists all departments. You can use the filtering options to search the required department. Options include filtering by department name, exception employees, and reviewers associated with the department.

---

3 In the **Properties** tab, click **Edit Department**.

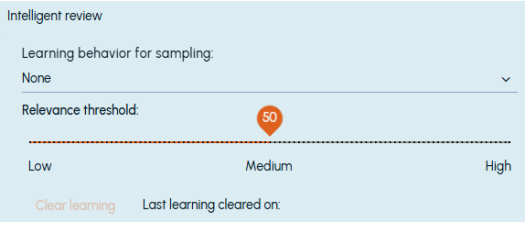
The **Edit Department** dialog box appears.

4 Refer to the following table and provide the relevant information in the respective fields.

Field	Description
Department	
Name	Type another unique name for the department, if required. The name can contain spaces, all the special and the text characters.
Status	Choose **Open** to make the department open for monitoring. Choose **Closed** to restrict monitoring of employees in the department. The department name does not appear on the start page of the application. However, employees who are also monitored in other departments continue to be monitored in those departments.
Owner	Select the name of the principal administrator for the department. Note: Each department has an owner, who must have a logon but does not need any special privileges assigned. By default, Insight Surveillance grants the permissions associated with the *Admin* role to department owners. These permissions are as follows: ■ Grant access to users ■ Add monitored employees ■ Configure department properties ■ View reports
Parent department	If the department itself is a parent department, do not select any previous department in this field. If you want to create this department under any existing department, click the search icon to select the parent department.

Field	Description
Options	
Can contain departments	Click the slider switch to turn it ON to allow creating nested departments under this department. Click the slider switch to turn it OFF to restrict creating nested departments under this department.
Can contain monitored employees	Click the slider switch to turn it ON to allow adding monitored employees to this department. Click the slider switch to turn it OFF to restrict adding monitored employees to this department. Note: You may want to clear this option in cases where you need to set up a department hierarchy, where the top-level department do not contain any monitored employees, but the nested departments do.
Search details	
Default percentage sample for new searches	Specifies the minimum percentage of the items that a search returns to add to the review set. When you create a search, you can qualify this option further by specifying the minimum number of items that are required per employee.
Lock	Click the slider switch to turn it OFF to allow department administrators to change the sample rate for new searches. Click the slider switch to turn it ON to restrict department administrators from changing the sample rate for new searches.
Intelligent review	

Field	Description
Learning behavior for sampling	The options that are available depend on whether you use guaranteed sampling, which is the default sampling mode, or statistical sampling. **None** Insight Surveillance samples items in the normal way, without implementing Intelligent Review. **Sample exact percentage and prioritize** Sample exact percentage and prioritize (guaranteed sampling). Insight Surveillance samples both relevant items and irrelevant items without favoring one over the other. So, if your monitoring policy requires that you capture and review 10% of items, Insight Surveillance captures 10% - but a substantial number of the items may be irrelevant. With this option, however, Insight Surveillance does give the items a status of either Unreviewed (Irrelevant) or Unreviewed (Relevant) as it adds them to the review set. When you later review the items in the Review pane, you can filter them by their Unreviewed status to distinguish between the relevant and irrelevant items. **Sample exact percentage of relevant content in addition to current sample** Sample exact percentage of relevant content in addition to current sample (guaranteed sampling only). Insight Surveillance adds both relevant items and irrelevant items to the review set until it has captured the required percentage of relevant items. With this option, therefore, Insight Surveillance may capture more items for review than your monitoring policy demands. For example, suppose that your policy requires you to review 10% of items. To achieve the required number of items, you may need to capture 20% of items, only half of which are relevant.

Field	Description
	Sample exact percentage of available relevant content Sample exact percentage of available relevant content (guaranteed sampling). Insight Surveillance discards all content that it considers irrelevant and samples relevant content only, until it has captured the required percentage. So, if your monitoring policy requires that you capture and review 10% of items, Insight Surveillance captures precisely 10%. In the case of guaranteed sampling only, if there are too few relevant items to fulfil the monitoring policy then Insight Surveillance supplements them with irrelevant items. For example, suppose that 100 items are available for sampling, and your monitoring policy requires you to capture 10% of them. If only seven items are relevant, Insight Surveillance adds three irrelevant items to achieve the required number of 10 items.
Relevance threshold	Relevance Threshold specifies the level of confidence that Insight Surveillance must have in the accuracy of its prediction before it marks the item as Unreviewed Relevant. Depending on the relevance threshold value, Insight Surveillance determines whether the item is relevant or irrelevant for review and accordingly marks the item as *Unreviewed relevant* or *Unreviewed irrelevant*. On a scale of 0 to 100, the default threshold value is 40, with a recommended range of 20 to 80. Though it is recommended to set the relevance threshold value between 20 and 80, depending on the requirement, it can still be set to a lower or higher value by adjusting the slider as shown in the sample image below.  An item with a relevance score greater than or equal to the set relevance threshold is classified as *Relevant*, or otherwise *Irrelevant*.
Clear learning	Discards all the accumulated learning behavior for this department.
Last learning cleared on	Specifies the date when the accumulated learning behavior for this department was discarded.

Field	Description
Monitoring policies	
For details, See "Editing monitoring policies" on page 65.	
Disable monitoring of employees	This option controls if the employees of the department will be eligible for random sampling. Do not select this check box if you want to allow employee monitoring in this department. Select this check box to disable monitoring of employees in the department. If you select this option, you disable all the other options on this tab. However, the reviewers and department administrator can still access the department. Employees who are also monitored in other departments continue to be monitored in those departments.
Review requirement for	■ Select **All policies** and specify the percentage of items to set the same monitoring policy for all the configured and enabled content sources (message types). For example, if you set the sampling percentage value as 5%, then 5% items of all these services will be captured and provided for review. Note: When new message types are added to the list, the existing monitoring policy automatically apply to them. ■ Select **Per policy** and specify the percentage of items to set different percentages for each individual content source (message type). For example, if you set the sampling percentage for one service as 5%, you can set different sampling percentage values for other services. Note: When new message types are added to the list, the default sampling percentage for these types will be set to 2%. For some message types, such as Exchange and Domino, you can also set percentages on the items that travel in a particular direction. Refer to the above-mentioned image. ■ **Internal**. Selects the items where the author and all recipients are internal to your organization. ■ **Inbound**. Selects the items where the author is external to your organization and at least one recipient is internal. ■ **Outbound**. Selects the items where the author is internal to your organization and at least one recipient is external.

5 Click **Save**.

Managing exception employees

The messages of certain employees such as senior managers and executives can be kept separate and reviewed by specially-assigned reviewers. Any employees falling into this category are called exception employees in Insight Surveillance.

Note: You must have *Manage Exceptions* permission in the department to make an employee an exception. By default, users with the role of *Compliance Supervisor*, *Rule Admin*, or *User Admin* have this permission.

Exception Reviewer

This role allows you to search the items of exception employees to whom you are assigned. You can also monitor, review, hold review, question, escalate, appraise, and comment on the items, export them, and generate and view reports. This role also lets you create searches within the department and manage department hotwords. You can also configure the monitoring policy that is assigned to employees and generate and view reports. In addition, you can assign exception reviewers to specific employees.

Designating employees as exception employee

You must have *Manage Exceptions* permission in the department to make an employee as an exception. By default, users that have the *Compliance Supervisor*, *Rule Admin*, or *User Admin* roles have this permission.

To designate employees as exception employee

1. In the left navigation pane, click **Departments**.
2. Search for and select the department in which you want to designate employees as exceptions.

Note: Insight Surveillance lists all departments. You can use the filtering options to search the required department. Options include filtering by department name, exception employees, and reviewers associated with the department.

---

3 In the **Monitored Employees** tab, select an individual employee.

A list appears, showing all monitored employees along with their configured and enabled content sources.

To search for employees by name, in the **Filter by Employee Name** field, enter keywords that characterize employee names or construct a query. Press ENTER or click the filter icon to view the filtered names. Avoid using wildcard characters (asterisk or question mark) for partial searching, as they do not yield results.

4 Click the **Actions** button, and click **Make an exception**.

The **Add Exception Reviewer** dialog box appears.

5 Search for and select the employee who will be the reviewer of the exception employee, and then click **Save**.

Assigning further exception reviewers to an exception employee

The employee must be assigned an exception status, otherwise they cannot be assigned exception reviewers. You must have the *Manage Exceptions* permission in the department to assign exception reviewers. By default, users that have the *Compliance Supervisor*, *Rule Admin*, or *User Admin* roles have this permission.

To assign further exception reviewers to an exception employee

1 In the left navigation pane, click **Departments**.

2 Search for and select the department in which you want to designate employees as exceptions.

Note: Insight Surveillance lists all departments. You can use the filtering options to search the required department. Options include filtering by department name, exception employees, and reviewers associated with the department.

---

3 In the **Monitored Employees** tab, select an individual employee.

A list appears, showing all monitored employees along with their configured and enabled content sources.

To search for employees by name, in the **Filter by Employee Name** field, enter keywords that characterize employee names or construct a query. Press ENTER or click the filter icon to view the filtered names. Avoid using wildcard characters (asterisk or question mark) for partial searching, as they do not yield results.

4 Click the **Actions** button, and click **Add exception reviewers**.

The **Add Exception Reviewer** dialog box appears.

5 Search for and select the employee who will be the reviewer of the exception employee, and then click **Save**.

6 To view recently added exception reviewers, click **Expand** icon adjacent to the reviewer name.

The application displays a list of all exception reviewers.

Removing exception status

The employee must already be assigned an exception status before the ability to remove the exception status is available.

When there is no need to monitor employees as exceptions, you can remove their exception status. After removing the exception status, the employees become regular monitored employees in their departments, and Insight Surveillance captures their communications in the normal way. However, any items that Insight Surveillance has captured while the employees had exception status remain in the exception review set.

You must have the *Manage Exceptions* permission in the department to remove exception status. By default, users that have the *Compliance Supervisor*, *Rule Admin*, or *User Admin* roles have this permission.

To remove exception status

1 In the left navigation pane, click **Departments**.

2 Search for and select the department.

Note: Insight Surveillance lists all departments. You can use the filtering options to search the required department. Options include filtering by department name, exception employees, and reviewers associated with the department.

---

3 In the **Monitored Employees** tab, select only one exception employee at a time.

A list appears, showing all monitored employees along with their configured and enabled content sources.

To search for employees by name, in the **Filter by Employee Name** field, enter keywords that characterize employee names or construct a query. Press ENTER or click the filter icon to view the filtered names. Avoid using wildcard characters (asterisk or question mark) for partial searching, as they do not yield results.

4 Click the **Actions** button, and then click **Remove the exception status**.

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

5 Click **Remove**.

Removing exception reviewers

You can remove the role of exception reviewer from employees when they do not need to perform the role anymore. Note that if an exception has one reviewer only, you cannot remove the reviewer while the exception is still active. Remove the exception status from the employee before you remove the reviewer.

Note: You must have the *Manage Exceptions* permission in the department to remove exception reviewers. By default, users that have the *Compliance Supervisor*, *Rule Admin*, or *User Admin* roles have this permission.

To remove an exception reviewer

1 In the left navigation pane, click **Departments**.

2 Search for and select the department.

Note: Insight Surveillance lists all departments. You can use the filtering options to search the required department. Options include filtering by department name, exception employees, and reviewers associated with the department.

---

3 In the **Monitored Employees** tab, select only one exception employee at a time.

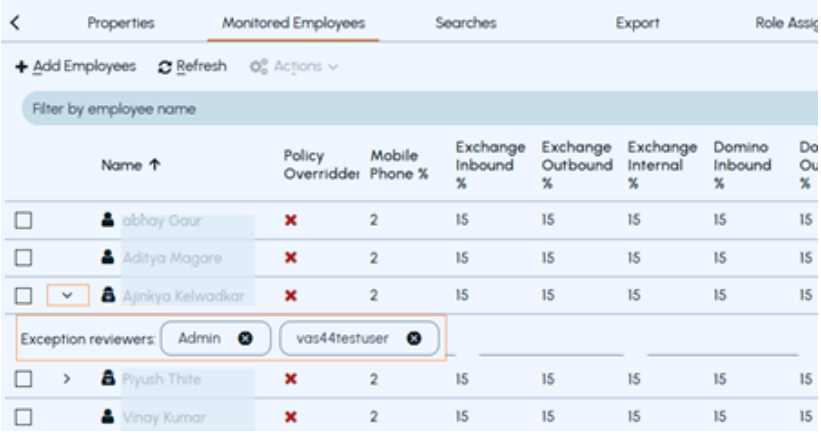
A list appears, showing all monitored employees along with their configured and enabled content sources.

To search for employees by name, in the **Filter by Employee Name** field, enter keywords that characterize employee names or construct a query. Press ENTER or click the filter icon to view the filtered names. Avoid using wildcard characters (asterisk or question mark) for partial searching, as they do not yield results.

4 Select only exception employees to which additional exception reviewers are assigned.

5 To view the associated exception reviewers, click **Expand** icon adjacent to the reviewer name.

The application displays a list of all exception reviewers.



6 Click the **X** (Remove) icon to remove the associated exception reviewers.

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

7 Click **Remove**.

Chapter 6

Managing department users

This chapter includes the following topics:

Assigning users to departments

Insight Surveillance makes it easy to add users (employees and employee groups) to departments and assign several key roles to them. Department reviewers can monitor, review, hold review, question, escalate, appraise, and comment on the items in a department, export items for offline review, and generate and view reports. Compliance supervisors can appraise the work of department reviewers and manage any exception employees in the department.

You must have the *Manage Roles* permission to add users to a department. By default, users that have the *Department Admin* role have these permissions.

To assign a user to a department

1 In the left navigation pane, click **Departments**.

2 Search for and select the department to which you want to add department reviewers and compliance supervisor.

Note: Insight Surveillance lists all departments. You can use the filtering options to search the required department. Options include filtering by department name, exception employees, and reviewers associated with the department.

---

3 In the **Role Assignment** tab, click **Add User**.

4 In the **Add Users** dialog box, search for and select one or more users (employees and employee groups).

Note: - Individual employees and employee group are distinguished using the different icons as shown in the sample image above.

- To select multiple adjacent users, hold down the Shift key and click the first and the last name in the range.

- To select multiple, non-adjacent users, hold down the Ctrl key and click the required names.

---

5 Click **Save**.

The added users are displayed under **User and Groups**.

6 Under **User and Groups**, select one user at a time, and click **Add Roles**.

The **Add Roles** dialog box appears.

7 Search for and select one or multiple roles.

8 To add a user as a department reviewer, assign the *Department Reviewer* role. To add a user as a compliance supervisor , assign the *Compliance Supervisor* role.

Note: To select multiple adjacent roles, hold down the Shift key and click the first and the last name in the range. To select multiple, non-adjacent roles, hold down the Ctrl key and click the required names.

---

9 Click **Save**.

Removing users from departments

You must have the *Manage Roles* permissions to remove users from a department. By default, users that have the *Department Admin* role have these permissions. Ensure that you are selecting the correct user you want to remove. When there is no need for a department user (reviewer), you can remove them.

To remove a user from department

1 In the left navigation pane, click **Departments**.

2 Search for and select the department from which you want to remove reviewers.

Note: Insight Surveillance lists all departments. You can use the filtering options to search the required department. Options include filtering by department name, exception employees, and reviewers associated with the department.

---

3 In the **Role Assignment** tab, under the **Users and Groups** pane, select only one user at a time.

4 Click **Remove User**.

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.

Adding new roles for users

To add a new role for a department user

1 In the left navigation pane, click **Departments**.

2 Search for and select the department for which users you want to assign new roles.

Note: Insight Surveillance lists all departments. You can use the filtering options to search the required department. Options include filtering by department name, exception employees, and reviewers associated with the department.

---

3 In the **Role Assignment** tab, under the **Users and Groups** pane, select only one user at a time.

4 Click **Add Roles**.

The **Add Roles** dialog box appears.

5 Search for and select one or multiple roles.

Note: To select multiple adjacent roles, hold down the Shift key and click the first and the last name in the range. To select multiple, non-adjacent roles, hold down the Ctrl key and click the required names.

---

6 Click **Save**.

Removing roles

To remove a role of a department user

1 In the left navigation pane, click **Departments**.

2 Search for and select the department from which you want to remove the roles of a department user.

Note: Insight Surveillance lists all departments. You can use the filtering options to search the required department. Options include filtering by department name, exception employees, and reviewers associated with the department.

---

3 In the **Role Assignment** tab, under the **Users and Groups** pane, select only one user at a time.

4 Under **Assigned Roles**, select one or multiple roles you want to remove, and click **Remove Roles.**

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

Note: Any user who is a department owner must have the *User Admin* role. There must be at least one exception reviewer for an exception department.

---

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

Managing role assignment for a user in departments

While you can add users to a department and assign several key roles to them using the **Department** > **Role Assignments** tab, you can also assign a specific role to users in one or more departments and exceptions using the **Department** > **Users** > **Assign** option. See "Assigning departments and exceptions to specific users" on page 82.

You can also remove a specific role to users in one or more departments and exceptions using the **Department** > **Users** > **Remove** option. See "Removing a specific role to users in one or more departments and exceptions" on page 84.

Assigning departments and exceptions to specific users

In addition to viewing the user summary, you can also perform the following actions using the **Department** > **Users** > **Assign** option:

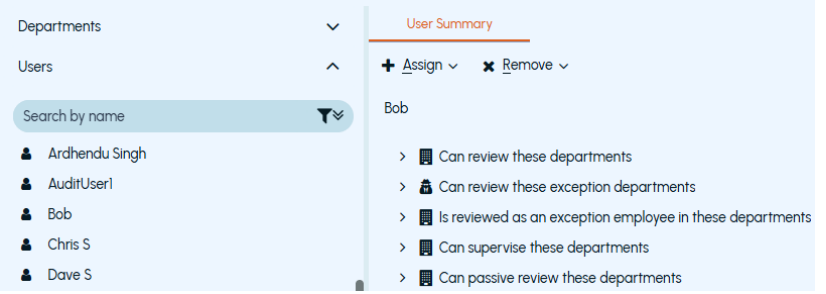
- Assign departments to a user for a review
  Associate departments to a user so that the user can review those departments.
- Assign exception employees to a user for review
  Associate exception employees to a user so that the user can review the items of the exception employees.
- Assign departments to a user for supervision
  Associate departments to a user so that the user can supervise these departments.
- Assign departments to a user for a passive review
  Make the user a *Passive Reviewer* for the selected departments so that the user can view items and review history, and then assign appraisal status.

Note: You must have the *Grant Users Access* permissions to perform these user actions. By default, users that have the *User Admin* role have these permissions.

To assign a department to a user for review:

1. In the left navigation pane, click **Departments**.
2. Expand **Users** in the filter pane.

3 Search for and select the user you want to assign to a department to a review.



4 Click the **Assign** button, and then click **Departments To Review**.

The **Select one or more departments to review** dialog box appears.

5 Search for and select the departments that you want to assign for review.

Note: A maximum of 100 departments are displayed and can be selected. If you have more than 100 results, repeat these steps for every 100 departments.

---

6 Click **OK**.

The **User Summary** page gets refreshed, and the associated departments are displayed for the user.

You can also go to the **Role Assignment** tab and check the users to whom the department has been assigned for review.

To assign exceptions to a user for review:

1 In the left navigation pane, click **Departments**.

2 Expand **Users** in the filter pane.

3 Search for and select the user you want to assign to an exception to a review.

Note: A maximum of 100 exceptions are displayed and can be selected. If you have more than 100 results, repeat these steps for every 100 exceptions.

---

4 Click the **Assign** button, and then click **Exceptions To Review**.

The **Select one or more exceptions to review** dialog box appears.

5 Search for and select the exceptions that you want to assign to review.

6 Click **OK**.

The **User Summary** page gets refreshed, and the associated exceptions are displayed for the user.

To assign departments to a user for supervision:

1 In the left navigation pane, click **Departments**.

2 Expand **Users** in the filter pane.

3 Search for and select the user you want to assign to a department to supervise.

4 Click the **Assign** button, and then click **Departments To Supervise**.

The **Select one or more departments to supervise** dialog box appears.

5 Search for and select the departments that you want to assign to supervise.

6 Click **OK**.

The **User Summary** page gets refreshed, and the associated departments are displayed for the user's supervision.

To assign departments to a user for a passive review:

1 In the left navigation pane, click **Departments**.

2 Expand **Users** in the filter pane.

3 Search for and select the user you want to assign to a department to a passive review.

4 Click the **Assign** button, and then click **Departments To Passive Review**.

The **Select one or more departments to passive review** dialog box appears.

5 Search for and select the departments that you want to assign to passive review.

6 Click **OK**.

The **User Summary** page gets refreshed, and the associated departments are displayed for the user's passive review.

Removing a specific role to users in one or more departments and exceptions

You can perform the following actions using the **Department** > **Users** > **Remove** option:

- Remove the *Department Reviewer* role for one or more departments

Dissociate departments to a user so that the user cannot review those departments.

- Remove the *Exception Reviewer* role for one or more exceptions
  Dissociate exception employees to a user so that the user cannot review the items of the exception employees.
- Remove the *Compliance Supervisor* role for one or more departments
  Dissociate departments to a user so that the user cannot supervise these departments.
- Remove the *Passive Reviewer* role for one or more departments
  Remove the *Passive Reviewer* role of a user for the selected departments so that the user cannot view items and review history, and or assign appraisal status.

Note: You must have the *Grant Users Access* permissions to perform these user actions. By default, users that have the *User Admin* role have these permissions.

To remove an *Exception Reviewer* role in an exception department, you should either have *Grant User Access* permission in the exception department or you should have *Mange Exception* permission in the parent department of the exception department.

You can perform the above-listed actions using the cross button displayed in front of the department and user names on the **User Summary** page. The cross button is not be displayed for departments where the selected user is an exception employee.

To remove the department reviewer role for one or more departments:

1. In the left navigation pane, click **Departments**.
2. Expand **Users** in the filter pane.

3 Search for and select the user you want to dissociate to the department to restrict a review.

4 Click the **Remove** button, and then click **Departments To Review**.

The **Select one or more departments to remove the department reviewer role** dialog box appears.

5 Search for and select the departments that you want to remove.

Note: A maximum of 100 departments are displayed and can be selected. If you have more than 100 results, repeat these steps for every 100 departments.

---

6 Click **OK**.

The **User Summary** page gets refreshed, and the removed departments are not displayed for the user.

To remove the exception reviewer role for one or more exceptions:

1 In the left navigation pane, click **Departments**.

2 Expand **Users** in the filter pane.

3 Search for and select the user you want to dissociate exception employees so that the user cannot review the items of the exception employees.

Note: A maximum of 100 exceptions are displayed and can be selected. If you have more than 100 results, repeat these steps for every 100 exceptions.

You cannot remove the last active exception reviewer for an exception. An active exception must have at least one exception reviewer.

4 Click the **Remove** button, and then click **Exceptions To Review**.

The **Select one or more departments to remove the exception reviewer role** dialog box appears.

5 Search for and select the exceptions that you want to remove to review.

6 Click **OK**.

The **User Summary** page gets refreshed, and the removed exceptions are not displayed for the user.

To remove the compliance supervisor role for one or more departments:

1 In the left navigation pane, click **Departments**.

2 Expand **Users** in the filter pane.

3 Search for and select the user you want to dissociate departments so that the user cannot supervise these departments..

4 Click the **Remove** button, and then click **Departments To Supervise**.

The **Select one or more departments to remove the compliance supervisor role** dialog box appears.

5 Search for and select the departments that you want to remove.

6 Click **OK**.

The **User Summary** page gets refreshed, and the associated departments are removed from the user's supervision.

To remove the passive reviewer role for one or more departments:

1 In the left navigation pane, click **Departments**.

2 Expand **Users** in the filter pane.

3 Search for and select the user you want to remove the *Passive Reviewer* role for the selected departments so that the user cannot view items and review history, and or assign appraisal status.

4 Click the **Remove** button, and then click **Departments To Passive Review**.

The **Select one or more departments to remove the passive reviewer role** dialog box appears.

5 Search for and select the departments that you want to remove for a passive review.

6 Click **OK**.

The **User Summary** page gets refreshed, and the associated departments are removed from the user's passive review.

Chapter 7

Managing department-level searches

This chapter includes the following topics:

About department-level searches

In Insight Surveillance, you can create department-level searches. These searches can run only in a single department. You can search for the items (emails and collaboration messages) that meet certain criteria and later review these items. The search operations are based on terms like subject, tags, content, sender, recipient, dates, communication direction, and so on. If the search results are not suitable, you can reject the result and create a new search until you get the

necessary information. If the search results are suitable, you can accept the search and review the items.

You can create search schedules if you want to run searches at set times or set up the recurrent searches that run automatically. You can stop and pause the searches that are still in progress, and resubmit the failed searches.

If you want to search for instances of certain words in the communication items, you can create a set of hotwords. When defining the search criteria, you can select these hotwords and hotword sets. Insight Surveillance searches for the selected hotwords in subject and content of searched items.

Sampling of communication items is performed once on the last 24-hours data. If the sampling is aborted, it is performed on the data that was generated since the last successful completion of a sampling.

Note: Collaboration searches does not support external employees.

Guidelines for effective searches

To increase the chances of retrieving the most relevant results when conducting searches, follow these guidelines:

- Make searches precise. For example, include the author or recipient details, or specify date ranges.
- Avoid the overuse of wildcards.
- Avoid the overuse of search terms. The inclusion of several search terms together can cause iterative searches, which may slow down performance and return overlapping results.
- Quickly accept or reject searches, as completed searches that have not been accepted or rejected may affect overall search performance.
- Use one or more hotword sets in scheduled searches to allow the hotwords used to be changed as needed. It is recommended to configure a hotword set that is used by the scheduled search so that the hotwords in the hotword set can be changed as needed, and the next instance of the search will use the changes in the hotword set.

Creating and running department-level searches

To run a one-time search, create an immediate search. To run a recurring search or one that runs on a specific time, create a search schedule and then create a scheduled search.

Note: You must have the *Manage GSS and Scheduled searches* and *Search Capture* permissions to create or edit searches. By default, users that have the *Rule Admin*, the *User Admin*, and the *Exception Reviewer* roles have this permission.

To create and run a department-level search

1 In the left navigation pane, click **Departments**.

2 Search for and select the department for which you want to create and run a search.

Note: Insight Surveillance lists all departments. You can use the filtering options to search the required department. Options include filtering by department name, exception employees, and reviewers associated with the department.

---

3 In the **Searches** tab, click **New Search**.

The **New Search** dialog box appears.

4 In the **Search Type** section, specify the relevant information in the following fields.

This section identifies the search and specifies when it runs.

Search In	Displays the name of the department.
Search Type	Choose **Immediate** to create one-time search that runs immediately. Choose **Scheduled** to specify a period during which the search is to run. Choose **Guaranteed Sample** to run a search at the selected sampling time by default. If the search returns fewer results than your monitoring policy requires, Insight Surveillance adds randomly-sampled items to the review set to make up the shortfall. This feature allows you to assemble more focused review sets that are weighted towards search-specific results instead of purely randomly-sampled items.
Enabled	Select the check box to enable scheduled searches and guaranteed sample searches. When a search is not enabled, it does not run.
Name	Type a name for the search.
Automatically accept search results	Select this check box to specify whether to add the search results to the review set automatically. This option is useful for verified searches that you intend to run on a regular basis. This option is enabled only if the **Accept searches** permission is assigned to the user who is creating the search. If you select this check box, you cannot reject the results and change the search criteria. Insight Surveillance recommends that you clear **Automatically accept search results** until you have tested that the search returns the expected results. A search that returns an error from any archive is not automatically accepted, regardless of this setting.
Include items already in review	Select this check box to specify whether the search results can include the items you previously captured and added to this department's review set. This option does not apply to the items you previously included in the review sets for other departments. For an immediate search or scheduled search, you can select this box to ensure that the results include the items that may already be in review from other searches.

5 In the **Sampling** section, specify the relevant information in the following fields.

This section lets you sample the search results and add a random selection of items to the review set. Insight Surveillance does not deduplicate randomly-sampled items.

Sampling percentage	Specify the percentage of search results to include in the review set. You can specify fractions, as in 10.25. You cannot change the sampling percentage if the owner of the department has locked this setting in the department properties.
Set minimum items per author	Specify the minimum number of items per author to include in the review set. If there are no items for an author in the search results, none can be included in the sample. Note: As the authors can be from outside the selected department, searches may return more results.
Set absolute item limit	Specify an upper limit on the total number of search results to add to the review set. This option takes precedence over any values that you set in the **Sampling percentage** field.

6 In the **Date range** section, specify the relevant information in the following fields.

This section lets you search for items according to when they were sent or received.

Specific date range	Specify the date and time duration to search items that were sent or received during the selected period.
Today / Yesterday / Last 7 days / Last 14 days / Last 28 days	The date ranges are relative to when the search runs, which is today in the case of an immediate search. You may find these options useful when creating a scheduled, recurrent search that runs once every day, week, two weeks, or four weeks. For example, if the search runs once a week, select **Last 7 days** to limit the range to the days since the search last ran.
Since search last ran	For a scheduled search only, lets you search the new items that have arrived since the last time you ran the search. This option is similar to options such as Today and Yesterday. However, it lets you set an explicit start date for the first run of the search. By default, this option searches from the date of the last run (or the start date for the first search) to the current day minus 1 (that is, up to yesterday).

7 In the **Authors and recipients** section, specify the relevant information in the following fields.

This section targets the departments for the search and the direction of the items to search. Any departments that you have organized into partitions can only search items to and from departments in the same partition.

Message Route

Specify the departments you wish to search as well as the direction of the items you wish to search. Search for the items that are **to** or **from** the selected departments, and for the items that have traveled **between** the selected departments and other departments.

You can search for the items that follow the following message route:

- **Between "the specified department" and**
  - other searchable departments
  - any department within the organization
  - department outside the organization
  - department internal AND/OR External to organization
- **TO "the specified department" from**
  - other searchable departments
  - any department within the organization
  - department outside the organization
  - department internal AND/OR External to organization
- **FROM "the specified department" to**
  - other searchable departments
  - any department within the organization
  - department outside the organization
  - department internal AND/OR External to organization

Any of / All of

To search within department tags, select a department. To search within the **To**/**From** fields, only select the employees.

You can expand the department tag to select monitored employees. If there are a large number of employees in the department, you can click the search icon in front of the department tag, which opens a new window where you can search and select monitored employees.

This field does not show the Employee Group names assigned to the departments. Instead, it displays the list of all the members from the employee groups individually.

Freeform email addresses / domains	This field is available for all possible message routes. Type one or more email addresses and domains. Type each address or domain on a line of its own to search for the items where the **From**, **To**, **CC**, or **BCC** fields contains any of the addresses or domains. Type all the addresses and domains on a single line to search for items in which they are all present. Place the minus sign (-) in front of an address or domain to exclude it from the search. To exclude multiple addresses or domains, type them all on a single line. You must exclude wildcard characters when entering email addresses or domains. Specify inputs without wildcard characters, such as ***user@domain.com***, ***arctera.io***, ***gmail.com***, etc. Note: You can use **Freeform email addresses / domains** to search for email addresses associated with the user accounts but now use the discontinued domain. To search for previously monitored employees, you should use **department internal AND/OR External to organization** message route, and then use the **Freeform email addresses / domains** option to provide email addresses or domains.
Department tree	Specify the departments and employees you want to include in the search. Click the arrows to the left of the department names to expand them and view the nested departments and exception employees. When you select a department, you do not automatically include any exception employees in the department. To search exception employees, you must select each one explicitly.

8 In the **Search terms** section, specify the relevant information in the following fields.

This section specifies the words or phrases for which Insight Surveillance should search in the subject lines of items and their bodies. By default, when you search for words in both the subject of an item and its content, Insight Surveillance finds those items that meet one or both criteria. However, it is possible to set up Insight Surveillance so that only those items that meet both criteria are found.

Subject

Type the keywords or phrases to be searched in subject lines of the review items. Press **Enter** to separate keywords and phrases from each other.

Alternatively, click **Hotwords** to select hotword sets and keywords.

If the department has a parent department, you can select hotwords/hotword sets from the current department and its parent department and global hotwords/hotword sets. Hotwords/hotword sets from any of the closed parent departments will not be available for selection. The application searches hotwords/hotword sets from both departments and its parent department and global hotwords/hotword sets.

Note:

- Use an asterisk (*) wildcard to represent zero or more characters in your search.
  For example, the search terms such as ***mismanag****, ***"paint* the tape"***, ***" can * switch to"***, and ***"ring * * blink"***, are supported and the search terms such as ***Inflati*n*** or ***Cra*h*** are supported.
- Use a question mark (?) wildcard to represent any single character. A wildcard search always finds items that match your search criteria and that were archived in Insight Surveillance.
  For example, the search terms such as ***saniti?ed***, ***"massive favo?r"***, and ***Indi?*** are supported.
- Use a minus sign (-) to indicate you want to exclude from the search results any items that contain the following word or phrase.
  For example, the search to find the items that contain the word 'Agent', but do not contain the word 'Cost':
  Agent AND -"Cost"
- A search term cannot comprise an excluded word or phrase only. When you specify such words or phrases, you must also specify a positive word or phrase you want to appear in the search results.
- A search term cannot start with any of the following characters on any line: = + - @. For example,
  "Agent AND -Cost" is a valid search term but "-Cost Agent" is not.
- Insight Surveillance does not allow any non-alphanumeric characters in the search term, except asterisk (*), apostrophe ('), question mark (?), and minus sign (-) as these characters have a special significance.

Content

Specify the keywords or phrases to be searched in the content of review items.

Alternatively, click **Hotwords** to select hotword sets and keywords.

Note:

- Use an asterisk (*) wildcard to represent zero or more characters in your search.
  For example, the search terms such as ***mismanag****, ***"paint* the tape"***, ***"can * switch to"***, and ***"ring * * blink"***, are supported and the search terms such as ***Inflati*n*** or ***Cra*h*** are supported.
- Use a question mark (?) wildcard to represent any single character. A wildcard search always finds items that match your search criteria and that were archived in Insight Surveillance.
  For example, the search terms such as ***saniti?ed***, ***"massive favo?r"***, and ***Indi?*** are supported.
- Use a minus sign (-) to indicate you want to exclude from the search results any items that contain the following word or phrase.
  For example, the search to find the items that contain the word 'Agent', but do not contain the word 'Cost':
  Agent AND -"Cost"
- A search term cannot comprise an excluded word or phrase only. When you specify such words or phrases, you must also specify a positive word or phrase you want to appear in the search results.
- A search term cannot start with any of the following characters on any line: = + - @. For example,
  "Agent AND -Cost" is a valid search term but "-Cost Agent" is not.
- Insight Surveillance does not allow any non-alphanumeric characters in the search term, except asterisk (*), apostrophe ('), question mark (?), and minus sign (-) as these characters have a special significance.

9 In the **Attachments** section, specify the relevant information in the following fields.

This section lets you search for items of a certain size and type or that have the specified retention category.

Number — Specify the required number of attachments.

You can search the items with specific number and type of attachments. The default option, **Does not matter**, means that the item can have zero or more attachments.

All following other options require you to type one or two values that specify the required number of attachments:

- **Equals**: requires a specific number of attachments.
- **Between**: requires the number of attachments messages must have to a value between those to be specified.
- **Less than**: requires a number of attachments below the number specified.
- **Greater than**: requires any number of attachments greater than the number specified.

File extensions — Specify the file name extensions of particular types of attachments for which to search. Separate the extensions with space characters.

For example, type the following to search for items with HTML or Microsoft Excel file attachments:.htm .xls.

10 In the **Miscellaneous** section, specify the relevant information in the following fields.

This section lets you search for items of a certain size and type or that have the specified retention category.

Message size — Specify the size in kilobytes of each item of configured and enabled content sources. The item size includes the size of attachments as well.

The following options are available:

- **Does not matter**: any number from 0 upward can be attached.
- **Equals**: requires a specific number of attachments.
- **Between**: requires the number of attachments messages must have to a value between those to be specified.
- **Less than**: requires a number of attachments below the number specified.
- **Greater than**: requires any number of attachments greater than the number specified.

Message type	Displays a list of configured and enabled content sources for the customer. See "Sampling support for content sources" on page 17. Select the **All content sources** check box to consider messages from all types of content sources simultaneously. When this option is selected, other options remain disabled. To select specific message type, clear the **All content sources** check box, and select one or more required options from the content sources available in the list.
Trash option	Select the appropriate option to search for items in trash: ■ **Ignore trash** - does not search for items in the trash. ■ **Include trash** - searches for items in other specified options along with the items in trash. ■ **Trash only** - only searches for items in trash.

11 In the **Tags** section, specify the relevant information in the following fields.

This section lets you search for items according to the tags with which any additional policy management software has classified them.

Filter	Select any of the following options to search for the items that match certain classification policies. There are several types of policies: ■ **Inclusions only**: Select this option to include items that your policy management software has classified for inclusion in the review set that may contain the most serious offenses, such as swearing, racism, or insider trading. ■ **Ignore inclusions**: Select this option to ignore items that Arctera Insight Classification has classified for inclusion in the review set that may contain the most serious offenses, such as swearing, racism, or insider trading. ■ **Exclusions only**: Select this option to include spam items and newsletters that your policy management software may classify for exclusion from the review set. ■ **Ignore exclusions**: Select this option to ignore spam items and newsletters that your policy management software may classify for exclusion from the review set. ■ **Categories only**: Select this option to include categorized items that exhibit certain characteristics, such as containing Spanish text. This type of policy provides no information on whether an item should be included in or excluded from the review set. ■ **Ignore inclusions and exclusions**: Select this option to ignore inclusion and exclusion items. ■ **Custom**: Select this option and type the names of one or more policies. Separate multiple tag names with commas, like this: CustomTag1,CustomTag2 ■ **All**: Select this option to include all tags. Note: Arctera Insight Classification is required to classify items based on their content and metadata. Implementing Arctera Insight Classification requires additional charges.
Name	Select tag names. Separate multiple tag names with commas, like this: CustomTag1,CustomTag2
Filter by current department	Select this check box to skip the unused policies in the current department.

12 In the **Intelligent Review** section, choose options for the learning engine in Insight Surveillance. This engine allows Insight Surveillance to search for items intelligently, based on the actions that reviewers have taken on earlier items.

For example, after a reviewer has marked a spam message or out-of-office reply as irrelevant then, when Insight Surveillance detects other items that have similar characteristics, it can handle them in the same way.

Note: Searches that use the intelligent review feature may take slightly longer to complete than those that do not use this feature.

Searches, by default, consider metadata and content of items to determine the relevance. However, if search results contain items that are older than 30 days, only metadata is considered to determine the relevance.

The options for **Learning behavior** are as follows:

None	Insight Surveillance searches for items in the normal way, without implementing Intelligent Review. This is the default option.
Search and prioritize	Insight Surveillance searches for both relevant items and irrelevant items without favoring one over the other. So, if your chosen **Sampling percentage value requires that you capture and review 10% of items**, Insight Surveillance captures 10% - but a substantial number of the items may be irrelevant. With this option, however, Insight Surveillance does give the items a status of either **Unreviewed (Irrelevant)** or **Unreviewed (Relevant)** as it adds them to the review set. When you later review the items in the **Review** pane, you can filter them by their **Unreviewed** status to distinguish between the relevant and irrelevant items.
Search and then sample ONLY relevant content	Insight Surveillance searches across all the items and captures the relevant ones only, until it has captured the required percentage. So, if your chosen **Sampling percentage value requires that you capture and review 10% of items**, Insight Surveillance captures 10% - all of them considered to be relevant. If there are too few relevant items to fulfil the chosen sampling percentage, Insight Surveillance does not supplement them with irrelevant items. This is an important difference between this option and the equivalent option, Sample exact percentage of ONLY relevant content, in the **Department Properties** pane.

13 Click **Save**.

Disabling scheduled searches

You cannot delete a search schedule if any scheduled search is linked to it. You need to disable scheduled searches so that you can delete their search schedules.

To disable scheduled searches

1. In the left navigation pane, click **Departments**.
2. Search for and select the department for which you want to disable the scheduled search.
3. Click the **Searches** tab. A list of searches appears.
4. Select the search you want to modify, and then click the **Edit Search** icon. The **Edit Search** dialog box appears.
5. In the **Search Type** section, change the **Search Schedule** to either another search schedule or **None**. If you have changed it to **None**, then clear the **Schedule run start date** and **Schedule run end date** fields.
6. Click **Save**.

Using proximity searches

Proximity search lets you find items (like emails or collaboration messages) where specific search words are within a defined distance from each other. You can use proximity operators to specify the distance between these search terms in your queries.

The following are some important points to remember when using proximity searches:

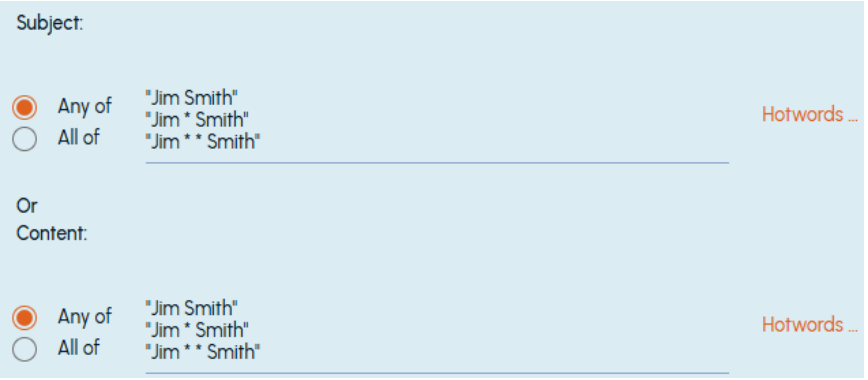
- **Word Limit**: Insight Surveillance restricts the proximity word count to a maximum of 49 words.
- **Stop Words**: Results may include stop words, but these are not counted in the proximity word count.

To understand proximity search, here are a few examples:

Asterisk (*):

This operator lets you specify a distance between the search terms.

To search for two words where the maximum distance between these words is only one word, use a single Asterisk. For example, “Jim*Smith” To search for two words where the maximum distance between these words is two words, use two Asterisk symbols. For example, “Jim * * Smith”.



This would return results for any email, document, or attachment containing variations of the name, such as "Jim Smith," "Jim Martin Smith," "Jim M. Smith" ("Jim * Smith"), or "Jim James Martin Smith" ("Jim * * Smith").

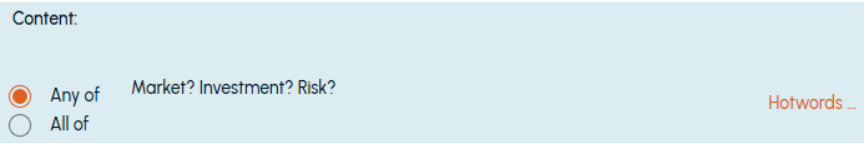
Diacritics:

This Unicode operator allows you to specify language-specific queries. For example, searching for “éléphant” retrieves only the French variant, so analyze your search criteria for non-English emails with special characters.

Question Mark:

This operator retrieves items with variations of a search term. It represents one or more characters, allowing you to search for singular or plural forms by placing a question mark at the end of the terms.

For example, if you're searching for the words “Market,” “Investment,” or “Risk” and want to include their plural forms in the results, you can use the syntax shown in the sample image below.



This would return results for any email, document, or attachment containing the words “Market,” “Markets,” “Investment,” “Investments,” “Risk,” or “Risks” in the body text (Market OR Markets OR Investment OR Investments OR Risk OR Risks).

Negation conditions:

This operator (minus sign) searches for items in which the first specified term appears outside the context that you have defined with the second term. It allows to extend the hotword length to a maximum of 2,000 characters.

Add the keyword AND before the first negation term, ensuring there is a space before and after AND. For example,

Search* AND -"search criteria", test* AND -"test crit?ria" -"te?st vas", "search criteria" AND -"search criteria Bloomberg"

Previewing search results

Insight Surveillance makes it easy for a reviewer to preview the search results before accepting or rejecting them and deciding if the search is based on their expectations and if it needs to modify search criteria. The **Search Preview** feature is available for the immediate or scheduled searches that are complete, but the search acceptance is pending.

Note: Insight Surveillance does not support previewing certain file types, such as ***.dll*** and **.exe** and large files (over 10MB to maintain browser responsiveness). For compressed files, Insight Surveillance supports previewing only the ***.zip*** file format and does not support other formats like ***.7z***, ***.tar***, and so on.

To preview the search results

1 In the left navigation pane, click **Department**.

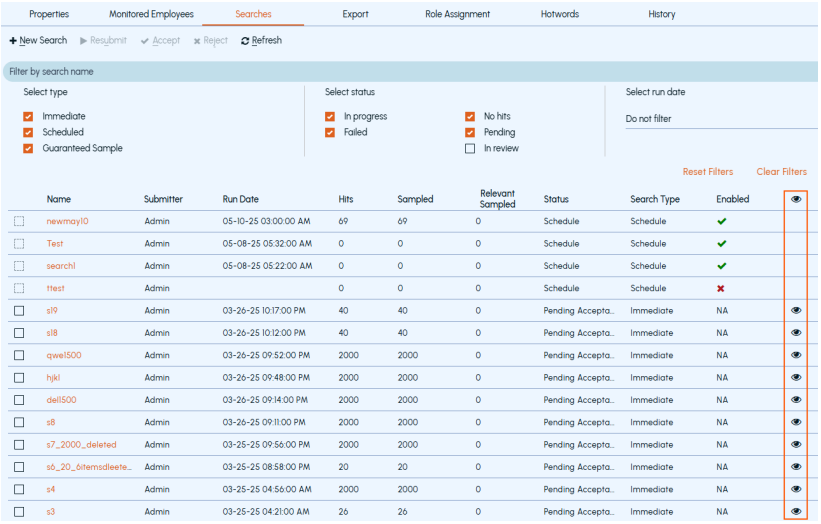
2 Search for and select the department to view the associated searches.

Note: Insight Surveillance lists all departments. You can use the filtering options to search for the required department. Options include filtering by department name, exception employees, and reviewers associated with the department.

---

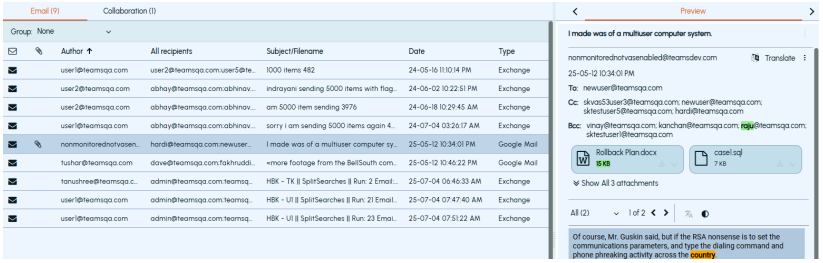
3 Click **Searches**. A list of search results is displayed.

Enter the desired value in the text field and click the **Search** icon to view the searched items , or the **Clear** icon to remove the value from the search field. To filter the searched items, click the **Filter** icon.



All the searches matching your filter criteria are displayed in a list form. A **Preview Search** icon is displayed for the searches whose acceptance is pending and for the scheduled searches as shown in the sample image above.

4 To preview the *immediate* and *scheduled* searches with the **Pending Acceptance** status, click the **Preview Search** icon. The search items are displayed in a new browser window.



5 To preview the *schedule* search, click the **Search Runs** (...) button for the desired scheduled search. To preview the desired scheduled search with the **Pending Acceptance** status, click the **Preview Search** icon. The search items are displayed in a new browser window.

Note: If only the **Exchange** service is enabled for you, the **Email** tab appears. If the **Exchange** and the **Microsoft Teams** services are enabled for you, the **Email** and the **Collaboration** tabs appear respectively.

When both the services are enabled, but the search does not find any email or collaboration message record, the corresponding tab is displayed without any items in it.

---

6 On the **Email** tab, perform the following actions:

Note: The selections made for the Group and sorting of items are persisted across all login sessions for the logged-in user.

- Group the search for the oldest or newest items based on a day or month.
- Preview an item and its attachments in the right-side **Preview** pane. You can double-click on the item to open it in a new browser window.
- Print the item or its attachment using the **Action** button on the **Preview** pane.
- Download the item in its native format or its attachment using the **Action** button on the **Preview** pane.

7 On the **Collaboration** tab, perform the following actions:

Note: You do not need to group the collaboration messages. The application groups the Teams Channel and Chat messages for your review. You can view record of maximum 100 groups per page and maximum 20 items per page within a group. Use the navigation bar options to go to previous and next pages.

- Expand the required Teams Channel and Chat message group to select items within the group.
- Preview an item and its attachments in the right-side **Preview** pane.

Accepting search results

Insight Surveillance does not add the captured items to the review set until you accept the search results. If you did not select **Automatically accept search results** in the search type section, you must manually accept the results.

The user must have the *Accept Searches* permission to accept immediate and scheduled searches. The guaranteed sample searches get accepted automatically.

To accept a search result

1 In the left navigation pane, click **Department**.

2 Search for and select the department to view associated searches.

Note: Insight Surveillance lists all departments. You can use the filtering options to search the required department. Options include filtering by department name, exception employees, and reviewers associated with the department.

---

3 Click **Searches**, and then filter and select a search name you want to accept.

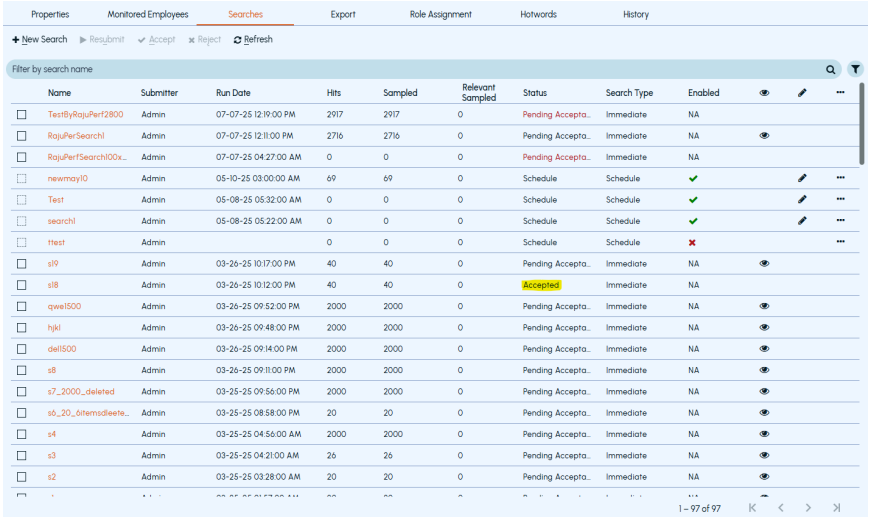
Note: To set a filter criterion to find a search, click the **Filter** icon. Select the required filter parameters, and then click **Apply Filters**.

---

4 Click **Accept**.

The application displays **Accepted** state in the **Status** column.

The **Status** column provides more details about the status depending on the user permissions.



Rejecting a search result

Note: An accepted search cannot be rejected.

To reject a search result

1 In the left navigation pane, click **Department**.

2 Search for and select the department to view associated searches.

Note: Insight Surveillance lists all departments. You can use the filtering options to search the required department. Options include filtering by department name, exception employees, and reviewers associated with the department.

3 Click **Searches**, and then filter and select a search name you want to reject.

Note: To set a filter criterion to find a search, click the **Filter** icon. Select the required filter parameters, and then click **Apply Filters**.

4 Click **Reject**.

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

5 Click **Reject**.

The application displays the **Create New Search** dialog box for modification.

6 Click **Cancel**.

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

7 Click **Discard** to complete the operation or click **Cancel** to cancel it.

Resubmitting a search

You can monitor the status of all Insight Surveillance searches. You can review the search criteria to ensure that it matches the desired query. If any of the criteria is incorrect, modify it and resubmit the search. You can do this even if you do not normally have access to the departments with which the searches are associated. However, you cannot view the search criteria or the results of the searches unless you normally have access permission.

Note: You must have the *Monitor Search* permission to resubmit searches. By default, users that have the *Compliance System Admin* role have this permission.

To resubmit a search criterion

1 In the left navigation pane, click **Monitor**.

2 Filter and select a search name you want to resubmit.

Note: To set a filter criterion to find a search, click the **Filter** icon. Select the required filter parameters, and then click **Apply Filters**.

---

3 Click **Resubmit**.

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

4 Click **Resubmit** to complete the operation or click **Cancel** to cancel it.

Chapter 8

Managing department-specific hotword sets

This chapter includes the following topics:

Overview

Hotwords are predefined words or phrases that you can search for in employee items. When creating a search, you can add and select hotwords to search for in the subject lines of items, their content, or both.

To simplify the management of department-specific hotwords, you can group them into hotword sets. For example, you can use one set of hotwords to monitor items for unacceptable language and another to monitor them for unethical business practice. You can define hotwords and hotword sets that can be used at the application level, where they are applicable to all departments, and at the department level, where they are specific to that department.

You must have the department-level *Add Hotwords* permission to add department-specific hotwords. By default, users that have the *Rule Admin* role have this permission.

Creating department-specific hotword sets

To create the department-specific hotword set

1 In the left navigation pane, click **Departments**.

2 Search for and select the department for which you want to add hotwords and hotword sets.

Note: Insight Surveillance lists all departments. You can use the filtering options to search the required department. Options include filtering by department name, exception employees, and reviewers associated with the department.

---

3 Navigate to the **Hotwords** tab, and then click **New Hotword Set**.

The **Create Hotword Set** dialog box appears.

4 In the **Name** and **Description** fields, type a unique name and an optional description for the hotword set.

Note: The hotword set name can contain up to 50 characters. The description can contain up to 250 characters.

---

5 Under the **Hotwords** section, click **Select** to search and choose hotwords from the available list.

On the **Hotwords** dialog box, select the hotwords, and then click **OK**.

To select multiple adjacent words, hold down the Shift key and click the first and the last words in the range. To select multiple, non-adjacent words, hold down the Ctrl key and click the required words.

6 If the required hotword is not available, click **Create Hotwords** to add new hotwords.

Before you create hotwords, it is recommended to understand the following rules:

- For a **single word** with a wildcard, do not enclose it in quotes.
  For example, `Test*`, `overprice*`, `mis?sell`

Note: It is recommended to limit hotword length to 100 characters.

- For **multiple words**, enclose them in double quotes.

For example, `"search criteria"`, `"search * * criteria"`, `"te?st vas"`

- For **negation conditions**, add the keyword *AND* before the first negation term, ensuring there is a space before and after *AND*.
  For example, `search* AND –"search criteria"`, `test* AND –"test crit?ria" –"te?st vas"`, `"search criteria" AND –"search criteria Bloomberg"`.

Note: To prevent inconsistent search results and improve search accuracy while using multiple negation conditions, the hotword length can be extended up to a maximum of 2,000 characters.

To add multiple hotwords simultaneously, press **Enter** after each word to separate the words with a new line character.

7 Click **OK** to add the words.

8 Click **Save**.

9 (Optional) In the **Hotword Set** pane, select a hotword set to view included hotwords.

Editing department-specific hotwords and hotword sets

To edit the department-specific hotwords and hotword set

1 In the left navigation pane, click **Departments**.

2 Search for and select the department for which you want to add hotwords and hotword sets.

Note: Insight Surveillance lists all departments. You can use the filtering options to search the required department. Options include filtering by department name, exception employees, and reviewers associated with the department.

---

3 Navigate to the **Hotwords** tab, and click **Edit Hotword Set**.

The **Edit Hotword Set** dialog box appears.

4 In the **Name** and **Description** fields, type a unique name and an optional description for the hotword set.

Note: The hotword set name can contain up to 50 characters. The description can contain up to 250 characters.

---

5 Under the **Hotwords** section, do the following:

- To add new hotwords, click **Create Hotwords**.
- To add an existing hotword, click **Select Hotword**.
- To remove the selected hotword, click **Remove from set**.

6 Click **Save**.

Deleting department-specific hotword sets

To delete a department-specific hotword set

1 In the left navigation pane, click **Departments**.

2 Search for and select the department for which you want to delete hotwords and hotword set.

Note: Insight Surveillance lists all departments. You can use the filtering options to search the required department. Options include filtering by department name, exception employees, and reviewers associated with the department.

---

3 Navigate to the **Hotwords** tab, and under the **Hotword Set**, select a hotword set you want to delete.

4 Click **Delete Hotword Set**.

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.

Chapter 9

Managing department-specific labels

This chapter includes the following topics:

Searching department-specific labels, label groups, and single choice groups

To search for existing department-specific label, label group, and single choice group

1. In the left navigation pane, click **Departments**.
2. Search for and select the department in which you want to search labels, label groups, and single choice groups.
3. Navigate to the **Labels** tab.

   All the available department-specific labels, label groups, and single choice groups appear.
4. Search for and select the label you want to view. If required, perform any of the following steps:
   - To navigate to the next or previous pages, use the navigation arrows available in the bottom right corner of the page.

- To find the required label, in the **Filter by name** field, enter the keywords that characterize the label names that you want to search for, and then press ENTER on a keyboard or click the **Search** icon.

  Note: Do not use the wildcard characters (Asterisk or question mark) for partial searching. It does not give you the result.

- To filter to the required labels, click the **Filter** icon. Set the filter criteria by selecting type options and activation/deactivation status. If required, specify the date range when the label, label group, or single choice group was created, and click **Apply Filters**.
- Click **Reset Filters** to reset applied filters back to the default filter.
- Click **Clear Filters** to remove applied filters.
- If required, click **Refresh** to update the data on the **Labels** page.

5 Click on the label, label group, or single choice group name to view its details.

Managing department-specific labels

Department-specific labels management covers creating, editing, deleting, activating, deactivating, propagating, and unpropagating operations. You must have the *Manage Labels* permissions to perform these operations.

Creating department-specific labels

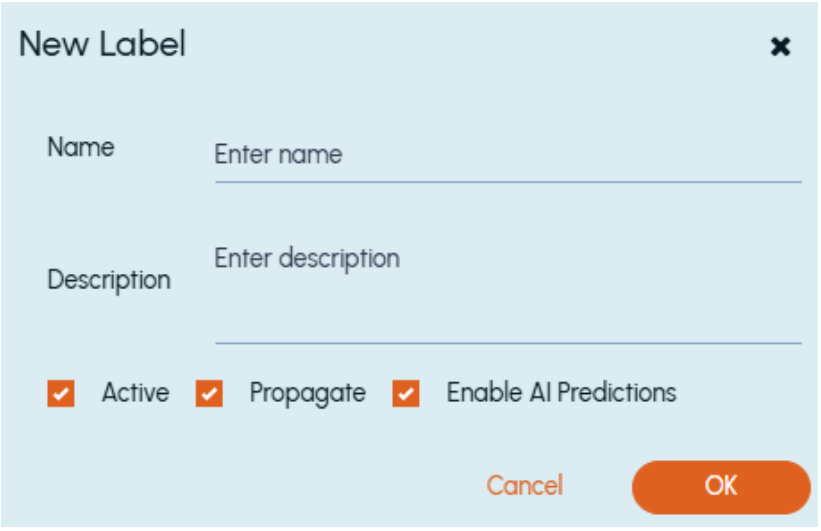
To create a department-specific label

1 In the left navigation pane, click **Departments**.

2 Search for and select the department in which you want to create a label.

3 Navigate to the **Labels** tab, and then click **New**.

The **New Label** dialog box appears.



4 In the **Name** filed, type a unique label name.

5 In the **Description** field, provide a description of this label.

6 Select the **Active** check box to activate the label.

Remember that -

- Only the active labels can be enabled for AI predictions, therefore, the **Enable AI Predictions** check box remains disabled until the label is activated.
- Do not select the **Active** check box if you want to keep the label in the deactivated state.

7 Select the **Propagate** check box to ensure the sub-departments inherit this label.

Do not select the **Propagate** check box if you do not want to propagate this label to sub-departments.

8 Select the **Enable AI Predictions** check box to consider this label for AI Prediction.

Note: Per department, only 20 active labels (including single choice group labels) can be enabled for AI predictions. Upon deactivation, the previously AI prediction-enabled labels and label groups get disabled.

---

9 Click **OK**.

Editing department-specific labels

To edit a department-specific label

1 In the left navigation pane, click **Departments**.

2 Search for and select the department in which you want to edit a label.

3 Navigate to the **Labels** tab.

4 Search for the label that you want to update. See "Searching application-specific labels, label groups, and single choice groups" on page 173.

5 Select the label that you want to edit, and click the **Edit** icon in the same row.

6 In the **Edit Label** dialog box, update the details of the required fields.

7 Click **OK**.

Activating department-specific labels

To activate a department-specific label

1 In the left navigation pane, click **Departments**.

2 Search for and select the department in which you want to activate a label.

3 Navigate to the **Labels** tab.

4 Search for the deactivated label that you want to activate.

See "Searching application-specific labels, label groups, and single choice groups" on page 173.

5 Select the label and do any of the following steps:

- On the action bar, click **Activate**.
- Click the **Edit** icon in the same row. In the **Edit Label** dialog box, select the **Active** check box.

Note: Per department, only 20 active labels (including single choice group labels) can be enabled for AI predictions.

The updated data appears on the **Labels** page. If required, click **Refresh** on the action bar.

Deactivating department-specific labels

To deactivate a department-specific label

1. In the left navigation pane, click **Departments**.
2. Search for and select the department in which you want to deactivate a label.
3. Navigate to the **Labels** tab.
4. Search for the active label that you want to deactivate.

   See "Searching application-specific labels, label groups, and single choice groups" on page 173.
5. Select the label and do any of the following steps:
   - On the action bar, click **Deactivate**.
   - Click the **Edit** icon in the same row. In the **Edit Label** dialog box, clear the **Active** check box.
     Deactivating a label or label group disables AI predictions for that label or label group.

   The updated data appears on the **Labels** page. If required, click **Refresh** on the action bar.

Propagating department-specific labels

To propagate a department-specific label

1. In the left navigation pane, click **Departments**.
2. Search for and select the department in which you want to propagate a label.
3. Navigate to the **Labels** tab.
4. Search for the unpropagated label that you want to propagate.
5. Select the label and do any of the following steps:
   - On the action bar, click **Propagate**.
   - Click the **Edit** icon in the same row. In the **Edit Label** dialog box, select the **Propagate** check box.

The updated data appears on the **Labels** page. If required, click **Refresh** on the action bar.

Unpropagating department-specific labels

To unpropagate a department-specific label

1. In the left navigation pane, click **Departments**.
2. Search for and select the department in which you want to unpropagate a label.
3. Navigate to the **Labels** tab.
4. Search for the propagated label that you want to unpropagate.
5. Select the label and do any of the following steps:
   - On the action bar, click **Unpropagate**.
   - Click the **Edit** icon in the same row. In the **Edit Label** dialog box, clear the **Propagate** check box.

   The updated data appears on the **Labels** page. If required, click **Refresh** on the action bar.

Deleting department-specific labels

To delete a department-specific label

1. In the left navigation pane, click **Departments**.
2. Search for and select the department from which you want to delete a label.
3. Navigate to the **Labels** tab.
4. Search for the label that you want to delete.
5. Select the label, and click **Delete** on the action bar.

Managing department-specific label groups

Department-specific label groups management covers creating, editing, deleting, activating, deactivating, propagating, and unpropagating operations. You must have the *Manage Labels* permissions to perform these operations.

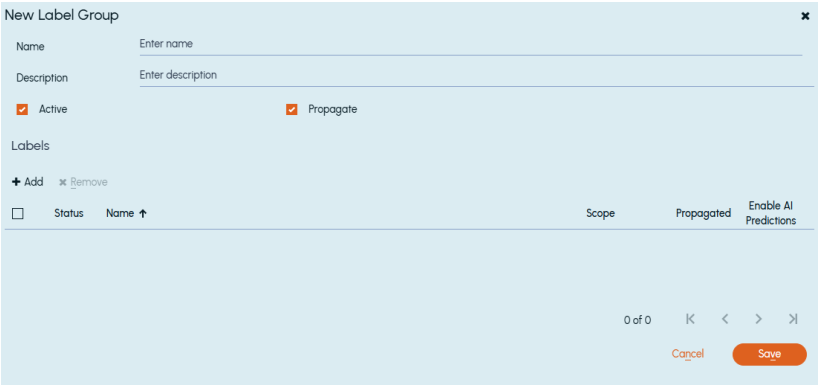
Creating department-specific label groups

To create a department-specific label group

1. In the left navigation pane, click **Departments**.
2. Search for and select the department in which you want to create a label group.

3 Navigate to the **Labels** tab, and then click **New**.

The **New Label Group** dialog box appears.



4 In the **Name** filed, type a unique label name.

5 In the **Description** field, provide a description of this label.

6 Select the **Active** check box to activate the label.

Do not select the check box if you want to keep the label in the deactivated state.

Note: The **Enable AI Predictions** check box is not shown for department level label groups because each label within the group can be enabled while creating or editing them individually.

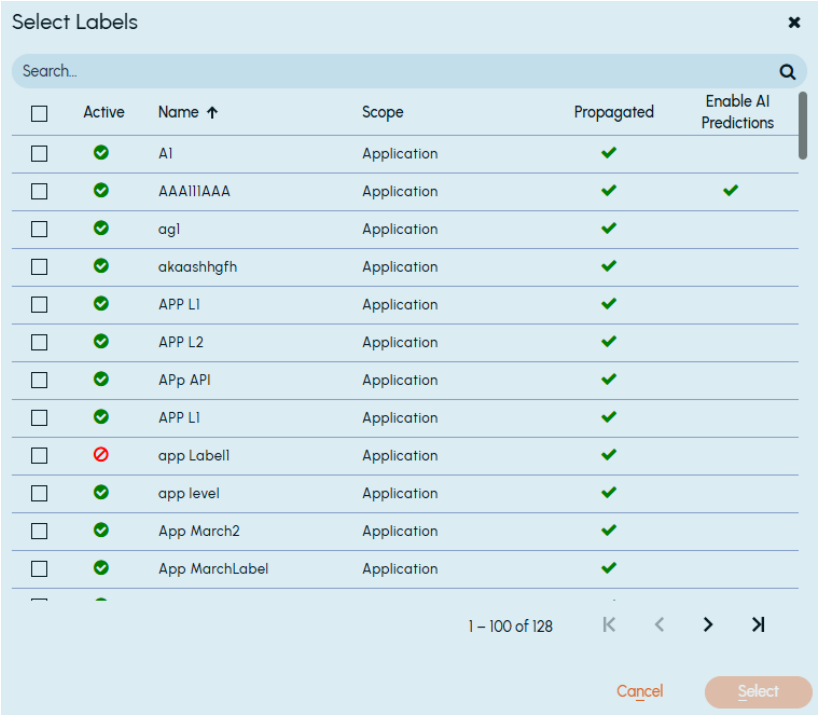
---

7 Select the **Propagate** check box to ensure the sub-departments inherit this label.

Do not select the check box if you do not want to propagate this label to sub-departments.

8 Click **Add** to open the **Select Labels** dialog box.

9 Search for and select the labels that you want to this label group, and click **Select** as shown in the sample image below.



10 Click **Save**.

Editing department-specific label groups

To edit a department-specific label group

1 In the left navigation pane, click **Departments**.

2 Search for and select the department in which you want to edit a label group.

3 Navigate to the **Labels** tab.

4 Search for the label group that you want to update. See "Searching application-specific labels, label groups, and single choice groups" on page 173.

5 Select the label group and click the **Edit** icon in the same row.

6 In the **Edit Label Group** dialog box, update the details of the required fields or add or remove labels.

7 Click **Save**.

Activating department-specific label groups

To activate a department-specific label group

1. In the left navigation pane, click **Departments**.
2. Search for and select the department in which you want to activate a label group.
3. Navigate to the **Labels** tab.
4. Search for the deactivated label group that you want to activate.

   See "Searching application-specific labels, label groups, and single choice groups" on page 173.
5. Select the label group and do any of the following steps:
   - On the action bar, click **Activate**.
   - Click the **Edit** icon in the same row. In the **Edit Label Group** dialog box, select the **Active** check box.

   The updated data appears on the **Labels** page. If required, click **Refresh** on the action bar.

Deactivating department-specific label groups

To deactivate a department-specific label group

1. In the left navigation pane, click **Departments**.
2. Search for and select the department in which you want to deactivate a label group.
3. Navigate to the **Labels** tab.
4. Search for the active label group that you want to deactivate.

   See "Searching application-specific labels, label groups, and single choice groups" on page 173.
5. Select the label group and do any of the following steps:
   - On the action bar, click **Deactivate**.
   - Click the **Edit** icon in the same row. In the **Edit Label Group** dialog box, clear the **Active** check box.

   The updated data appears on the **Labels** page. If required, click **Refresh** on the action bar.

Propagating department-specific label groups

To propagate a department-specific label group

1. In the left navigation pane, click **Departments**.
2. Search for and select the department in which you want to propagate a label group.
3. Navigate to the **Labels** tab.
4. Search for the unpropagated label group that you want to propagate.
5. Select the label group and do any of the following steps:
   - On the action bar, click **Propagate**.
   - Click the **Edit** icon in the same row. In the **Edit Label Group** dialog box, select the **Propagate** check box.

   The updated data appears on the **Labels** page. If required, click **Refresh** on the action bar.

Unpropagating department-specific label groups

To unpropagate a department-specific label group

1. In the left navigation pane, click **Departments**.
2. Search for and select the department in which you want to unpropagate a label group.
3. Navigate to the **Labels** tab.
4. Search for the propagated label group that you want to unpropagate.
5. Select the label group and do any of the following steps:
   - On the action bar, click **Unpropagate**.
   - Click the **Edit** icon in the same row. In the **Edit Label Group** dialog box, clear the **Propagate** check box.

   The updated data appears on the **Labels** page. If required, click **Refresh** on the action bar.

Deleting department-specific label groups

To delete a department-specific label group

1. In the left navigation pane, click **Departments**.
2. Search for and select the department from which you want to delete a label group.
3. Navigate to the **Labels** tab.

4 Search for the label group that you want to delete.

5 Select the label group, and click **Delete** on the action bar.

Managing department-specific single choice label groups

Department-specific single choice label groups management covers creating, editing, deleting, activating, deactivating, propagating, and unpropagating operations. You must have the *Manage Labels* permissions to perform these operations.

Creating department-specific single choice label groups

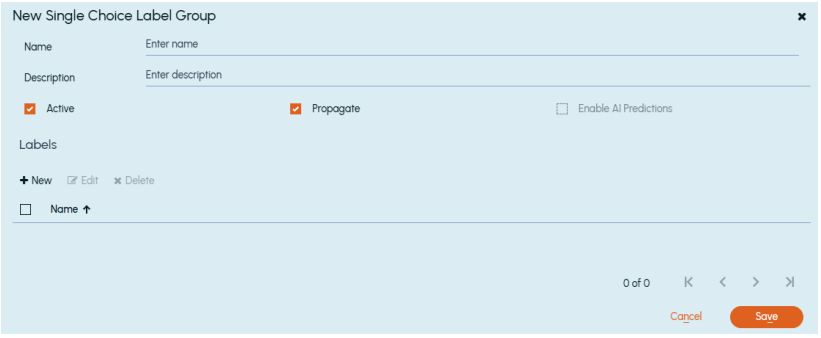
To create a department-specific single choice label group

1 In the left navigation pane, click **Departments**.

2 Search for and select the department in which you want to create a single choice label group.

3 Navigate to the **Labels** tab, and then click **New Single Choice Group**.

The **New Single Choice Label Group** dialog box appears.



4 In the **Name** filed, type a unique single choice label group name.

5 In the **Description** field, provide a description of this single choice label group.

6 Select the **Active** check box to activate the single choice label group.

Remember that -

- Only the active single choice label groups can be enabled for AI predictions, therefore, the **Enable AI Predictions** check box remains disabled until the label is activated.

- Do not select the **Active** check box if you want to keep the single choice label group in the deactivated state.

7 Select the **Propagate** check box to ensure the sub-departments inherit this single choice label group.

Do not select the check box if you do not want to propagate this single choice label group to sub-departments.

8 Select the **Enable AI Predictions** check box to consider this single choice label group for AI Prediction.

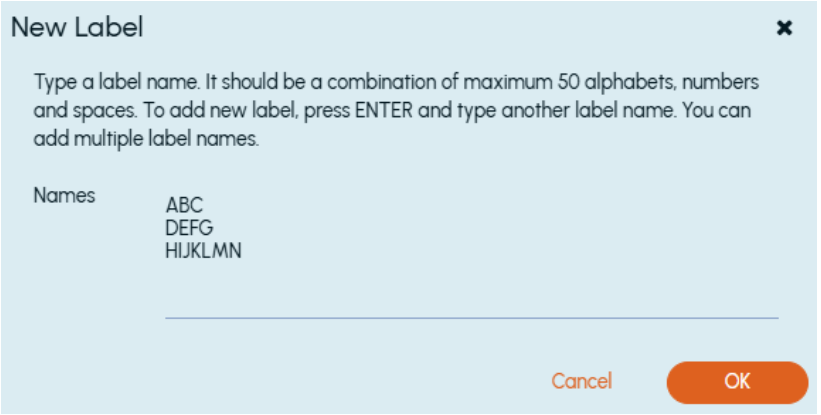
Note: Per department, only 20 active labels (including single choice group labels) can be enabled for AI predictions. Upon deactivation, the previously AI prediction-enabled labels and label groups get disabled.

---

9 Click **Add** to open the **New Label** dialog box.

10 Manually type new labels, and click **OK**.

Note: New label names must be a combination of maximum 50 characters that includes alphabets, numbers and spaces. After adding a label name, press ENTER to add the next label. You can add multiple label names as shown in the sample image below.



11 Click **Save**.

Editing department-specific single choice label groups

To edit a department-specific single choice label groups

1. In the left navigation pane, click **Departments**.
2. Search for and select the department in which you want to edit a single choice label group.
3. Navigate to the **Labels** tab.
4. Search for the single choice label group that you want to update. See "Searching application-specific labels, label groups, and single choice groups" on page 173.
5. Select the single choice label group, and click the **Edit** icon in the same row.
6. In the **Edit Single Choice Label Group** dialog box, update the details of the required fields.

   If required, select an individual label and do any of the following.

   - Click **Edit** to update the label name.
   - Click **Delete** to remove the label entry from the group.
7. Click **Save**.

Activating department-specific single choice label groups

To activate a department-specific single choice label group

1. In the left navigation pane, click **Departments**.
2. Search for and select the department in which you want to activate a single choice label group.
3. Navigate to the **Labels** tab.
4. Search for the deactivated single choice label group that you want to activate.

   See "Searching application-specific labels, label groups, and single choice groups" on page 173.
5. Select the single choice label group and do any of the following steps:

   - On the action bar, click **Activate**.
   - Click the **Edit** icon in the same row. In the **Edit Single Choice Label Group** dialog box, select the **Active** check box.

Note: Per department, only 20 active labels (including single choice group labels) can be enabled for AI predictions.

The updated data appears on the **Labels** page. If required, click **Refresh** on the action bar.

Deactivating department-specific single choice label groups

To deactivate a department-specific single choice label group

1. In the left navigation pane, click **Departments**.
2. Search for and select the department in which you want to deactivate a single choice label group.
3. Navigate to the **Labels** tab.
4. Search for the active single choice label group that you want to deactivate.

   See "Searching application-specific labels, label groups, and single choice groups" on page 173.
5. Select the single choice label group and do any of the following steps:
   - On the action bar, click **Deactivate**.
   - Click the **Edit** icon in the same row. In the **Edit Single Choice Label Group** dialog box, clear the **Active** check box.
     Deactivating a single choice label group disables AI predictions for that single choice label group.

   The updated data appears on the **Labels** page. If required, click **Refresh** on the action bar.

Propagating department-specific single choice label groups

To propagate a department-specific single choice label group

1. In the left navigation pane, click **Departments**.
2. Search for and select the department in which you want to propagate a single choice label group.
3. Navigate to the **Labels** tab.
4. Search for the unpropagated single choice label group that you want to propagate.
5. Select the single choice label group and do any of the following steps:
   - On the action bar, click **Propagate**.
   - Click the **Edit** icon in the same row. In the **Edit Single Choice Label Group** dialog box, select the **Propagate** check box.

   The updated data appears on the **Labels** page. If required, click **Refresh** on the action bar.

Unpropagating department-specific single choice label groups

To unpropagate a department-specific single choice label group

1. In the left navigation pane, click **Departments**.
2. Search for and select the department in which you want to unpropagate a single choice label group.
3. Navigate to the **Labels** tab.
4. Search for the propagated single choice label group that you want to unpropagate.
5. Select the single choice label group and do any of the following steps:
   - On the action bar, click **Unpropagate**.
   - Click the **Edit** icon in the same row. In the **Edit Single Choice Label Group** dialog box, clear the **Propagate** check box.

   The updated data appears on the **Labels** page. If required, click **Refresh** on the action bar.

Deleting department-specific single choice label groups

To delete a department-specific single choice label group

1. In the left navigation pane, click **Departments**.
2. Search for and select the department from which you want to delete a single choice label group.
3. Navigate to the **Labels** tab.
4. Search for the single choice label group that you want to delete.
5. Select the single choice label group, and click **Delete** on the action bar.

Chapter 10

Managing department-specific trash rules

This chapter includes the following topics:

Overview

Trash rules let you define when to ignore or include inbound items from specific email addresses or domains.

Trash rules are used during search. By default, a trash rule causes items coming in from specified email addresses or domains to be omitted from search results.

You can define trash rules to be used at the department level, but they can be propagated to sub-departments. Application-specific trash rules can be deactivated at the department-level. A deactivated department trash rule does not modify the original application trash rule. Trash rules cannot be deleted or modified; they can only be deactivated.

You must have the department-level *Manage Trash rules* permission to add department-specific trash rules. By default, users that have the *Rule Admin* role have this permission.

Creating department-specific trash rules

To create a department-specific trash rule

1 In the left navigation pane, click **Departments**.

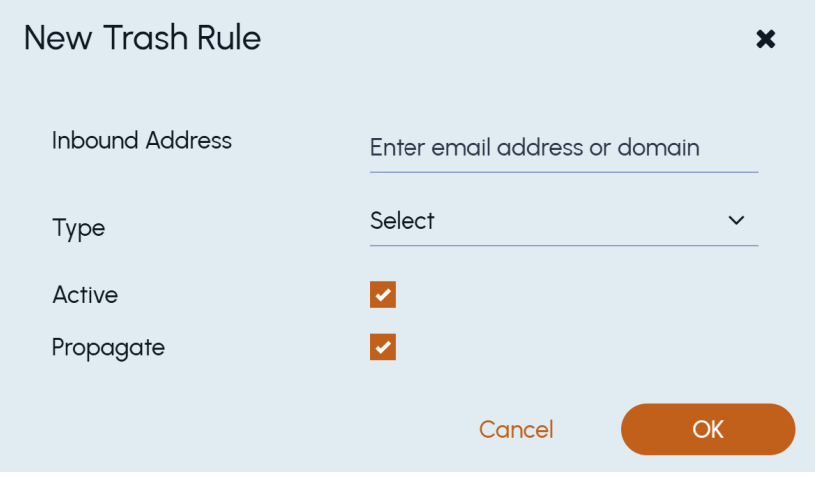
2 Search for and select the department for which you want to add a trash rule.

Note: Insight Surveillance lists all departments. You can use the filtering options to search the required department. Options include filtering by department name, exception employees, and reviewers associated with the department.

---

3 Navigate to the **Trash** tab, and then click **New**.

The **New Trash Rule** dialog box appears.



4 In the **Inbound Address** filed, type an email address or domain.

Note: When you specify a domain, do not add the @ symbol.

---

5 In the **Type** field, select a Domain or an Email Address.

6 Select the **Status** check box to activate the rule.

Do not select the check box if you want to keep the rule in the deactivated state.

7 Select the **Propagate** check box to ensure the sub-departments inherit the rule.

Do not select the check box if you do not want to propagate rule to sub-departments.

8 Click **OK**.

Activating department-specific trash rules

To activate a department-specific trash rule

1 In the left navigation pane, click **Departments**.

2 Search for and select the department for which you want to activate a trash rule.

Note: Insight Surveillance lists all departments. You can use the filtering options to search the required department. Options include filtering by department name, exception employees, and reviewers associated with the department.

---

3 Navigate to the **Trash** tab.

4 Select a deactivated trash rule you want to activate and click **Activate** on the action bar.

Deactivating department-specific trash rules

To deactivate a department-specific trash rule

1 In the left navigation pane, click **Departments**.

2 Search for and select the department for which you want to activate a trash rule.

Note: Insight Surveillance lists all departments. You can use the filtering options to search the required department. Options include filtering by department name, exception employees, and reviewers associated with the department.

---

3 Navigate to the **Trash** tab.

4 Select an activated trash rule you want to deactivate, and then click **Deactivate** on the action bar.

Note: If an application-specific trash rule is deactivated, the scope indicates Application. A deactivated application-specific trash rule creates a department-specific trash rule with a deactivated status. This process ensures that Insight Surveillance ignores the global application-specific trash rule that was previously propagated to the selected department.

Propagating department-specific trash rules

To globally propagate a department-specific trash rule

1 In the left navigation pane, click **Departments**.

2 Navigate to the **Trash** tab.

3 Select an unpropagated trash rule you want to propagate and click **Propagate** on the action bar.

Note: This action propagates the trash rule to the selected department's, including the sub-departments.

Unpropagating department-specific trash rules

To unpropagate a department-specific trash rule

1 In the left navigation pane, click **Departments**.

2 Navigate to the **Trash** tab.

3 Select a propagated trash rule you want to unpropagate and click **Unpropagate** on the action bar.

Note: This action removes the trash rule from the selected department, including the sub-departments.

Chapter 11

Managing department-specific allowlist rules

This chapter includes the following topics:

Overview

Allowlist rules let you define the text that is contained within the items that are always considered compliant. This functionality does not apply to item attachments.

If Insight Surveillance finds an active word or phrase from the lexicon within allowlisted text, the word or phrase is not flagged. Many customers use this feature to allowlist the disclaimers that appear at the bottom of their outgoing emails. Having the allowlist rule in place means that the disclaimer does not cause an email to be flagged with violations for review.

For example, assume you used the following disclaimer in your email address:

Email that is sent through the Internet is not secure. Do not use email to send us confidential information such as credit card numbers, changes of address, PIN numbers, passwords, or other important information. Do not email orders to buy or sell securities, transfer funds, or send time sensitive instructions. We do not accept such orders or instructions. This email is not an official trade confirmation for the transactions that are executed for your account. Your email message is

not private in that it is subject to review by the Firm, its officers, agents and employees.

You can add the entire paragraph to your allowlist rules so that every outgoing item is not flagged for review since *PIN numbers* and *passwords* are words that could be used as search hotwords. Although this functionality is generally reserved for the outgoing email, you can allowlist words and phrases for any inbound item or instant message.

You must have the department-level *Manage Allowlist rules* permission to add department-specific allowlist rules. By default, users that have the *Rule Admin* role have this permission.

Creating department-specific allowlist rules

To create a department-specific allowlist rule

1 In the left navigation pane, click **Departments**.

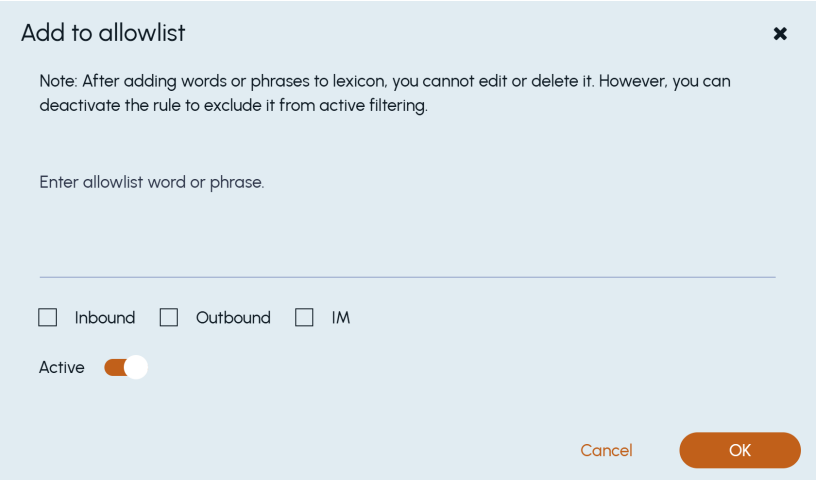
2 Search for and select the department for which you want to add a allowlist rule.

Note: Insight Surveillance lists all departments. You can use the filtering options to search the required department. Options include filtering by department name, exception employees, and reviewers associated with the department.

---

3 Navigate to the **Allowlist** tab, and then click **New**.

The **Add to allowlist** dialog box appears.



4 In the **Enter allowlist word or phrase** field, type a word or phrase.

Note: The allowlist rule can contain up to 1024 characters, but a word should not be longer than 50 characters. After adding words or phrases to the lexicon, you cannot edit or delete it. However, you can deactivate the rule to exclude it from active filtering.

---

5 To create a allowlist rule, select any or all of the following options:

- Select the **Inbound** check box to apply this allowlist rule to all inbound items.
- Select the **Outbound** check box to apply this allowlist rule to all outbound items.
- Select the **IM** check box to apply this allowlist rule to all instant messages.

Note: Clear the respective check boxes if you do not want to apply rule to Inbound, Outbound, or Instant Messages.

---

6 Select the **Active** check box to activate the rule.

7 Click **OK**.

Editing department-specific allowlist rules

To edit a department-specific allowlist rule

1. In the left navigation pane, click **Departments**.
2. Search for and select the department for which you want to edit a allowlist rule.

   Note: Insight Surveillance lists all departments. You can use the filtering options to search the required department. Options include filtering by department name, exception employees, and reviewers associated with the department.

   ---

3. Select an active allowlist rule you want to deactivate, and then click the **Edit allowlist** icon.

   The **Edit allowlist** dialog box appears.

   Note: You cannot change the words or phrases mentioned in the rule.

   ---

4. Modify the options to which to apply the allowlist rule: **Inbound**, **Outbound**, or **IM** (Instant Messages).
5. Modify the allowlist rule status to activate or deactivate
6. Click **OK**.

Chapter 12

Managing department-specific review comments

This chapter includes the following topics:

About department-level review comments

While performing the department-level reviews, sometimes it is tedious for reviewers to type the same comments again and again. To make review process easier, as an administrators and reviewers, you can use the **Review Comments** functionality to save various commonly used comments that can be often used by them.

As a compliance supervisor, you can add, edit, and delete such frequently used reviewing comments. The department-level *Manage Reviewing Comments* permission is used to control the department-level review comments, and can be configured from the **Roles and Permissions** section. This permission is by default assigned to the *Compliance Supervisor* role. See "Managing role assignment for a user in departments" on page 82.

Adding department-level review comments

To add a department-level review comment

1. In the left navigation pane, click **Departments**.
2. Search for and select the department for which you want to add review comments.

   Note: Insight Surveillance lists all the available departments. You can use the filtering options to search the required department.

3. In the **Review Comments** tab, click **New** to add a new department-level review comment.

   The **New review comment** dialog box appears.
4. Specify the following information:

Summary	Provide a short comment name.
Comment	Provide the actual comment text that describes your comment.

5. Click **Save**.
6. (Optional) On the **Review Comments** page, click **Refresh** to update the page with the latest records.

Editing department-level review comments

To edit a department-level review comment

1. In the left navigation pane, click **Departments**.
2. Search for and select the department for which you want to edit review comments.

   Note: Insight Surveillance lists all the available departments. You can use the filtering options to search the required department.

3. In the **Review Comments** tab, select the reviewing comment that you want to edit, and click the **Edit** icon in the same row.

4 In the **Edit review comment** dialog box, update the following information:

Summary	Provide an updated short comment name, if required.
Comment	Provide the updated comment description for your comment.

5 Click **Save**.

6 (Optional) On the **Review Comments** page, click **Refresh** to update the page with the latest records.

Deleting department-level review comments

To delete a department-level review comment

1 In the left navigation pane, click **Departments**.

2 Search for and select the department for which you want to delete review comments.

Note: Insight Surveillance lists all the available departments. You can use the filtering options to search the required department.

---

3 In the **Review Comments** tab, perform any of the following actions:

- To delete an individual review comment, select the reviewing comment that you want to delete, and click the **Delete** icon in the same row. You can select the comments across pages.
- To delete multiple review comments simultaneously, select the reviewing comments that you want to delete. Click **Delete** on the action bar. The application displays number of the selected items in the bottom of the page. You can select maximum 200 comments across pages at a time.
- To delete all the comments on the page, select the top-most checkbox in the first column, and click **Delete** on the action bar.

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

4 Click **Yes**.

5 (Optional) On the **Review Comments** page, click **Refresh** to update the page with the latest records.

Updating order of department-level review comments

To update order of a department-level review comment

1 In the left navigation pane, click **Departments**.

2 Search for and select the department in which you want to reorder the review comments.

Note: Insight Surveillance lists all the available departments. You can use the filtering options to search the required department.

---

3 In the **Review Comments** tab, ensure that there are more than one comment added.

Else, the **Update Order** option remains disabled.

4 Click **Update Order**, and select the comment you want to move up or down.

5 Click the up or down arrow next to each item to change their order.

Alternatively, you can drag and drop items above or below another comment.

6 Click **Save Order**.

7 (Optional) On the **Review Comments** page, click **Refresh** to update the page with the updated order of records.

Chapter 13

Viewing employees associated with departments

This chapter includes the following topics:

Viewing employee association history

You can view the current and previous employees with their dates of commencement with and exit from the department.

To view the employee association history for a department

1 In the left navigation pane, click **Departments**.

2 Search for and select the department.

Note: Insight Surveillance lists all departments. You can use the filtering options to search the required department. Options include filtering by department name, exception employees, and reviewers associated with the department.

---

3 Click **History**.

The application shows following type of log of employees associated with that department.

Chapter 14

Managing users, roles, and permissions

This chapter includes the following topics:

Overview

You can assign roles to employees to determine what they can access and the tasks that they can perform in Insight Surveillance. For example, you can assign the role of reviewer to an employee who needs to monitor, review, hold review, question, escalate, appraise, and comment on the items in a department. Some roles are effective at the application level, across Insight Surveillance, whereas others apply at the department level only.

Insight Surveillance has several predefined roles, but, if none precisely meets your requirements, you can customize new roles. You can delete only customized roles if you have no use for them, and not the predefined roles.

Predefined user roles and permissions

You can create application and department level roles. You can restrict the associated permissions to a department level or the application level. Users with application roles can only perform tasks in a specific department if they have been assigned the appropriate roles in that department. To perform tasks in more than one department, the users must be assigned the appropriate role in every department that they need to access.

Application-specific roles

Table 14-1 Application-specific roles in Insight Surveillance

Role	Description	Default Permission
App Rule Admin	This role lets you set up search schedules, create searches across departments, and manage global hotwords and reviewing comments.	■ Add Hotwords ■ Application Search ■ Manage Reviewing Comments ■ Manage Schedules ■ Modify and Delete Hotwords ■ Manage Allowlist rules ■ Manage Trash rules ■ Manage DataRequests ■ Manage Labels
App User Admin	This role lets you add users (employees) and employee groups to Insight Surveillance, create and manage departments, assign application roles, and create delegate users.	■ Create Departments ■ Grant Users Access ■ Manage Delegates ■ Manage Department Users ■ Manage Employee Groups ■ Manage Roles ■ Add Hotwords ■ Manage DataRequests
Compliance System Admin	This role lets you monitor the progress of searches.	■ Monitor Search ■ Manage Labels

Table 14-1 Application-specific roles in Insight Surveillance *(continued)*

Role	Description	Default Permission
System Admin	Lets you perform the administrative activities on the application. These activities include department management and role assignment.	Add Hotwords Application Search Configure Reporting API Endpoint Create Departments Delete Department Export Configuration Data Grant Users Access Import Configuration Data Manage Allowlist rules Manage Data Request Manage Delegates Manage Department Partitions Manage Department Users Manage Employee Groups Manage Labels Manage Reviewing Comments Manage Roles Manage Schedules Manage Trash rules Modify & Delete Hotwords Modify Audit Settings Modify System Configuration Monitor Search View Audit Information View Audit Settings View System Configuration

Department-specific roles

Table 14-2 Department-specific roles in Insight Surveillance

Role	Description	Default Permission
Compliance Supervisor	This role lets you use the appraisal features to check the work of department reviewers and manage exception employees in the department.	■ Add Own Review Comments ■ Apply Appraisal Status ■ Apply Bulk Review Action ■ Apply Review Action ■ Export Messages ■ Manage Exceptions ■ Perform Ad Hoc Searches ■ Review Messages ■ View Reports ■ View Task Status ■ Add or remove content snippet ■ Show Intelligent Review Details in Review ■ Apply Labels
Department Reviewer	This role lets you monitor, review, hold review, question, escalate, appraise, and comment on the items within the department, export items for offline review, and generate and view reports.	■ Add Own Review Comments ■ Apply Bulk Review Action ■ Apply Review Action ■ Escalate Messages ■ Export Messages ■ Perform Ad Hoc Searches ■ Review Messages ■ Show Reviewer Summaries On Home Page ■ View Reports ■ View Task Status ■ Show Intelligent Review Details in Review ■ Apply Labels

Table 14-2 Department-specific roles in Insight Surveillance *(continued)*

Role	Description	Default Permission
Escalation Reviewer	This role lets you receive the items that other reviewers in the department have escalated to a higher authority for further review. Departments lower in the hierarchy inherit this role, so an escalation reviewer automatically has access to nested departments.	■ Apply Bulk Actions to Escalations ■ Apply Comments to Escalations ■ Apply Review Action to Escalations ■ Change Escalation Status ■ Export Escalations ■ Review Escalations ■ Show Reviewer Summaries On Home Page ■ View Task Status ■ Show Intelligent Review Details in Review ■ Apply Labels
Exception Reviewer	This role lets you search the items of exception employees to whom you are assigned. You can also monitor, review, hold review, question, escalate, appraise, and comment on the items, export them, and generate and view reports.	■ Add Own Review Comments ■ Apply Bulk Review Action ■ Apply Review Action ■ Escalate Messages ■ Export Messages ■ Perform Ad Hoc Searches ■ Review Messages ■ Search Capture ■ Show Hotwords in Search ■ Show Reviewer Summaries On Home Page ■ View Reports ■ Manage GSS and Scheduled searches ■ Accept searches ■ View Task Status ■ Show Intelligent Review Details in Review ■ Apply Labels

Table 14-2 Department-specific roles in Insight Surveillance *(continued)*

Role	Description	Default Permission
Rule Admin	This role lets you create searches within the department and manage department hotwords. You can also configure the monitoring policy that is assigned to employees and generate and view reports. In addition, you can assign exception reviewers to specific employees.	■ Add Hotwords ■ Assign % Review Requirement ■ Manage Exceptions ■ Modify and Delete Hotwords ■ Search Capture ■ Show Hotwords in Search ■ View Reports ■ Manage Allowlist rules ■ Manage Trash rules ■ Manage GSS and Scheduled searches ■ Accept searches ■ View Task Status ■ Manage Labels
User Admin	This role lets you manage the properties of the department and of monitored employees. You can also assign department roles to users, generate and view reports on department details, and review progress.	■ Add Monitored Employees ■ Configure Department Properties ■ Grant Users Access ■ Manage Exceptions ■ View Reports ■ Search Capture ■ Show Hotwords in Search ■ Manage GSS and Scheduled searches ■ Accept searches ■ View Task Status
Passive Reviewer	Lets you view and export the department's messages generate and view reports and use the appraisal features to check and mark the work of department reviewers. You cannot apply review status marks to messages.	■ Apply Appraisal Status ■ Export Messages ■ Review Messages ■ View Reports ■ View Task Status ■ Show Intelligent Review Details in Review

Adding new roles for users (employees) and employee groups

You can manage application level users (employees), employee groups, and their roles by accessing the **Application** tab. These customized roles can then be assigned to the department users and employee groups. If none of the predefined roles provides the exact set of permissions you want to assign to users, you can create your own roles.

By default, you can view the content of the **Roles** tab. The **Roles** tab content is further classified in three sections – **Action** bar, **Roles**, and **Permissions**. The **Roles** section displays a list of all available roles. After selecting any role, the **Permissions** section displays a list of permissions associated with the selected role.

Note: You must have the *Manage Roles* and the *Grant Users Access* permissions to create roles. By default, users or groups that have the *App User Admin* role have this permission.

To add a new user role

1 In the left navigation pane, click **Application**.

2 In the **Roles** tab, click **Add Role**.

The **Add Role** dialog box appears.

3 In the **Name** and **Description** fields, type a unique name and an optional description for the role respectively.

Note: The role name can contain up to 50 characters. The description can contain up to 250 characters.

---

4 In the **Scope** field, do any of the following:

- To allow the department-level permissions, select the **Department** option.
- To allow the application-level permissions, select the **Application** option.

5 Under the **Permission** section, choose the required associated permissions.

6 Click **Save**.

Editing user roles and permissions

You can change the permissions that are associated with any Insight Surveillance role. If none of the predefined roles provide the exact set of permissions you want to assign to users, you can custom create new roles. You can rename them and change their descriptions. However, you cannot rename any predefined role. Arctera recommends creating new roles instead of altering any predefined role's permissions.

Note: You must have the *Manage Roles* and the *Grant Users Access* permissions to create roles. By default, users that have the *App User Admin* Insight Surveillance have this permission.

To edit a user Insight Surveillance and permissions

1 In the left navigation pane, click **Application**.

2 In the **Insight Surveillances** tab, select a Insight Surveillance to which you want to add or remove permissions, and then click **Edit Insight Surveillance**.

The **Edit Insight Surveillance** dialog box appears.

3 In the **Name** and **Description** fields, type a unique name and an optional description for the Insight Surveillance respectively.

Note: The Insight Surveillance name can contain up to 50 characters. The description can contain up to 250 characters.

---

4 In the **Scope** field, do any of the following:

- To allow the department-level permissions, select the **Department** option.
- To allow the application-level permissions, select the **Application** option.

5 Under the **Permission** section, in the **Allow** column, do the following:

- Select the required associated permissions effective at the department level.
- Unselect (clear) the permissions that are not required anymore to be associated with this role.

6 Click **Save**.

7 Re-log in the user who is assigned the role that had been edited.

Deleting user roles

When you have no further use for a customized role, you can delete it. You can delete custom roles only, and not the predefined roles. If you delete a role while it is assigned to someone, that person does not retain the permissions associated with the role.

Note: You must have the *Manage Roles* and the *Grant Users Access* permissions to delete roles. By default, users that have the *App User Admin* Insight Surveillance have this permission.

To delete a user Insight Surveillance

1 In the left navigation pane, click **Application**.

2 In the **Insight Surveillances** tab, select a customized Insight Surveillance you want to delete.

3 Click **Delete Insight Surveillance**.

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.

Assigning Insight Surveillances to users (employees) and employee groups

You can use the **Insight Surveillance Assignment** tab to view associated Insight Surveillances of users (employees) and employee groups, assign new Insight Surveillances to them, and remove unneeded Insight Surveillances. The **User and Groups** section displays a list of available users and employee groups. When you select a user or a group from this list, the **Assigned Insight Surveillance** section shows a list of Insight Surveillances assigned to the selected user or the group. You can assign one or multiple Insight Surveillances to a user or a group.

Note: You must have the *Manage Roles* and the *Grant Users Access* permissions to assign roles. By default, users that have the *App User Admin* role have this permission.

To assign a role to a user

1 In the left navigation pane, click **Application**.

2 Navigate to the **Role Assignment** tab.

3 In the **Users and Groups** pane, search for and select a user or a group to which you want to assign roles.

Note: If a user or a group is unavailable in the list, you can add it first. To add a new user, click **Add User**. Select the required user or the group from the **Add User** dialog box, and then click **Save**.

---

4 In the **Assigned Roles** pane, search for and select one or multiple roles you want to assign.

Note: If a role is unavailable in the list, add a new user role.

See "Adding new roles for users (employees) and employee groups" on page 149.

---

5 Click **Save**.

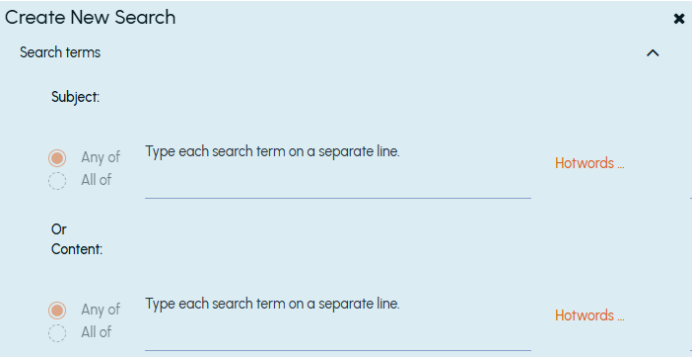
Restricting users to use hotwords in searches

As an administrator, you can restrict users with department-level permissions from using hotwords when creating or running searches. To do this, disable the following department-level permissions:

- **Search Capture**: This permission allows users to create searches. If this permission is not enabled then users cannot view the **Search** tab.
- **Show Hotwords in Search**: This permission allows users to view and use the **Hotwords** buttons under the **Search Terms** section.

Note: For users with the **Search Capture** permission is enabled, the **Show Hotwords in Search** permission is enabled by default.

If the **Search Capture** and the **Show Hotwords in Search** permissions are enabled, users can view the **Hotwords** buttons under the **Search Terms** section. Users can click **Hotwords** to select existing hotwords and provide new hotwords for searches. See the sample image below.



If the *Search Capture* permission is enabled and the *Show Hotwords in Search* permission is disabled, users can create and view the searches, but cannot view the **Hotwords** button under the **Search Terms** section.

Therefore, to restrict the users to view and use the Hotwords, you must enable the *Search Capture* permission and disable the *Show Hotwords in Search* permission.

To enable or disable these permissions, See "Editing user roles and permissions" on page 150.

Removing a user role

You must have the *Manage Roles* and the *Grant Users Access* permissions to remove roles. By default, users that have the *App User Admin* role have this permission.

To remove a user role

1 In the left navigation pane, click **Application**.

2 In the **Role Assignment** tab, search for and select the user you wish to remove a role from.

Note: In the **Assigned Roles** pane, application displays a list of roles assigned to the selected user. To select multiple adjacent roles, hold down the Shift key and click the first and the last name in the range. To select multiple, non-adjacent roles, hold down the **Ctrl** key and click the required roles.

---

3 Select a role, and then click **Remove Roles** on the action bar.

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.

Chapter 15

Managing application-level searches

This chapter includes the following topics:

About application-level searches

With the application-level search feature, you can create an application-wide searches that can run in a single or multiple departments. This feature is useful when you want to run the same search in multiple departments, with same criteria - be it date-range, hotword, keywords, and so on. When the search runs in the selected departments, the author and recipient information will be based on the individual departments.

To create and manage application-level searches, you must possess the *Application Search* and *Search Capture* permissions. By default, the *App Rule Admin* role have these permission. However, administrator can assign you these permissions on demand.

You can search for the items that meet certain criteria and later review these items. The search operations are based on terms like subject, tags, content, sender, recipient, dates, communication direction, and so on.

To view the search result and status, select the **Searches** tab of the department in which the search is executed. Application-level searches can be rejected and resubmitted from the **Searches** tab of the individual departments.

You can create Guaranteed Sample searches and Scheduled searches only, and not the Immediate searches. Configure search schedules if you want to run searches at set times or set up the recurrent searches that run automatically.

If you want to search certain words or phrases in the searched items, you can create a set of hotwords. When defining the search criteria, you can select these hotwords and hotword sets. Insight Surveillance searches for the selected hotwords in subject and content of searched items.

Viewing existing application-level searches

To view existing application-level searches

1 In the left navigation pane, click **Application**.

2 Navigate to the **Searches** tab.

All the available searches appear.

3 Search for and select the search. If required, perform any of the following steps:

- To navigate to the next or previous pages, use the navigation arrows available in the bottom right corner of the application.
- To find the required search, in the **Filter by search name** field, enter the keywords that characterize the search names that you want to search for, and then press ENTER on a keyboard or click the **Search** icon.

Note: Do not use the wildcard characters (Asterisk or question mark) for partial searching. It does not give you the result.

- To filter to the required search, click the **Filter** icon. Select the search type(s). Currently, you can search from the *Guaranteed Sample Searches*, *Scheduled Searches*, and *Immidiate Searches*. If required, specify the date range when the search was created, and click **Apply Filters**.
- Click **Reset Filters** to reset applied filters back to the default filter.
- Click **Clear Filters** to remove applied filters.
- If required, click **Refresh** to update the data on the **Searches** page.

4 Click on the search name to view the search details.

Creating and running application-level searches

To understand the prerequisites, See "About application-level searches" on page 155.

To create and run an application-level search

1 In the left navigation pane, click **Application**.

2 In the **Searches** tab, click **New Search**.

The **Create New Search** dialog box appears. If the sections in this dialog box are in the collapsed state, expand them to view the corresponding fields.

3 In the **Search Type** section, specify the relevant information in the following fields.

The **New Search** dialog box appears. This section identifies the search and specifies when it runs.

Search In	Displays the departments in which the search will run. In the case of an application-wide search, by default this value is <*All Departments*>.
Based on search	Select an existing search as the basis on which you can set the criteria for the new search.
Search Type	Select the type of search as needed. ■ Select the **Scheduled** option to specify a period during which the search is to run. Specify the schedule run start date and end date. ■ Select the **Guaranteed Sample** option to run the search at the selected sampling time, which is 1:00 A.M. by default. Select the **Enabled** check box to enable the search.
Name	Type a name for the search.
Include items already in review	Select this check box to specify whether the search results can include the items you previously captured and added to this department's review set. This option does not apply to the items you previously included in the review sets for other departments. For an immediate search or scheduled search, you can select this box to ensure that the results include the items that may already be in review from other searches.
Search Schedule	Select a required search schedule based on which the search runs at set times or set intervals.
Schedule run start date	Select a date on which the search needs to run.

Schedule run end date	Select a date on which the search needs to stop running.

4 In the **Sampling** section, specify the relevant information in the following fields.

This section lets you sample the search results and add a random selection of items to the review set.

Sampling percentage	Specify the percentage of search results to include in the review set. You can specify fractions, as in 10.25. You cannot change the sampling percentage if the owner of the department has locked this setting in the department properties.
Set minimum items per author	Specify the minimum number of items per author to include in the review set. If there are no items for an author in the search results, none can be included in the sample. Note: As the authors can be from outside the selected department, searches may return more results.
Set absolute item limit	Specify an upper limit on the total number of search results to add to the review set. This option takes precedence over any values that you set in the **Sampling percentage** field.

5 In the **Date range** section, specify the relevant information in the respective fields.

This section lets you search for items according to when they were sent or received.

Specific date range	Specify the date and time duration to search items that were sent or received during the selected period.
Today / Yesterday / Last 7 days / Last 14 days / Last 28 days	The date ranges are relative to when the search runs, which is today in the case of an immediate search. You may find these options useful when creating a scheduled, recurrent search that runs once every day, week, two weeks, or four weeks. For example, if the search runs once a week, select **Last 7 days** to limit the range to the days since the search last ran.
Since search last ran	For a scheduled search only, lets you search the new items that have arrived since the last time you ran the search. This option is similar to options such as Today and Yesterday. However, it lets you set an explicit start date for the first run of the search. By default, this option searches from the date of the last run (or the start date for the first search) to the current day minus 1 (that is, up to yesterday).

6 In the **Authors and recipients** section, specify the relevant information in the following fields.

This section targets the departments for the search and the direction of the items to search. Any departments that you have organized into partitions can only search items to and from departments in the same partition.

Message Route

Specify the departments you wish to search as well as the direction of the items you wish to search. Search for the items that are **to** or **from** the selected departments, and for the items that have traveled **between** the selected departments and other departments.

You can search for the items that follow the following message route:

- **Between "the specified department" and**
  - custom addresses / domains
  - any department within the organization
  - department outside the organization
  - department internal AND/OR External to organization
- **TO "the specified department" from**
  - custom addresses / domains
  - any department within the organization
  - department outside the organization
  - department internal AND/OR External to organization
- **FROM "the specified department" to**
  - custom addresses / domains
  - any department within the organization
  - department outside the organization
  - department internal AND/OR External to organization

Any of / All of

To search within department tags, select a department. To search within the **To**/**From** fields, only select the employees.

You can expand the department tag to select monitored employees. If there are a large number of employees in the department, you can click the search icon in front of the department tag, which opens a new window where you can search and select monitored employees.

Use inheritance, automatically include new departments

Specify whether to apply the search to the subdepartments of the selected departments.

By default, any new departments that are subdepartments of others automatically inherit any active, recurring searches that are applied to those departments. This is also true of any existing departments that you move under departments that have recurring searches.

Department tree

Specify the departments you want to include in the search. Click the arrows to the left of the department names to expand them and view the nested departments.

Freeform email addresses / domains	This field is available for all possible message routes. Type one or more email addresses and domains. Type each address or domain on a line of its own to search for the items where the **From**, **To**, **CC**, or **BCC** fields contains any of the addresses or domains. Type all the addresses and domains on a single line to search for items in which they are all present. Place the minus sign (-) in front of an address or domain to exclude it from the search. To exclude multiple addresses or domains, type them all on a single line. Note: You can use **Freeform email addresses / domains** to search for email addresses associated with the user accounts but now use the discontinued domain. To search for previously monitored employees, you should use **department internal AND/OR External to organization** message route, and then use the **Freeform email addresses / domains** option to provide email addresses or domains.

7 In the **Search terms** section, specify the relevant information in the following fields.

This section specifies the words or phrases for which the application should search in the subject lines of items and their bodies. By default, when you search for words in both the subject of an item and its content, the application finds those items that meet one or both criteria. However, it is possible to set up the application so that only those items that meet both criteria are found.

Subject

Type the keywords or phrases to be searched in the review items either in their subject lines or in the file names of their attachments. Press **Enter** to separate keywords and phrases from each other.

Alternatively, click **Hotwords** to select hotword sets and keywords.

If the department has a parent department, you can select hotwords/hotword sets from the current department and its parent department and global hotwords/hotword sets. Hotwords/hotword sets from any of the closed parent departments will not be available for selection. The application searches hotwords/hotword sets from both departments and its parent department and global hotwords/hotword sets.

Note:

- Use an asterisk (*) wildcard to represent zero or more characters in your search. Use a question mark (?) wildcard to represent any single character. A wildcard search always finds items that match your search criteria and that were archived in Insight Surveillance.
- Use a minus sign (-) to indicate you want to exclude from the search results any items that contain the following word or phrase.
  For example, the search to find the items that contain the word 'Agent', but do not contain the word 'Cost':
  Agent AND -"Cost"
- A search term cannot comprise an excluded word or phrase only. When you specify such words or phrases, you must also specify a positive word or phrase you want to appear in the search results.
- A search term cannot start with any of the following characters on any line: = + - @. For example,
  "Agent AND -Cost" is a valid search term but "-Cost Agent" is not.
- Insight Surveillance ignores any non-alphanumeric characters in the search term, except for those that have special significance, such as the plus sign, minus sign, and question mark. For example, a search for the term US@100 may find instances not only of US@100 but also of US 100 and US$100. Including non-alphanumeric characters in the search term may therefore return more results than you expect.

Content

Specify the keywords or phrases to be searched in the content of review items.

Alternatively, click **Hotwords** to select hotword sets and keywords.

8 In the **Attachments** section, specify the relevant information in the respective fields.

This section lets you search for items of a certain size and type or that have the specified retention category.

Number — Specify the required number of attachments.

You can search the items with specific number and type of attachments. The default option, **Does not matter**, means that the item can have zero or more attachments.

All following other options require you to type one or two values that specify the required number of attachments:

- **Equals**: requires a specific number of attachments.
- **Between**: requires the number of attachments messages must have to a value between those to be specified.
- **Less than**: requires a number of attachments below the number specified.
- **Greater than**: requires any number of attachments greater than the number specified.

File extensions — Specify the file name extensions of particular types of attachments for which to search. Separate the extensions with space characters.

For example, type the following to search for items with HTML or Microsoft Excel file attachments:.htm .xls.

9 In the **Miscellaneous** section, specify the relevant information in the respective fields.

This section lets you search for items of a certain size and type or that have the specified retention category.

Message size — Specify the size in kilobytes of each item for which to search, as reported by the message store (Exchange, Domino, and so on). The item size includes the size of any attachments.

The following options are available:

- **Does not matter**: any number from 0 upward can be attached.
- **Equals**: requires a specific number of attachments.
- **Between**: requires the number of attachments messages must have to a value between those to be specified.
- **Less than**: requires a number of attachments below the number specified.
- **Greater than**: requires any number of attachments greater than the number specified.

Message type	Displays a list of configured and enabled content sources for the customer. Select the **All content sources** check box to consider messages from all types of content sources simultaneously. When this option is selected, other options remain disabled. To select specific message type, clear the **All content sources** check box, and select one or more required options from the content sources available in the list.
Trash option	Select the appropriate option to search for items in trash: ■ **Ignore trash** - does not search for items in the trash. ■ **Include trash** - searches for items in other specified options along with the items in trash. ■ **Trash only** - only searches for items in trash.

10 In the **Tags** section, specify the relevant information in the respective fields.

This section lets you search for items according to the tags with which any additional policy management software has classified them.

Filter

Select any of the following options to search for the items that match certain classification policies. There are several types of policies:

- **Inclusions only**: Select this option to include items that your policy management software has classified for inclusion in the review set that may contain the most serious offenses, such as swearing, racism, or insider trading.
- **Ignore inclusions**: Select this option to ignore items that Arctera Insight Classification has classified for inclusion in the review set that may contain the most serious offenses, such as swearing, racism, or insider trading.
- **Exclusions only**: Select this option to include spam items and newsletters that your policy management software may classify for exclusion from the review set.
- **Ignore exclusions**: Select this option to ignore spam items and newsletters that your policy management software may classify for exclusion from the review set.
- **Categories only**: Select this option to include categorized items that exhibit certain characteristics, such as containing Spanish text. This type of policy provides no information on whether an item should be included in or excluded from the review set.
- **Ignore inclusions and exclusions**: Select this option to ignore inclusion and exclusion items.
- **Custom**: Select this option and type the names of one or more policies. Separate multiple tag names with commas, like this: CustomTag1,CustomTag2
- **All**: Select this option to include all tags.

Note: Arctera Insight Classification is required to classify items based on their content and metadata. Implementing Insight Classification requires additional charges.

Name

Select tag names. Separate multiple tag names with commas, like this:

CustomTag1,CustomTag2

11 In the **Intelligent Review** section, choose options for the learning engine in Insight Surveillance.

This engine allows Insight Surveillance to search for items intelligently, based on the actions that reviewers have taken on earlier items. For example, after a reviewer has marked a spam message or out-of-office reply as irrelevant then, when Insight Surveillance detects other items that have similar characteristics, it can handle them in the same way.

Note: Searches that use the intelligent review feature may take slightly longer to complete than those that do not use this feature.

Searches, by default, consider metadata and content of items to determine the relevance. However, if search results contain items that are older than 30 days, only metadata is considered to determine the relevance.

The options for **Learning behavior** are as follows:

None	Insight Surveillance searches for items in the normal way, without implementing Intelligent Review. This is the default option.
Search and prioritize	Insight Surveillance searches for both relevant items and irrelevant items without favoring one over the other. So, if your chosen **Sampling percentage value requires that you capture and review 10% of items**, Insight Surveillance captures 10% - but a substantial number of the items may be irrelevant. With this option, however, Insight Surveillance does give the items a status of either **Unreviewed (Irrelevant)** or **Unreviewed (Relevant)** as it adds them to the review set. When you later review the items in the **Review** pane, you can filter them by their **Unreviewed** status to distinguish between the relevant and irrelevant items.
Search and then sample ONLY relevant content	Insight Surveillance searches across all the items and captures the relevant ones only, until it has captured the required percentage. So, if your chosen **Sampling percentage value requires that you capture and review 10% of items**, Insight Surveillance captures 10% - all of them considered to be relevant. If there are too few relevant items to fulfil the chosen sampling percentage, Insight Surveillance does not supplement them with irrelevant items. This is an important difference between this option and the equivalent option, Sample exact percentage of ONLY relevant content, in the **Department Properties** pane.

12 Click **Save**.

Note: When more than 500 departments are selected in an application search, the search gets disabled for performance reason. Navigate to **Application** > **Searches** > **Edit** to confirm departments, and then enable the search.

Editing application-level searches

To edit an application-level search

1. In the left navigation pane, click **Application**.
2. Click the **Searches** tab.

   A list of available application-level searches appears.
3. Search for and select the search that you want to update.

   A few details such as a name of a search creator, search creation date, search type, and a search status (enabled/disabled) are displayed.
4. Click the **Edit** icon in the same row.
5. Update the details under the corresponding sections.
6. Click **Save**.

Excluding departments from application searches

You can customize application searches by excluding certain departments if you do not want to search them for any reason. After excluding the department, the application skips searching items within it.

To include the department in the search again, you can remove the department from the excluded departments list. See "Reinstating the excluded department for application searches" on page 168.

To exclude departments from application searches

1. In the left navigation pane, click **Application**.
2. In the **Searches** tab, click **Exclude Department**.

   A list of excluded departments is displayed.

   - Use arrows at the bottom of the page to navigate between pages, if the list is large.
   - Hover over icons in the **Status** column to view each department's current status (open, closed, active, or inactive).
   - Click the **Remove department** icon in the row to include the department in the search again.

- Click **Back** to access the **Searches** page.

3 To exclude additional departments, click **Add**.

The **Select Departments To Exclude** dialog box appears. It lists all open departments and active exceptions. The departments that are already excluded, closed, or marked for deletion are not displayed.

4 Search for and select the departments that you want to exclude from the application searches, and click **Save**.

Newly excluded departments appear in the list of excluded departments. Optionally, click **Refresh** to update page for the latest records in the list.

Reinstating the excluded department for application searches

To include the department in the search again, you can remove the department from the excluded departments list.

To reinstate/include departments for application searches

1 In the left navigation pane, click **Application**.

2 In the **Searches** tab, click **Exclude Department**.

A list of excluded departments is displayed.

3 Select a single or multiple departments that you want to include in application searches again.

4 Perform any of the following as necessary:

- Click **Remove** on the action bar.
- Click the **Remove department** icon in the selected department's row.

Note: Clicking **Remove** on the action bar allows you to remove one or multiple departments. In contrast, clicking the **Remove department** icon in a specific department row removes only that particular department.

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.

Chapter 16

Managing application-specific hotword sets

This chapter includes the following topics:

Overview

Hotwords are predefined words or phrases that you can search for in employee items. When you create a search, you can add and select hotwords to search for in the subject lines of items, their content, or both.

To simplify the management of application-specific hotwords, you can group them into hotword sets. For example, you can use one set of hotwords to monitor items for unacceptable language and another set to monitor them for unethical business practice. You can define hotwords and hotword sets that can be used at the application level, where they are applicable to all departments.

You must have the application-level *Add Hotwords* permission to add global hotwords. By default, users that have the *App Rule Admin* role have this permission.

Creating application-specific hotword sets

To create an application-specific hotword set

1 In the left navigation pane, click **Application**.

2 Navigate to the **Hotwords** tab.

3 Click **New Hotword Set**.

The **Create Hotword Set** dialog box appears.

4 In the **Name** and **Description** fields, type a unique name and an optional description for the hotword set respectively.

Note: The hotword set name can contain up to 50 characters. The description can contain up to 250 characters.

---

5 Under **Hotwords** section, click **Select Hotwords** to search and choose hotwords from the available list.

Note: To select multiple adjacent words, hold down the Shift key and click the first and the last words in the range. To select multiple, non-adjacent words, hold down the Ctrl key and click the required words.

---

6 If the required hotword is not available, click **Create Hotwords** to add new hotwords.

Before you create hotwords, it is recommended to understand the following rules:

- For a **single word** with a wildcard, do not enclose it in quotes.
  For example, `Test*`, `overprice*`, `mis?sell`

Note: It is recommended to limit hotword length to 100 characters.

- For **multiple words**, enclose them in double quotes.
  For example, `"search criteria"`, `"search * * criteria"`, `"te?st vas"`
- For **negation conditions**, add the keyword *AND* before the first negation term, ensuring there is a space before and after *AND*.
  For example, `search* AND -"search criteria"`, `test* AND -"test crit?ria" -"te?st vas"`, `"search criteria" AND -"search criteria Bloomberg"`.

Note: To prevent inconsistent search results and improve search accuracy while using multiple negation conditions, the hotword length can be extended up to a maximum of 2,000 characters.

To add multiple hotwords simultaneously, press **Enter** after each word to separate the words with a new line character.

7 Click **OK** to add the words.

8 Click **Save**.

9 (Optional) In the **Hotword Set** pane, select a hotword set to view included hotwords on the right side.

Editing application-specific hotwords and hotword sets

To edit an application-specific hotwords and hotword set

1 In the left navigation pane, click **Application**.

2 Navigate to the **Hotwords** tab.

3 Select the hotword set you want to modify, and then click **Edit Hotword Set**.

The **Edit Hotword Set** dialog box appears.

4 In the **Name** and **Description** fields, type a unique name and an optional description for the hotword set respectively.

Note: The hotword set name can contain up to 50 characters. The description can contain up to 250 characters.

5 In the **Hotwords** section, you can perform the following tasks:

- To add new hotwords, click **Create Hotwords**.
- To add existing hotwords, click **Select Hotwords**.
- To remove the selected hotword, click **Remove from Set**.
  After you successfully perform any of these tasks in this section, an alert message box appears to indicate that the hotword set is updated.

6 Click **OK**.

Deleting application-specific hotword sets

To delete an application-specific hotword set

1. In the left navigation pane, click **Application**.
2. Navigate to the **Hotwords** tab.
3. Select the hotword set you want to delete.
4. Click **Delete Hotword Set**.

   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.

Chapter 17

Managing application-specific labels

This chapter includes the following topics:

Searching application-specific labels, label groups, and single choice groups

To search for existing application-specific label, label group, and single choice group

1. In the left navigation pane, click **Application**.
2. Navigate to the **Labels** tab.

   All the available application-specific labels, label groups, and single choice groups appear.
3. Search for and select the label you want to view. If required, perform any of the following steps:
   - To navigate to the next or previous pages, use the navigation arrows available in the bottom right corner of the application.
   - To find the required label, in the **Filter by name** field, enter the keywords that characterize the label names that you want to search for, and then press ENTER on a keyboard or click the **Search** icon.

Note: Do not use the wildcard characters (Asterisk or question mark) for partial searching. It does not give you the result.

- To filter to the required labels, click the **Filter** icon. Set the filter criteria by selecting type options and activation/deactivation status. If required, specify the date range when the label, label group, or single choice group was created, and click **Apply Filters**.
- Click **Reset Filters** to reset applied filters back to the default filter.
- Click **Clear Filters** to remove applied filters.
- If required, click **Refresh** to update the data on the **Labels** page.

4 Click on the label, label group, or single choice group name to view its details.

Managing application-specific labels

Application-specific labels management covers creating, editing, deleting, activating, deactivating, propagating, and unpropagating operations. You must have the *Manage Labels* permissions to perform these operations. By default, the *App Rule Admin* and *Compliance System Admin* have these permission.

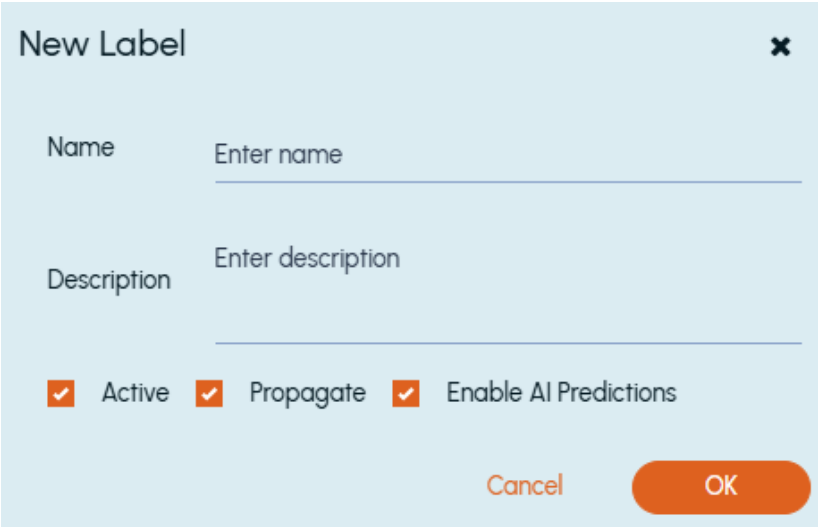
Creating application labels

To create an application label

1 In the left navigation pane, click **Application**.

2 Navigate to the **Labels** tab, and then click **New**.

The **New Label** dialog box appears.



3 In the **Name** filed, type a unique label name.

4 In the **Description** field, provide a description of this label.

5 Select the **Active** check box to activate the label.

Remember that -

- Only the active labels can be enabled for AI predictions, therefore, the **Enable AI Predictions** check box remains disabled until the label is activated.
- Do not select the **Active** check box if you want to keep the label in the deactivated state.

6 Select the **Propagate** check box to ensure the sub-departments inherit this label.

Do not select the check box if you do not want to propagate this label to sub-departments.

7 Select the **Enable AI Predictions** check box to consider this label for AI Prediction.

Note: At application level, only 20 active labels (including single choice group labels) can be enabled for AI predictions. Upon deactivation, the previously AI prediction-enabled labels and label groups get disabled.

---

8 Click **OK**.

Editing application labels

To edit an application label

1 In the left navigation pane, click **Application**.

2 Navigate to the **Labels** tab.

3 Search for the label that you want to update. See "Searching application-specific labels, label groups, and single choice groups" on page 173.

4 Select the label that you want to edit, and click the **Edit** icon in the same row.

5 In the **Edit Label** dialog box, update the details of the required fields.

6 Click **OK**.

Activating application labels

To activate an application label

1 In the left navigation pane, click **Application**.

2 Navigate to the **Labels** tab.

3 Search for the deactivated label that you want to activate.

See "Searching application-specific labels, label groups, and single choice groups" on page 173.

4 Select the label and do any of the following steps:

- On the action bar, click **Activate**.
- Click the **Edit** icon in the same row. In the **Edit Label** dialog box, select the **Active** check box.

Note: At application level, only 20 active labels (including single choice group labels) can be enabled for AI predictions.

The updated data appears on the **Labels** page. If required, click **Refresh** on the action bar.

Deactivating application labels

To deactivate an application label

1. In the left navigation pane, click **Application**.
2. Navigate to the **Labels** tab.
3. Search for the active label that you want to deactivate.

   See "Searching application-specific labels, label groups, and single choice groups" on page 173.
4. Select the label and do any of the following steps:
   - On the action bar, click **Deactivate**.
   - Click the **Edit** icon in the same row. In the **Edit Label** dialog box, clear the **Active** check box.

   Deactivating a label or label group disables AI predictions for that label or label group.

   The updated data appears on the **Labels** page. If required, click **Refresh** on the action bar.

Propagating application labels

To propagate an application label

1. In the left navigation pane, click **Application**.
2. Navigate to the **Labels** tab.
3. Search for the unpropagated label that you want to propagate.
4. Select the label and do any of the following steps:
   - On the action bar, click **Propagate**.
   - Click the **Edit** icon in the same row. In the **Edit Label** dialog box, select the **Propagate** check box.

   The updated data appears on the **Labels** page. If required, click **Refresh** on the action bar.

Unpropagating application labels

To unpropagate an application label

1. In the left navigation pane, click **Application**.
2. Navigate to the **Labels** tab.

3 Search for the propagated label that you want to unpropagate.

4 Select the label and do any of the following steps:

- On the action bar, click **Unpropagate**.
- Click the **Edit** icon in the same row. In the **Edit Label** dialog box, clear the **Propagate** check box.

The updated data appears on the **Labels** page. If required, click **Refresh** on the action bar.

Deleting application labels

To delete an application label

1 In the left navigation pane, click **Application**.

2 Navigate to the **Labels** tab.

3 Search for the label that you want to delete.

4 Select the label, and click **Delete** on the action bar.

Managing application-specific label groups

Application-specific label groups management covers creating, editing, deleting, activating, deactivating, propagating, and unpropagating operations. You must have the *Manage Labels* permissions to perform these operations. By default, the *App Rule Admin* and *Compliance System Admin* have these permission.

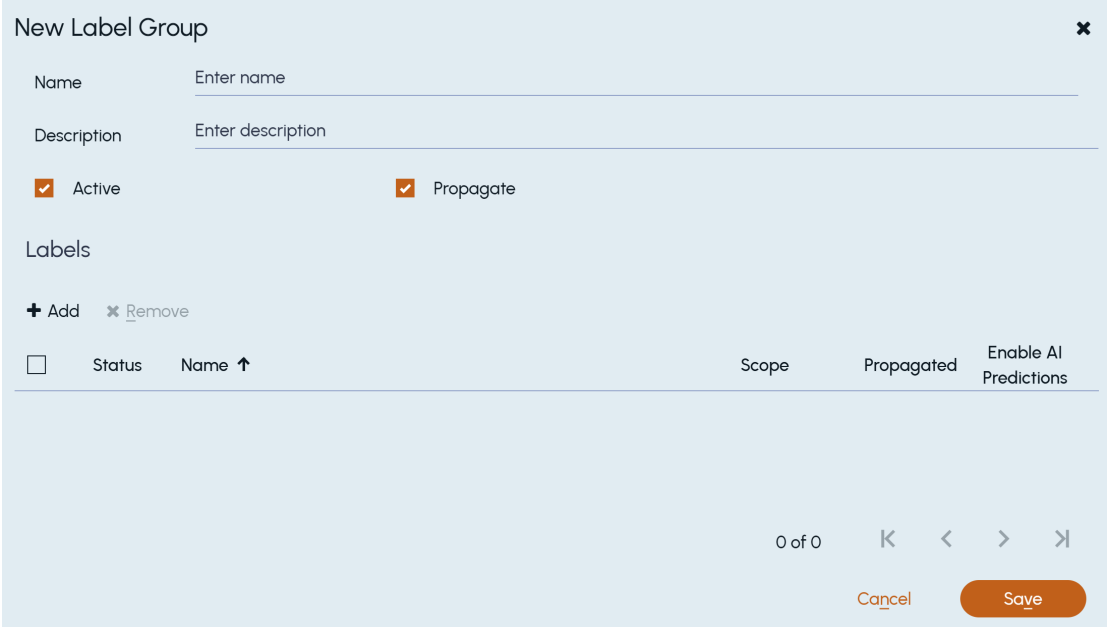
Creating application-specific label groups

To create an application-specific label group

1 In the left navigation pane, click **Application**.

2 Navigate to the **Labels** tab, and then click **New Group**.

The **New Label Group** dialog box appears.



3 In the **Name** filed, type a unique label name.

4 In the **Description** field, provide a description of this label.

5 Select the **Active** check box to activate the label.

Do not select the check box if you want to keep the label in the deactivated state.

Note: The **Enable AI Predictions** check box is not shown for the customer level label groups because each label within the group can be enabled while creating or editing them individually.

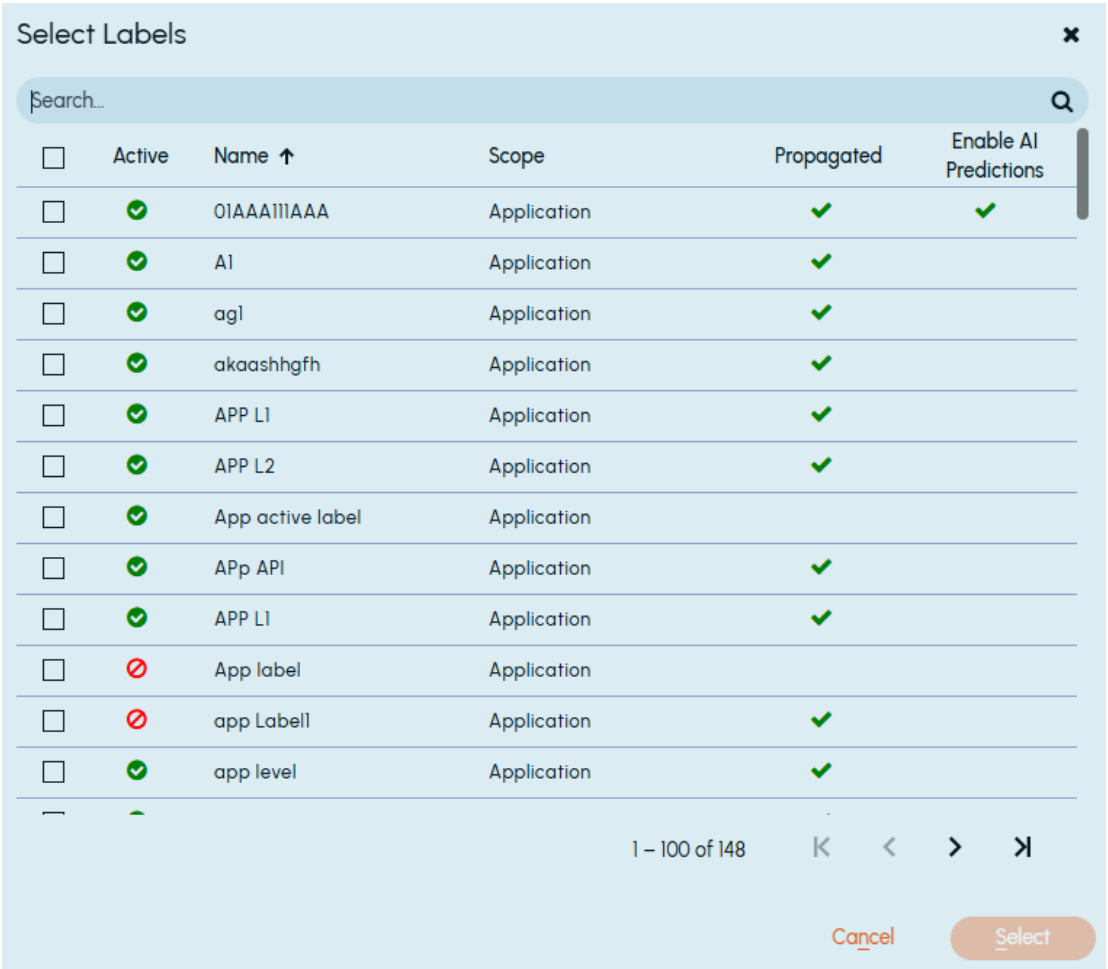
---

6 Select the **Propagate** check box to ensure the sub-departments inherit this label.

Do not select the check box if you do not want to propagate this label to sub-departments.

7 Click **Add** to open the **Select Labels** dialog box.

8 Search for and select the labels that you want to this label group, and click **Select** as shown in the sample image below.



9 Click **Save**.

Editing application-specific label groups

To edit an application-specific label group

1 In the left navigation pane, click **Application**.

2 Navigate to the **Labels** tab.

3 Search for the label group that you want to update. See "Searching application-specific labels, label groups, and single choice groups" on page 173.

4 Select the label group and click the **Edit** icon in the same row.

5 In the **Edit Label Group** dialog box, update the details of the required fields or add or remove labels.

6 Click **Save**.

Activating application-specific label groups

To activate an application-specific label group

1 In the left navigation pane, click **Application**.

2 Navigate to the **Labels** tab.

3 Search for the deactivated label group that you want to activate.

See "Searching application-specific labels, label groups, and single choice groups" on page 173.

4 Select the label group and do any of the following steps:

- On the action bar, click **Activate**.
- Click the **Edit** icon in the same row. In the **Edit Label Group** dialog box, select the **Active** check box.

The updated data appears on the **Labels** page. If required, click **Refresh** on the action bar.

Deactivating application-specific label groups

To deactivate an application-specific label group

1 In the left navigation pane, click **Application**.

2 Navigate to the **Labels** tab.

3 Search for the active label group that you want to deactivate.

See "Searching application-specific labels, label groups, and single choice groups" on page 173.

4 Select the label group and do any of the following steps:

- On the action bar, click **Deactivate**.

- Click the **Edit** icon in the same row. In the **Edit Label Group** dialog box, clear the **Active** check box.

The updated data appears on the **Labels** page. If required, click **Refresh** on the action bar.

Propagating application-specific label groups

To propagate an application-specific label group

1. In the left navigation pane, click **Application**.
2. Navigate to the **Labels** tab.
3. Search for the unpropagated label group that you want to propagate.
4. Select the label group and do any of the following steps:
   - On the action bar, click **Propagate**.
   - Click the **Edit** icon in the same row. In the **Edit Label Group** dialog box, select the **Propagate** check box.

   The updated data appears on the **Labels** page. If required, click **Refresh** on the action bar.

Unpropagating application-specific label groups

To unpropagate an application-specific label group

1. In the left navigation pane, click **Application**.
2. Navigate to the **Labels** tab.
3. Search for the propagated label group that you want to unpropagate.
4. Select the label group and do any of the following steps:
   - On the action bar, click **Unpropagate**.
   - Click the **Edit** icon in the same row. In the **Edit Label Group** dialog box, clear the **Propagate** check box.

   The updated data appears on the **Labels** page. If required, click **Refresh** on the action bar.

Deleting application-specific label groups

To delete an application-specific label group

1. In the left navigation pane, click **Application**.
2. Navigate to the **Labels** tab.

3 Search for the label group that you want to delete.

4 Select the label group, and click **Delete** on the action bar.

Managing application-specific single choice label groups

Application-specific single choice label groups management covers creating, editing, deleting, activating, deactivating, propagating, and unpropagating operations. You must have the *Manage Labels* permissions to perform these operations. By default, the *App Rule Admin* and *Compliance System Admin* have these permission.

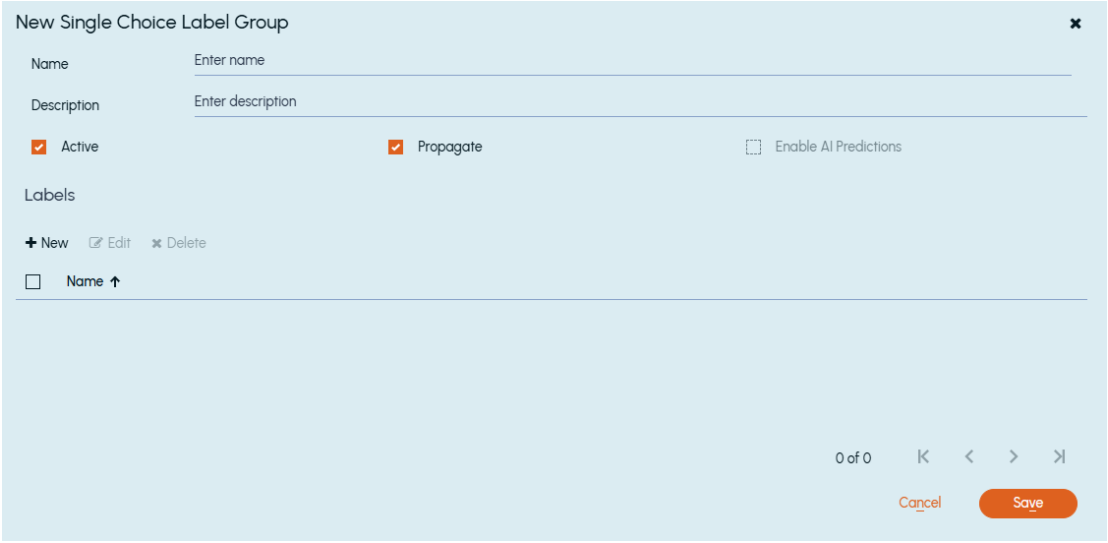
Creating application-specific single choice label groups

To create an application-specific single choice label group

1 In the left navigation pane, click **Application**.

2 Navigate to the **Labels** tab, and then click **New Single Choice Group**.

The **New Single Choice Label Group** dialog box appears.



3 In the **Name** filed, type a unique single choice label group name.

4 In the **Description** field, provide a description of this single choice label group.

5 Select the **Active** check box to activate the single choice label group.

Remember that -

- Only the active single choice label groups can be enabled for AI predictions, therefore, the **Enable AI Predictions** check box remains disabled until this group is activated.
- Do not select the **Active** check box if you want to keep the single choice label group in the deactivated state.

6 Select the **Propagate** check box to ensure the sub-departments inherit this single choice label group.

Do not select the check box if you do not want to propagate this single choice label group to sub-departments.

7 Select the **Enable AI Predictions** check box to consider this single choice label group for AI Prediction.

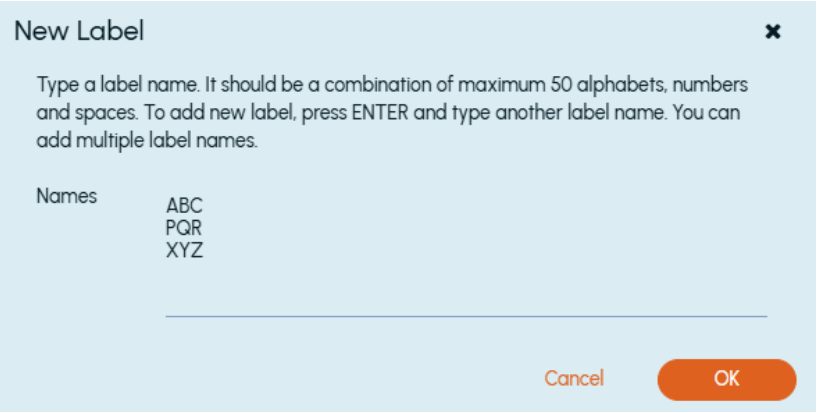
Note: At application level, only 20 active labels (including single choice group labels) can be enabled for AI predictions. Upon deactivation, the previously AI prediction-enabled labels and label groups get disabled.

---

8 Click **Add** to open the **New Label** dialog box.

9 Manually type new labels, and click **OK**.

Note: New label names must be a combination of maximum 50 characters that includes alphabets, numbers and spaces. After adding a label name, press ENTER to add the next label. You can add multiple label names as shown in the sample image below.



10 Click **Save**.

Editing application-specific single choice label groups

To edit an application-specific single choice label groups

1 In the left navigation pane, click **Application**.

2 Navigate to the **Labels** tab.

3 Search for the single choice label group that you want to update. See "Searching application-specific labels, label groups, and single choice groups" on page 173.

4 Select the single choice label group, and click the **Edit** icon in the same row.

5 In the **Edit Single Choice Label Group** dialog box, update the details of the required fields.

If required, select an individual label and do any of the following:

- Click **Edit** to update the label name.
- Click **Delete** to remove the label entry from the group.

6 Click **Save**.

Activating application-specific single choice label groups

To activate an application-specific single choice label group

1 In the left navigation pane, click **Application**.

2 Navigate to the **Labels** tab.

3 Search for the deactivated single choice label group that you want to activate.

See "Searching application-specific labels, label groups, and single choice groups" on page 173.

4 Select the single choice label group and do any of the following steps:

- On the action bar, click **Activate**.
- Click the **Edit** icon in the same row. In the **Edit Single Choice Label Group** dialog box, select the **Active** check box.

Note: At application level, only 20 active labels (including single choice group labels) can be enabled for AI predictions.

The updated data appears on the **Labels** page. If required, click **Refresh** on the action bar.

Deactivating application-specific single choice label groups

To deactivate an application-specific single choice label group

1 In the left navigation pane, click **Application**.

2 Navigate to the **Labels** tab.

3 Search for the active single choice label group that you want to deactivate.

See "Searching application-specific labels, label groups, and single choice groups" on page 173.

4 Select the single choice label group and do any of the following steps:

- On the action bar, click **Deactivate**.
- Click the **Edit** icon in the same row. In the **Edit Single Choice Label Group** dialog box, clear the **Active** check box.

Deactivating a single choice label group disables AI predictions for that single choice label group.

The updated data appears on the **Labels** page. If required, click **Refresh** on the action bar.

Propagating application-specific single choice label groups

To propagate an application-specific single choice label group

1. In the left navigation pane, click **Application**.
2. Navigate to the **Labels** tab.
3. Search for the unpropagated single choice label group that you want to propagate.
4. Select the single choice label group and do any of the following steps:
   - On the action bar, click **Propagate**.
   - Click the **Edit** icon in the same row. In the **Edit Single Choice Label Group** dialog box, select the **Propagate** check box.

   The updated data appears on the **Labels** page. If required, click **Refresh** on the action bar.

Unpropagating application-specific single choice label groups

To unpropagate an application-specific single choice label group

1. In the left navigation pane, click **Application**.
2. Navigate to the **Labels** tab.
3. Search for the propagated single choice label group that you want to unpropagate.
4. Select the single choice label group and do any of the following steps:
   - On the action bar, click **Unpropagate**.
   - Click the **Edit** icon in the same row. In the **Edit Single Choice Label Group** dialog box, clear the **Propagate** check box.

   The updated data appears on the **Labels** page. If required, click **Refresh** on the action bar.

Deleting application-specific single choice label groups

To delete an application-specific single choice label group

1. In the left navigation pane, click **Application**.
2. Navigate to the **Labels** tab.
3. Search for the single choice label group that you want to delete.
4. Select the single choice label group, and click **Delete** on the action bar.

Chapter 18

Managing application-specific trash rules

This chapter includes the following topics:

Overview

Trash rules let you define when to ignore or include inbound items from specific email addresses or domains.

Trash rules are used during search. By default, a trash rule causes items coming in from specified email addresses or domains to be omitted from search results.

You can define trash rules to be used at the application level, but they can be propagated to sub-departments. Application-specific trash rules can be deactivated at the application level. A deactivated department trash rule does not modify the original application trash rule. Trash rules cannot be deleted or modified; they can only be deactivated.

Note: You must have the application-level *Manage Trash Rules* permission to add application-specific trash rules. By default, users that have the *Rule Admin* role have this permission.

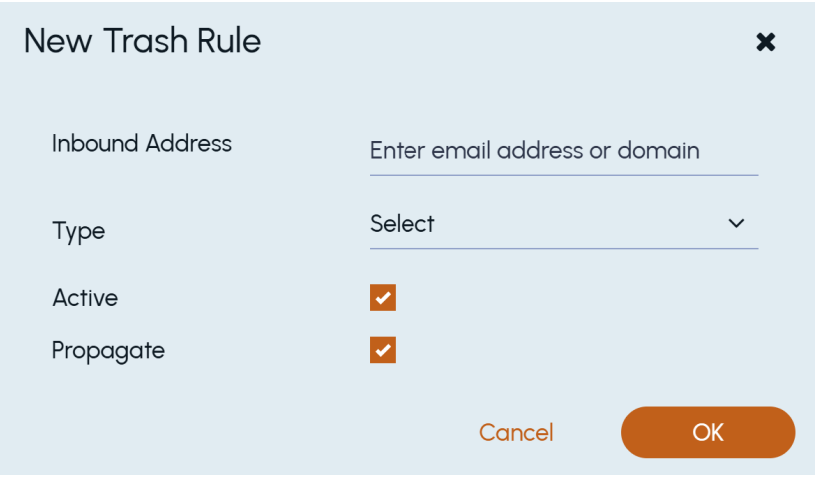
Creating application-specific trash rules

To create an application-specific trash rule

1 In the left navigation pane, click **Application**.

2 Navigate to the **Trash** tab, and then click **New**.

The **New Trash Rule** dialog box appears.



3 In the **Inbound Address** filed, type an email address or domain.

Note: When you specify a domain, do not add the @ symbol.

4 In the **Type** field, select a **Domain** or an **Email Address**.

5 Select the **Status** check box to activate the rule.

Do not select the check box if you want to keep the rule in the deactivated state.

6 Select the **Propagate** check box to ensure the sub-departments inherit the rule.

Do not select the check box if you do not want to propagate rule to sub-departments.

7 Click **OK**.

Activating application-specific trash rules

To activate an application-specific trash rule

1 In the left navigation pane, click **Application**.

2 Navigate to the **Trash** tab.

3 Select a deactivated trash rule you want to activate and click **Activate** on the action bar.

Deactivating application-specific trash rules

To deactivate an application-specific trash rule

1 In the left navigation pane, click **Application**.

2 Navigate to the **Trash** tab.

3 Select an activated trash rule you want to deactivate, and click **Deactivate** on the action bar.

Propagating application-specific trash rules

To globally propagate an application-specific trash rule

1 In the left navigation pane, click **Application**.

2 Navigate to the **Trash** tab.

3 Select an unpropagated trash rule you want to propagate and click **Propagate** on the action bar.

Note: This action propagates the trash rule globally to all existing open departments, including any open sub-departments. If a closed department is later opened, any active trash rules configured to propagate will be applied to the department once opened.

Unpropagating application-specific trash rules

To unpropagate an application-specific trash rule

1. In the left navigation pane, click **Application**.
2. Navigate to the **Trash** tab.
3. Select a propagated trash rule you want to unpropagate and click **Unpropagate** on the action bar.

Note: This action removes trash rule globally from all existing open departments, including sub-departments.

Chapter 19

Managing application-specific allowlist rules

This chapter includes the following topics:

Overview

Allowlist rules let you define the text that is contained within the items that are always considered compliant. This functionality does not apply to item attachments.

If Insight Surveillance finds an active word or phrase from the lexicon within allowlisted text, the word or phrase is not flagged. Many customers use this feature to allowlist the disclaimers that appear at the bottom of their outgoing emails. Having the allowlist rule in place means that the disclaimer does not cause an email to be flagged with violations for review.

For example, assume you used the following disclaimer in your email address:

Email that is sent through the Internet is not secure. Do not use email to send us confidential information such as credit card numbers, changes of address, PIN numbers, passwords, or other important information. Do not email orders to buy or sell securities, transfer funds, or send time sensitive instructions. We do not accept such orders or instructions. This email is not an official trade confirmation for the transactions that are executed for your account. Your email message is

not private in that it is subject to review by the Firm, its officers, agents and employees.

You can add the entire paragraph to your allowlist rules so that every outgoing item is not flagged for review since *PIN numbers* and *passwords* are words that could be used as search hotwords. Although this functionality is generally reserved for the outgoing email, you can allowlist words and phrases for any inbound item or instant message.

Note: You must have the *Manage Allowlist Rules Department* permission to add department-specific allowlist rules. By default, users that have the *Rule Admin* role have this permission.

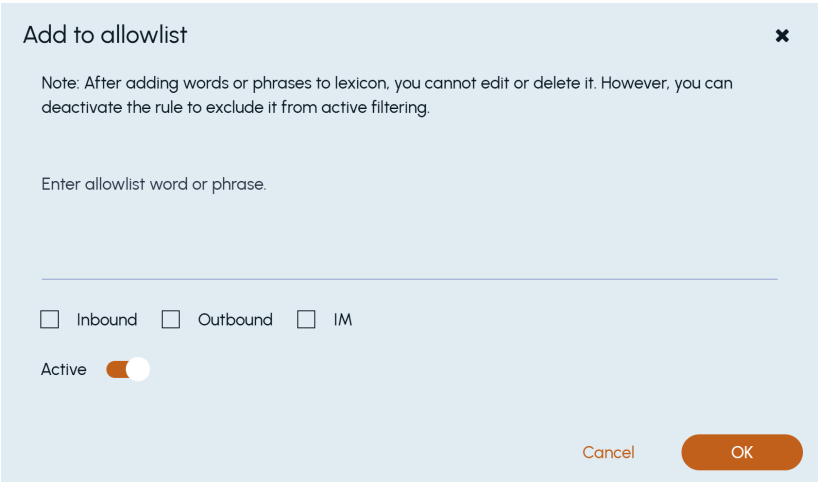
Creating application-specific allowlist rules

To create an application-specific allowlist rule

1 In the left navigation pane, click **Application**.

2 Navigate to the **Allowlist** tab, and click **New**.

The **Add to allowlist** dialog box appears.



3 In the **Enter allowlist word or phrase** field, type a word or phrase.

Note: The allowlist rule can contain up to 1024 characters, but a word should not be longer than 50 characters. After adding words or phrases to the lexicon, you cannot edit or delete it. However, you can deactivate the rule to exclude it from active filtering.

4 To create a allowlist rule, select any or all of the following options:

- Select the **Inbound** check box to apply this allowlist rule to all inbound items.
- Select the **Outbound** check box to apply this allowlist rule to all outbound items.
- Select the **IM** check box to apply this allowlist rule to all instant messages.

Note: Clear the respective check boxes if you do not want to apply rule to Inbound, Outbound, or Instant Messages.

5 Select the **Active** check box to activate the rule.

6 Click **OK**.

Editing application-specific allowlist rules

To edit an application-specific allowlist rule

1 In the left navigation pane, click **Application**.

2 Select an active allowlist rule you want to deactivate, and click the **Edit allowlist** icon.

The **Edit allowlist** dialog box appears.

Note: You cannot change the words or phrases mentioned in the rule.

3 Modify the options to which to apply the allowlist rule: **Inbound**, **Outbound**, or **IM** (Instant Messages).

4 Modify the allowlist rule status to activate or deactivate.

5 Click **OK**.

Chapter 20

Managing application-specific review comments

This chapter includes the following topics:

About application-level review comments

While performing the application-level reviews, sometimes it is tedious for reviewers to type the same comments again and again. To make review process easier, as an administrators and reviewers, you can use the **Review Comments** functionality to save various commonly used comments that can be often used by them.

You can add, edit, and delete such frequently used reviewing comments. The application specific *Manage Reviewing Comments* permission is used to control the application-level review comments, and can be configured from the **Roles and Permissions** section. See "Adding new roles for users (employees) and employee groups" on page 149.

Adding application-level review comments

To add an application-level review comment

1. In the left navigation pane, click **Application**.
2. In the **Review Comments** tab, click **New** to add a new application-level review comment.

   The **New review comment** dialog box appears.
3. Specify the following information:

Summary	Provide a short comment name.
Comment	Provide the actual comment text that describes your comment.

4. Click **Save**.
5. (Optional) On the **Review Comments** page, click **Refresh** to update the page with the latest records.

Editing application-level review comments

To edit an application-level review comment

1. In the left navigation pane, click **Application**.
2. In the **Review Comments** tab, select the reviewing comment that you want to edit, and click the **Edit** icon in the same row.
3. In the **Edit review comment** dialog box, update the following information:

Summary	Provide an updated short comment name, if required.
Comment	Provide the updated comment description for your comment.

4. Click **Save**.
5. (Optional) On the **Review Comments** page, click **Refresh** to update the page with the latest records.

Deleting application-level review comments

To delete an application-level review comment

1. In the left navigation pane, click **Application**.
2. In the **Review Comments** tab, perform any of the following actions:
   - To delete an individual review comment, select the reviewing comment that you want to delete, and click the **Delete** icon in the same row.
     You can select the comments across pages.
   - To delete multiple review comments simultaneously, select the reviewing comments that you want to delete. Click **Delete** on the action bar.
     The application displays number of the selected items in the bottom of the page. You can select maximum 200 comments across pages at a time.
   - To delete all the comments on the page, select the top-most check box in the first column, and click **Delete** on the action bar.

   The application prompts you to confirm that you want to perform the operation.
3. Click **Yes**.
4. (Optional) On the **Review Comments** page, click **Refresh** to update the page with the latest records.

Updating order of application-level review comments

To update order of an application-level review comment

1. In the left navigation pane, click **Application**.
2. In the **Review Comments** tab, ensure that there are more than one comment added.

   Else, the **Update Order** option remains disabled.
3. Click **Update Order**, and select the comment you want to move up or down.
4. Click the up or down arrow next to each item to change their order.

   Alternatively, you can drag and drop items above or below another comment.
5. Click **Save Order**.
6. (Optional) On the **Review Comments** page, click **Refresh** to update the page with the updated order of records.

Chapter 21

Managing data requests

This chapter includes the following topics:

About data request

Insight Surveillance provides the capability to generate data requests to search and export emails (including attachments) in PST format across the entire review set that spans across all departments, specifying various search criteria. The time required to process a data request depends on the size of the review set, the complexity of your query, and the date range.

Insight Surveillance supports data request for emails, but does not support it for the collaboration messages (Microsoft Teams).

Each PST file can contain up to 1.0 GB of emails or 25,000 emails. If your exported data exceeds this limit, Insight Surveillance exports additional PST files.

Note: Only the users with the *Manage Data Request* permission can perform data requests using the **Application** > **Data Request** tab. By default, users that have the *System Administrator* role have this permission.

Creating a new data request

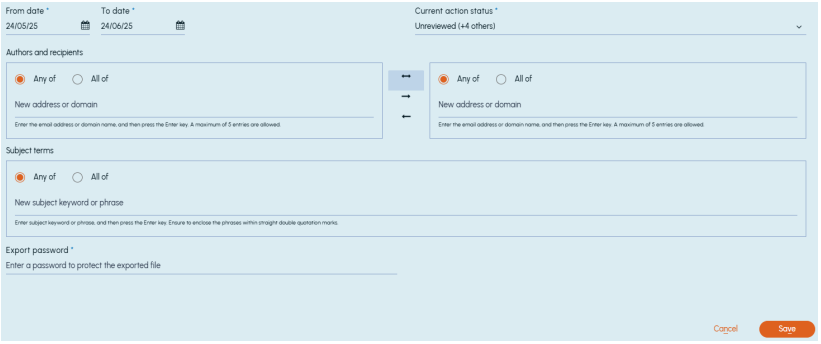
The New data request page is where a data request is created and submitted. This page provides multiple sections where parameters can be defined to fine-tune your search.

To create a new data request

1 In the left navigation pane, click **Application**.

2 Click **Data Request**.

3 Click **New**. The **New data request** window appears.



4 Refer to the following table and provide the relevant information in the respective fields.

Name	Enter a unique name for the data request. This name appears within the **Data Request** page. The data request name is also used as the exported ZIP file name with the number sequence when the user downloads the exported file. Note: The name cannot contain any of the characters: /*?":<>|
From date / To date	Specify the start date and end date of the emails to search.
Current action status	Select items by their action status, such as **Unreviewed**, **Pending**, **Questioned**, **Reviewed Irrelevant**, and **Reviewed Relevant**.

Authors and recipients

Enter the email address or domain name, and then press the **Enter** key.

- Use these fields to filter a search for specific FROM or TO email addresses or domains. Up to five Senders and Recipients can be specified.
- Address or domain must not contain wildcard characters and a space character.
- Addresses on the left side cannot be blank.
- If no address or domain is specified on the right, items will be searched for any internal or external user. If addresses or domains are specified, then items will be searched for any of those addresses or domains.

Select the message direction for email communication between addresses or domains. The three options available are listed below. The message direction can be:

- Search between the authors and recipients mentioned on both sides: This option retrieves ALL emails exchanged between the email address or domain name on the left and the email address or domain name specified on the right.
- Search between the authors on the right and recipients on the left: This option retrieves ALL emails from any of the sender email address or domain name on the right and any of or all of the recipient email address or domain name on the left.
- Search between the authors on the left and recipients on the right: This option retrieves ALL emails from any of the sender email address or domain name on the left and any of or all of the recipient email address or domain name on the right.

Note: The search items must be part of a review set.

Subject

Enter the subject keyword or phrase, and then press the Enter key.

Note: If you need to use phrases, then enclose the phrases within straight double quotation marks.

Export Password	Enter a password with which to protect the files that are returned from this request. The exported PST file would be protected with a password. The password must have at least 4 characters and a maximum of 6 characters. Note: Make sure that you can remember this password. If you forget the password, you will be unable to access the files returned from the data request, and your only course of action is to create another data request.

5 Click **Save**.

The newly created data request will appear on the **Data Request** page with a link to get the exported PST file.

6 Click the links to download the zipped file of the exported PST file.

Note: The export link gets expired in 15 days from its creation date. If you see a message about expired export, you should create a new data request.

Chapter 22

Managing search schedules

This chapter includes the following topics:

Overview

In addition to random sampling, you can configure searches to run on a schedule that is created based on your business needs. You can configure schedules to run searches at set times or set intervals.

Setting up new search schedules

Note: You must have the *Manage Schedules* permission to set up new search schedules. By default, users with the application role of *App Rule Admin* have this permission.

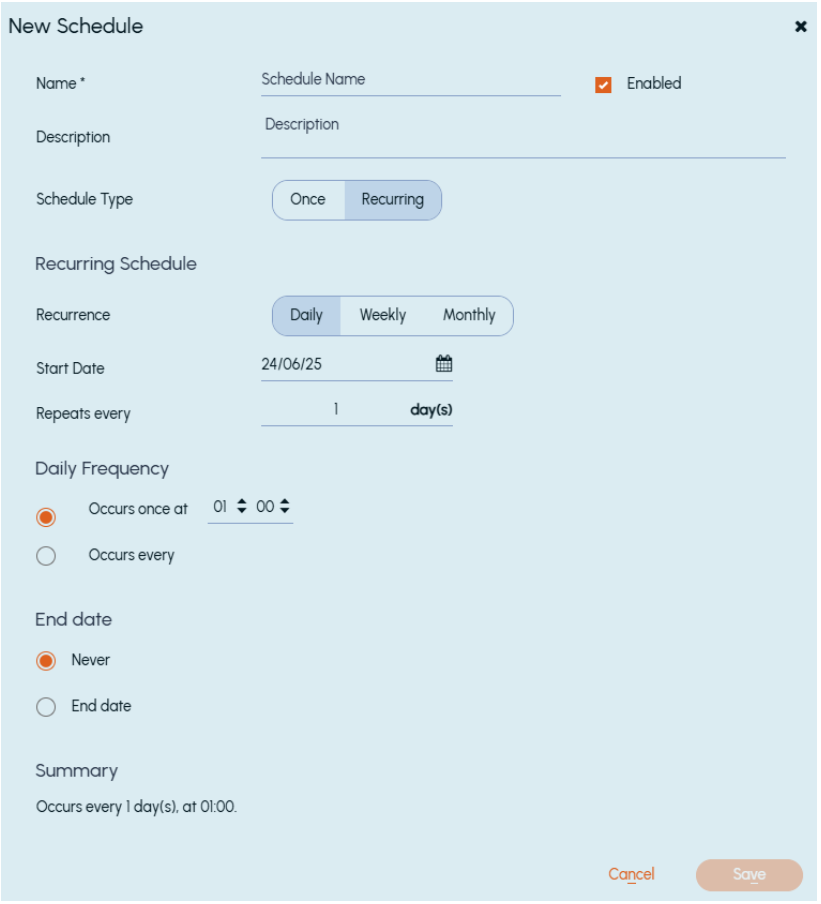
To set up a new search schedule

1 In the left navigation pane, click **Configuration**.

2 Click **Search Schedules**.

3 Click **New Schedule**.

The **New Schedule** dialog box appears.



4 In the **Name** and **Description** fields, type a unique name and an optional description for the schedule respectively.

Note: The search schedule name can contain up to 50 characters and cannot be edited once created. The description can contain up to 250 characters.

---

5 Select the **Enable** check box so that the schedule is available for selection when you define the criteria for a new search.

6 Select the required schedule type. The options are as follows:

Schedule type	Description
Once	Causes any searches that use this schedule to run only once, at the time that you set in the schedule.
Recurring	Causes any searches that use this schedule to run automatically at the interval that you specify in the schedule.

7 Click **Save**.

Setting up one-time search schedules

You can set up a new one-time search schedule to run a search just one time. This is different from a recurring search schedule.

Note: You must have the *Manage Schedules* permission to set up new search schedules. By default, users that have the *App Rule Admin* role have this permission. Before you set time for search schedule, ensure that scheduled searches do not run at the same time as system backups.

To set up a new one-time search schedule

1 In the left navigation pane, click **Configuration**.

2 Click **Search Schedules**.

3 Click **New Schedule**.

The **New Schedule** dialog box appears.

4 In the **Name** and **Description** fields, type a unique name and an optional description for the schedule respectively.

Note: The search schedule name can contain up to 100 characters. The description can contain up to 250 characters.

5 Select the **Enable** check box so that the schedule is available for selection when you define the criteria for a new search.

6 Select a schedule type option as **Once**.

7 Under the **Single Run** section, set the required date and time to execute the search.

8 Click **Save**.

Example of a one-time search schedule

Any searches that use the following schedules run automatically at the interval that you specify in the schedule. Insight Surveillance considers datacenter time zone - PST for all customers. To create a schedule that should run on 01-Jan-2020 at 6:00 AM, you can configure a search schedule in the following way:

- In the **On Day** field, select date as 01-Jan-2020.
- In the **At time** field, select time as 6:00 AM.
- Click **Save**.

Setting up recurring search schedules

You can set up a new recurring search schedule to run a search at a specific time. This is different from a one-time search schedule.

You must have the *Manage Schedules* permission to set up new search schedules. By default, users that have the *App Rule Admin* role have this permission. Before you set time for search schedule, ensure that scheduled searches do not run at the same time as system backups.

To set up a new recurring search schedule

1 In the left navigation pane, click **Configuration**.

2 Click **Search Schedules**.

3 Click **New Schedule**.

The **New Schedule** dialog box appears.

4 In the **Name** and **Description** fields, type a unique name and an optional description for the schedule respectively.

Note: The search schedule name can contain up to 100 characters. The description can contain up to 250 characters.

---

5 Select the **Enable** check box so that the schedule is available for selection when you define the criteria for a new search.

6 Select a schedule type option as **Recurring**.

7 Under the **Recurring Schedule** section, do the following:

- Select **Daily** to configure daily recurring schedule, and then specify the schedule start date and the repeat frequency.
- Select **Weekly** to configure weekly recurring schedule, and then specify the schedule start date and the repeat frequency.
- Select **Monthly** to configure monthly recurring schedule, and then specify the schedule start date and the repeat frequency.

8 Under the **Daily frequency** section, do any of the following:

- Select the **Occurs once at** option, and then specify the time.
- Select the **Occurs every** option, and then specify frequency of schedule that runs once a day or several times a day within a given period.

9 Under the **End date** section, specify the schedule end date.

10 Under the **Summary** section, verify the schedule summary.

11 Click **Save** to save the schedule, or click **Cancel** to abort the dialog box.

Example of a recurring search schedule

To create a schedule that runs every 3 hours on Mondays, between 9 AM and 6 PM PST, for the period between 01-Mar-2020 and 01-Aug-2020, you can configure a search schedule in the following way:

- In the **Recurrence** field, select weekly.
- In the **Start Date** field, select the date as 01-Mar-2020.
- In the **Repeats every** field, select the recurrence frequency as 1 and the day as Monday.
- In the **Occurs every** field, specify the frequency as 3.

- In the starting at and ending at fields, specify time as 9: 00 AM and 6: 00 PM respectively.
- In the **End Date** field, select the date as 01-Aug-2020.
- Click **Save**.

Editing search schedules

You can modify search schedules according to your review requirements.

To edit a search schedule

1. In the left navigation pane, click **Configuration**.
2. Click **Search Schedules**.
3. Select a search schedule you want to modify, and then click the **Edit Schedule** icon.

   The **Edit Schedule** dialog box appears.
4. Select or clear the **Enable** check box so that the schedule is available or disable for selection when you define the criteria for a new search.
5. Modify the schedule parameters, and click **Save**.

Deleting search schedules

You can delete search schedules if these are not of use any more.

Note: A search schedule cannot be deleted if any scheduled search is linked to it. When any scheduled search is linked to a search schedule, then the trash icon is not displayed for that schedule.

See "Disabling scheduled searches" on page 102.

To delete a search schedule

1. In the left navigation pane, click **Configuration**.
2. Click **Search Schedules**.
3. Select a search schedule you want to modify, and then click the **Delete** icon.

   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.

Chapter 23

Managing export operations

This chapter includes the following topics:

About exporting items

If you want to review items offline or provide them to an approved third-party organization, then you must export them from Insight Surveillance.

Insight Surveillance supports only EML file format for exporting the content.

Note: An export run can be performed only when items are available in the department for review.

Performing export runs

You can export the review items from Insight Surveillance if you want to review items offline or present them as evidence to a third party.

You must have the *Export Messages* permission to export items from a department. By default, all the reviewers in the department have this permission. The option to export escalated items is available to those with the *Export Escalations* permission only. By default, only users that have the *Escalation Reviewer* role have this permission.

You can perform the following export tasks. The keyboard shortcut keys are listed in parenthesis:

- **New (Alt + N)** - perform a new export run.
- **Refresh (Alt + R)** - refresh the list of existing exports.

To perform an export run

1 In the left navigation pane, click **Departments**.

2 Search for and select the department in which you want to perform export run.

Note: Insight Surveillance lists all departments. You can use the filtering options to search the required department. Options include filtering by department name, exception employees, and reviewers associated with the department.

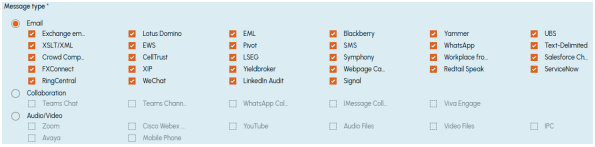
---

3 In the **Export** tab, click **New**.

The **New Export** dialog box appears.

4 Refer to the following table and provide the relevant information in the respective fields.

Field	Description
Name	(Mandatory) Type a name for the export run.
Message type	(Mandatory) Select message type of items based on their category—such as Emails, Collaboration, or Audio/Video—as shown in the sample image below.



Notes:

1. If the message types available are from only one category, they are not grouped by category. Instead, all available message types from the single category is shown directly for selection.

2. If the search criteria do not produce any results belonging to supported message types, the export cannot be saved. In such cases, the system displays the following alert message:

Your selection did not return any items to export.

Field	Description
Message direction	Select items that are traveling in a certain direction. You have the following options: ■ **All** – includes messages from all directions. ■ **Internal** – Includes the items where the author and all recipients are internal to your organization ■ **External Inbound** – includes the items where the author is external to your organization and at least one recipient is internal. ■ **External Outbound** – Includes the items where the author is internal to your organization and at least one recipient is external.
Capture method	Select items by the method that Insight Surveillance has used to capture them and add them to the review set. The options are: ■ **All** – Select all methods. ■ **Search** – Select to choose items that have been captured as a result of searches. ■ **Random Sampling** – Select to choose items that Insight Surveillance has captured and added to the review set according to your designated monitoring policy. ■ **Guaranteed Sample Search** – Select to choose the results of guaranteed sample searches. ■ **Tags** – Select to choose items that Insight Surveillance has captured and added to the review set according to designated tags.
Tags action	Select 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** (item is subject to normal random sampling)
Date captured	Select items that Insight Surveillance has captured over the specified period.
Search	Select items that the specified search has captured.
Current action status	Select items by their action status, such as Unreviewed, Pending, or Questioned.
Current action status author	Select items by the person who last assigned a review action to them. ■ Select **All** to consider all reviewers who assigned a review action. ■ Select **User Selection** to browse a particular reviewer who lastly assigned a review action

Field	Description
Escalation status	Select items by whether they have been escalated to an escalation reviewer and subsequently closed by that reviewer.
Escalation owner	Select items by the escalation reviewer who has responsibility for them. ■ Select **All** to consider all escalation owners. ■ Select **Unassigned** to consider items to which no escalation owner is assigned. ■ Select **User Selection** to browse a particular escalation owner
Escalated by	Select items by the person who escalated them to an escalation reviewer for further attention. ■ Select **All** to consider all reviewers. ■ Select **User Selection** to browse a particular reviewer.
Current appraisal status	Select items by whether a supervisor has appraised them. This option is only visible to supervisors with *Apply Appraisal Status* permission.
Current appraisal status owner	Select items by the supervisor who has currently appraised them. This option is only visible to supervisors with *Apply Appraisal Status* permission. ■ Select All to consider all appraisal status owner. ■ Select User Selection to browse a particular appraisal status owner.
Tags	Select items by the specific tag with which your policy management software has tagged them.
Export as	Select type of file to be exported. ■ **Original type** - to choose to output items in their native format. For example, Microsoft Exchange items as individual MSG files, SMTP items as individual EML files, and so on.
Include in reports	Select any or both of the following options: ■ **Journal Recipients**: Select this option to include recipient information from the journal envelope of Exchange or SMTP journal items. This lists all the recipients of each item, regardless of their placement in the To, CC and BCC fields. ■ **Item History**: Select this option to include comments, status, appraisal, and escalation history of items in the export report. Refer to the step 9 for sample report with the appended history and the recipients in To, CC, and BCC fields.

Field	Description
Number of items to export	Type the required number of items. Insight Surveillance exports the oldest items. For example, if you choose to export 100 items, Insight Surveillance exports the 100 oldest items that match the selected options.
Password	(Mandatory) Set an alphanumeric password.

5 Click **Save**.

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

6 Click **Save** to complete the operation or click **Cancel** to cancel it.

7 In the **Export** tab, ensure that the export you have created is available and its status is *In progress* or *Completed*.

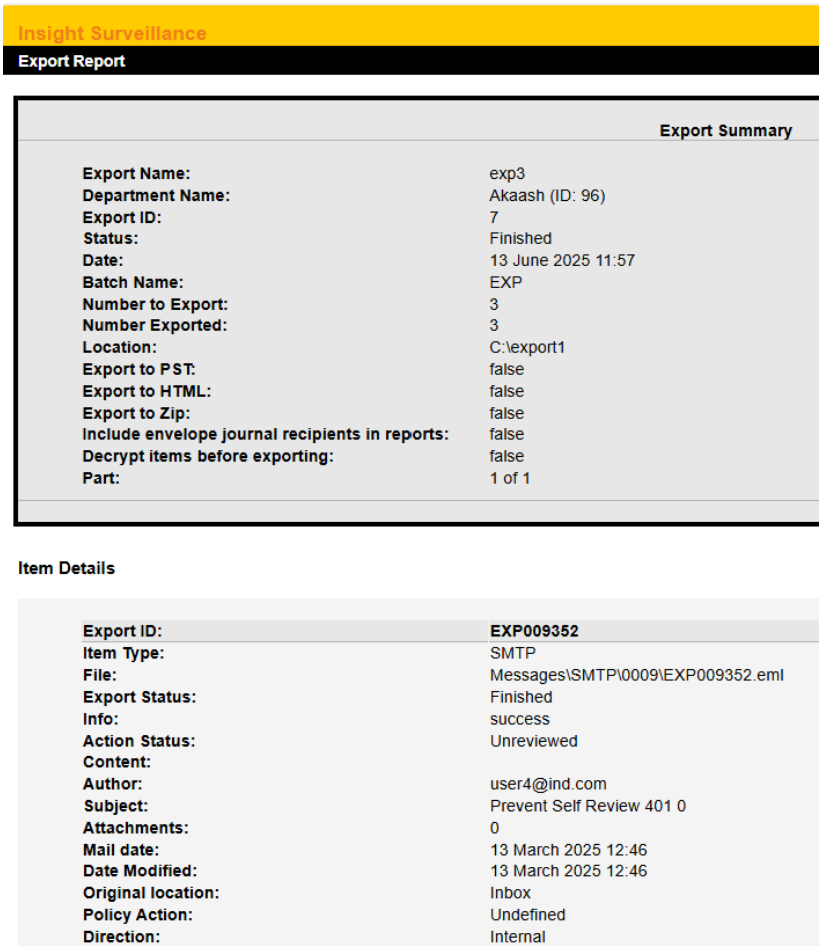
Note: If the status of your export run is displayed as **Failed**, you need to execute another export run.

---

8 After the export is finished, click the **Browse** icon to browse to the exported file.

9 Click the links to download the zipped file of the exported items.

Provide a password to open the report as shown in the sample image below.



Insight Surveillance

Export Report

Export Summary

Export Name:	exp3
Department Name:	Akaash (ID: 96)
Export ID:	7
Status:	Finished
Date:	13 June 2025 11:57
Batch Name:	EXP
Number to Export:	3
Number Exported:	3
Location:	C:\export1
Export to PST:	false
Export to HTML:	false
Export to Zip:	false
Include envelope journal recipients in reports:	false
Decrypt items before exporting:	false
Part:	1 of 1

Item Details

Export ID:	**EXP009352**
Item Type:	SMTP
File:	Messages\SMTP\0009\EXP009352.eml
Export Status:	Finished
Info:	success
Action Status:	Unreviewed
Content:	
Author:	user4@ind.com
Subject:	Prevent Self Review 401 0
Attachments:	0
Mail date:	13 March 2025 12:46
Date Modified:	13 March 2025 12:46
Original location:	Inbox
Policy Action:	Undefined
Direction:	Internal

Note: The export report feature supports only Email message types. It is not available for message types from other categories such as Collaboration or Audio/Video.

Chapter 24

Managing reviews

This chapter includes the following topics:

- Escalating the review items
- Applying labels to items
- Viewing history of items
- Printing and downloading the items and attachments
- Viewing Intelligent Review Details

About reviewing with Insight Surveillance

Insight Surveillance simplifies the compliance assessment process for reviewers by allowing them to review the outcomes of random sampling and searches. Furthermore, the compliance review process is facilitated by the following key aspects:

- **Distinct reviewer roles**: Arctera Insight Surveillance has several predefined reviewing roles, such as *Escalation reviewer*, *Exception reviewer*, and *Passive reviewer* that possess the following characteristics:
  - **Passive reviewers** can view items and review history, but they cannot assign or change review status. However, passive reviewers can assign appraisal status to the items that other users have reviewed.
  - **Exception reviewers** can view the items of their assigned exception employees only.
  - **Escalation reviewers** can receive items that other reviewers in the department have escalated to a higher authority for further review.
  - All roles except the *Passive Reviewer* role permit a user to assign the pending, question, escalation, and appraisal status to the review items.
  - All the exception reviewers and escalation reviewers assigned to the departments can assess the review status and comments that reviewers have applied and add appraisal status and comments.
- **Filter pane**: This pane lets you set criteria to refine the search records in the review items grid.
- **Comments**: Reviewers can comment on the review items to promotes documentation and transparency, facilitates collaboration and communication, supports auditing and accountability, enables effective risk management, and contributes to continuous improvement in the compliance review process.
- **Labels, label groups, and their AI-based predictions**: Reviewers can assign labels, label groups, and single choice label groups to review items. If the AI-based label predictions option is enabled for labels or single choice label

groups, only 20 active labels (including single choice group labels) per department or at application level can be enabled for AI predictions. To enable AI-based label predictions, labels and single choice label groups must be marked as active and the **Enable AI Predictions** option must be selected.

Deactivated labels and label groups are not considered for analysis and AI-based label predictions.

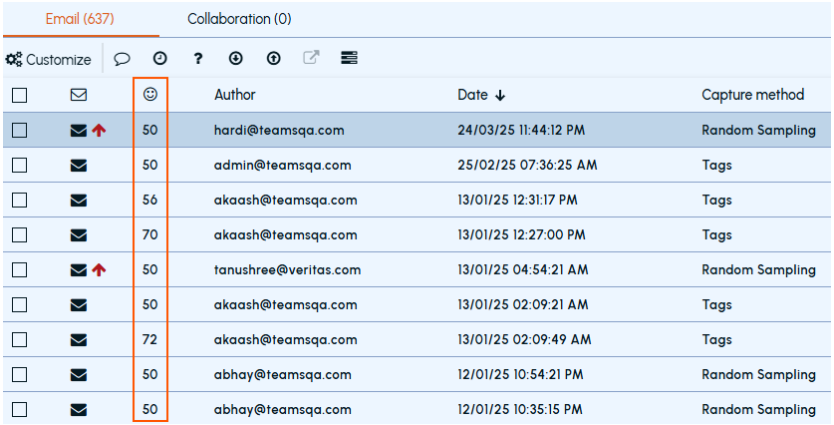
The *Predicted labels* column is displayed in the items grid on the **Review** page as shown in the sample image below. If multiple labels are predicted, they are separated by semicolon.

		Author	Date ↓	Capture method	Type	Escalation status	Predicted labels
	50	hardi@teamsqa.com	24/03/25 11:44:12 PM	Random Sampling	Exchange	Escalated	HBK21st
	50	admin@teamsqa.com	25/02/25 07:36:25 AM	Tags	Exchange	Not Escalated	
	56	akaash@teamsqa.com	13/01/25 12:31:17 PM	Tags	Exchange	Not Escalated	HBK21st
	70	akaash@teamsqa.com	13/01/25 12:27:00 PM	Tags	Exchange	Not Escalated	HBK21st
	50	tanushree@veritas.com	13/01/25 04:54:21 AM	Random Sampling	Exchange	Escalated	HBK21st
	50	akaash@teamsqa.com	13/01/25 02:09:21 AM	Tags	Exchange	Not Escalated	HBK21st
	72	akaash@teamsqa.com	13/01/25 02:09:49 AM	Tags	Exchange	Not Escalated	HBK21st
	50	abhay@teamsqa.com	12/01/25 10:54:21 PM	Random Sampling	Exchange	Not Escalated	HBK21st
	50	abhay@teamsqa.com	12/01/25 10:35:15 PM	Random Sampling	Exchange	Not Escalated	HBK21st

- **Tags and hotwords statistics**: Arctera Insight Surveillance provides tags and hotword statistics for all message types it supports. Reviewers can quickly view the tags and hotwords-specific statistics per item and can navigate to individual matches in the **Preview** pane.
- **Review items grid customization**: Arctera Insight Surveillance lets you set the **Preview** pane position to the bottom or the right side of the review items grid for better readability. It also allows you to rearrange columns of the grid according to your specific requirements. You can sort the resulted reviewing items by increasing or decreasing relevance score, tags, and so on. You can collapse and expand the panes for better readability.
- **Relevance Score**: This score is an integer value ranging from 0 to 100, assigned to all review items. It indicates the degree of relevance for review. A lower relevance score suggests that the item is more irrelevant, while a higher score indicates that the item is more relevant and requires closer attention during the review process. This functionality enables reviewers to promptly prioritize items for review, focusing on the most relevant ones first.

  The Relevance Score column is displayed in the list pane by default. The score is calculated and displayed only if the Intelligent Review service is enabled for the selected departments. For the departments that are not enabled for the intelligent review service, the application displays the column, but the values remain blank.

- **Sentiment score**: In Arctera Insight Archiving, when Arctera Insight Classification is enabled as part of the retention plan, the sentiments expressed in the textual content are analyzed and the sentiment score is generated at the item level, which measures attitudes, opinions, and emotions. The sentiment score value ranges from 0 to 100, where a 0-39 score represents negative sentiment, a 40-59 score represents neutral sentiment, and a 60-100 score represents positive sentiment. The Insight Surveillance users can sort and filter items based on their sentiment scores.
  The sentiment score column is by default displayed in the items grid On the **Review** page. A smile-emoji is used as a column heading. You can change the column position in the grid if required. You can click the column heading to sort the items based on the ascending or descending sentiment score as shown in the sample image below.



Limitations on reviewing certain types of Skype for Business content

Insight Surveillance uses the Arctera Insight Archiving platform for accessing data, including Skype for Business instant messaging and conferencing communications. Arctera Insight Archiving archives each of these communications as an individual email (EML) file that, in Insight Surveillance, has a message type of Instant Messaging.

Skype for Business communications can include whiteboards and polls that users share during a conference. The content of these two conference features is stored in a Microsoft-proprietary XML format, which Arctera Insight Archiving cannot

index. As a result, you cannot use the facilities in either Arctera Insight Archiving or Insight Surveillance to search the text content of these items.

Understanding the Review page

The following image highlights the standard features of the **Review** page.

Figure 24-1 A sample page showing review summary of selected departments

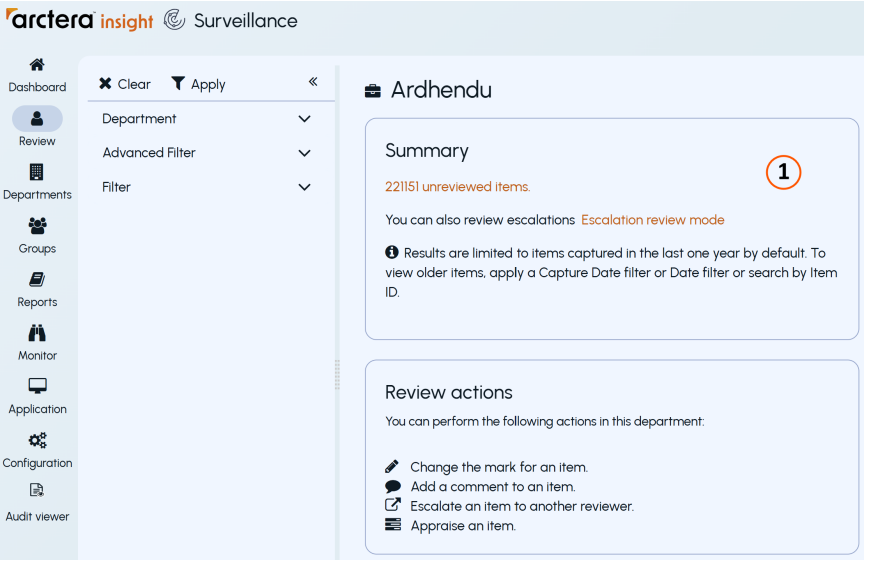
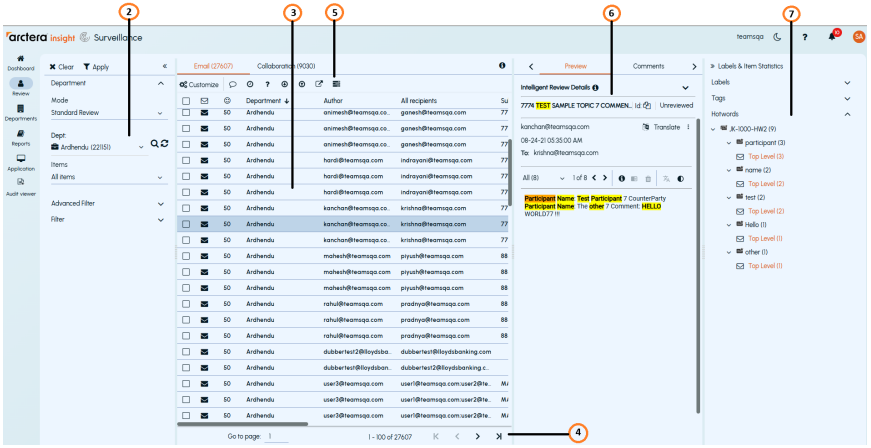


Figure 24-2 A sample page showing other panes with details



1. Summary and instruction pane

This page displays the summarized information of review items. You can click the summary items to view the details.

2. Filter pane

Insight Surveillance lists only those departments for which the reviewers have access. Reviewers can use the filter facets to set criteria to refine the search records. You can collapse this pane for better readability as and when required.

See "Filtering the items in the Review pane" on page 228.

3. Review item grid

This grid shows the items in the review set that match the filter options you have selected. You can use the **Group** drop-down list to group or sort the items according to relevance, ascending or descending dates and months, alphabetical author and subject names, and tags. The unreviewed items are displayed in bold text.

Click on the column heading to sort items in ascending or descending order. The changes are persisted across different login sessions for the logged-in user.

4. Footer area

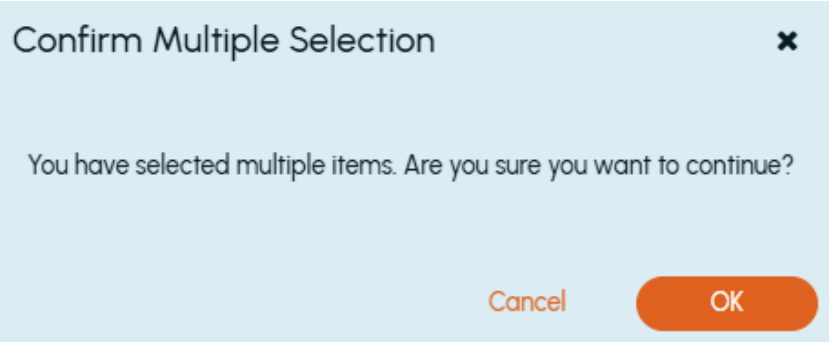
This area provides the navigation arrows at the bottom of the items grid to go to the first, previous, next, or last page.

5. Action bar

The action bar lets you perform the following actions:

- Apply review statuses and add comments to single or multiple selected items.

When applying a review status to a single item, the application does not prompt to confirm the selection of the item. However, while applying a review status to multiple items, the application prompts a confirmation to ensure accurate selection and avoid errors, as shown in the sample image below.

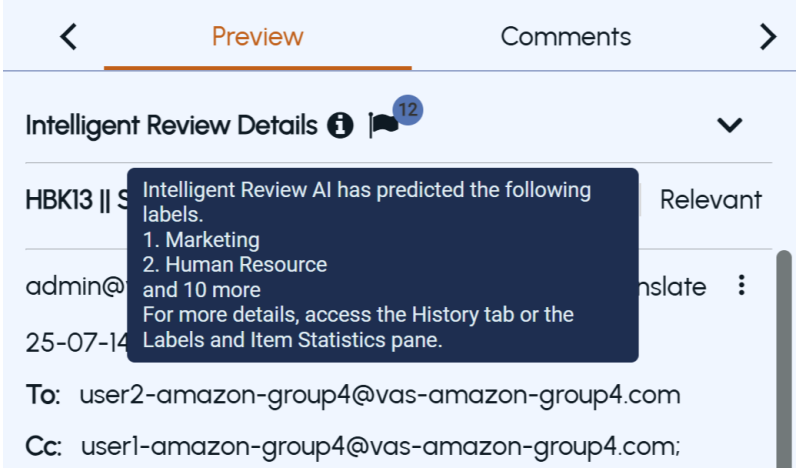


- Rearrange the column order for improved review experience. See "Rearranging columns in the item list pane" on page 227.
- Change the position of the reading pane (Preview, Comments, and History) to right or bottom of item list pane. See "Changing the Preview pane position" on page 226.

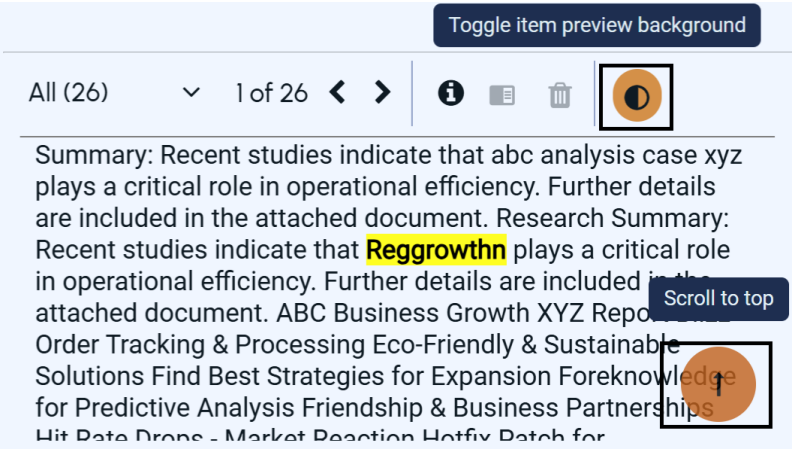
6. Reading pane

This pane has three tabs and two functions.

- The **Preview** tab displays an HTML preview of the selected item.
  In addition, it provides the following interfaces:
  - The **Intelligent Review Details** section provides the facts of why the item is classified as *Unreviewed Relevant* or *Unreviewed Irrelevant*. The application shows the Relevant and Irrelevant labels (links) and the respective contributions. See "Viewing Intelligent Review Details" on page 295.
  - The **Learning** bar lets you select the text samples for the intelligent review process. You can add or remove the selected text samples from the item being reviewed.
  - The flag icon, representing **AI-based Label Predictions**, shows AI-predicted labels and their count for each review item if the *Enable AI Predictions* option is selected for active labels and label groups. Refer to the sample image below.



- The **Display Name** of the email author and recipients are displayed along with their email IDs. If a tag is applied to the author or recipient email IDs, the application highlights these display names and considered for tag statistics calculations.
- The **Toggle Item Preview Background** icon enhances text readability by allowing to highlight or remove highlighting from the preview text. Refer to the sample image below.



- The **Scroll to Top** icon allows users to quickly return to the top of the preview pane, especially when viewing lengthy paragraphs of text.

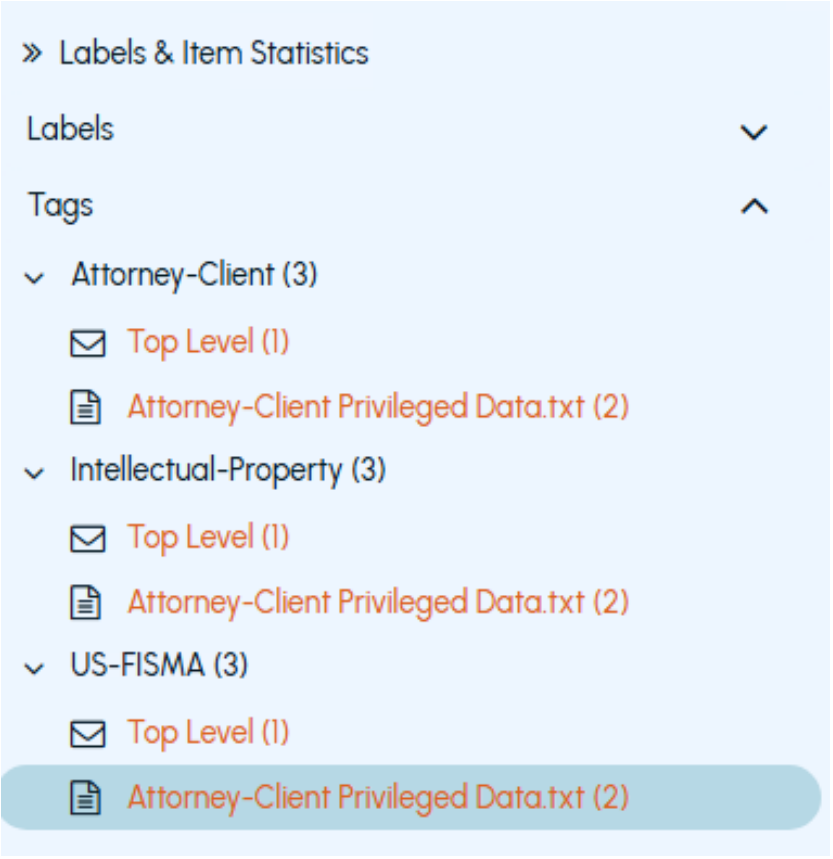
- The **Comments** tab shows the comments that reviewers have assigned to the selected item.
- The **History** tab displays the detailed summary of the operations that are performed on the selected item.
- The **Kebab** icon (three vertical dots) provides the **Print** option to view the printable version of the item, and the **Download** option to save the printed file to your computer.

7. Labels & Item Statistics

This pane has the following sections:

- **Labels**: This section displays active labels, labels within label groups, and labels within single-choice label groups. You can visually distinguish between application-specific, department-specific, and AI-predicted labels.
  AI-predicted labels are marked with a flag icon. Flag icon color varies with prediction confidence.
  Application-specific labels are marked with a monitoring screen icon, while the Department-specific labels lack an icon. Refer to the sample image below.

- **Tags**: This section shows the classification policy tags-specific statistics when a user selects an email for review.
  The displayed information includes tag names. Next to each entry, the number of incidents that match the corresponding tags in the selected items is shown. After you expand the tag name node, the application displays the number of matches in the top-level content of the email and in each attachment of the email.



This section displays statistics only for the tags that have a match. Tags that do not match are not shown in the list.

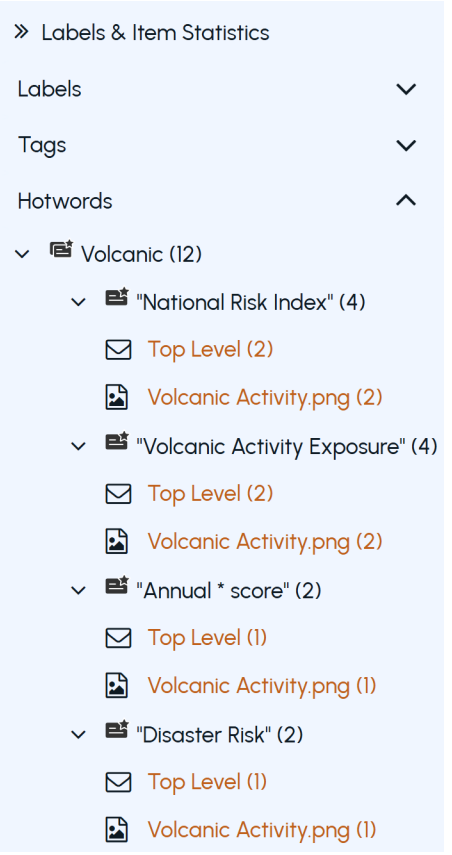
The **Top Level** node and the attachments nodes are visible only if the content within them contains the specified tags. In case there are no matches for the tags in the primary emails, the **Top Level** node will not be displayed. Similarly, if there are no matches for the tags in the attachments, those attachments will also not be displayed.

You can click the hyperlinks to view the respective tags in the **Preview** pane. Click the arrows to navigate to the next or previous match. The navigation is limited to the content of email body message and attachments, and not within the email metadata.

- **Hotwords**: This section shows the hotwords-specific statistics when a user selects an item for review.

  The displayed information includes the names of hotwords sets and individual hotwords. Next to each entry, the number of incidents that match the

corresponding hotwords or hotwords sets in the selected items is shown. After you expand the hotwords set name, the application displays the included hotwords and their number of matches in the top-level content of the item and in each attachment of the item.



This section displays statistics only for hotwords or hotword sets that have a match. Hotwords and hotword sets that do not match are not shown in the list.

The **Top Level** node and the attachments nodes are visible only if the content within them contains the specified hotwords. In case there are no matches for the hotwords in the primary emails, the **Top Level** node will not be displayed. Similarly, if there are no matches for the hotwords in the attachments, those attachments will also not be displayed.

You can click the hyperlinks to view the respective hotwords in the **Preview** pane. Click the arrows to navigate to the next or previous match. The

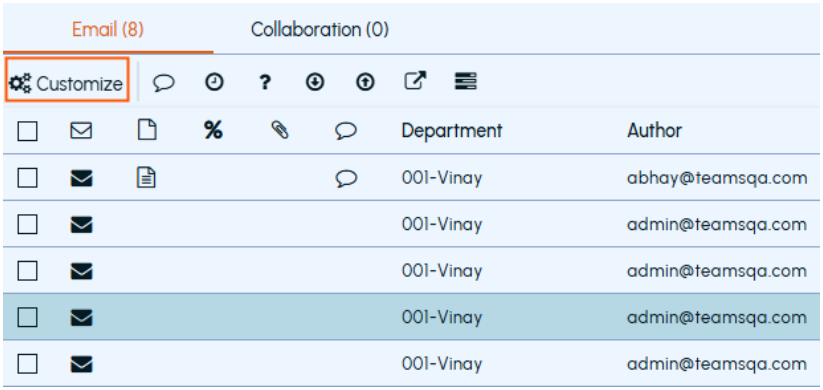
navigation is limited to the content of email body message and attachments, and not within the email metadata.

Changing the Preview pane position

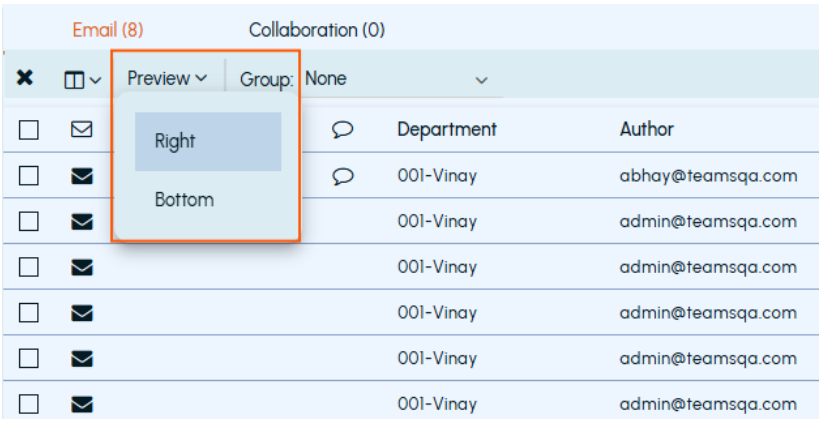
To change the Preview pane position

1 In the left navigation pane, click **Review**.

2 In the item list pane, on the action menu bar, click **Customize**.



After you click **Customize**, the application displays another action menu bar that is specific to the view customization.



3 Click the **Preview** drop down and select any of the following options:

- Select **Right** to preview content on right side of the item list pane.

- Select **Bottom** to preview content on bottom side of the item list pane.

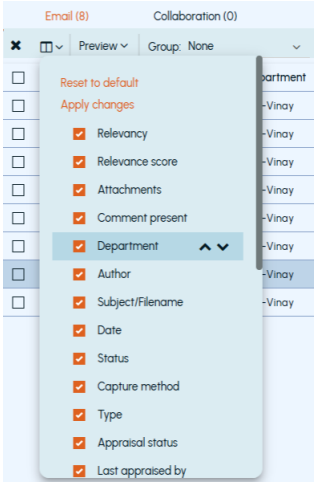
This setting is saved and remains persistent until changed.

Note: As per your requirement, the preview pane can be located below or to the right of the **Emails** and **Collaboration** items list. You can also set the preview pane position inversely for the Emails and Collaboration items. For example, you can set the position of the preview pane for the email items to right, whereas for the collaboration items to the bottom, or vice versa.

Rearranging columns in the item list pane

To rearrange columns in the item list pane

1. In the left navigation pane, click **Review**.
2. Click **Customize** and expand the **Select Columns** drop down as shown in the sample image below and select the check boxes adjacent to the column options that you want to move.



3. To change the order of column to left or right in the item list pane, click the **Up** or **Down** arrows respectively, and click **Apply changes**.
4. To reset the default arrangement of columns, click **Reset to default**.

Filtering the items in the Review pane

The search and filter options available in the **Review** pane provide several parameters to filter items for review.

To filter the items in the review pane

1 In the left navigation pane, click **Review**.

2 In the **Department** drop-down list, do the following steps:

Note: The selections are persisted across all login sessions for the logged-in user.

- In the **Mode** drop-down list, choose whether to perform a standard review of the items in the review set or an escalation review.

  Note: Escalation Review mode is available to escalation reviewers only. It lets these reviewers view and change review status of the items that other reviewers have escalated to them for further attention.

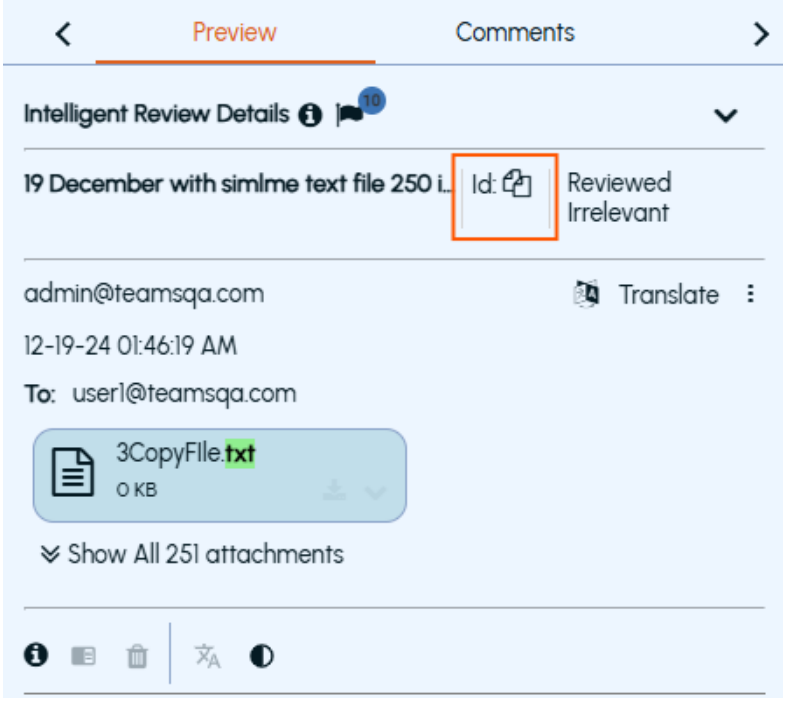
- In the **Dept** drop-down list, select the department, or a nested department for which you want to display the items in the review set.
- In the **Items** drop-down list, select a group of items you want to review. The following options are available:
  - **Temporary Assignment**: This option allows you to temporarily reserve a predefined number of unassigned items from the review set for your current session. These items are not permanently assigned to you, but while your session is active, other reviewers cannot access or review them.
    For example, if you log in and select **Temporary Assignment** with a limit of 200 unassigned items, you can review these items without permanently assigning them to yourself. While your session is active, other reviewers in the department cannot see or access these items. However, once you log out or end the session, any unmarked items become available again for other reviewers.
  - **All Items**: This option allows you to view all review items in the review set, including those assigned to other reviewers. However, using this option may lead to duplicate work if multiple reviewers mark the same items.

For example, if you select **All Items**, you can view every item in the review set, including those assigned to other reviewers. However, if you mark these items, you may duplicate the work of others, leading to inconsistencies. To prevent this, use this option only for browsing these items and not reviewing them.

3 In the **Advanced Filter** drop-down list, specify the following if needed to filter review items.

- **Item Id**: This field allows reviewers to search shared emails within specific departments using Item ID.
  Note:
  - The Item ID is searchable only if the reviewer (logged-in user) has review permission for the associated department.
  - This functionality is available only for emails and is not extended to collaboration messages at present.

  During review, when an email is selected in the item grid, the **Preview** pane displays the **Item ID** icon. You can click the icon to copy the ID for sharing with other reviewers.



When you search for this Item ID using *Advanced Filter*, the application clears the current filter settings and displays a single item from specific department from where the item ID is shared.

- **Author/Domain**: This field is used to search emails and collaboration messages for a specific user or email domain. Enter a full or a partial email domain that you want to search. For example, *gmail, gmail.com, or @gmail.com*. The application searches items from all users belonging to the specified domain.

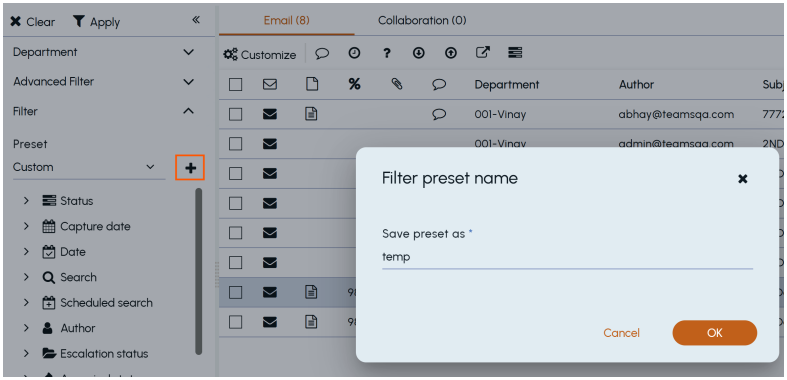
Note: While providing input for this filter, do not enter multiple authors or domains, a semicolon (;), or a string of two hyphen marks (--).

- **Subject**: This field is used to search emails only, and not applicable for searching collaboration messages. Enter a word or phrase that you want to search. The application filters the emails in which the subject field contains the specified words.

4 In the **Filter** drop-down, do any of the following as required:

- Choose the filter criteria from the default **Preset** options. By default, the following preset options are available:
  - All Unreviewed
  - Today's Unreviewed
  - All Unreviewed Exchange
  - All Unreviewed Instant Messaging
  - All Unreviewed Bloomberg
  - All Unreviewed Domino
  - All Messages
- Expand the necessary facets and select the item classification options you want to apply.

  If you want to use the same facet settings frequently, you can save this setting as a filter preset option. In the **Preset** drop-down, select **Custom**, then click the **+** icon next to the drop-down arrow. In the **Save preset as** field, enter a unique name of the filter preset, and click **OK**.



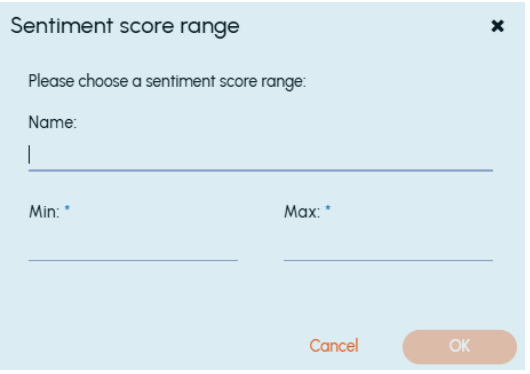
Upon successful addition, the newly saved filter preset appears in the **Preset** drop-down.

The following table lists the available filter facets.

Facets	Description
Status	Select items by their status, like pending, reviewed, questioned, and so on.
Capture date	Selects items that Insight Surveillance has captured over the specified period. The default options are - Today, Yesterday, Last 7 days, Last 14 days, and Last 28 days. Click **Set date range** to filter the items based on the date range specified. Clicking the calendar icon displays the review item count beneath the date, month, and year wise view. When selected, the application also displays day-wise, month-wise, and year-wise item counts beneath the respective dates, months, and years. If there is no items count, a hyphen (-) is displayed. For more details, See "Viewing dynamic review item counts on the calendar" on page 235.

Facets	Description
Date	Select items by the date on which they were created. The default options are - Today, Yesterday, and Last week. The last week defines Monday to Sunday range of the last week. You can use this option to review weekly items. When you hover over the Last week option, you can view the last week Monday to Sunday date range. For example, if you are working on 18th Nov 2021, the last week dates are displayed as 8th Nov 2021 to 14th Nov 2021. Click **Set date range** to filter the items based on the date range specified. Clicking the calendar icon displays the review item count beneath the date, month, and year wise view. When selected, the application also displays day-wise, month-wise, and year-wise item counts beneath the respective dates, months, and years. If there is no items count, a hyphen (-) is displayed. For more details See "Viewing dynamic review item counts on the calendar" on page 235. See "Date format support in Insight Surveillance " on page 21.
Search	Select items that one or more searches have captured. If there are more than 20 items, the application displays the **Show all** option. To view all the items, click **Show all** and select maximum 20 items. To select multiple items, select the corresponding check boxes. You can select items from multiple pages. You can use the **Go to page** field to select the available page number you want to view. Else, the application displays the message as ***Invalid page***. The total of selected items is displayed in the bottom. To remove entire selection, click the **Clear** icon. To remove any of the selected items, click on the link (which is adjacent to the **Clear** icon), search for the employee record, and click the **Remove** icon.
Scheduled search	Select items that one or more searches have captured according to their search schedules.
Author	Select items by the name of the person who sent them.
Escalation status	Select items by whether they have been escalated to an escalation reviewer or subsequently closed by that reviewer.
Appraisal status	Select items by their appraisal status.

Facets	Description
Type	Select one or more supported message types. For more information on the Insight Surveillance supported message types, See "Sampling support for content sources" on page 17. The available options are displayed based on the services subscribed and enabled for you. For example - ■ If MS Teams Archiving is enabled for you, the *Teams Chat* and *Teams Channel* options are available for filtering. ■ If the search result has audio or video items, then the *Audio-Video Transcript* option is available for filtering.
Direction	Select items that have traveled in the specified direction. The options are as follows: ■ **Not specified** - Select to avoid choosing any direction. ■ **Internal** - Selects items where the author and all recipients are internal to your organization. ■ **External Inbound** - Selects items where the author is external to your organization and at least one recipient is internal. ■ **External Outbound** - Selects items where the author is internal to your organization and at least one recipient is external.
Predicted labels	Select items by their predicted labels.
Labels	Select items by their labels.
Tags	Select items by their tags.
Tags action	Select items by their tag actions.

Facets	Description
Sentiment score	Select items based on the predefined sentiment score categories. A score in the range of 0 to 100 is assigned, where... ■ 0 - 39 indicates that the item expresses the negative sentiment. ■ 40 - 59 indicates that the item represents the neutral sentiment. ■ 60 - 100 indicates that the item represents the positive sentiment. To customize a different sentiment score range and use it as a preset later, click **New sentiment score range**. Specify the minimum and maximum score you want to capture, and provide a unique name to this preset. Click **OK** to save the preset as shown in the sample image below. 
Last marked by	Select items by the person who has lastly changed a review status of the items.
Comments	Select items to which reviewers have added comments.
Size	Select items by their size in kilobytes.
Number of attachments	Select items by the number of attachments that they have.

Facets	Description
Capture method	Select items by the method that Insight Surveillance has used to capture them and add them to the review set. The options are: ■ **Not specified** - Select to avoid choosing any direction. ■ **Search** - Select to choose items that have been captured as a result of searches. ■ **Random Sampling** - Select to choose items that Insight Surveillance has captured and added to the review set according to your designated monitoring policy. ■ **Guaranteed Sample Search** - Select to choose the results of guaranteed sample searches. ■ **Tags** - Select to choose items that Insight Surveillance has captured and added to the review set according to designated tags.
Escalation owner	Select items by the escalation reviewer who has responsibility for them.
Escalated by	Select items by the person who escalated them to an escalation reviewer for further attention.
Last appraised by	Select items by the person who appraised the items.

5 Click **Apply**.

The application displays the **Email** and **Collaboration** tabs based on the services subscribed and enabled for you.

Notes:

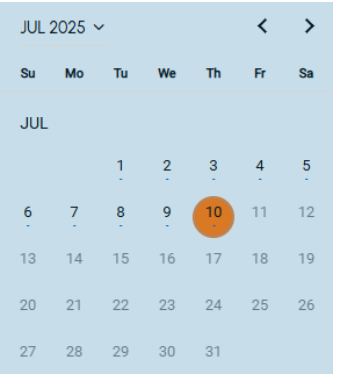
1. If only the **Exchange** service is enabled for you, the **Email** tab appears. If the **Exchange** and the **Microsoft Teams** services are enabled for you, the **Email** and the **Collaboration** tabs appear respectively.

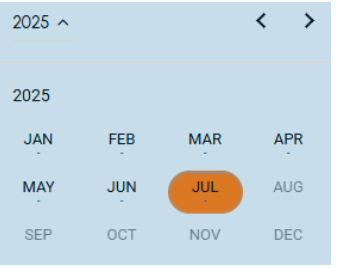
2. When no capture date or date is selected in the filters, Arctera Insight Surveillance, by default, displays only review items captured within the last one year. This restriction does not apply when the user selects a specific date range outside the one-year window in the capture date filter or date filter, or searches using a specific Item ID.

Viewing dynamic review item counts on the calendar

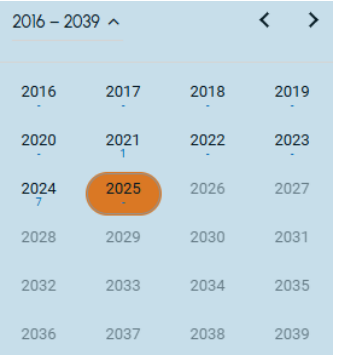
The calendar shows the review item count in the day, month, or year view. The count dynamically updates based on the applied filters.

Day view ***Month view***

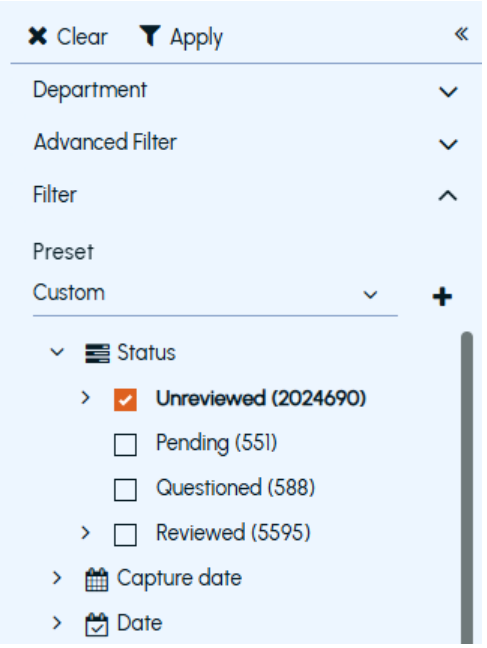




Year view

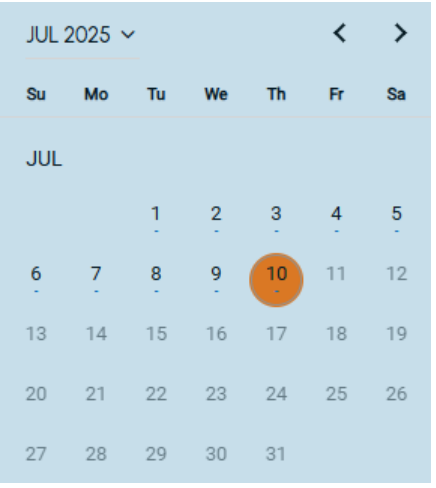


The dynamic review item count is visible on calendar when you specify the date range through the *Capture Date* and *Date* filter options. The item count appears only if at least one filter is applied to populate the Review Set with items for review. The calendar can display a maximum of 50,000 review items, aligning with the Review Set's maximum limit of 50,000 items as shown in the image below.



The calendar does not show item counts when filters are not applied, instead asks you to ensure that the reviewer set has items to be reviewed.

The calendar shows a hyphen (-) sign instead of item count (as shown in the image below) if the filters are applied, but there are no items for review.



To view the review item counts on calendar

1. In the left navigation pane, click **Review**.
2. In the **Department** drop-down list, select the department or a nested department for which you want to display the items in the review set.
3. In the **Filter** drop-down list, set the filter criteria by using the provided filter options, and click **Apply**.

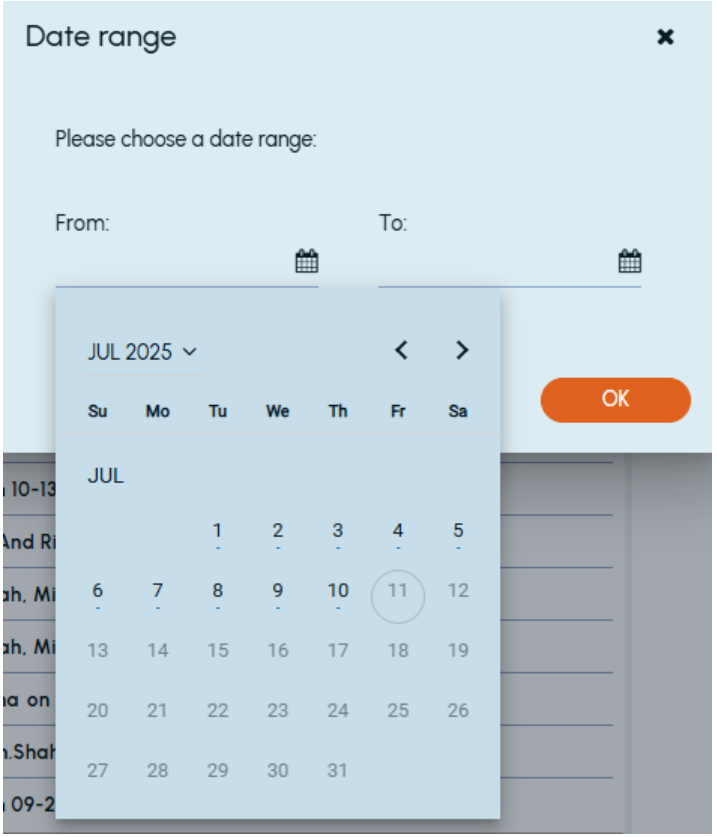
Note: Apply at least one filter; otherwise, the item count will not appear, as there will be no review items in the review set.

---

4 In the **Filter** drop-down list, expand the **Capture date** or **Date** option, and click **Set date range**.

In the **Date range** dialog box, click the calender icons to set the start and end date.

Clicking the calendar icon displays the item count. When you select a day, month or year view, the application displays day-wise, month-wise, and year-wise item counts beneath the respective dates, months, and years. If there is no items count, a hyphen (-) is displayed.



After specifying the date range, click **OK**.

5 Click **Apply** to filter the items based on the specified filter options.

Reviewing searched items

Before you start reviewing items, you must know that you can view emails if the **Exchange** service is enabled for you. You can view collaboration messages if the **MS Teams Archiving** service is enabled for you. When both the services are enabled, but the search does not find any email or collaboration message record, the corresponding tab is displayed without any items in it. The **Email** and the **Collaboration** tabs individually displays total number of searched and filtered review items.

To review items and checking their tags and hotwords statistics

1 In the left navigation pane, click **Review**.

2 Search for and select the department for which you want to review items.

Insight Surveillance lists all departments for which you have the review permissions.

3 (Optional) Use **Advanced Filter** and **Filters** to view the precise review items quickly. To reset the filtering criteria, click **Clear**, set a new criterion, and click **Apply**.

The application displays items from the selected departments.

The item grid displays multiple columns. Based on your review priorities and focus, you can:

- Sort items by clicking the column headings.
  For example, to view more relevant items for review, click the **Relevance Score** column heading. Items with higher relevance scores are more relevant, while lower scores suggest irrelevance.
- Rearrange the column sequence. See "Rearranging columns in the item list pane" on page 227.
- Use the navigation arrows at the bottom of the items grid to go to the first, previous, next, or last page.

These changes are persisted across different login sessions for the logged-in user.

Note: The **Relevance Score** column is displayed in the list pane by default. However, the score (value) is calculated and displayed only if the intelligent review service is enabled for the selected departments. For the departments that are not enabled for the intelligent review service, the application displays the column, but the values remain blank.

---

4 To review the filtered emails, on the **Email** tab, select the email.

- If you select an individual email in the items grid, you can view the *Preview*, *Comments*, and the *History* tabs.
  - On the **Preview** tab, you can view email metadata and content, print, and download the item.
  - On the **Comments** tab, you can view previous review comments for the selected email.
  - On the **History** tab, you can view the detailed summary of the operations that are performed on the selected email.
- If you select multiple items in the items grid, you cannot view the *Preview*, *Comments*, and the *History* tabs. Instead, you get options to assign a review statuses to all the selected messages simultaneously.

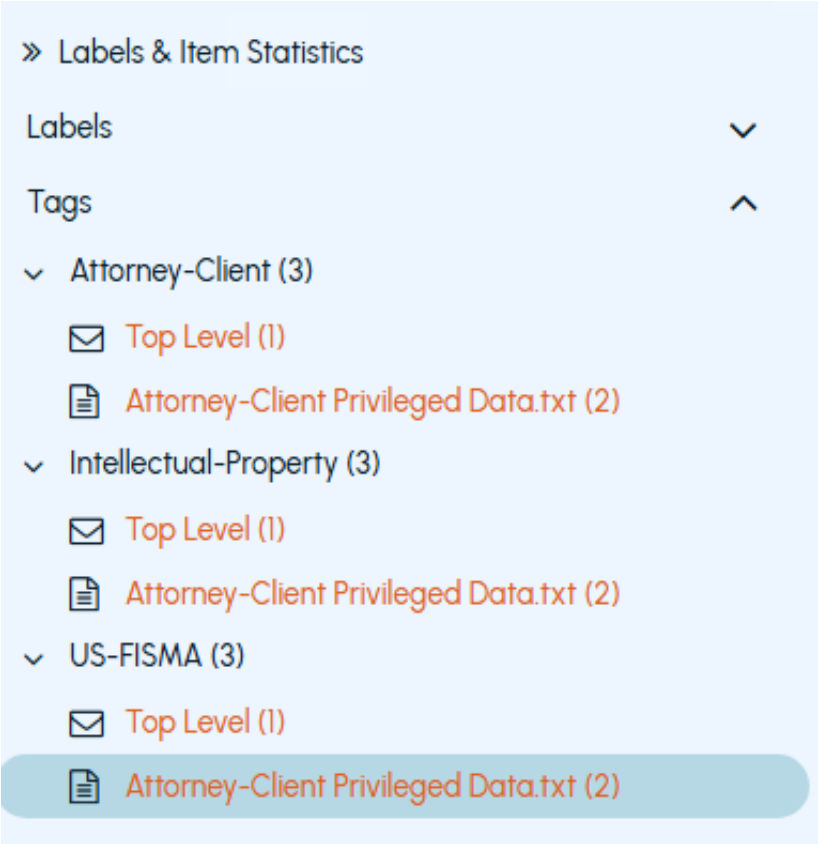
Note: Since the *Preview* tab is not visible, the flag icon depicting AI-predicted labels and their count is also not visible.

To comment on the selected email, click **Add Comment**. See "Adding comments to items" on page 282.

To assign status to the selected email, click *Pending*, *Questioned*, *Review Irrelevant*, *Reviewed Relevant*, *Escalate*, or *Appraised* as required.

5 To view the tags-specific statistics of the selected email, in the **Labels & Item Statistics** pane, expand the **Tags** section.

The displayed information includes the names of applied tags or classification policies. Next to each tag name, the number of incidents that match the corresponding tags or policies in the selected items is shown. After you expand the tag name, the application displays number of matches in the top-level content of the item and in each attachment of the item. See the sample image below.



Note:

By default, Insight Surveillance analyses and displays statistics only for tags that have a match. Tags that do not match are not shown in the list.

The **Top Level** node and the attachments nodes are visible only if the emails have the specified tags. In case there are no matches for the tags in the

primary emails, the **Top Level** node will not be displayed. Similarly, if there are no matches for the tags in the attachments, those attachments will also not be displayed.

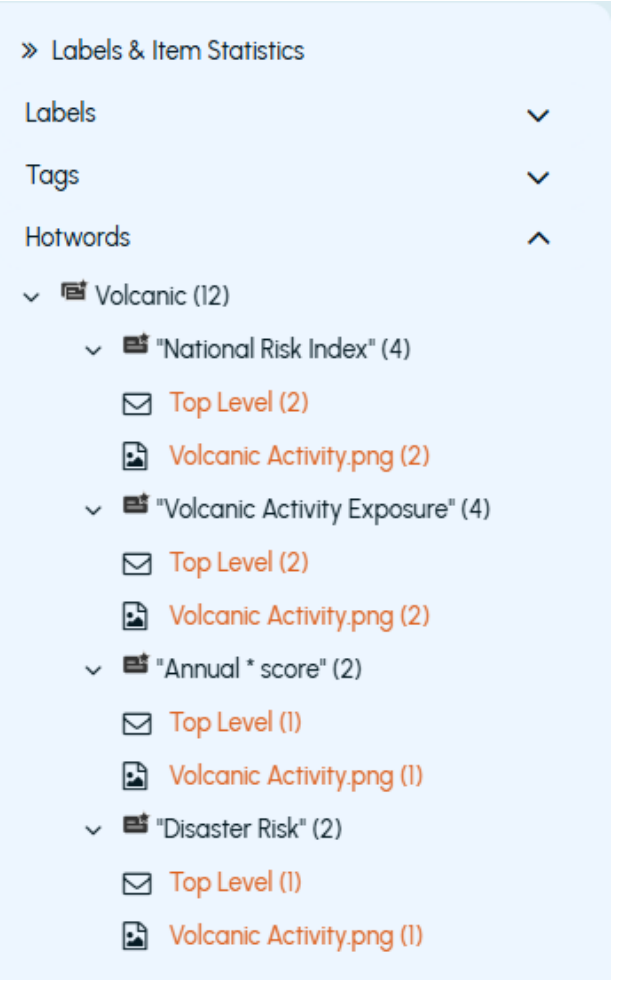
Click the hyperlinks to view the respective tags in the **Preview** pane. Click the arrows to navigate to the next or previous match. The navigation is limited to the content of email body message and attachments, and not within the email metadata.

If the attached image contains tags, clicking the hyperlink from the tags statistics pane opens the image in text format for convenient review of the tags.

---

6 To view the hotwords-specific statistics of the selected email, in the **Item Statistics** pane, expand the **Hotwords** section.

The displayed information includes the names of hotwords sets and individual hotwords. Next to each entry, the number of incidents that match the corresponding hotwords or hotwords sets in the selected items is shown. After you expand the hotwords set name, the application displays the included hotwords and their number of matches in the top-level content of the email and in each attachment of the email. See the sample image below.



By default, Insight Surveillance analyses and displays the statistics of hotwords that are found in each item and have a match. Hotwords and hotword sets that do not match are not shown in the list.

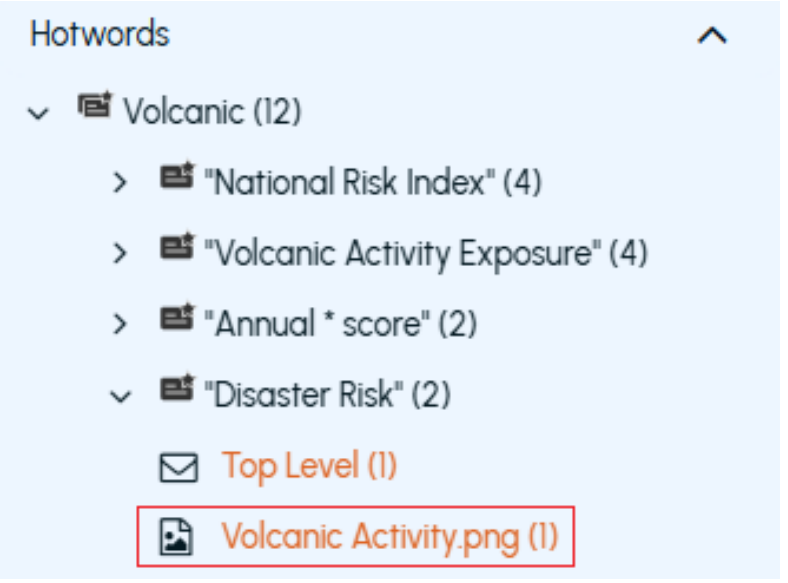
The **Top Level** node and the attachments nodes are visible only if the content within them contains the specified hotwords. In case there are no matches for the hotwords in the primary emails, the **Top Level** node will not be displayed. Similarly, if there are no matches for the hotwords in the attachments, those attachments will also not be displayed.

Click the hyperlinks to view the respective hotwords in the **Preview** pane. Click the arrows to navigate to the next or previous match. The navigation

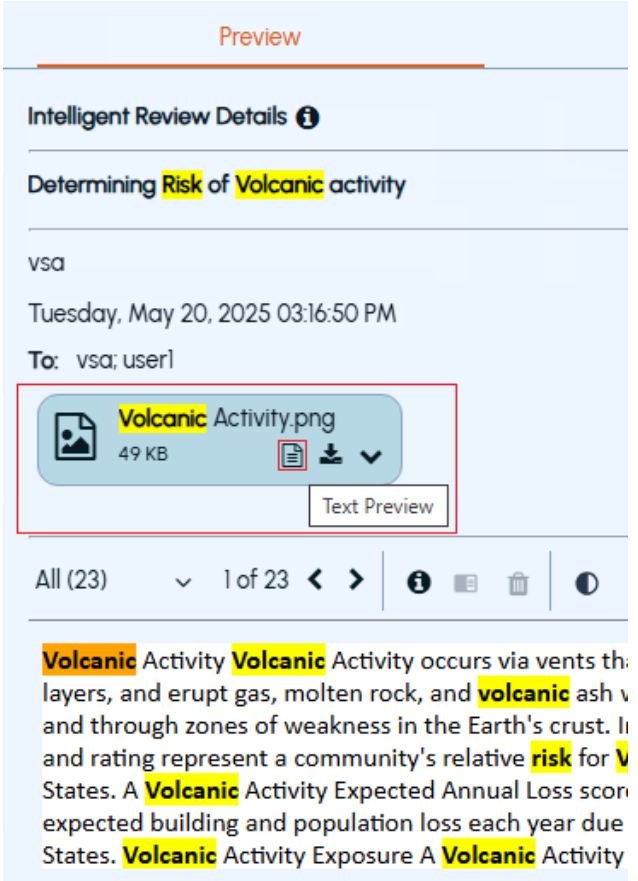
is limited to the content of email body message and attachments, and not within the email metadata.

Insight Surveillance supports viewing image attachments in review items in both text and Native formats. If the attached image contains hotwords, clicking the hyperlink from the hotwords statistics pane opens the image in text format for convenient review of the hotwords. You can preview the hotwords in the images in the following ways:

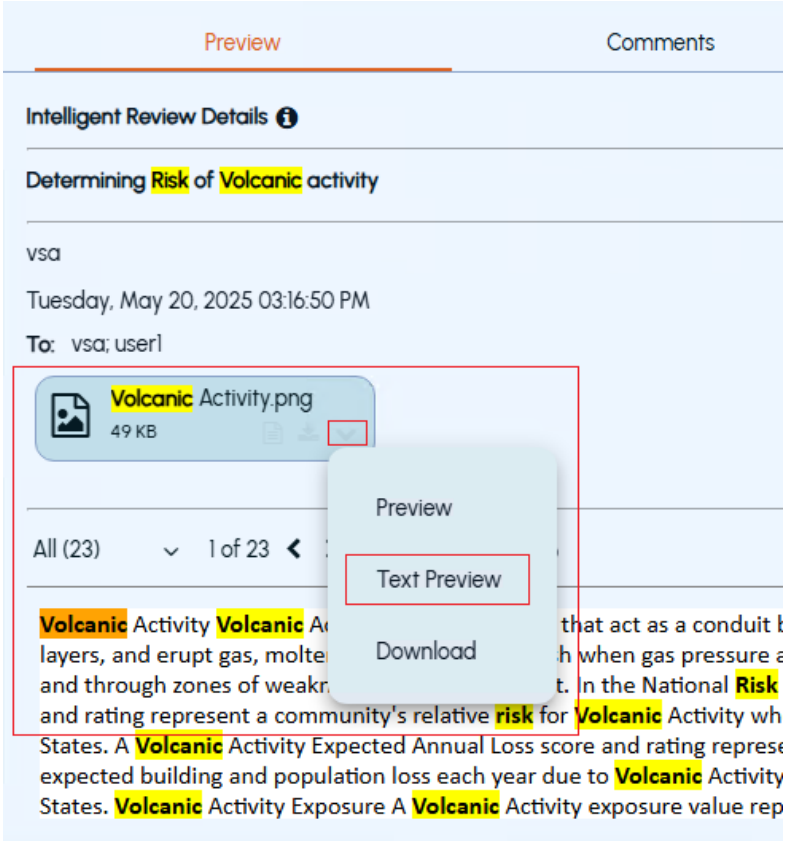
- Access the Hotwords pane. Expand the top-level hotword and check for the image hyperlink. If listed, click the hyperlink to open the text preview of the image directly.



- In the **Preview** pane, select the image and click the **Text Preview** icon to open the image in the text format.

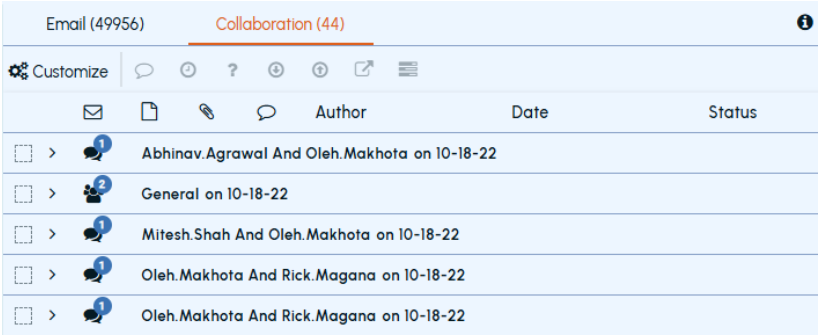


- In the **Preview** pane, click the down caret symbol and select the **Text Preview** option.



7 To review the filtered collaboration messages, select the **Collaboration** tab.

Collaboration tab displays maximum 100 groups per page. To view the next records in the group, use the navigation bar available in the bottom of a page. The chat or channel icons displays number of items in an individual group. The check box of a group remains disabled when the groups are in the collapsed state.



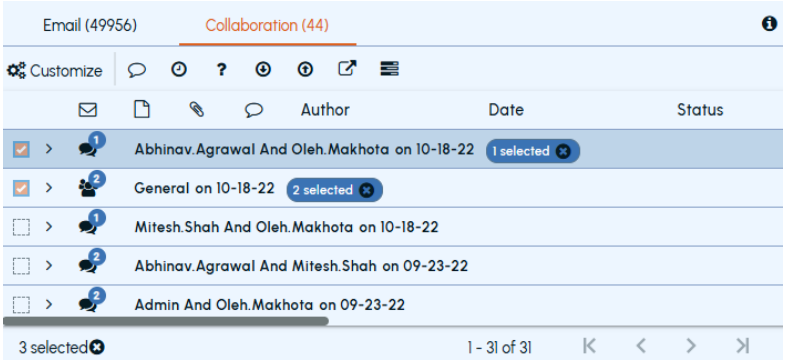
- Expand the chat or channel group to view and select the review items. Each group displays record of maximum 20 messages per page. However, if the group contains more than 20 items that are spread across multiple pages, you can do any of the following:
  - To select all the items displayed on the page of the expanded group, expand the group and select the parent check box of the group. After selecting the items, on the navigation bar of the page of the expanded group, the application displays the total count of selected items from that group.
  - To select items from the multiple pages of the expanded groups, expand the groups and use the navigation bar to access pages, and then select the items. After selecting the items from multiple pages of multiple groups,

    - On the navigation bar of a group row, the application displays the total count of selected items from that group.

    - On the navigation bar of the **Collaboration** page, the application displays the total count of selected items from multiple groups.

    - On the **Collaboration** page, if you select items from multiple groups and navigate to the next page, application clears the selection.

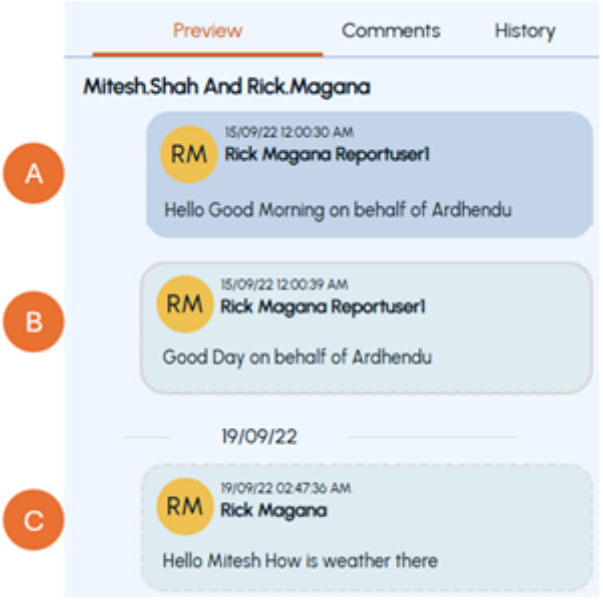
    - However, on the **Collaboration** page, if you select items from the same group and navigate to the next page, the application retains the item selection.

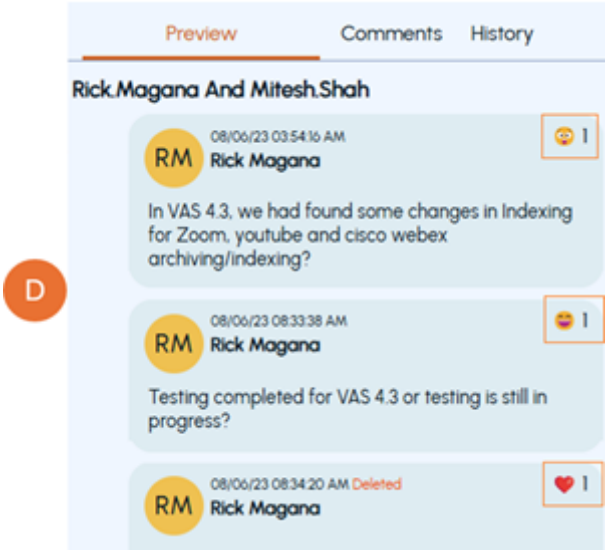


- After you expand the chat or the group, select an individual message for review.
  - On the **Preview** tab, you can do the following:
    - Scroll up or down to view more messages to understand the context of the selected message. The application displays 30 previous conversation messages above and 30 conversation messages below the selected message. However, you can further scroll up or down to read more messages.

      The typography of the displayed messages in the preview pane and its meaning is explained below.

Message Typography





Meaning...

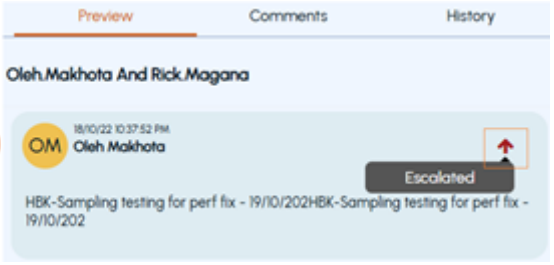
A. The messages that are selected for review after performing a search are highlighted in the yellow box.

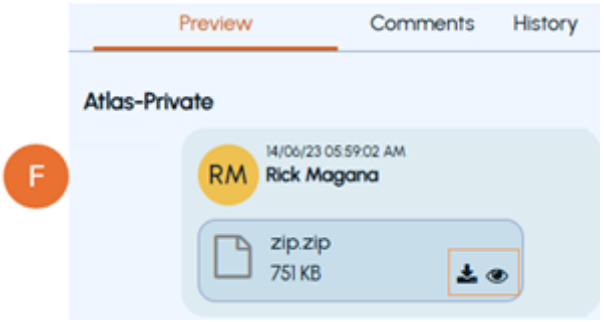
B. The messages that are part of the review process, and are displayed to get context for the reviewer, are marked in the grey box.

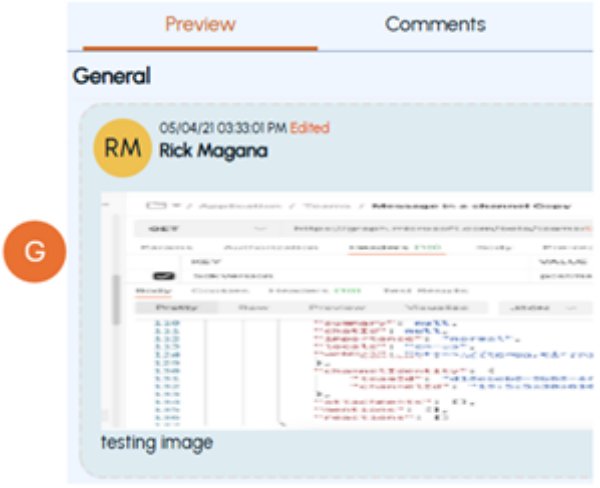
C. The messages that are not a part of the review set for that department are highlighted in the dashed box.

D. The messages displaying the reactions (smileys).

Message Typography







Meaning...

E. The messages displaying various statuses applied. For example, pending, escalated, appraised, and so on. You can hover over the status symbols to view the status name.

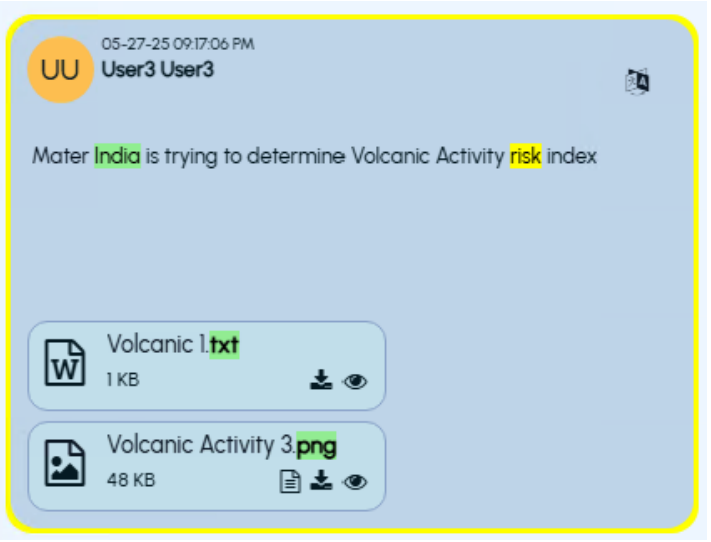
F. The messages containing attachments.

To download the attachment from the chat messages, click the **Download** icon provided on the attachment.

To preview the attachment from the chat messages without downloading it, either click on the attachment itself or click the **Preview** icon provided on the attachment

G. The messages containing images. You cannot download the images. However, to copy or save the images from the chat messages, right-click on the images and select appropriate actions.

- Preview and download attachments



Refer to the sample image above.

- To preview content of an attachment in a new window without downloading the attachment, either click on the attachment itself or click the **Preview** icon provided on the attachment.
- To download an attachment, access the attachment and click the download icon.
- The attachment preview also supports displaying hotwords and classification hit highlighting along with navigation.
- Click the **Text Preview** icon to open the image in the text format.

- On the **Comments** tab, you can view previous review comments for the selected message.
- On the **History** tab, you can view the detailed summary of the operations that are performed on the selected message.

- To comment on the selected collaboration message, click **Add Comment**. A reviewer can comment on individual messages, not on the entire conversation thread.See "Adding comments to items" on page 282.
- To assign status to the selected collaboration message, click *Pending*, *Questioned*, *Review Irrelevant*, *Reviewed Relevant*, *Escalate* (See "Escalating the review items" on page 283.), or *Appraised* as required.

Note: While reviewing collaboration messages, you cannot select more than 100 messages for commenting and assigning status.

Translating email and attachment content for review

While reviewing emails or attachments, you may encounter non-English content. To address this, Insight Surveillance provides a **Translate** feature to help you convert non-English text into English. After reviewing the translated content, you can revert it to the original language.

If translation is not enabled for your user account, clicking the **Translate** button displays the following message:

This feature is not enabled by your administrator. To enable, please do so in Management Console.

To enable translation

1. Navigate to: **Arctera Insight Management Console** > **Policy Management** > **Archive Options**.
2. Scroll to **Surveillance Translation**.
3. Set the status to **Enabled**, and click **Save**.

Note: Text contained within images cannot be translated.

To translate email and attachment content for review

1. In the left navigation pane, click **Review**.
2. Search for the items you want to review.

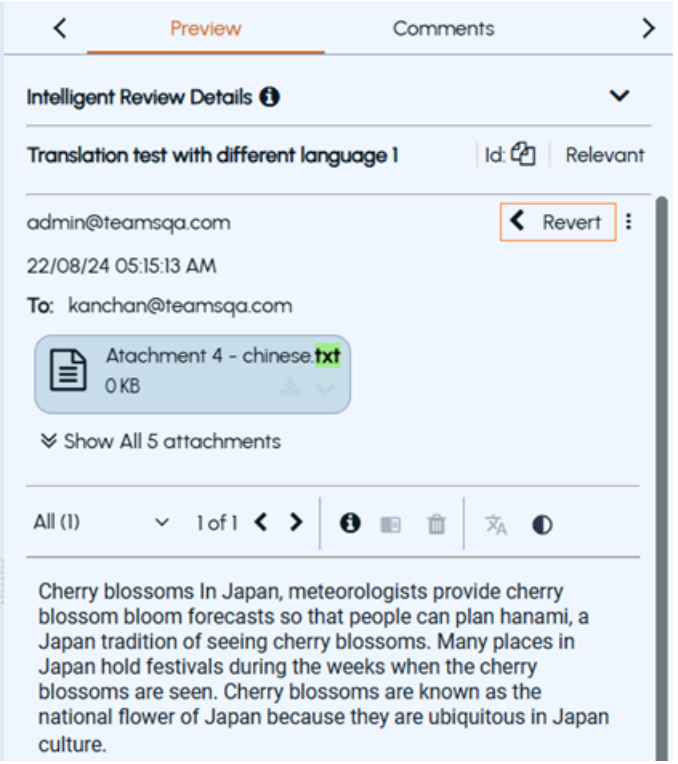
   Use **Advanced Filter** and **Filters** to narrow down your results.
3. On the **Email** tab, select an individual email in the items grid.

   The **Preview**,**Comments**, and **History** tabs appear to the right side of the selected email.

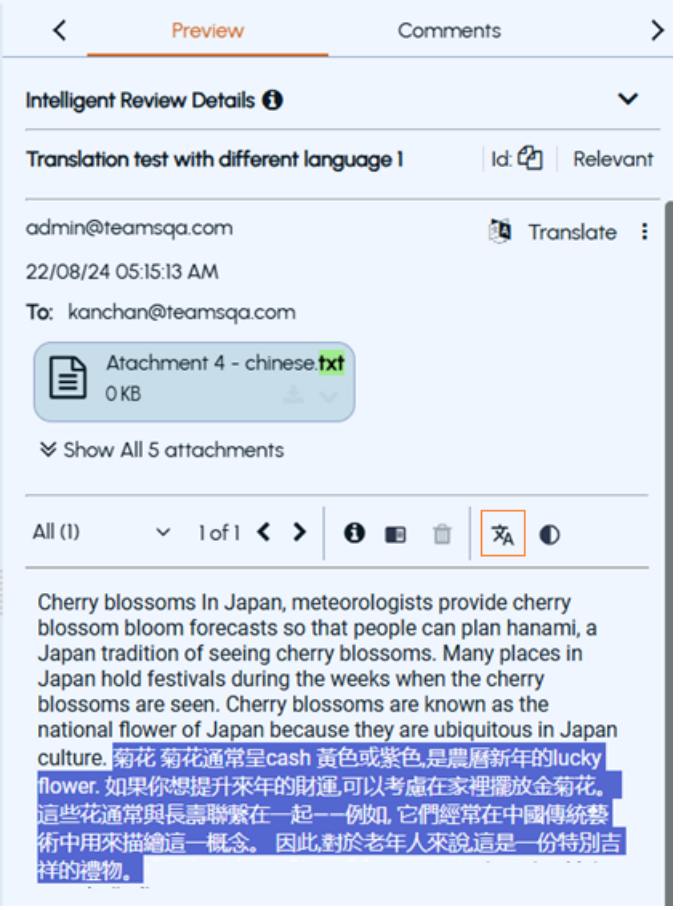
   Note: If you select multiple emails, these tabs are hidden. Instead, you see options to apply review statuses to all the selected messages.
4. On the **Preview** tab, do any of the following as needed:

- To translate the email body content into English, click **Translate** as shown in the sample image below:

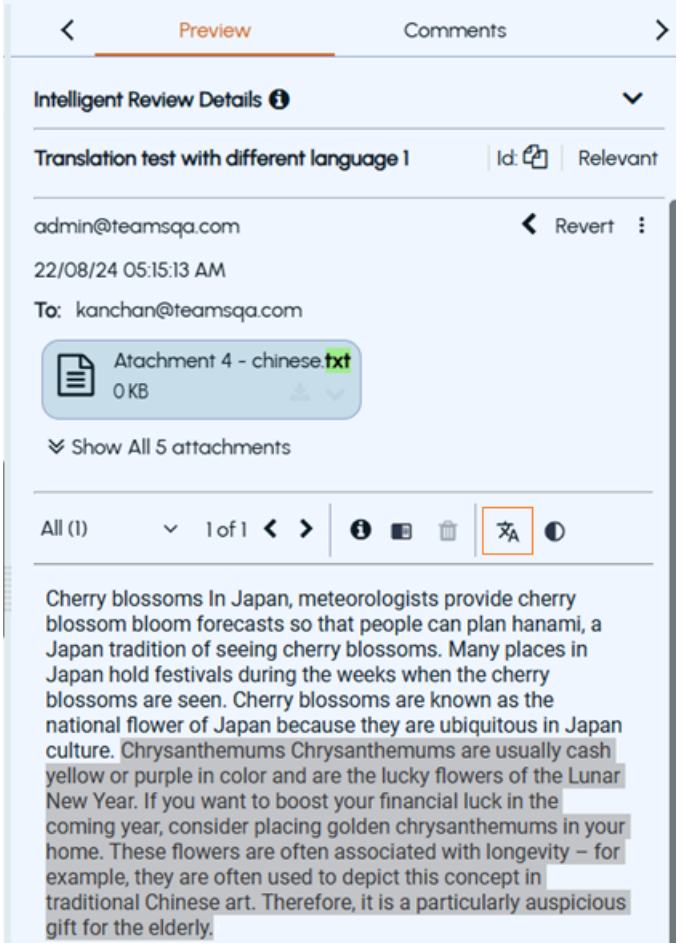
The **Translate** button changes to **Revert** after translation as shown in the sample image below:



- To translate only a part of the content into English, click the **Translate the selected text** icon as shown in the sample image below:



The application translates the content into English, as shown in the sample image below:



5 To translate the content of an attachment:

- Click the attachment.
  The attachment content appears in the preview panel as shown in the sample image below:

- To translate the entire content, click **Translate**.
- To translate a part of the content, select the text to translate and click the **Translate the selected text** icon.
- To return to the original language, click **Revert**.

Note: If the content includes a mix of languages, some text may remain untranslated. Use the **Translate the selected text** option to translate the untranslated text.

Translating collaboration message for review

While reviewing collaboration messages, you may encounter non-English content. To address this, Insight Surveillance provides a **Translate** feature to help you convert non-English text into English. After reviewing the translated content, you can revert it to the original language.

If translation is not enabled for your user account, clicking the **Translate** button displays the following message:

This feature is not enabled by your administrator. To enable, please do so in Management Console.

To enable translation

1 Navigate to: **Arctera Insight Management Console** > **Policy Management** > **Archive Options**.

2 Scroll to **Surveillance Translation**.

3 Set the status to **Enabled**, and click **Save**.

Note:

1. Text contained within images cannot be translated.
2. Partial text translation is not supported in the translation feature for collaboration messages.

To translate collaboration message for review

1 In the left navigation pane, click **Review**.

2 Search for the message you want to translate.

Use **Advanced Filter** and **Filters** to narrow down your results.

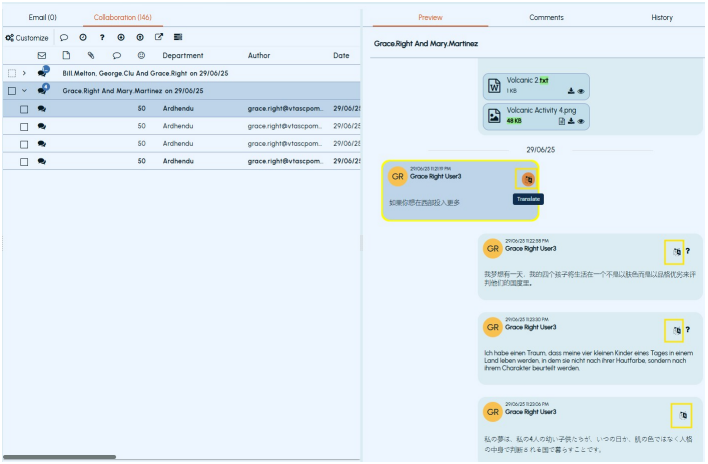
3 On the **Collaboration** tab, select an individual message in the items grid.

The **Preview**,**Comments**, and **History** tabs appear to the right side of the selected message.

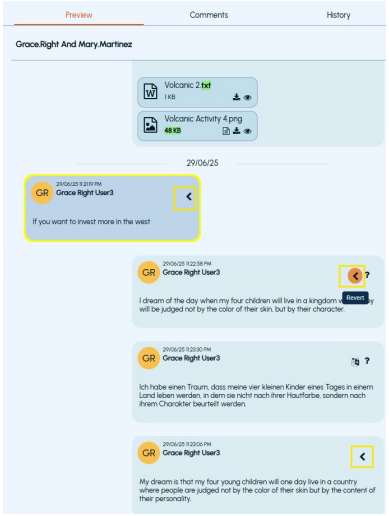
Note: If you select multiple messages, these tabs are hidden. Instead, you see options to apply review statuses to all the selected messages.

---

4 To translate the collaboration message content into English, click **Translate** as shown in the sample image below:



The **Translate** button changes to **Revert** after translation as shown in the sample image below:



Click **Revert** to return to the original language, if required.

Adding or removing text for machine learning

To review items and add or remove text for machine learning

1 In the left navigation pane, click **Review**.

2 Search for and select the department of which you want to review items.

Note: Insight Surveillance lists all departments. You can use the filtering options to search the required department. Options include filtering by department name, exception employees, and reviewers associated with the department.

---

3 (Optional) To reset the filtering criteria, click **Clear**, and set a new criterion.

4 Click **Apply**.

5 To review the searched and filtered emails, select the item to view its details in the reading pane.

The application displays email details and content in the **Preview** pane.

6 On the **Preview** tab of the reading pane, ensure that the **Learning** action bar is displayed.

Learning action bar lets you select the text samples for the intelligent review process. You can add or remove the selected text samples from the item being reviewed.

- To add text to the machine learning algorithm, select the desired text from the review item content or its attachment (if available), and click the *add* icon, located within the boxed area in the image above.

- To remove text to the machine learning algorithm, select the desired text from the review item content or its attachment (if available), and click the *remove* icon, located within the boxed area in the image above.

Note:

1. You can select up to 3000 characters in a single selection block from review item content or each attachment. Intelligent Review feature uses this data for identifying, categorizing, and quickly delivering items to reviewers.

2. The add or remove text for the machine learning feature is not available for Microsoft Teams chat and channel messages and the associated attachments.

Assigning review status to items

As part of the review process, you can assign a review status to each message to indicate that you have reviewed it and have no concerns—or conversely, that you do have some concerns, and therefore want to question the message.

The *Apply Review Action* permission restricts you to assign marks to the messages one at a time. In addition to the *Apply Review Action* permission, you need the following additional permissions to apply a specific action status mark to the message in a review set:

- Apply Review Action - Pending
- Apply Review Action - Questioned
- Apply Review Action - Reviewed Irrelevant
- Apply Review Action - Reviewed Relevant

If you have the *Apply Bulk Review Action* permission, you can assign review status to several messages at once. In addition to the *Apply Bulk Review Action* permission, you need the following additional permissions to apply a specific action status mark to multiple messages at a time while viewing messages in the List View mode:

- Apply Bulk Review Action - Pending
- Apply Bulk Review Action - Questioned
- Apply Bulk Review Action - Reviewed Irrelevant
- Apply Bulk Review Action - Reviewed Relevant

To assign a review mark to an item

1 In the left navigation pane, click **Review**.

2 Filter the items in the review pane.

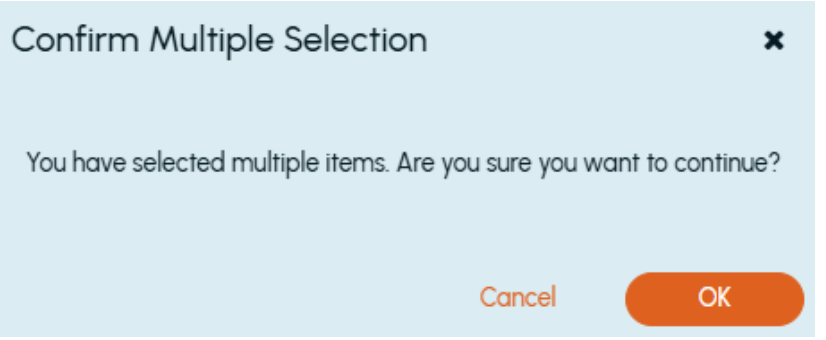
See "Filtering the items in the Review pane" on page 228.

3 Click **Apply**.

The application displays a list of review items from the selected departments.

4 During manual review, select one or more items to which you want to assign a review status.

When applying a review status to a single item, the application does not prompt to confirm the selection of the item. However, while applying a review status to multiple items, the application prompts a confirmation to ensure accurate selection and avoid errors, as shown in the sample image below.



5 Click the **Action** drop-down list, and do the following:

- Select **Pending** to keep the items pending for review.
  The key combination Alt+P typically assigns the **Pending** mark to an item.
- Select **Questioned** to raise query on the items.
  The key combination Alt+Q typically assigns the **Questioned** mark to an item.
- Select **Reviewed Irrelevant** to apply the compliance irrelevant mark to the selected items.
  The key combination Alt+I typically assigns the **Reviewed Irrelevant** mark to an item.

- Select **Reviewed Relevant** to apply the compliance relevant mark to the selected items.
  The key combination Alt+R typically assigns the **Reviewed Relevant** mark to an item.
- Select **Escalated** to escalate the items to the escalated reviewer for further attention.
  The key combination Alt+E typically assigns the **Escalated** mark to an item.
- Select **Appraised** to appraise the work of department reviewers and manage any exception employees in the department.
  The key combination Alt+A typically assigns the **Appraised** mark to an item.

Viewing hotwords highlighting

Insight Surveillance provides the option to highlight keywords in a hotword set that are added as search terms. Highlighting applies to subject, body content, and the HTML/text preview of an attachment. See "Creating and running department-level searches" on page 90.

A search with a hotword returns the exact matches only. When an asterisk character is used with the hotword, the search returns items with partial matches also. For example, two hotwords, "code" and "codebreaker," are available. A search with "code" returns items where "code" is present as an independent word. A search with "code*" returns all items that contain "codebreaker" as well as items that contain only the "code" keyword.

To view highlighted hotwords of an item

1 In the left navigation pane, click **Review**.

2 Search for and select the department for which you want to review items.

Note: Insight Surveillance lists all departments. You can use the filtering options to search the required department. Options include filtering by department name, exception employees, and reviewers associated with the department.

---

3 (Optional) To reset the filtering criteria, click **Clear**, and set a new criterion.

4 Click **Apply**.

The application displays emails and collaboration messages from the selected departments.

Note: If only the **Exchange** service is enabled for you, then only emails are displayed. If the MS Teams Archiving service is enabled for you, then collaboration messages are also displayed.

---

5 During the manual review, select the item to view its details in the **Preview** pane.

6 Navigate across the hits for a phrase, all hotwords, or a specific hotword.

Note: Highlighting navigation control is shown only if at least one hotword or a tag is applied to the review item.

The hotwords and the tags are highlighted in the **Preview** pane of emails and collaboration messages. However, the navigation option to go to the next or previous hotword or a tag is available only for emails, and not for collaboration messages.

A sample image to show hotwords highlighting and navigation in **email** is shown below.

7 In the **Preview** pane, click the drop-down arrow to view a list of hotwords and phrases.

Note: The application lets you review maximum hotword instance in the content by highlighting them. Therefore, when any search is based on multiple hotwords and phrases, and if any word or a fragment of a phrase is common among the hotwords and phrases, the improved hit-highlighting feature displays that word or a phrase as a separate hotword in the drop-down list.

For example, the word ***draft*** is a part of the sentence - ***The email includes the updated draft in the attachment***. In this case, the hit-highlighting feature provides you the hotword options like ***draft***, ***updated draft***, and ***The email includes the updated draft in the attachment*** as the word 'draft' is common in all instances.

You can select **All** to highlight all the hotwords. Else, you can select a specific hotword from the list that you want to get highlighted for review.

Note that multiple negative hotwords are excluded from hit highlighting.

---

8 Select the required hotword in the list to get it highlighted in the content.

Hover over the hotword instance to view the search that is applied to the review item.

9 Click the Next arrow icon to view the next highlighted hotword instance. To view the previous instance of highlighted hotword, click the Previous arrow icon.

10 (Optional) Preview an attachment content and navigate across the hits for all hotwords or a specific hotword.

Viewing hotwords in collaboration message

Insight Surveillance provides the option to highlight keywords in a hotwords set that are added as search terms. Highlighting applies to message content and attachment content only. See "Creating and running department-level searches" on page 90.

If the collaboration message contains the hotwords and tagged instances, the hotwords are highlighted in yellow color and the tags are highlighted in green color.

A search with a hotword returns the exact matches only. When an asterisk character is used with the hotword, the search returns items with partial matches also. For example, two hotwords, "code" and "codebreaker," are available. A

search with “code” returns items where “code” is present as an independent word. A search with “code*” returns all items that contain “codebreaker” as well as items that contain only the “code” keyword.

To view highlighted hotwords in a collaboration message

1 In the left navigation pane, click **Review**.

2 Search for and select the department for which you want to review items.

Note: Insight Surveillance lists all departments. You can use the filtering options to search the required department. Options include filtering by department name, exception employees, and reviewers associated with the department.

---

3 (Optional) To reset the filtering criteria, click **Clear**, and set a new criterion.

4 Click **Apply**.

The application displays emails and collaboration messages from the selected departments.

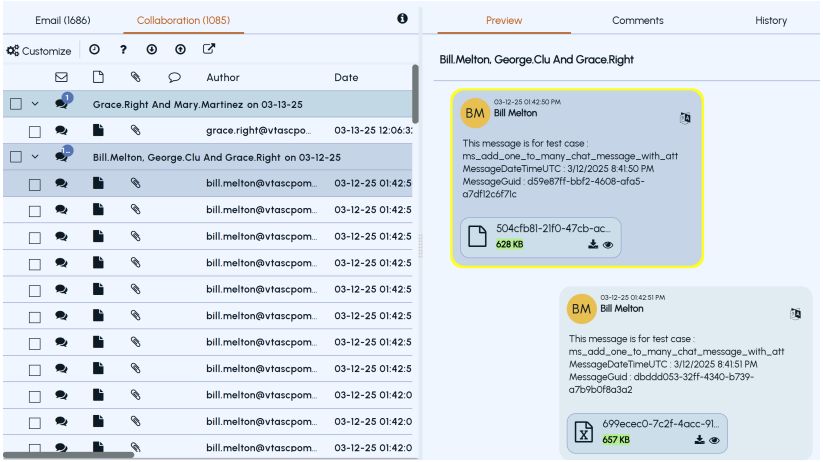
5 Select a Teams Chat or Channel item to view its details in the **Preview** pane.

Note: If the search applied to the item has configured with hotwords, these hotwords are shown in the Preview pane and are highlighted in yellow color. However, highlighting is shown only if at least one hotword is applied to the review item.

---

6 To navigate through older chat messages, use the scroll bar.

7 To view the search that is applied to the review item, hover over the hotword instance.



Viewing tags highlighting

Arctera Insight Surveillance provides the option to highlight tags applied to the item you want to review. Tags are highlighted only if the items are applied with at least one tag. The tag statistics section lists the tags for which Insight Surveillance performs highlighting.

Arctera Insight Surveillance supports tag highlighting in the following fields of emails:

- Subject
- Primary email content
- Message body(Policy condition created in Insight Classification to classify only message body and not the attachment content. The corresponding highlights is shown in Insight Surveillance.)
- Attachment name
- Attachment content
- Attachment size
- Attachment extension
- Author
- Recipient (To/Cc/Bcc)
- Date

Arctera Insight Surveillance does not support tag highlighting in the following fields of emails:

- Process date
- Attachment count
- Attachment date
- Recipient count
- Item size
- Direction

The item can have multiple tags applied to it. The hotwords and tags are highlighted in the **Preview** pane of emails and collaboration messages. You can hover over the highlighted content to see other tags applied to it. If the email contains the hotwords and tagged instances, the hotwords are highlighted in yellow color and the tags are highlighted in green color. The hotwords navigation option is available only for emails, and not for collaboration messages.

Note: When the tags suggested by Arctera Insight Classification have a content match length exceeding 300 characters, Insight Surveillance does not highlight those tags in the **Preview** pane.

To view highlighted tagged content of an item

1 In the left navigation pane, click **Review**.

2 Search for and select the department for which you want to review items.

Note: Arctera Insight Surveillance lists all departments. You can use the filtering options to search the required department. Options include filtering by department name, exception employees, and reviewers associated with the department.

---

3 (Optional) To reset the filtering criteria, click **Clear**, and set a new criterion.

4 Click **Apply**.

The application displays a list of review items from the selected departments.

5 During the manual review, select the item to view its details in the reading pane.

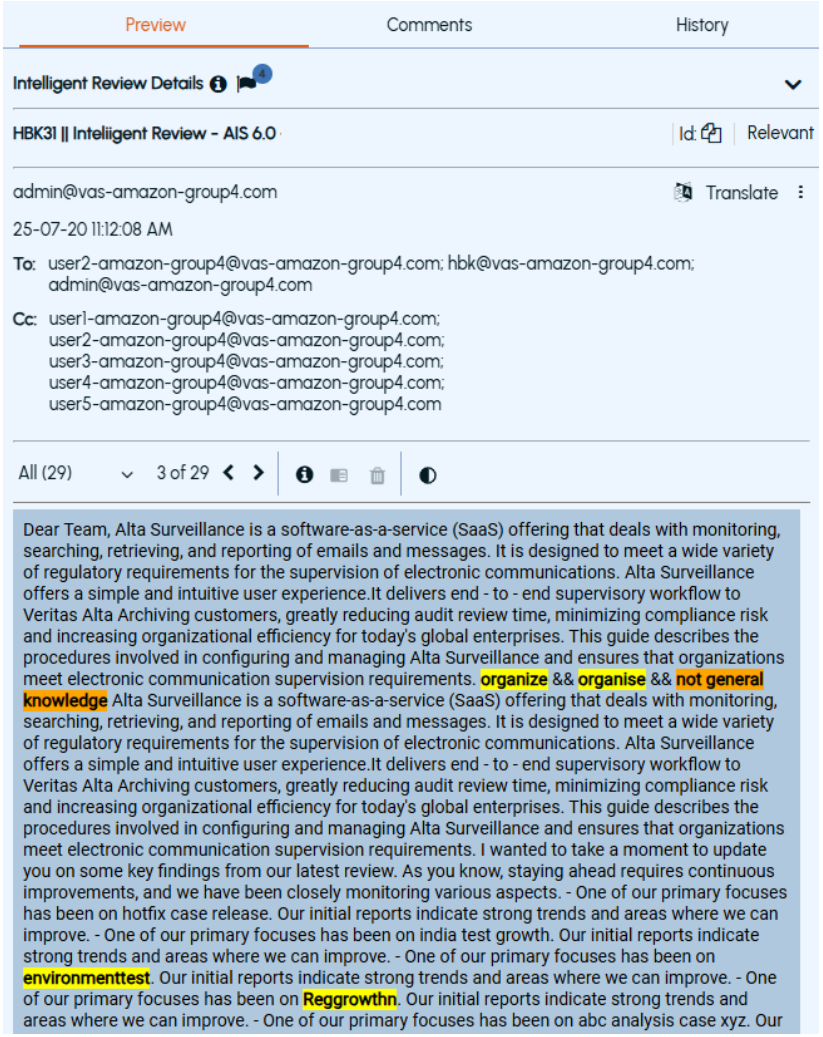
To view tagged items, from the **Filter** pane in the left navigation pane, expand the **Tags** option, and select the specific tags. The application displays only those items to which the selected tags are applied. The **Tags summary** column shows the tags applied to the items.

6 Navigate across the hits for tags.

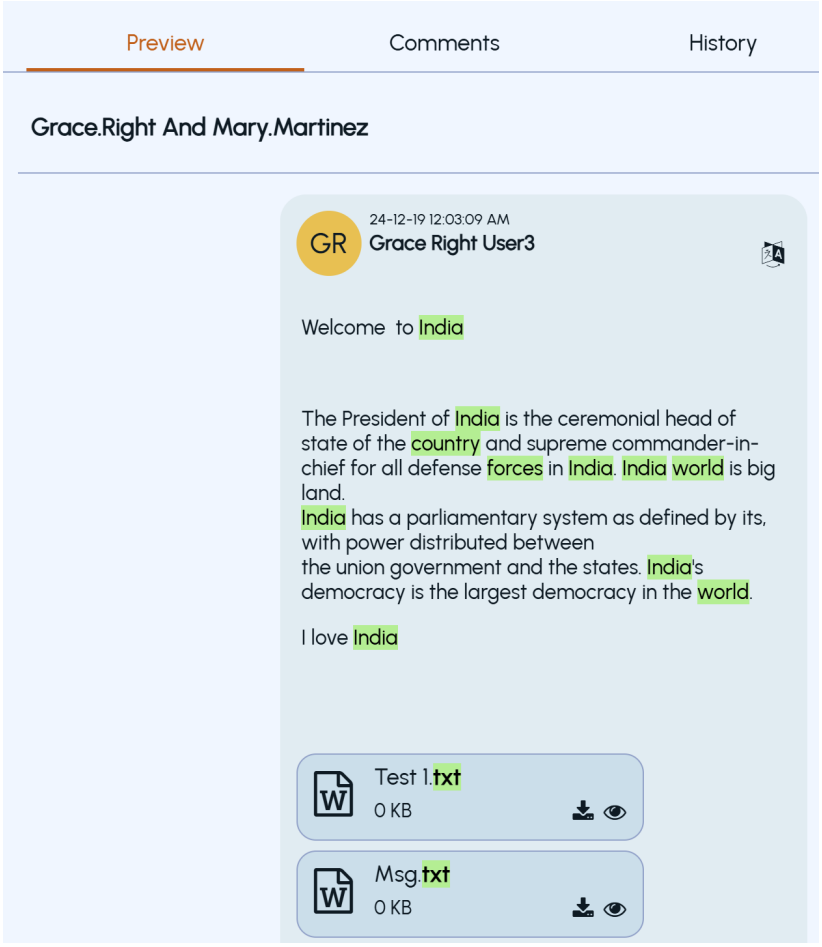
Note: Highlighting navigation control is shown only if at least one hotword or a tag is applied to the review item.

The hotwords and the tags are highlighted in the **Preview** pane of emails and collaboration messages. However, the navigation option to go to the next or previous hotword or a tag is available only for emails, and not for collaboration messages.

A sample image to show tags highlighting and navigation in **email** is shown below.



A sample image to show tags highlighting in **collaboration messages** is shown below.



7 In the **Preview** pane, click the drop-down arrow and do any the following:

- Select **All** to highlight all the hotwords and all the tags in the item simultaneously.
- Select **Tags** to highlight only the tagged instances.
  This option displays the total count of matching contents corresponding to tags applied to that item. For example, Tags (2) represents two matching content found in that item corresponding to tags applied to the item. Hover over this option to see the tag names.
- Select individual words under **Hotwords** to highlight only the selected hotword.

8 Click the Next arrow icon and the Previous arrow icon to navigate across the hits for tagged instances.

9 Hover over the highlighted tagged instance to view which other tags are applied to the same content.

10 To print the review item's content, click the Ellipses icon (three vertical dots) in the upper-right corner of the **Preview** pane. Click **Print** and select the format and location to save the file at your accessible location.

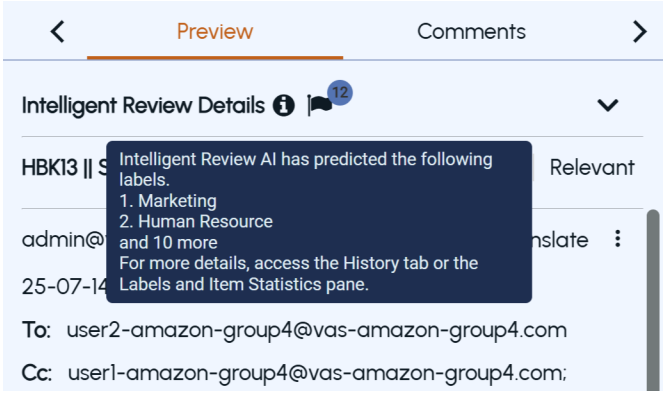
11 To download the review item's content with the highlighted tagged instances, click the Ellipses icon (three vertical dots) in the upper-right corner of the **Preview** pane. Click **Download** and select the format and location to save the file at your accessible location.

Viewing predicted labels of review items

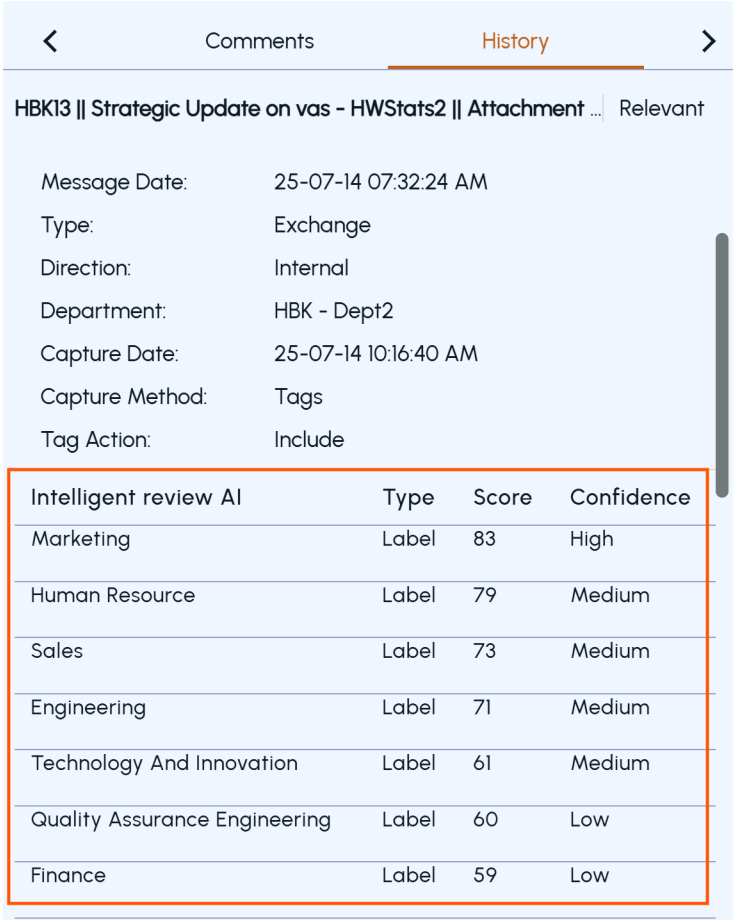
Reviewers can view predicted labels assigned to the review items in the following ways:

- **Item Grid pane**: In the item grid on the **Review** page, access the *Predicted labels* column to view the predicted labels for each item. If multiple labels are predicted, they are separated by semicolon. Refer to the image below:

- **Preview pane**: In the **Preview** pane on the **Review** page, hover over the flag icon (representing **AI-based Label Predictions**) to view a tooltip containing information about the predicted labels and groups, including their count. Refer to the image below:



- **History pane**: On the **Review** page, access the **History** pane.
  The table displays details as shown in the sample image below:



- Intelligent Review mark as *Relevant* or *Irrelevant* and its relevancy score.
- Labels associated to the item, its score and confidence level.

- **Labels and Items Statistics pane**: On the **Review** page, access the **Labels and Items Statistics** pane. Expand the **Labels** section and select the check box next to all the labels you need to apply. It does not select the labels from the single choice group. Refer to the sample image below.

- To remove any label, just uncheck the label. It gets removed and the same is reflected in **Labels Summary** column.

Viewing the full content in a new window

Insight Surveillance provides an option to double-click on emails to view their content in a new browser window and navigate to the next and previous items from the current page. However, you cannot double-click on collaboration messages to view their content in a new browser.

To view the full content of an item

1 In the left navigation pane, click **Review**.

2 Search for and select the department for which you want to review items.

Note: Insight Surveillance lists all departments. You can use the filtering options to search for the required department. Options include filtering by department name, exception employees, and reviewers associated with the department.

---

3 (Optional) To reset the filtering criteria, click **Clear**, and set a new criterion.

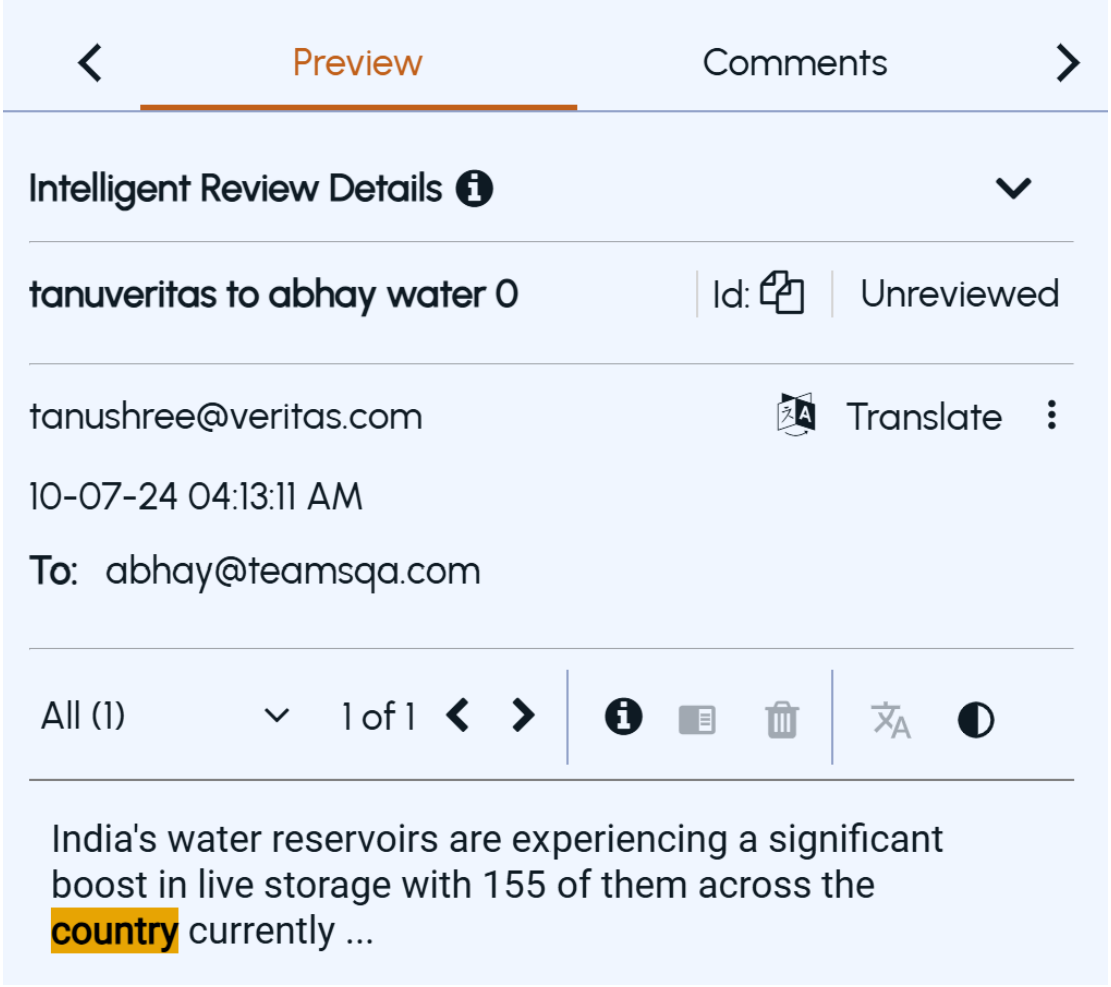
4 Click **Apply**.

The application displays a list of review items from the selected departments.

5 During the manual review, select an email and double-click on a corresponding row to view its content in a new window.

Note: Double-clicking an item to view its content in a new browser is supported for emails only, and not for collaboration messages.

6 Navigate to **Next** or **Previous** item using the cross-navigation buttons.



Note: Cross-navigation works on the current page from the items list.

Adding comments to items

As like assigning a review mark to an item, you can add a comment to it.

The permissions that are assigned to you determine the types of comments that you can add. You must have the *Add Own Review Comments* permission in order to add comments in your own words.

To add comments to an item

1 In the left navigation pane, click **Review**.

2 Filter the items in the review pane.

See "Filtering the items in the Review pane" on page 228.

3 Click **Apply**.

The application displays emails and collaboration messages from the selected departments.

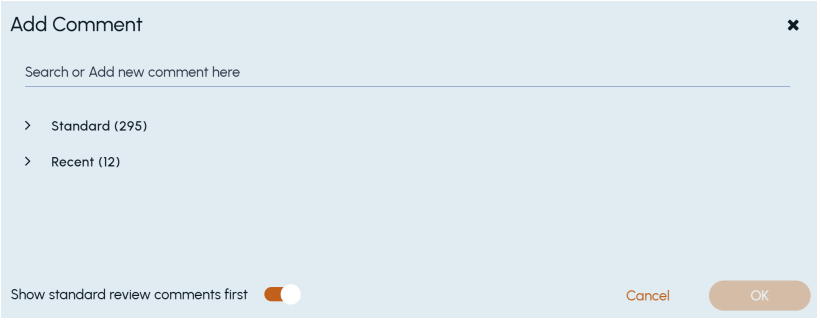
Note: If only the **Exchange** service is enabled for you, then only emails are displayed. If the MS Teams Archiving service is enabled for you, then collaboration messages are also displayed.

---

4 During manual review, select the item to view its details in the **Preview** pane.

5 Click **Add Comment**.

Alternatively, use the Alt+M shortcut key to add comments to an item. The **Add Comment** dialog box appears.



6 Expand the **Standard** or **Recent** comments group, and select a relevant predefined comment, depending on your permission level.

If you do not find a relevant predefined comment, enter a new comment for the item.

Note: To view the Standard review comments first always, enable the **Show standard review comments first** option.

---

7 Click **OK**.

The item is marked with the comment symbol.

A comment indicator is displayed in the **Comment present** column of the item list to show that you have added the comment. Click the **Comments** tab at the bottom of the Reading pane to view the comments assigned to an item. You can also customize the item list columns to add a column that shows the comments on items.

Escalating the review items

Like adding comments to the review items (emails and collaboration messages), you can escalate the review items to an individual reviewer or a group of escalation reviewers.

To escalate a review item

1 In the left navigation pane, click **Review**.

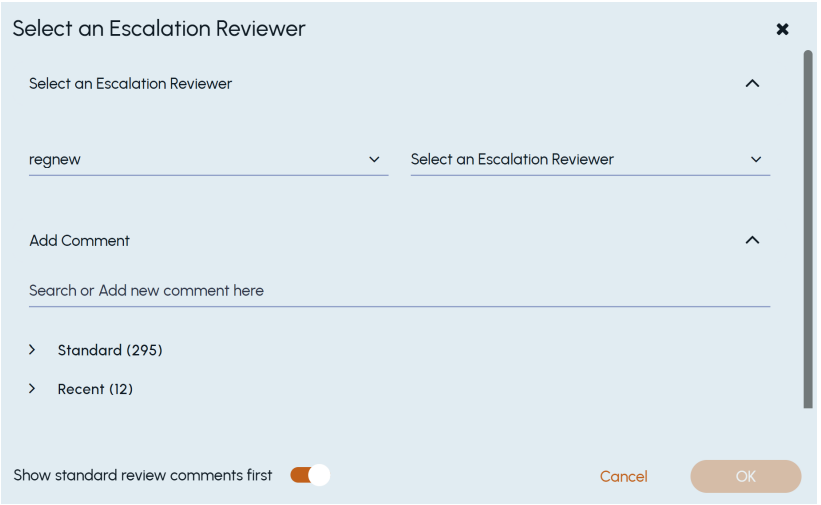
2 Search for and select the department and the item you want to escalate from that department.

See "Filtering the items in the Review pane" on page 228.

3 View the details in the **Preview** pane.

4 On the action bar, click **Escalate**.

The **Select an Escalation Reviewer** dialog box appears.



The department name appears in the first drop-down field.

5 In the **Select an Escalation Reviewer** drop-down, select an individual reviewer or an escalation reviewers group to whom you want to escalate the review item.

Selecting an escalation reviewers group is beneficial, as any member can review escalated items, whereas an individual reviewer's absence may cause delays.

6 Under **Add Comments**, expand the **Standard** or **Recent** comments group, and select a relevant predefined comment, depending on your permission level.

If you do not find a relevant predefined comment, enter a new comment for the item.

Note: To view the Standard review comments first always, enable the **Show standard review comments first** option.

---

7 Click **OK**.

The item is marked with the escalation symbol.

After an item is escalated, you can view the selected escalation reviewer or escalation reviewer group in the **Escalation Owner** column of the items grid, within the **History** pane of the item, and in the **Escalation Reviewer** facet under **Filters**.

Applying labels to items

During a review, you can apply labels to review items such as emails and collaboration messages. The application displays only the currently active labels that can be utilized for labeling the items. The example explained in this section is applying labels to emails. You can use the same procedure to apply labels to the collaboration messages.

The permissions that are assigned to you determine the labels that you can add. By default, the *Compliance Supervisor, Exception Reviewer, Department Reviewer*, and the *Escalation Reviewer* roles have the *Apply Labels* permission.

To apply labels to an item

1 In the left navigation pane, click **Review**.

2 Filter the items in the review pane.

See "Filtering the items in the Review pane" on page 228.

3 Click **Apply** to view the review items (emails and collaboration messages) from the selected departments.

4 Select the item to view its details in the **Preview** pane.

Along with the content preview, the application displays comments and history of the review item in the respective tabs.

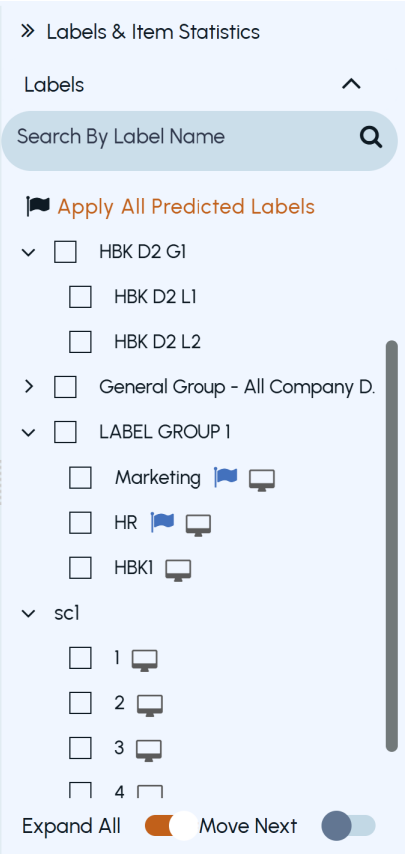
5 In the **Labels & Item Statistics** pane, expand the **Labels** section.

The application displays only active labels that are listed under the available label groups and single choice label groups as shown in the following sample image:

6 Expand the groups, or search for and select one or more relevant labels that are listed under the available label groups and single choice label groups. The individual labels that are not part of any group are listed under the **No Group** node.

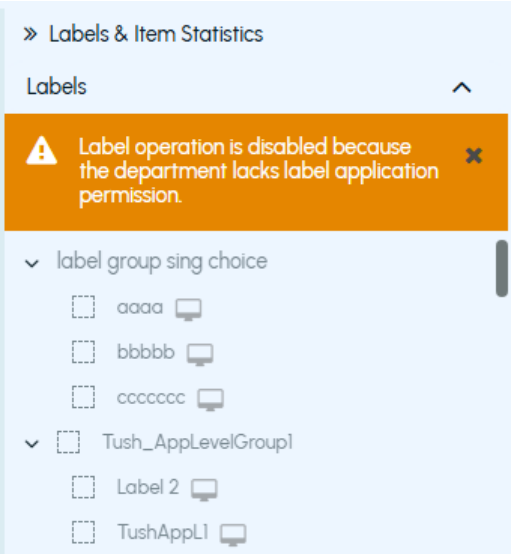
7 In the **Labels** pane, select the check box next to all the labels you need to apply.

Note: You can easily distinguish between the application-specific, department-specific labels, and AI-predicted labels. The department-specific labels do not have any icon. The application-specific labels are displayed along with the monitor icon. The AI-predicted labels are displayed along with the flag icon. Refer to the following sample image:

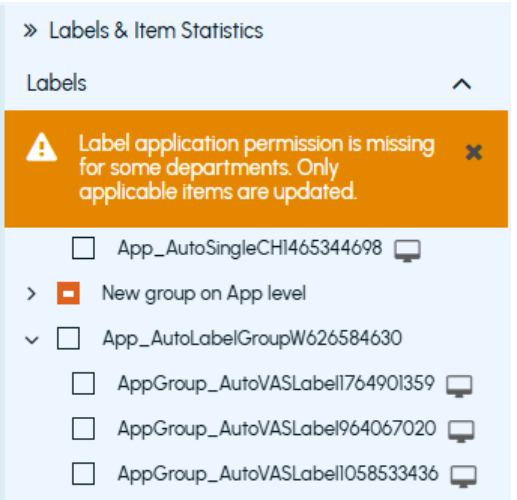


Notifications and Permissions Behaviour

- If a department does not have permission to apply labels, the label pane is disabled, and a notification is displayed:
  Label operation is disabled because the department lacks label application permission.



- If you select multiple departments items and only some have label permissions, the label pane remains enabled, and a notification is displayed:
  Label application permission is missing for some departments. Only applicable items are updated.



  In this case, labels are applied only to items from departments with the appropriate permissions. The same can be confirmed by label checkbox which shows a partial selection.

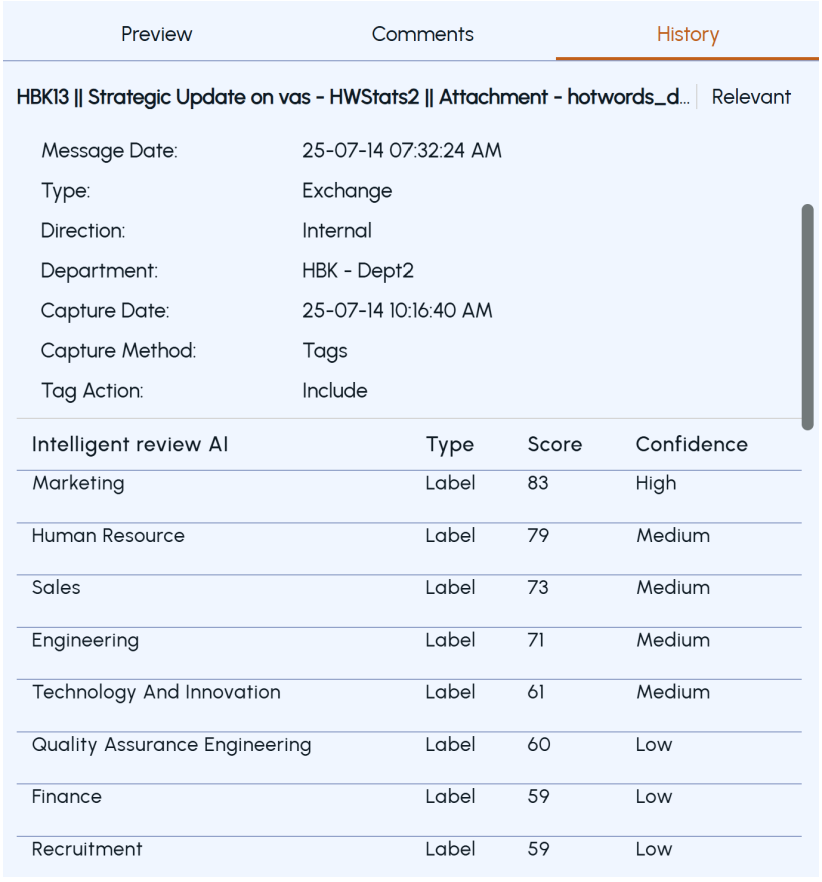
- Click **Apply All Predicted Labels** to apply all the AI-predicted labels to the selected items, except those from single choice groups.
- Click **Expand All** to switch between the collapsed and expanded views to view the available labels.
- Click **Move Next** to perform a single label action and proceed to the next item automatically.

Applied labels appear in the **Labels Summary** column, while AI-predicted labels appear in the **Predicted Labels** column. Multiple labels are separated by semicolons (;) as shown in the following sample image. You cannot sort the items using this column.

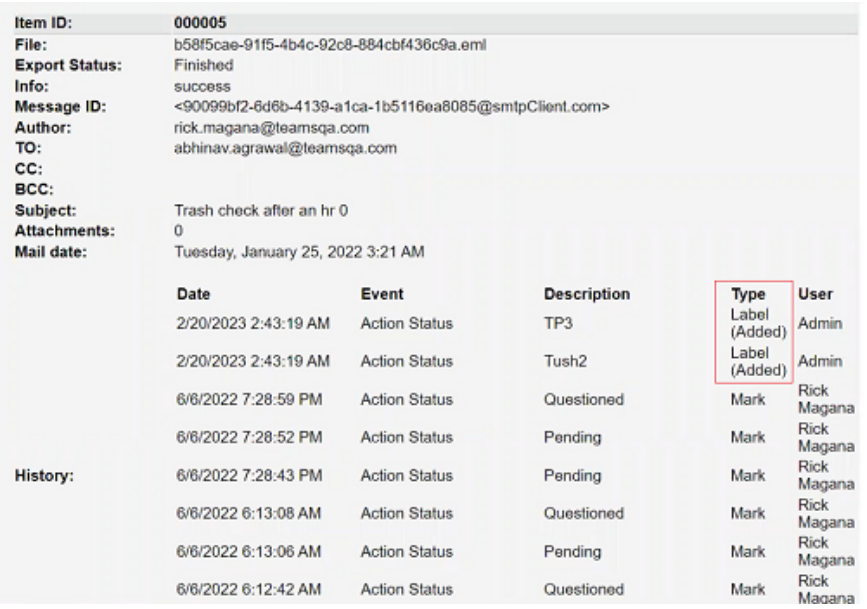
8 To remove any label, just uncheck the label. It gets removed and the same is reflected in **Labels Summary** column.

9 Click on the same review item and select the **History** tab.

The labels history is shown as shown in the following sample image:



Note: Upon exporting, the export report includes the details and the history of added and deleted labels under the **Type** column as shown in the sample image below.



Item ID:	**000005**				
File:	b58f5cae-91f5-4b4c-92c8-884cbf436c9a.eml				
Export Status:	Finished				
Info:	success				
Message ID:	<90099bf2-6d6b-4139-a1ca-1b5116ea8085@smtpClient.com>				
Author:	rick.magana@teamsqa.com				
TO:	abhinav.agrawal@teamsqa.com				
CC:					
BCC:					
Subject:	Trash check after an hr 0				
Attachments:	0				
Mail date:	Tuesday, January 25, 2022 3:21 AM				
	Date	**Event**	**Description**	**Type**	**User**
	2/20/2023 2:43:19 AM	Action Status	TP3	Label (Added)	Admin
	2/20/2023 2:43:19 AM	Action Status	Tush2	Label (Added)	Admin
	6/6/2022 7:28:59 PM	Action Status	Questioned	Mark	Rick Magana
	6/6/2022 7:28:52 PM	Action Status	Pending	Mark	Rick Magana
History:	6/6/2022 7:28:43 PM	Action Status	Pending	Mark	Rick Magana
	6/6/2022 6:13:08 AM	Action Status	Questioned	Mark	Rick Magana
	6/6/2022 6:13:06 AM	Action Status	Pending	Mark	Rick Magana
	6/6/2022 6:12:42 AM	Action Status	Questioned	Mark	Rick Magana

Viewing history of items

Insight Surveillance provides ready access to historical information on a selected item, such as the dates and times at which the reviewers assigned marks and comments to it.

You must have the *Review Messages* permission to view the history of items. By default, all reviewers and supervisors have this permission.

To view the history of an item

1 In the left navigation pane, click **Review**.

2 Filter the items in the review pane.

See "Filtering the items in the Review pane" on page 228.

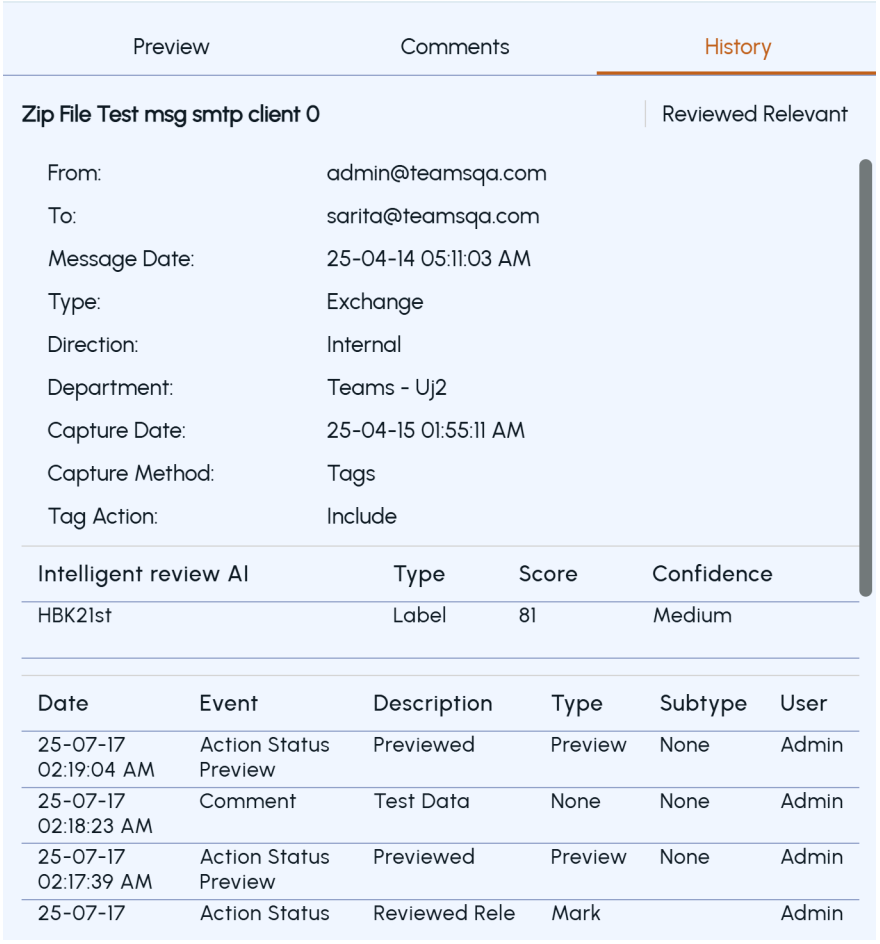
3 Click **Apply**.

The application displays a list of review items from the selected departments.

4 During manual review, select the item to view its history details in the reading pane.

5 In the reading pane, click **History**.

The following details appear as shown in the sample image below:



- The subject, date, and details of the sender and recipients.
- The item type, such as Microsoft Exchange or Bloomberg, and its direction (Internal, External Inbound, or External Outbound).
- The department in which Insight Surveillance has captured the item.
- Capture date and method by which the item was captured.

- The event history, tag actions history, the X-Header history, IR marking and labels history of the item.
- The reviewer's actions in the **Preview** pane.
  If the administrator has enabled the setting to log preview actions, whenever an item is viewed in the **Review** pane, Insight Surveillance records the reviewer's preview activity in the item history.

Note: By default, the feature is disabled. To enable this feature, please contact Arctera Technical Support.

Printing and downloading the items and attachments

Besides the HTML-rendered view of the items in the **Preview** pane, you can print and download the item in its original form. The downloaded items exclude audit-specific information, like reviewer comments. To obtain the item and its audit information, you need to export the item.

Note: Insight Surveillance does not support previewing certain file types, such as ***.dll*** and **.exe** and large files (over 10MB to maintain browser responsiveness). For compressed files, Insight Surveillance supports previewing only the ***.zip*** file format and does not support other formats like ***.7z***, ***.tar***, and so on.

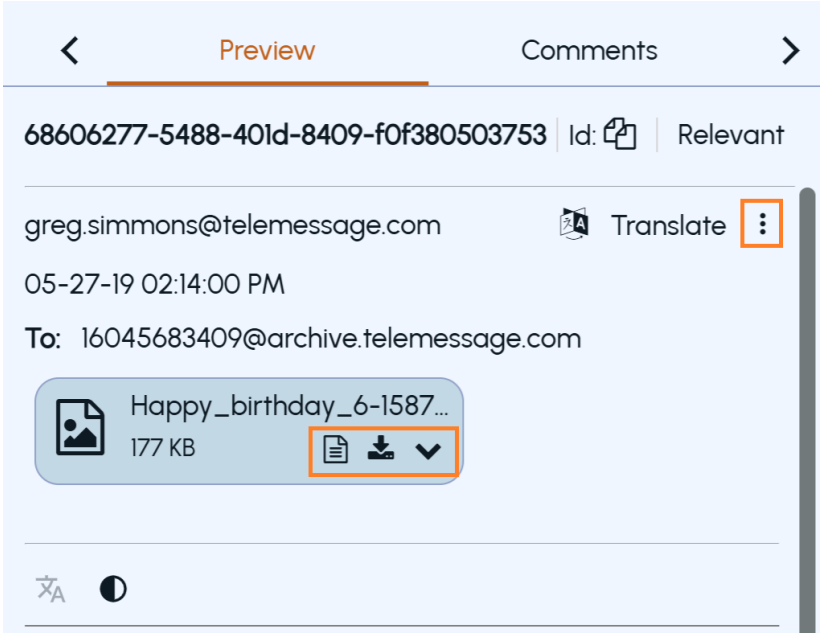
You must possess the *Review Messages* permission to download items. By default, all reviewers and supervisors have this permission.

To print and download the item and attachment

1. In the left navigation pane, click **Review**.
2. Filter the items in the review pane. See "Filtering the items in the Review pane" on page 228.

   In the items grid, a list of review items from the selected departments appears.

3 Select the review item in the items grid, and access the **Preview** tab as shown in the sample image below.



Note: If you select multiple items, you cannot print or download these items simultaneously.

4 Do the following as required.

- To download an attachment, hover over the attachment, and click the **Download** icon. The file is downloaded to a location based on your settings, mostly in the *Downloads* folder.
- To download the original version of item, click the kebab icon and click **Download**.
- To print the item, click the kebab icon and click **Print**.
  In the **Print** dialog box, ensure the correct file format and specify the location to save the file.

Viewing Intelligent Review Details

The **Intelligent Review Details** section provides the facts of why the item is classified as *Unreviewed Relevant* or *Unreviewed Irrelevant*. It shows the **Relevant** and **Irrelevant** labels (links) and the respective contribution.

During review, the **Intelligent Review Details** section appears on the **Preview** tab only if the departments you want to review are enabled for Intelligent Review, and the *Show Intelligent Review Details in Review* permission is enabled for the logged-in user. This permission is by default enabled for the *Department Reviewer, Escalation Reviewer, Compliance Supervisor, Exception Reviewer, and Passive Reviewer* roles, where either the *Review Messages* or the *Review Escalations* permissions are enabled. By default, Intelligent Review Details section is collapsed. Users can expand and collapse it as required.

The total relevant and irrelevant contribution value is shown besides the respective labels. These values (between 0 to 100) are factor of relevant and irrelevant contributions found inside the item. When you click the Relevant and Irrelevant labels, the corresponding details appear which shows the factors that have contributed towards relevant or irrelevant. The calculated values of a contribution of each factor are mentioned so that a reviewer can understand the reason behind the item being relevant or irrelevant.

If the contribution value of the relevant factors is more than the contribution value of the irrelevant factors, the item will have higher relevance score (greater than 50). If the contribution value of the irrelevant factors is more than the contribution value of the relevant factors, the item will have lower relevance score (less than 50). If the contribution values of the relevant and irrelevant factors are almost similar, the item will have the relevance score around 50.

The factors that contribute are Author, Recipient, Subject, Content, Direction, Tags, and Department influence. Department Influence shows the extent to which prediction is inclined in favor of or against the marking based on the department's learning. If reviewers in a department favor marking items as irrelevant, then Department Influence will contribute towards irrelevance and vice versa. If factors do not have values, they can still contribute as relevant or irrelevant. It happens when the algorithm weighs the lack of details (such as the presence of zero tags or absence of content) as a contributing factor to its learning.

If the contribution of any factor is insignificant, but not absolutely zero (0), then value can be rounded to and displayed as zero (0). If the factor does not contribute at all, then this factor is not displayed. The amount of contribution of each factor is also shown with the color legend.

The flag icon, representing **AI-based Label Predictions**, shows AI-predicted labels and their count for each review item if the *Enable AI Predictions* option is selected for active labels and label groups.

Refer to the sample images below.

Figure 24-3 Preview pane showing the IR details, hit highlighting, managing text for learning, and AI-predicted labels

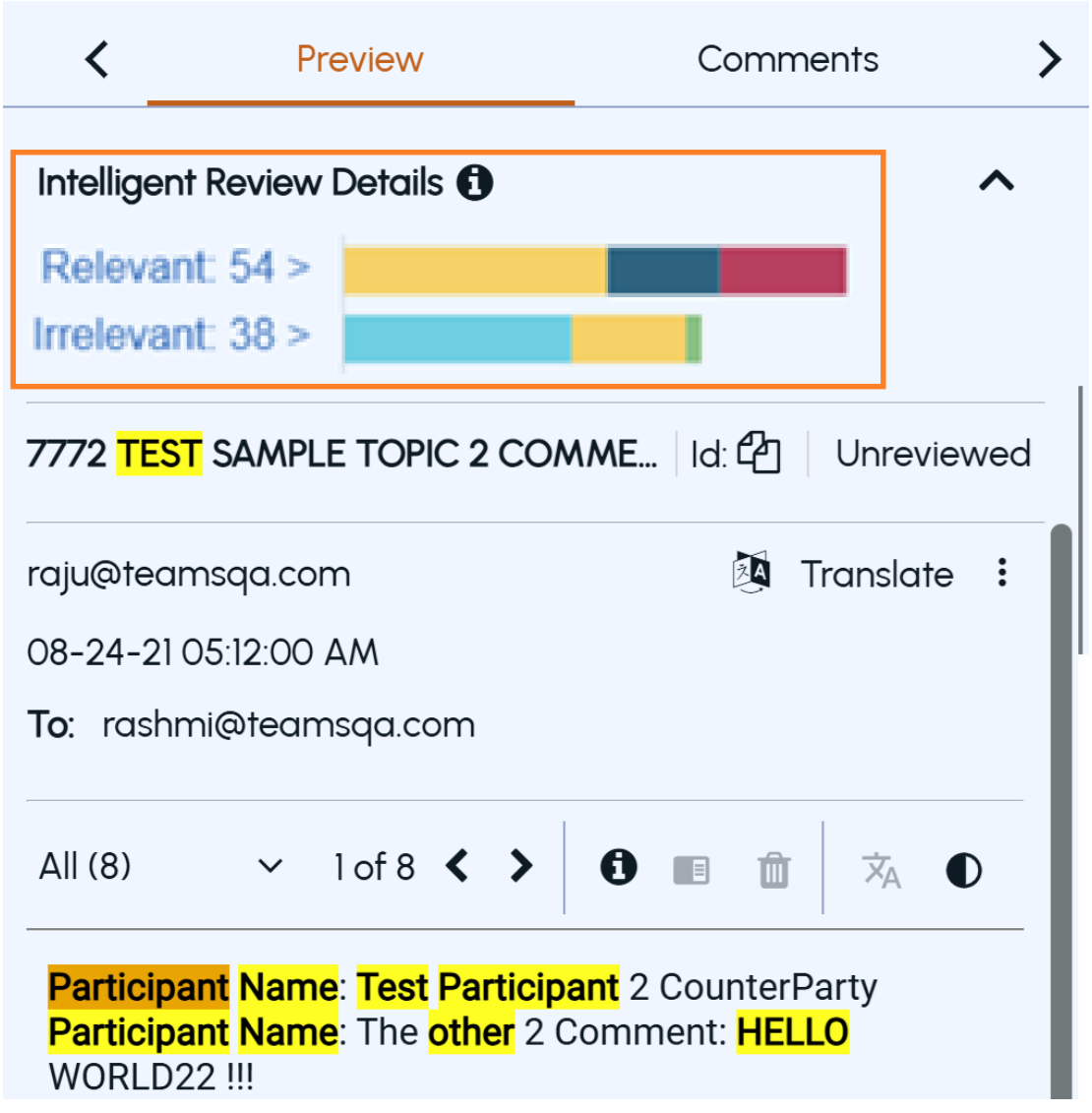
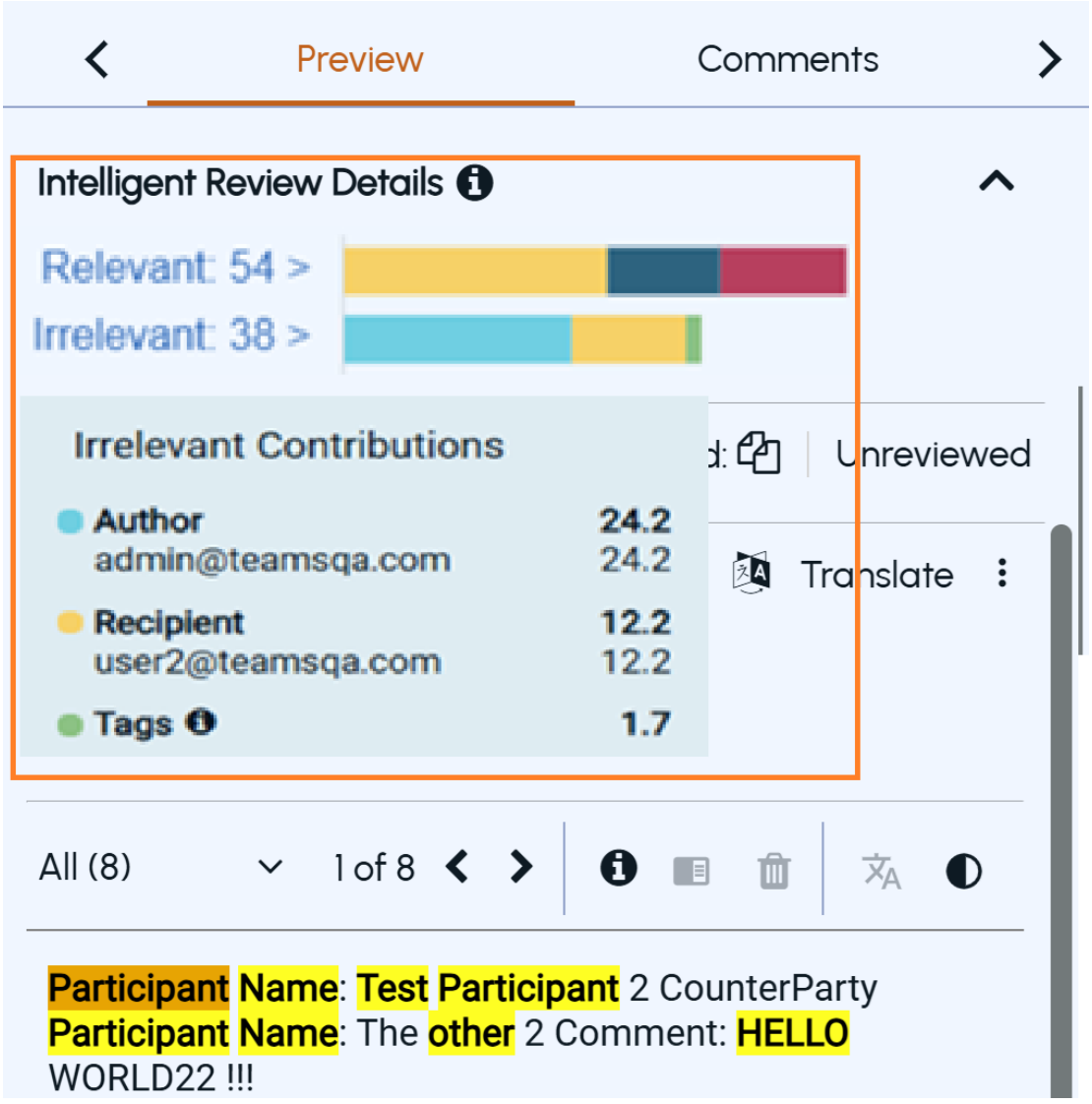


Figure 24-4 Contributing factors and their contribution



Following are some circumstances when the Intelligent Review Details are not available, and the application displays different messages for users.

Circumstance	Displayed message
Item is not processed by the Intelligent Review engine	Details not available
Data for machine learning is inadequate	Intelligent Review is still learning. Details are not yet available.
Technical problem during loading Intelligent Review Details	Error loading Intelligent Review Details

Chapter 25

Working with reports

This chapter includes the following topics:

About Insight Surveillance reports

Predefined reports

Insight Surveillance provides several predefined reports that are used to provide review information for different message types. After generating the reports, you can export them in a number of formats, including XML, comma-separated values (CSV), Acrobat (PDF), web archive (MHTML), Excel, Word, and TIFF.

See "Predefined reports" on page 300.

Enhanced reporting

Insight Surveillance has introduced reporting endpoint APIs to improve reporting and analytics capabilities. To utilize these reporting endpoints, the administrator must configure them in Insight Surveillance. Upon successful configuration, Insight Surveillance generates a base URL and API keys to ensure secure access to the reporting endpoints. To securely access data, the primary or secondary API access keys are provided. The specified IP addresses during the configuration of these API keys determine the allowed sources from which the reporting endpoints can be accessed.

See "Enhanced reporting" on page 302.

Predefined reports

Predefined report types in Insight Surveillance

This section explains the function of the predefined Insight Surveillance report types.

Report Type	Description
Evidence of Bloomberg Review by Department	Extracts information on the required number and percentage of sampled items received from Bloomberg channel that have been captured and reviewed for the selected department or employee.
Evidence of Domino (External) Review by Department	Extracts information on the required number and percentage of sampled items received from Domino external channel that have been captured and reviewed for the selected department or employee.
Evidence of Domino (Internal) Review by Department	Extracts information on the required number and percentage of sampled items received from Domino internal channel that have been captured and reviewed for the selected department or employee.
Evidence of Exchange (External) Review by Department	Extracts information on the required number and percentage of sampled items received from Exchange external channel that have been captured and reviewed for the selected department or employee.
Evidence of Exchange (Internal) Review by Department	Extracts information on the required number and percentage of sampled items received from Exchange internal channel that have been captured and reviewed for the selected department or employee.
Evidence of SMTP (External) Review by Department	Extracts violated information on the required number and percentage of sampled items received from SMTP external channel that have been captured and reviewed for the selected department or employee.

Report Type	Description
Evidence of SMTP (Internal) Review by Department	Extracts information on the required number and percentage of sampled items received from SMTP internal channel that have been captured and reviewed for the selected department or employee.
Evidence of IM Review by Department	Extracts information on the required number and percentage of sampled items received from Instant Messaging channel that have been captured and reviewed for the selected department or employee.
Evidence of Review by Reviewer	Extracts information about the reviewerArcteras activities in departments. The report is configured by selecting departments and a time range. Reviewers within those departments are included in the report. The report includes every department where reviewer actions occurred within the time range, even if every department is not specifically selected during the configuration of the report.

Generating predefined reports

You must have the *View Reports* permission to generate a new report. By default, most users with a department role have this permission.

To generate a report

1 In the left navigation pane, click **Reports**.

2 In the **Select report** type field, select the type you want to generate.

See "Predefined reports" on page 300.

3 Enter the start date and end date in respective fields to specify the duration for which you want to generate report.

4 Click **Select Department** to search for and select departments for which you want to generate a report.

Note: To select multiple adjacent departments, hold down the Shift key and click the first and the last name in the range. To select multiple, non-adjacent departments, hold down the Ctrl key and click the required names.

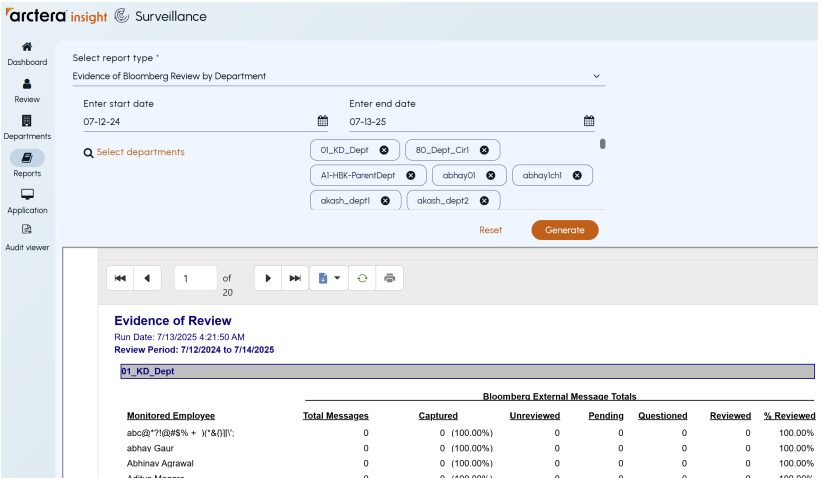
---

5 (Optional) To remove all the selected departments, click **Reset**. To remove a particular department from the selection, click remove icon of that department.

6 Click **Generate**.

7 After generating the report, perform the following on the toolbar as required.

A sample report pane that depicts its standard options is shown below.



- To print a report, click the **Print** icon.
- To export a report, click the **Export** icon, and select one of the available export types (CSV, Excel, MHTML, PDF, TIFF, WORD, or XML).
- To refresh the view, click the **Refresh** icon.
- 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.

Enhanced reporting

Insight Surveillance has introduced reporting endpoint APIs to improve reporting and analytics capabilities. Currently there are two types of reporting endpoint APIs.

Synchronous API: This API executes requests in a blocking manner, where each request is processed sequentially. Upon execution of the request, the server waits to complete the first task before proceeding with another tasks. The client remains idle during this time.

Asynchronous API: This API executes a request and continue to perform other tasks without waiting for the immediate response from servers. The server processes the requests independently. Client receives a response from asynchronous API with details to track the request. When the data is ready, the client calls the API to retrieve data. Insight Surveillance reporting asynchronous API returns report status and report data location in response. The client uses this location URL to track the status of report generation and get the data when the report is ready.

Synchronous APIs do not possess suffix after the API name. However, asynchronous APIs are indicated with the "Async" as a suffix. For example, *EvidenceOfReview* is synchronous API name and *EvidenceOfReviewAsync* is the asynchronous API name.

Refer to the details below for the available synchronous and asynchronous APIs.

- Departments API
  - **Synchronous method**: Supported (`https://<Reporting endpoint Base URL>/odata/departments`)
  - **Asynchronous method**: Not supported
- Roles API
  - **Synchronous method**: Supported (`https://<Reporting endpoint Base URL>/odata/roles`)
  - **Asynchronous method**: Not supported
- Users API
  - **Synchronous method**: Supported (`https://<Reporting endpoint Base URL>/odata/users`)
  - **Asynchronous method**: Not supported
- UserRoles API
  - **Synchronous method**: Supported (`https://<Reporting endpoint Base URL>/odata/userroles`)
  - **Asynchronous method**: Supported (`https://<Reporting endpoint Base URL>/odata/userrolesAsync`)
- Classification Tags API

- **Synchronous method**: Supported (`https://<Reporting endpoint Base URL>/odata/ClassificationTags`)
- **Asynchronous method**: Not supported

- Labels API
  - **Synchronous method**: Supported (`https://<Reporting endpoint Base URL>/odata/Labels`)
  - **Asynchronous method**: Not supported
- Searches API
  - **Synchronous method**: Supported (`https://<Reporting endpoint Base URL>/odata/Searches`)
  - **Asynchronous method**: Not supported
- ItemMetrics API
  - **Synchronous method**: Supported (`https://<Reporting endpoint Base URL>/odata/itemmetrics`)
  - **Asynchronous method**: Not supported
- ReviewerMapping API
  - **Synchronous method**: Supported (`https://<Reporting endpoint Base URL>/odata/reviewermapping`)
  - **Asynchronous method**: Supported (`https://<Reporting endpoint Base URL>/odata/reviewermappingAsync`)
- MonitoredEmployees API
  - **Synchronous method**: Supported (`https://<Reporting endpoint Base URL>/odata/monitoredemployees`)
  - **Asynchronous method**: Not supported
- EvidenceOfReview API
  - **Synchronous method**: Supported (`https://<Reporting endpoint Base URL>/odata/EvidenceOfReview`)
  - **Asynchronous method**: Supported (`https://<Reporting endpoint Base URL>/odata/EvidenceOfReviewAsync`)
- ItemClassificationMetrics API
  - **Synchronous method**: Supported (`https://<Reporting endpoint Base URL>/odata/ItemClassificationMetrics`)

- **Asynchronous method**: Supported (`https://<Reporting endpoint Base URL>/odata/ItemClassificationMetricsAsync`)

- ItemLabelMetrics API
  - **Synchronous method**: Supported (`https://<Reporting endpoint Base URL>/odata/ItemLabelMetrics`)
  - **Asynchronous method**: Supported (`https://<Reporting endpoint Base URL>/odata/ItemLabelMetricsAsync`)
- ItemArchivedMetrics API
  - **Synchronous method**: Supported (`https://<Reporting endpoint Base URL>/odata/ItemArchivedMetrics`)
  - **Asynchronous method**: Supported (`https://<Reporting endpoint Base URL>/odata/ItemArchivedMetricsAsync`)
- ItemHotwordMetrics API
  - **Synchronous method**: Supported (`https://<Reporting endpoint Base URL>/odata/ItemHotwordMetrics`)
  - **Asynchronous method**: Supported (`https://<Reporting endpoint Base URL>/odata/ItemHotwordMetricsAsync`)
- ItemDetails API
  - **Synchronous method**: Supported (`https://<Reporting endpoint Base URL>/odata/ItemDetails`)
  - **Asynchronous method**: Supported (`https://<Reporting endpoint Base URL>/odata/ItemDetailsAsync`)
- ReviewerAssessmentMetrics API
  - **Synchronous method**: Supported (`https://<Reporting endpoint Base URL>/odata/ReviewerAssessmentMetrics`)
  - **Asynchronous method**: Supported (`https://<Reporting endpoint Base URL>/odata/ReviewerAssessmentMetricsAsync`)
- ReportStatus API
  - **Synchronous method**: Supported (`https://<Reporting endpoint Base URL>/odata/reportstatus`)
  - **Asynchronous method**: Not supported

To utilize these reporting endpoints, the administrator must configure them in Insight Surveillance. Upon successful configuration, Insight Surveillance generates a base URL and API keys to ensure secure access to the reporting endpoints.

To securely access data, the primary or secondary API keys serve as passwords, unique to each reporting endpoint configuration. The specified IP addresses during the configuration of these enhanced reporting endpoints are authorized and permitted for API calls.

See "Configuring a reporting endpoint" on page 307.

See "Departments API" on page 311.

See "Users API" on page 312.

See "User Roles Async API" on page 316.

See "User Roles API" on page 321.

See "Roles API" on page 314.

See "Classification Tags API" on page 322.

See "Labels API" on page 323.

See "Searches API" on page 325.

See "ItemMetrics API" on page 328.

See "Reviewer Mapping Async API" on page 333.

See "Reviewer Mapping API" on page 337.

See "MonitoredEmployees API" on page 339.

See "Evidence Of Review Async API" on page 343.

See "Evidence of Review API" on page 351.

See "Item Classification Metrics Async API" on page 355.

See "Item Classification Metrics API" on page 360.

See "Item Label Metrics Async API" on page 361.

See "Item Label Metrics API" on page 367.

See "Item Archived Metrics Async API" on page 371.

See "Item Archived Metrics API" on page 375.

See "Item Hotword Metrics Async API" on page 376.

See "Item Hotword Metrics API" on page 381.

See "Item Details Async API" on page 383.

See "Item Details API" on page 396.

See "Reviewer Assessment Metrics Async API" on page 401.

See "Reviewer Assessment Metrics API" on page 407.

See "Report Status API" on page 409.

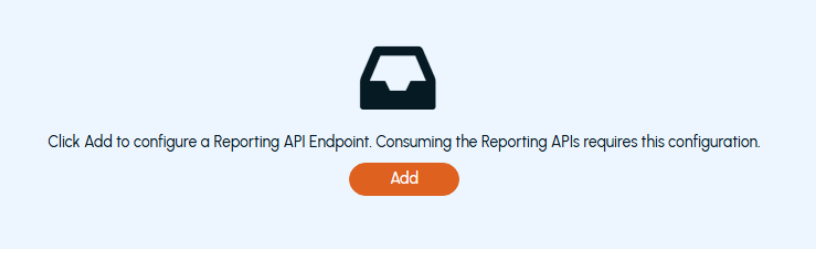
Configuring a reporting endpoint

To configure a reporting endpoint, you must have a *System Admin* role or the *Configure Reporting API Endpoint* permission to your role. If you do not have this permission, contact your system administrator.

In this release, only one reporting endpoint configuration can be created. After the endpoint is configured, you can change the configuration, regenerate API keys, and activate or suspend the endpoint as needed.

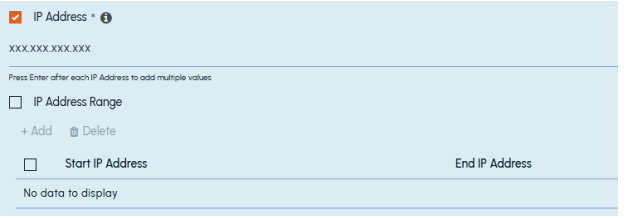
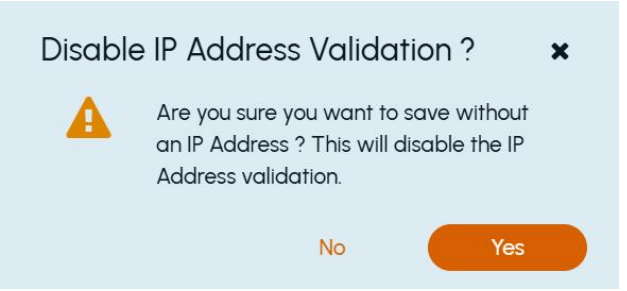
To configure a reporting endpoint

1 In the left navigation pane, select **Configuration** > **Reporting Endpoint** tab.



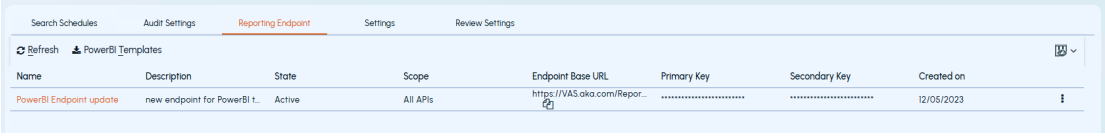
2 Click **Add**.

3 On the **Add New Endpoint Configuration** page, specify the following details and click **Save**.

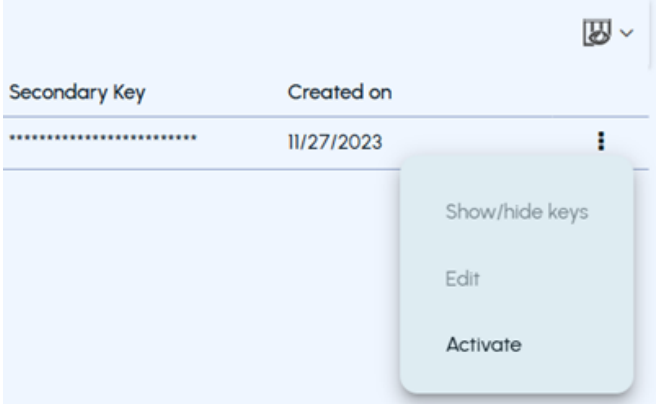
Name	Specify a unique name for the reporting endpoint configuration.
Description	Provide a brief description of the reporting endpoint configuration.
Scope	Decides which APIs are accessible via current configuration. By default, it is set to **All API**.
IP Address	Specify individual IP Addresses that are allowed to access APIs via current configuration.  Note: Only IPv4 addresses are supported in this release.
IP Address range	Specify the range of sequential IP Addresses that are allowed to access APIs via current configuration. IP addresses outside of that range are not permitted to access the API. Note: Only IPv4 addresses are supported in this release. Select at least one of the checkboxes (**IP Address** or **IP Address Range**) and provide valid IP values for the same. If neither **IP Address** nor **IP Address Range** is selected, IP address validation is disabled, allowing unrestricted API access. In such cases, a confirmation message is displayed before saving the configuration. 

Primary and Secondary API Key	After saving the reporting endpoint configuration, the application automatically generates primary and secondary API keys and saves them to the reporting endpoint configuration. API callers need to specify any of these API keys to access these APIs. **Note**: The primary and secondary API keys are provided so that if you want to replace any of the keys, you can use another one without experiencing any downtime.
Endpoint Base URL	After saving the reporting endpoint configuration, the application generates the Endpoint Base URL automatically. API callers must use this URL as the starting point for accessing API.

Ensure that the configured reporting endpoint is listed on the **Reporting Endpoint** tab. If required, click the **Refresh** icon. The application masks primary and secondary keys for security reasons.



4 Click the kebab icon (three vertical dots) in the same row to perform the following actions:

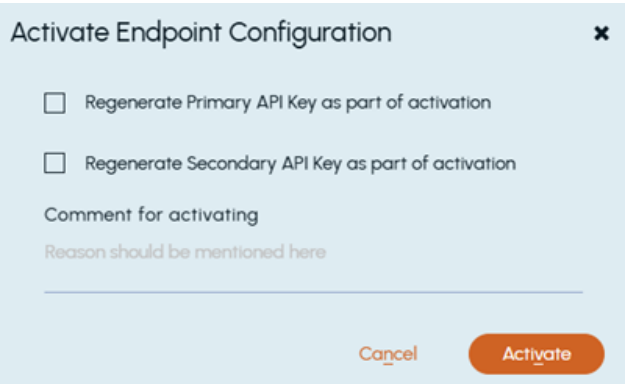


- To view or hide the keys, select **Show/hide keys**.

- To copy the base URL, primary key, and secondary key, click the **Copy** icon in the respective column, or click the reporting endpoint name and copy the required information.
- To edit the reporting endpoint configuration, select **Edit**. Modify the configuration as needed and click **Save**.
- To regenerate the API keys, click **Regenerate** adjacent to the primary and secondary API key fields.

Note: API keys can be regenerated for the active reporting endpoints only.

- To suspend the active reporting endpoint, select **Suspend** to block access to the Reporting APIs. Specify the reason for suspending the reporting endpoint and click **Suspend**.
- To activate the suspended reporting endpoint and regenerate primary and secondary keys, select **Activate**.



Select the primary and secondary API key generation check boxes as needed. Specify the reason for activating the reporting endpoint and click **Activate**. The application displays the date of expiry for these API keys.

Authentication

To ensure the security and integrity of data access, the Reporting API requires authentication. Authentication is used to verify the identity of the requesting client or application and determine whether it has the necessary permissions to access the API resources. There are two primary authentication methods supported for this API:

API Key authentication

Upon configuring the reporting endpoint API, a Base URL, a primary and secondary API Keys are generated. Include either primary or secondary API key in the **X-API-Key** header of your API requests.

For example,

```
X-API-Key:<Primary or Secondary API Key>
```

Basic authentication

Basic Authentication is a method where API clients provide a username and password with each request. Users use an encoded string in the Authorization header for this method. The recipient of the request uses this string to verify the users' identity and their access rights to a resource.

For example,

```
Authorization: Basic <Base64 encoded credentials>
```

To generate a Base64 encoded credentials:

1. Combine the credentials (username and password) with a colon (:).

   Note: The username must be **ReportingApiUser**. The password can be either a primary or a secondary API Key provided after configuring the reporting endpoint. Use either one as your password.

   For example, `ReportingApiUser:32adasdf3asdcvzxcweasd`

2. After specifying the credentials as mentioned in the step above, generate a Base64 encoded credentials. It is required while setting authorization header.

   For example, `dGVuYW50OmtleQ==`

Therefore, requests made by this user would be sent with the following header:

```
Authorization: Basic dGVuYW50OmtleQ==
```

When a server receives this request, it can access the Authorization header, decode the credentials, and look up the user to determine whether access to the requested resource should be allowed.

Departments API

Supported Operations

Departments - List	Gets the list of departments.

Departments - List

```
GET https://<Reporting endpoint Base URL>/odata/departments
```

Sample request

```
GET https://<Reporting endpoint Base URL>/odata/departments
```

Sample response

Status code: 200 OK


```
{
    "@odata.context": "https://<Reporting endpoint Base UR>/odata/$metadata#Departments",
    "value": [
        {
            "departmentId": 38,
            "departmentName": "Atlas-Group1-D1",
            "status": "Closed",
            "createDate": "2019-09-23T15:15:15.983-07:00",
            "modifiedDate": "2023-08-31T03:00:08.553-07:00"
        },
        {
            "departmentId": 39,
            "departmentName": "Atlas-Group1-D2",
            "status": "Open",
            "createDate": "2019-09-23T15:15:16.03-07:00",
            "modifiedDate": "2023-08-31T03:00:08.553-07:00"
        }
    ],
    "@odata.nextLink": "https://<Reporting endpoint Base UR>/odata/departments?$skiptoken=6890"
}
```


Supported OData Filters

See "Supported OData query options" on page 410.

Responses

See "Responses" on page 415.

Users API

Supported Operations

Users - List	Gets the list of users.

Users - List

```
GET https://<Reporting endpoint Base URL>/odata/users
```

Sample requests

```
GET https://<Reporting endpoint Base URL>/odata/users
```

Sample response

Status code: 200 OK

```
{
    "@odata.context": "https://<Reporting endpoint base URL>/odata/$metadata#
    "value": [
        {
            "userId": 1,
            "userName": "Active Directory Container",
            "userLogin": "TargetGroup_1",
            "userEmail": null
        },
        {
            "userId": 2,
            "userName": "Active Directory Search",
            "userLogin": "TargetGroup_2",
            "userEmail": null
        },
        {
            "userId": 3,
            "userName": "New Employee Group",
            "userLogin": "TargetGroup_3",
            "userEmail": null
        },
        {
            "userId": 4,
            "userName": "DEV",
            "userLogin": "TargetGroup_4",
            "userEmail": null
        }
    ]
}
```

Note: The userEmail parameter corresponds to the primary email address, or it may be null if no email is available.

Supported OData Filters

See "Supported OData query options" on page 410.

Responses

See "Responses" on page 415.

Roles API

Supported Operations

Roles - List	Gets the list of roles and role permissions.
Roles - List by filters	Gets the list of roles and role permissions by applying filters.

Roles - List

```
GET https://<Reporting endpoint Base URL>/odata/roles
```

Sample request

```
GET https://<Reporting endpoint Base URL>/odata/roles
```

Sample response

Status code: 200 OK


```
{
    "@odata.context": "https://<Reporting endpoint Base URL>/odata/$metadata#Roles",
    "value": [
        {
            "roleId": 236,
            "department": 23,
            "roleName": "Department ACL User",
            "roleDesc": "User is on department ACL",
            "scope": "Department",
            "roleType": "Department ACL User",
            "rolePermissions": []
        },
        {
            "roleId": 237,
            "department": null,
            "roleName": "User Admin",
            "roleDesc": "Lets you manage the properties of the department and monitored employees, assign
            department roles such as Department Reviewer to users, generate and view reports on department
            details, and review progress.",
            "scope": "Department",
            "roleType": "System",
            "rolePermissions": [
                "Review Messages",
                "Add Own Review Comments",
                "Assign % Review Requirement",
                "Search Capture",
                "Export Messages",
                "Add Hotwords",
                "Grant Users Access",
                "Add Monitored Employees",
                "Configure Department Properties",
                "View Reports",
                "Manage Exceptions",
                "Escalate Messages",
                "Manage Reviewing Comments",
                "Show Reviewer Summaries On Home Page",
                "Accept searches",
                "View Task Status",
                "View Audit Information",
                "Show Hotwords In Search",
                "Show Intelligent Review Details in Review"
            ]
        }
    ],
    "@odata.nextLink": "https://<Reporting endpoint Base URL>/odata/roles?$skiptoken=2390"
}
```

Supported OData Filters

See "Supported OData query options" on page 410.

Roles - List by filters

```
POST https://<Reporting endpoint Base URL>/odata/roles
```

Request body

Specify the following filters to obtain refined and selective results from this report.

Name	Type	Description
Departments	Optional	Specifies IDs of the departments to which roles belongs to. **Limitations**: The Roles API can pass a maximum of 100 Departments IDs as input. **Data Type**: JSON array of integers 'id'(identifier fields) that is Departments.
Scopes	Optional	Specifies the scope of the roles. Possible values are: 160 for application-level roles and 161 for department-level roles. **Data Type**: JSON array of integers 'id'(identifier fields) that is Scopes.

Sample request

```
POST https://<Reporting endpoint Base URL>/odata/Roles

{

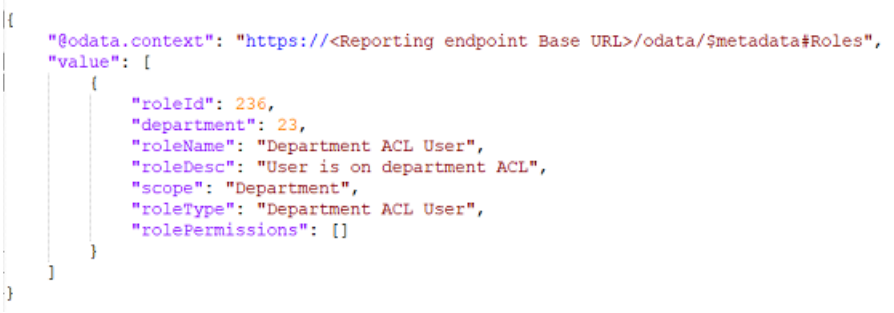
"Departments": [5,6],

"Scopes" :[161]

}
```

Sample response

Status code: 200 OK



Supported OData Filters

See "Supported OData query options" on page 410.

Responses

See "Responses" on page 415.

User Roles Async API

UserRolesAsync	This API submits the report generation request which executes asynchronously. The result of this API contains the identifier for the report, status, and location for retrieving the report data. The report identifier and locations in the result can be used to track the report generation operation.

To use the *UserRolesAsync* API, follow the steps below:

1. Call the *UserRolesAsync* API to submit a report generation request.

   This asynchronous API supports GET and POST query methods. Use any of the following as needed:

   - `GET https://<Reporting endpoint base URL>/OData/UserRolesAsync?ReportName=<Name of the report>&Users=[list of comma-separated values]&Departments=[list of comma-separated values]&Scopes=[list of comma-separated values]`
   - `POST https://<Reporting endpoint base URL>/OData/UserRolesAsync`

   Sample Input

   - `GET https://<Reporting endpoint Base URL>/odata/UserRolesAsync?ReportName=<Name of the report>Users=[1247,3821]`

- `POST https://<Reporting endpoint base URL>/OData/UserRolesAsync`

UserRolesAsync - URL Parameter/Filters

The following parameters/filters can be used with the *UserRolesAsync* API when invoked using the GET and POST methods. The system uses the AND operator between the filters to return the result based on the specified filters.

ReportName	Mandatory	Specify the name of the report you want to generate. **Limitations** ■ The report name can be up to a maximum of 256 characters long. ■ Special characters are not allowed; only alphanumeric values are permitted.
Departments	Optional	Specifies IDs of the departments to which users and their roles belongs to. **Limitations**: This API can pass a maximum of 100 Departments IDs as input. **Data Type**: JSON array of integers 'id'(identifier fields) that is Departments. Note: To get the Department IDs, See "Departments API" on page 311. Refer to the **departmentId** field only.
Scopes	Optional	Specifies the scope of the users roles. Possible values are: 160 for application-level roles and 161 for department-level roles. **Data Type**: JSON array of integers 'id'(identifier fields) that is Scopes.
Users	Optional	Specifies IDs of the users. **Limitations** This API can pass a maximum of 100 User IDs as input. **Data Type**: JSON array of integers 'id'(identifier fields) that is Users. Note: To get the User IDs, See "Users API" on page 312. Refer to the **userId** field only.

Scenario 1: When Users are mentioned, but Departments and Scopes are not specified..

Sample input:

```
POST https://<Reporting endpoint base URL>/OData/UserRolesAsync
{
"ReportName":"TestUserRolesReport",
"Departments":[],
"Scopes":"[],
"Users":[3821]
}
```

Sample response:


```
{
    "@odata.context": "https://vas.aka.com/Reporting/odata/$metadata#UserRolesAsync/$entity",
    "reportId": "ff2dc415-bf15-49b1-bd25-74f9abfbc102",
    "reportName": "DhirajPost",
    "reportType": "User Roles",
    "reportDate": "2025-06-06T00:20:00.79-07:00",
    "reportStatus": "Queued",
    "info": "Successfully queued the report request.",
    "newReportInstanceQueued": true,
    "reportStatusLocation": "https://vas.aka.com/Reporting/odata/ReportStatus?ReportId=ff2dc415-bf15-49b1-bd25-74f9abfbc102",
    "reportDataLocation": "https://vas.aka.com/Reporting/odata/UserRoles?ReportId=ff2dc415-bf15-49b1-bd25-74f9abfbc102"
}
```


Scenario 2: When Departments are mentioned, but Users and Scopes are not specified.

Sample input:

```
POST https://<Reporting endpoint base URL>/OData/UserRolesAsync
{
"ReportName":"TestUserRolesReport",
"Departments":[23],
"Scopes":"[],
"Users":[]
}
```

Sample response:


```
{
    "@odata.context": "https://vas.aka.com/Reporting/odata/$metadata#UserRolesAsync/$entity",
    "reportId": "ff2dc415-bf15-49b1-bd25-74f9abfbc102",
    "reportName": "DhirajPost",
    "reportType": "User Roles",
    "reportDate": "2025-06-06T00:20:00.79-07:00",
    "reportStatus": "Queued",
    "info": "Successfully queued the report request.",
    "newReportInstanceQueued": true,
    "reportStatusLocation": "https://vas.aka.com/Reporting/odata/ReportStatus?ReportId=ff2dc415-bf15-49b1-bd25-74f9abfbc102",
    "reportDataLocation": "https://vas.aka.com/Reporting/odata/UserRoles?ReportId=ff2dc415-bf15-49b1-bd25-74f9abfbc102"
}
```


Scenario 3: When Departments, Users, and Scopes are mentioned.

Sample input:

```
POST https://<Reporting endpoint base URL>/OData/UserRolesAsync
{
"ReportName":"TestUserRolesReport",
"Departments":[23],
"Scopes":"[160,161],
"Users":[55,67]
}
```

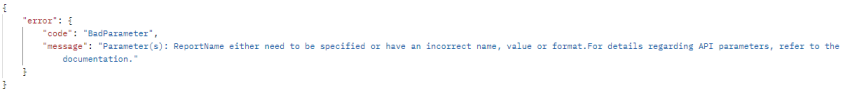
Sample response:

Scenario 4: When Departments, Users and Scopes are mentioned, but ReportName is not specified.

Sample input:

```
POST https://<Reporting endpoint base URL>/OData/UserRolesAsync
{
"ReportName":"",
"Departments":[23],
"Scopes":"[160],
"Users":[3821]
}
```

Sample response:



The following table explains the parameters showcased in the response to a User Roles Async API request.

Name	Description
reportId	Displays report ID. It is generated upon successful execution of API.

Name	Description
reportName	Displays report name. It is generated upon successful execution of API.
reportType	Displays the report type as *User Roles*.
reportDate	Displays the date of report generation after successful execution of API.
reportStatus	Displays report status. For more information on statuses, See "Report Status API" on page 409..
info	Displays a message if the report request has queued successfully or not.
newReportInstanceQueued	Specifies whether a new report generation request has been submitted or not. The *Rate Limiting* feature restricts submission of multiple requests with identical input parameters if attempted within one minute. It returns the following values: ***True***: The value is shown as *True*, if the new report request has been queued successfully. ***False***: The value is shown as *False*, if the input parameters of the current request are identical to the parameters of the already submitted request *within one minute*, a new report will not be queued. As a result, the details of the existing report request are returned.
reportStatusLocation	Displays a URL with report ID. To view the status of this report, use the same URL.
reportDataLocation	Displays a URL for the location of report data. To access the report data, use the same URL.

2. Call the *ReportStatus* API to get the status of the *UserRolesAsync* API report. See "Report Status API" on page 409.
3. Once the report is ready, call the *UserRoles* API to get the report data from the asynchronous API. See "User Roles API" on page 321.

User Roles API

UserRoles - List	This report provides the department-level and application-level roles for the specified users.

UserRoles - List

```
GET https://<Reporting endpoint Base URL>/odata/UserRoles
```

Sample requests

```
GET https://<Reporting endpoint Base URL>/odata/UserRoles?reportid=<ID of the UserRolesAsync API report>
```

```
GET https://<Reporting endpoint Base URL>/odata/UserRoles?reportid=d53960f0-dbd0-4aa9-b7cf-23bd6ab7875f
```

Parameter/Filters

The following filter can be used with the UserRoles API when invoked using the GET method only. The system uses the AND operator between the filters to return the result based on the specified filters.

ReportID	Mandatory	Specify the ID of report you want to view.

Scenario 1

```
GET https://<Reporting endpoint Base URL>/odata/UserRoles?reportid=d0558287-3349-4df3-9528-11168637a83b
```

Sample response

Status code: 200 OK

```
"@odata.context": "https://<server>/odata/$metadata#userroles",
"value": [
    {
      "userId": 3821,
      "roleId": 915,
      "department": 2784,
      "scope": "Department",
      "details": "Inherited from parent department - kd dept updates"
    },
    {
      "userId": 1,
      "roleId": 102,
      "department": 5,
      "scope": "Department",
      "details": "Explicitly assigned in this department"
    }
```


Supported OData Filters

See "Supported OData query options" on page 410.

Responses

See "Responses" on page 415.

Classification Tags API

Supported Operations

Classification Tags - List	Gets a list of classification tags.

Classification Tags - List

```
GET https://<Reporting endpoint Base URL>/odata/ClassificationTags
```

Sample request

```
GET https://<Reporting endpoint Base URL>/odata/ClassificationTags
```

Sample response

Status code: 200 OK

```
"@odata.context": "https://<<Reporting endpoint Base URL>/odata/$metadata#Classifica
"value": [
    {
        "tagID": 201,
        "tagName": "Market Abuse",
        "tagType": "Category",
        "createDate": "2022-02-09T03:30:00-08:00",
        "modifiedDate": "2022-02-09T03:30:00-08:00"
    },
    {
        "tagID": 202,
        "tagName": "Money Laundering",
        "tagType": "Category",
        "createDate": "2022-02-09T03:30:00-08:00",
        "modifiedDate": "2022-02-09T03:30:00-08:00"
    },
    {
        "tagID": 203,
        "tagName": "Offensive Language",
        "tagType": "Inclusion",
        "createDate": "2022-02-09T03:30:00-08:00",
        "modifiedDate": "2022-02-09T03:30:00-08:00"
    },
    {
        "tagID": 204,
        "tagName": "Off-Channel Communications",
        "tagType": "Inclusion",
        "createDate": "2022-02-09T03:31:00-08:00",
        "modifiedDate": "2022-02-09T03:31:00-08:00"
    },
]
```


Supported OData Filters

See "Supported OData query options" on page 410.

Responses

See "Responses" on page 415.

Labels API

Supported Operations

Labels - List	Gets a list of labels.

Labels - List

```
GET https://<Reporting endpoint Base URL>/odata/Labels
```

Sample request

```
GET https://<Reporting endpoint Base URL>/odata/Labels
```

Sample response

Status code: 200 OK


```
{
    "@odata.context": "https://<Reporting endpoint Base
    URL>/odata/$metadata#Labels",
    "value": [
        {
            "labelID": 20,
            "labelName": "Label1",
            "description": "Label1 description",
            "isActive": true,
            "caseID": 6491,
            "isPropagated": true,
            "modifiedDt": "2023-01-18T21:11:19.663-08:00",
            "scope": "Department"
        },
        {
            "labelID": 21,
            "labelName": "Test1",
            "description": "Test1",
            "isActive": true,
            "caseID": 6073,
            "isPropagated": true,
            "modifiedDt": "2023-01-23T04:12:39.477-08:00",
            "scope": "Department"
        },
        {
            "labelID": 207,
            "labelName": "@",
            "description": "nediuqye",
            "isActive": true,
            "caseID": 7096,
            "isPropagated": true,
            "modifiedDt": "2023-01-16T22:25:58.323-08:00",
            "scope": "Department"
        }
]}
```


Supported OData Filters

See "Supported OData query options" on page 410.

Responses

See "Responses" on page 415.

Searches API

Supported Operations

Searches - List	Gets a list of Searches.

Searches - List

```
GET https://<Reporting endpoint Base URL>/odata/Searches
```

Sample request

```
GET https://<Reporting endpoint Base
URL>/odata/Searches?StartDate=2025-01-01&EndDate=2025-01-10
```

Request body

Specify the following filters to obtain refined and selective results from this report.

Name	Type	Description
Start Date	Mandatory	StartDate is the date on which the searches are created in Insight Surveillance. This filter specifies the start date for returning count of searches whose creation date is greater than or equal to this start date. **Data Type** Date in the YYYY-MM-DD format that is StartDate. **Limitations** For the cloud-based application, a maximum of one year duration is allowed.

Name	Type	Description
End Date	Mandatory	This filter specifies the end date for returning count of searches whose creation date is less than or equal to this date. **Data Type** Date in the YYYY-MM-DD format that is StartDate. **Limitations** For the cloud-based application, a maximum of one year duration is allowed.

Sample response

Status code: 200 OK

```
"@odata.context": "https://<Reporting endpoint base
URL>/odata/$metadata#Searches",
    "value": [
        {
            "parentSearchID": null,
            "parentSearch": null,
            "searchID": 1105959,
            "name": "19463-DeptIm1",
            "scope": "Department",
            "runDate": "2025-01-02T02:27:00-08:00",
            "deptID": 19463,
            "department": "AutoEorIR1-20125020806",
            "hits": 9,
            "sampled": 9,
            "relevantSampled": 0,
            "status": "In Review",
            "searchType": "Immediate"
        },
        {
            "parentSearchID": null,
            "parentSearch": null,
            "searchID": 1105960,
            "name": "19463-DeptSch2",
            "scope": "Department",
            "runDate": "2025-01-02T02:31:00-08:00",
            "deptID": 19463,
            "department": "AutoEorIR1-20125020806",
            "hits": -1,
            "sampled": -1,
            "relevantSampled": -1,
            "status": "Schedule",
            "searchType": "Schedule"
        }
        ]
```


Supported OData Filters

See "Supported OData query options" on page 410.

Responses

See "Responses" on page 415.

ItemMetrics API

Supported Operations

ItemMetrics - List	Gets the count of items within a specified date range.
ItemMetrics - List by filter	Gets the count of items captured in Insight Surveillance within a specified date range by using the filters.

ItemMetrics - List

```
GET https://<Reporting endpoint Base URL>/odata/ItemMetrics?CaptureDateStart=<YYYY-MM-DD>&CaptureDateEnd=<YYYY-MM-DD>
```

ItemMetrics - URL Parameter/Filters

The following filters can be used with the ItemMetrics API when invoked using the GET method. The system uses the **AND** operator between the filters to return the result based on the specified filters.

Name	Type	Description
CaptureDateStart	Mandatory	CaptureDate is the date on which items are captured or ingested in Insight Surveillance is recorded as the CaptureDate for that item. This filter specifies the start date for returning count of items whose CaptureDate is greater than or equal to this start date. **Data Type**: Date in the *YYYY-MM-DD* format that is CaptureDateStart.
CaptureDateEnd	Mandatory	This filter specifies the end date for returning count of items whose CaptureDate is greater than or equal to this date. **Data Type**: Date in the *YYYY-MM-DD* format that is CaptureDateEnd.

Sample requests

To get count of all items captured between 2023-01-01 and 2023-12-31, the sample query will be as below.

```
GET https://<Reporting endpoint Base URL>/odata/ItemMetrics?CaptureDateStart=2023-01-01&CaptureDateEnd=2023-12-31
```

Responses

See "Responses" on page 415.

ItemMetrics - List by filter

```
POST https://<Reporting endpoint Base URL>/odata/ItemMetrics
```

Request body

The following filters can be used with the ItemMetrics API when invoked using the POST method. The system uses the **AND** operator between the filters to return the result based on the specified filters.

Name	Type	Description
Departments	Optional	Specifies the department to which the captured item belongs and returns item counts for items within that department. **Data Type**: JSON array of integers 'id'(identifier fields) that is department IDs. **Limitation**: As an input, the ItemMetrics API can pass maximum of 1000 Departments IDs.
CaptureTypes	Optional	Specifies the mode/technique used to capture the item in Insight Surveillance and returns item counts for items with the specified capture type. **Data Type**: JSON array of integers 'id'(identifier fields) that is CaptureTypes IDs. **Limitation**: As an input, the ItemMetrics API can pass maximum 10 CaptureTypes IDs.
CaptureDateStart	Mandatory	Specifies the date on which items are captured or ingested in Insight Surveillance is recorded as the CaptureDate for that item. Returns item counts whose CaptureDate is greater than or equal to the specified CaptureDateStart. **Data Type**: Date in the *YYYY-MM-DD* format that is CaptureDateStart.

Name	Type	Description
CaptureDateEnd	Mandatory	Specifies the date on which items are captured or ingested in Insight Surveillance is recorded as the CaptureDate for that item. Returns item counts whose CaptureDate is less than or equal to the specified CaptureDateEnd. **Data Type**: Date in the *YYYY-MM-DD* format that is CaptureDateEnd.
MessageDirections	Optional	Specifies whether the item was sent/received from within the organization or from an external source and returns item counts for items that have the specified message direction. **Data Type**: JSON array of integers 'id'(identifier fields) that is MessageDirections IDs **Limitation**: As an input, the ItemMetrics API can pass maximum 5 MessageDirections IDs.
MessageTypes	Optional	Specifies the type of captured items and returns item counts for items that have the specified message type. **Data Type**: JSON array of integers 'id'(identifier fields) that is MessageTypes IDs. **Limitation**: As an input, the ItemMetrics API can pass maximum 100 MessageTypes IDs on a single page.

Scenario 1:

To get the item counts for *Departments ID* 11154, between *CaptureDateStart* 2023-11-24 and *CaptureDateEnd*2024-10-24. and having *CaptureType* as 1.

Sample Requests

```
{
"CaptureDateStart": "2023-11-24",
"CaptureDateEnd": "2024-10-24",
"Departments": [11154],
"CaptureTypes": [1]
}
```

Scenario 2

To get item counts for *Department IDs* 9 and 5, between *CaptureDateStart* 2023-06-01 and *CaptureDateEnd* 2023-08-02 and having *MessageTypes* as 7 or 8.

Sample request

```
POST https://<Reporting endpoint Base URL>/odata/ItemMetrics

{

"CaptureDateStart": "2023-06-01",

"CaptureDateEnd": "2023-08-02",

"Departments": [9,5],

"MessageTypes": [7,8]

}
```

Scenario 3:

To get item counts for *Departments IDs* 9 and 5 , between *CaptureDateStart* 2023-06-01 and *CaptureDateEnd* 2023-08-02 and having *MessageDirections* as 1 or 2.

```
POST https://<Reporting endpoint Base URL>/odata/ItemMetrics

{

"CaptureDateStart": "2023-06-01",

"CaptureDateEnd": "2023-08-02",

"Departments": [9,5],

"MessageDirections": [1,2]

}
```

Scenario 4:

To get item counts for *Departments IDs* 9 and 5, between *CaptureDateStart* 2023-06-01 and *CaptureDateEnd* 2023-08-02 and having *MessageTypes* as 7 or 8.

```
POST https://<Reporting endpoint Base URL>/odata/ItemMetrics

{

"CaptureDateStart": "2023-06-01",

"CaptureDateEnd": "2023-06-02",
```

```
"Departments": [9,5],

"MessageTypes": [7,8]

}
```

Sample response

Status code: 200 OK


```
{
    "@odata.context": "https://<Server>/odata/$metadata#ItemMetrics",
    "@odata.count": 3249,
    "value": [
        {
            "capturedItemCountId": 1,
            "captureDate": "2023-10-03T00:00:00-07:00",
            "departmentId": 9,
            "department": "Administration",
            "messageTypeId": 7,
            "messageType": "SMTP",
            "captureType": "Internal",
            "captureTypeId": 1,
            "messageDirectionId": 1,
            "messageDirection": "Internal",
            "capturedItemsCount": 17,
            "captureTypeDisplayName": "Search",
            "captureTypeDescription": "Indicates that items were captured based on
            immediate or scheduled search",
            "messageDirectionDisplayName": "Internal",
            "messageDirectionDescription": "The items where the author and all
            recipients are internal to the organization."
        }
    ]
}
```


Supported OData Filters

See “Supported OData query options” on page 410.

Responses

See “Responses” on page 415.

Reviewer Mapping Async API

ReviewerMappingAsync	This API submits the report generation request which executes asynchronously. The result of this API contains the identifier for the report, status, and location for retrieving the report data. The report identifier and locations in the result can be used to track the report generation operation.

To use the *ReviewerMappingAsync* API, follow the steps below:

1. Call the *ReviewerMappingAsync* API to submit a report generation request.

   This asynchronous API supports GET and POST query methods. Use any of the following as needed:

   - `GET https://<Reporting endpoint base URL>/OData/ReviewerMappingAsync?ReportName=<Name of the report>&ReviewerUsers=[list of comma-separated values]`
   - `POST https://<Reporting endpoint base URL>/OData/ReviewerMappingAsync`

   Sample Input

   - `GET https://<Reporting endpoint Base URL>/odata/ReviewerMappingAsync?ReportName=<Name of the report>&ReviewerUsers=[1,2,5]`
   - `POST https://<Reporting endpoint base URL>/OData/ReviewerMappingAsync`

   ReviewerMappingAsync - URL Parameter/Filters

   The following parameters/filters can be used with the *ReviewerMappingAsync* API when invoked using the GET and POST methods. The system uses the AND operator between the filters to return the result based on the specified filters.

ReportName	Mandatory	Specify the name of the report you want to generate. **Limitations** ■ The report name can be up to a maximum of 256 characters long. ■ Special characters are not allowed; only alphanumeric values are permitted.

ReviewerUsers	Optional	Specify a list of UserIDs for the reviewers whose details you want to retrieve. **Data Type** JSON array of integers 'id'(identifier fields) that is ReviewerUsersIDs. Note: The valid value of the ReviewerUsers is an ID of any user from the Insight Surveillance User ID list. The User ID list can be fetched from the Users API endpoint. See "Users API" on page 312. Refer to the **userId** field only. If no reviewer user ID is provided, Insight Surveillance retrieves the details of all ReviewerUsers.

Scenario 1: New request to submit a report.

Sample input:

```
POST https://<Reporting endpoint base URL>/OData/ReviewerMappingAsync
{
"ReportName":"TestReviewerMappingReport",
"ReviewerUsers":[1]
}
```

Sample response:


```
{
    "@odata.context": "https://<Reporting endpoint base URL>/odata/$metadata#ReviewerMappingAsync/$entity",
    "reportId": "f8451bde-8983-402b-9769-e9bfda2b1970",
    "reportName": "TestReviewerMappingReport",
    "reportType": "Reviewer Mapping",
    "reportDate": "2025-06-09T17:38:25.293+05:30",
    "reportStatus": "Queued",
    "info": "Successfully queued the report request.",
    "newReportInstanceQueued": true,
    "reportStatusLocation": "https://<Reporting endpoint base URL>/odata/ReportStatus?ReportId=f8451bde-8983-402b-9769-e9bfda2b
    "reportDataLocation": "https://<Reporting endpoint base URL>/odata/ReviewerMapping?ReportId=f8451bde-8983-402b-9769-e9bfda2
}
```


Scenario 2: When ReportName is mentioned, but ReviewerUsers is not.

Sample input:

```
POST https://<Reporting endpoint base URL>/OData/ReviewerMappingAsync
{
"ReportName":"TestReviewerMappingReport"
}
```

Sample response:

```
{
    "@odata.context": "https://<Reporting endpoint base URL>/odata/$metadata#ReviewerMappingAsync/$entity",
    "reportId": "34f691be-ec76-4312-be22-00fd4f4f73f7",
    "reportName": "TestReviewerMappingReport",
    "reportType": "Reviewer Mapping",
    "reportDate": "2025-06-09T18:52:59.987+05:30",
    "reportStatus": "Queued",
    "info": "Successfully queued the report request.",
    "newReportInstanceQueued": true,
    "reportStatusLocation": "https://<Reporting endpoint base URL>/odata/ReportStatus?ReportId=34f691be-ec76-4312-be22-00fd4f4f
    "reportDataLocation": "https://<Reporting endpoint base URL>/odata/ReviewerMapping?ReportId=34f691be-ec76-4312-be22-00fd4f4
}
```


Scenario 3: Default behavior when no ReviewerUsers are provided; the request is submitted for all available ReviewerUsers

Sample input:

```
POST https://<Reporting endpoint base URL>/OData/ReviewerMappingAsync
{
"ReportName":"TestReviewerMappingReport",
"ReviewerUsers":[]
}
```

Sample response:


```
{
    "@odata.context": "https://<Reporting endpoint base URL>/odata/$metadata#ReviewerMappingAsync/$entity",
    "reportId": "9f3df184-6392-452f-96b3-182b63a38f44",
    "reportName": "TestReviewerMappingReport",
    "reportType": "Reviewer Mapping",
    "reportDate": "2025-06-11T13:53:36.06+05:30",
    "reportStatus": "Queued",
    "info": "Successfully queued the report request.",
    "newReportInstanceQueued": true,
    "reportStatusLocation": "https://<Reporting endpoint base URL>/odata/ReportStatus?ReportId=9f3df184-6392-452f-96b3-182b63a3
    "reportDataLocation": "https://<Reporting endpoint base URL>/odata/ReviewerMapping?ReportId=9f3df184-6392-452f-96b3-182b63a
}
```


Scenario 4: ReportName is not mentioned.

Sample Input:

```
POST https://<Reporting endpoint base URL>/OData/ReviewerMappingAsync
{
"ReportName":"",
"ReviewerUsers":[1,3]
}
```

Sample Response:


```
{
    "error": {
        "code": "BadParameter",
        "message": "Parameter(s): ReportName either need to be specified or have an incorrect name,
        value or format.For details regarding API parameters, refer to the documentation."
    }
}
```


The following table explains the parameters showcased in the response to a Reviewer Mapping Async API request.

Name	Description
reportId	Displays report ID. It is generated upon successful execution of API.
reportName	Displays report name. It is generated upon successful execution of API.
reportType	Displays the report type as *Reviewer Mapping*.
reportDate	Displays the date of report generation after successful execution of API.
reportStatus	Displays report status. For more information on statuses, See "Report Status API" on page 409..
info	Displays a message if the report request has queued successfully or not.
newReportInstanceQueued	Specifies whether a new report generation request has been submitted or not. The *Rate Limiting* feature restricts submission of multiple requests with identical input parameters if attempted within one minute. It returns the following values: ***True***: The value is shown as *True*, if the new report request has been queued successfully. ***False***: The value is shown as *False*, if the input parameters of the current request are identical to the parameters of the already submitted request *within one minute*, a new report will not be queued. As a result, the details of the existing report request are returned.
reportStatusLocation	Displays a URL with report ID. To view the status of this report, use the same URL.
reportDataLocation	Displays a URL for the location of report data. To access the report data, use the same URL.

2. Call the *ReportStatus* API to get the status of the *ReviewerMappingAsync* API report. See "Report Status API" on page 409.

3. Once the report is ready, call the *ReviewerMapping* API to get the report data from the asynchronous API. See "Reviewer Mapping API" on page 337.

Reviewer Mapping API

ReviewersMapping - List	This report provides the department-level monitoring percentage details for all *message types* in each department.

ReviewersMapping - List

```
GET https://<Reporting endpoint Base URL>/odata/ReviewerMapping
```

Sample requests

```
GET https://<Reporting endpoint Base
URL>/odata/ReviewerMapping?reportid=<ID of the ReviewerMappingAsync
API report>
```

```
GET https://<Reporting endpoint Base
URL>/odata/ReviewerMapping?reportid=d0558287-3349-4df3-9528-11168637a83b
```

Parameter/Filters

The following filter can be used with the ReviewerMapping API when invoked using the GET method only. The system uses the AND operator between the filters to return the result based on the specified filters.

ReportID	Mandatory	Specify the ID of report you want to view.

Scenario 1

```
GET https://<Reporting endpoint Base
URL>/odata/ReviewerMapping?reportid=3890a807-970c-4c71-b849-c1611fe11a53
```

Sample response

Status code: 200 OK

```
"@odata.context": "https://<Reporting endpoint Base
URL>/odata/$metadata#ReviewerMapping",
"@odata.count": 7,
"value": [
  {
    "departmentId": 5,
    "departmentName": "Administration",
    "reviewerUserId": 1,
    "reviewerUserName": "admin",
    "reviewerUserLogin": "domain\\admin",
    "isException": false,
    "disableCapping": 0,
    "bypassMonitoring": false,
    "messageType": [
      {
        "contentSourceId": 1,
        "contentSourceName": "Exchange",
        "isDirectional": true,
        "percentageReviewInternal": 2.0,
        "percentageReviewExtIn": 2.0,
        "percentageReviewExtOut": 2.0,
        "cleanSampleCap": 0
      },
      {
        "contentSourceId": 2,
        "contentSourceName": "Instant Massaging",
        "isDirectional": false,
        "percentageReviewInternal": 2.0,
        "percentageReviewExtIn": 0.0,
        "percentageReviewExtOut": 0.0,
        "cleanSampleCap": 0
      }
    ]
  }
]
```


Supported OData Filters

See "Supported OData query options" on page 410.

Responses

See "Responses" on page 415.

MonitoredEmployees API

Supported Operations

MonitoredEmployees - List	Gets department-level monitoring percentage details for all message types in each department for each monitored employee by using the HTTP GET and POST methods.

MonitoredEmployees - List

```
GET https://<Reporting endpoint Base URL>/odata/MonitoredEmployees?Departments=[list of comma-separated values]
```

```
POST https://<Reporting endpoint Base URL>/odata/MonitoredEmployees
```

Sample requests

```
GET https://<Reporting endpoint Base URL>/odata/MonitoredEmployees?Departments=[1,2,4,7]
```

```
POST https://<Reporting endpoint Base URL>/odata/MonitoredEmployees
```

Request filter/body

Specify the following filters to obtain refined and selective results from this report.

Name	Type	Description
Departments	Optional	Specifies IDs of the departments to get monitoring percentage details for all message types for each monitored employee in the departments. ■ If Department IDs are specified, the result returns details for those departments only. ■ If Department IDs are not specified, the result returns details for every available department. **Data Type**: JSON array of integers 'id'(identifier fields) that is Departments. Note: To get the Department IDs, See "Departments API" on page 311. Refer to the **departmentId** field only.

Scenario 1

To get the monitored employees level monitoring percentages for a specified single department.

Input:

```
POST https://<Reporting endpoint Base URL>/odata/MonitoredEmployees
{
    "Departments": [66],
}
```

Scenario 2

Input:

To get the monitored employees level monitoring percentages for specified list of departments.

```
POST https://<Reporting endpoint Base URL>/odata/MonitoredEmployees
{
    "Departments": [66,67],
}
```

Scenario 3

Input:

To get the monitored employees level monitoring percentages for all departments.

```
POST https://<Reporting endpoint Base URL>/odata/monitoredEmployees
{
"Departments" : []
}
```

Scenario 4

Input:

To get the monitored employees level monitoring percentages for all departments.

```
POST https://<Reporting endpoint Base URL>/odata/monitoredEmployees
{

}
```

Sample response for scenarios 1 to 4

Sample response for scenarios 1 to 4: Status code: 200 OK

```
"@odata.context": "https://<Reporting endpoint Base
URL>/odata/$metadata#MonitoredEmployees",
"@odata.count": 59,
"value": [
    {
        "departmentId": 66,
        "monitoredEmployeeId": 2,
        "monitoredEmployeeName": "johndoe",
        "monitoredEmployeeLogin": "AKA\\johndoe",
        "monitoredEmployeeEmail": [
            "johndoe@aka.com",
            "johndoe_new@aka.com"
        ],
        "messageType": [
            {
                "contentSourceId": 1,
                "contentSourceName": "Exchange",
                "isDirectional": true,
                "percentageReviewInternal": 2.0,
                "percentageReviewExtIn": 2.0,
                "percentageReviewExtOut": 2.0,
                "cleanSampleCap": 0
            },
            {
                "contentSourceId": 2,
                "contentSourceName": "Instant Messaging",
                "isDirectional": false,
                "percentageReviewInternal": 2.0,
                "percentageReviewExtIn": 0.0,
                "percentageReviewExtOut": 0.0,
                "cleanSampleCap": 0
            }
        ]
    }
]
```


Supported OData Filters

See "Supported OData query options" on page 410.

Responses

See "Responses" on page 415.

Evidence Of Review Async API

EvidenceOfReviewAsync	This API submits the report generation request which executes asynchronously. Result of this API contains identifier for report, status and location for retrieving the report data. The report identifier and locations in the result can be used to track the report generation operation.

Note: This note is intended to those who have used earlier versions of this API.

- There were two separate reporting endpoint APIs: ***EvidenceOfReviewByDept*** and ***EvidenceOfReviewByUsers***. However, from this release, these two APIs have been merged into one API called ***EvidenceOfReview***. This unified API offers the same detailed reports which is conveniently accessible in one place.
- The ***users*** field is changed to ***monitoredemployees***.
- A new filter ***Searches*** is added.
- ***ReturnByDepartment***: This parameter has been added to get the records grouped by departments and is set to ***False*** by default. When set to ***False***, the ***monitoredEmployeeId***, ***monitoredEmployee***, and ***totalMessagesForSampling*** parameters are applicable, thus, returned the searched values in the response. Conversely, if set to ***True***, the ***monitoredEmployeeId***, ***monitoredEmployee***, and ***totalMessagesForSampling*** parameters are not applicable, thus, returned the ***-1*** value in the response.
- ***ReturnZeroCaptureRecords***: This parameter has been added and is set to ***False*** by default. When set to ***False***, parameters with a result count of zero will not be displayed in the output. Conversely, if set to ***True***, parameters with a result count of zero will be included in the output.
- The ***Reviewed*** output parameter has been removed and replaced with the ***ReviewedRelevant*** and ***ReviewedIrrelevant*** parameters.
  However, the ***Unreviewed*** output parameter has been retained. In addition, the ***UnreviewedRelevant*** and ***UnreviewedIrrelevant*** parameters are added.
- In the response, the ***-1*** value for ***searchHits*** signifies ***Not Applicable***.

To use the *EvidenceOfReviewAsync* API, follow the steps below:

1 Call the *EvidenceOfReviewAsync* API to submit report generation request.

  This asynchronous API supports GET and POST query methods. Use any of the following as needed:

```
GET https://<Reporting endpoint Base
URL>/odata/EvidenceOfReviewAsync
```

```
POST https://<Reporting endpoint Base
URL>/odata/EvidenceOfReviewAsync
```

Sample input

- ```
  GET https://<Reporting endpoint Base URL>/odata/
  EvidenceOfReviewAsync?ReportName= <name of report>
  & StartDate=<YYYY-MM-DD>&EndDate=<YYYY-MM-DD> &Departments=
  [<DeptID1>,<DeptID2>,...]&MessageTypes=[<MessageTypeID1>,<MessageTypeID2>,...]
  &MessageDirections
  =[<MessageDirectionID1>,<MessageDirectionID2>, ...] &
  CaptureTypes=[<CaptureTypeID1>, <CaptureTypeID2>,...]
  &ReturnByDepartment=True&ReturnZeroCaptureRecords=False
  ```
- ```
  GET https://<Reporting endpoint Base URL>/odata/
  EvidenceOfReviewAsync?ReportName=TestReport1
  &StartDate=2024-01-01&EndDate=2024-06-30 &Departments=[101,
  102] &MessageTypes=[1,7]&MessageDirections=[1,2]
  &CaptureTypes=[6,99]
  &ReturnByDepartment=True&ReturnZeroCaptureRecords=False
  ```
- ```
  POST https://<Reporting endpoint Base
  URL>/odata/EvidenceOfReviewAsync
  ```

EvidenceOfReviewAsync - URL Parameter/Filters

The following filters can be used with the *EvidenceOfReviewAsync* API when invoked using the GET and POST methods. The system uses the **AND** operator between the filters to return the result based on the specified filters.

Name	Type	Description
ReportName	Mandatory	Specify a name of the report.
StartDate	Mandatory	StartDate is the date on which items are captured or ingested in Insight Surveillance is recorded as the CaptureDate for that item. This filter specifies the start date for returning count of items whose CaptureDate is greater than or equal to this start date. **Data Type**: Date in the *YYYY-MM-DD* format that is StartDate.
  ```

Name	Type	Description
EndDate	Mandatory	This filter specifies the end date for returning count of items whose CaptureDate is less than or equal to this date. **Data Type**: Date in the *YYYY-MM-DD* format that is EndDate.
MessageTypes	Optional	Specifies the type of captured items and returns item counts for items that have the specified message type. **Data Type**: JSON array of integers 'id'(identifier fields) that is MessageType IDs. **Limitation**: As an input, this API can pass maximum 100 MessageType IDs.
Departments	Optional	Specifies the departments to which the captured item belongs and returns item counts for items within that department. **Data Type** JSON array of integers 'id'(identifier fields) that is Department IDs. **Limitation** As an input, this API can pass maximum of 1000 Departments IDs. **Note** ■ To include results for all departments of a specified customer in a report, do not specify any department IDs in a query. ■ To include results for specific departments of a specified customer in a report, specify department IDs in the query.

Name	Type	Description
MonitoredEmployees	Optional	This field specifies the monitored employee IDs for which the report has to be generated. For example, if a department has 10 monitored employees but only 2 are specified in this filter, the report will include item counts for only those 2 monitored employees. **Note:** ■ To include all monitored employees in a report, do not specify any monitored employee IDs in a query. ■ To include results for specific monitored employees of a specified customer in a report, specify monitored employee IDs in the query ■ The valid values of monitored employees are the IDs of any monitored employee from the Insight Surveillance MonitoredEmployee ID list. This ID list can be fetched from the MonitoredEmployee API endpoint. See "MonitoredEmployees API" on page 339. Refer to the **MonitoredEmployeeId** field only. **Data Type**: Integer ID of the user.
MessageDirections	Optional	Specifies whether the item was sent/received from within the organization or from an external source and returns item counts for items that have the specified message direction. **Data Type**: JSON array of integers 'id'(identifier fields) that is MessageDirection IDs. **Limitation**: As an input, this API can pass maximum 5 MessageDirection IDs.

Name	Type	Description
CaptureTypes	Optional	Specifies the mode/technique used to capture the item in Arctera and returns item counts for items with the specified capture type. **Data Type**: JSON array of integers 'id'(identifier fields) that is CaptureType IDs. **Limitation**: ■ As an input, this API can pass maximum 10 CaptureTypes IDs. ■ Only CaptureTypes IDs 2, 6, and 99 are supported.
ReturnByDepartment	Mandatory to get department wise report	This parameter value is set to ***False*** by default. ■ When set to ***False***, it returns the count at monitored employee level (that is grouping by monitored employees). The *monitoredEmployeeId*, *monitoredEmployee*, and *totalMessagesForSampling* parameters are applicable, and return the corresponding values in the response. ■ When set to ***True***, it returns the evidence of review count at department level (that is grouping by departments). The *monitoredEmployeeId*, *monitoredEmployee*, and *totalMessagesForSampling* parameters are not applicable, and return the **-1** value in the response.

Name	Type	Description
ReturnZeroCaptureRecords:	Mandatory to get monitored employees wise report	This parameter value is set to ***False*** by default. ■ When set to ***False***, parameters with a result count of zero will not be displayed in the output. ■ When set to ***True***, parameters with a result count of zero will be included in the output.
Searches	Optional	Specifies IDs of the searches. Note: If the IDs of the parent searches are specified, the generated report includes result for corresponding child searches. In the response, the ***-1*** value for ***searchHits*** signifies ***Not Applicable***. The *searchHits* are applicable to Evidence Of Review By Department only and not applicable for Evidence Of Review By Monitored Employee.

Scenario 1: New request to submit a report.

Sample input for Return By Monitored Employee

```
"@odata.context": https://<Reporting endpoint Base
URL>/odata/$metadata#EvidenceOfReviewAsync
    {
    "reportName":"evidence of review by Monitored Employees",
    "StartDate":"2025-01-01",
    "EndDate":"2025-01-03",
    "MonitoredEmployees":[632,634],
    "Searches": [1234,3457]
    }
```

Sample input for Return By Department

```
"@odata.context": https://<Reporting endpoint Base
URL>/odata/$metadata#EvidenceOfReviewAsync
    {
    "reportName":"evidence of review by Departments",
    "StartDate":"2025-01-01",
    "EndDate":"2025-01-03",
    "Departments":[237,17604],
    "ReturnByDepartment": true,
    "Searches": [1234,3457]
    }
```

Sample response

```
{
    "@odata.context": "https://<Reporting endpoint Base
    URL>/odata/$metadata#EvidenceOfReviewAsync/$entity",
    "reportId": "a337e782-aa81-40fd-a65c-589b1bb6da55",
    "reportName": "TestReport_1",
    "reportType": "Evidence Of Review",
    "reportDate": "2024-08-13T11:52:21.373+05:30",
    "reportStatus": "Queued",
    "info": "Successfully queued the report request.",
    "newReportInstanceQueued": true,
    "reportStatusLocation": "https://<Reporting endpoint Base
    URL>/odata/ReportStatus?ReportId=a337e782-aa81-40fd-a65c-589b1bb6da55",
    "reportDataLocation": "https://<Reporting endpoint Base
    URL>/odata/EvidenceOfReview?ReportId=a337e782-aa81-40fd-a65c-589b1bb6da55"
}
```

Name	Description
reportId	Displays report ID. It is generated upon successful execution of API.
reportName	Displays report name. It is generated upon successful execution of API.
reportType	Displays the report type as *Evidence Of Review*.
reportDate	Displays the date of report generation after successful execution of API.
reportStatus	Displays report status. For more information on statuses, See "Report Status API" on page 409.
info	Displays a message if the report request has queued successfully or not.

Name	Description
newReportInstanceQueued	Specifies whether a new report generation request has been submitted or not. The *Rate Limiting* feature restricts submission of multiple requests with identical input parameters if attempted within one minute. It returns the following values: ***True***: The value is shown as *True*, if the new report request has been queued successfully. ***False***: The value is shown as *False*, if the input parameters of the current request are identical to the parameters of the already submitted request *within one minute*, a new report will not be queued. As a result, the details of the existing report request are returned.
reportStatusLocation	Displays a URL with report ID. To view the status of this report, use the same URL.
reportDataLocation	Displays a URL for the location of report data. To access the report data, use the same URL.

Scenario 2: The same request has been submitted again within one minute.

Sample response

```
{
    "@odata.context": "https://<Reporting endpoint Base
    URL>/odata/$metadata#EvidenceOfReviewAsync/$entity",
    "reportId": "a337e782-aa81-40fd-a65c-589b1bb6da55",
    "reportName": "TestReport_1",
    "reportType": "Evidence Of Review",
    "reportDate": "22024-07-05T14:07:20.503+05:30",
    "reportStatus": "Queued",
    "info": "Requested report is already queued with details in this response. In
    case you want to generate new instance of this report then please try after
    some time.",
    "newReportInstanceQueued": false,
    "reportStatusLocation": https://<Reporting endpoint Base
    URL>/odata/ReportStatus?ReportId=a337e782-aa81-40fd-a65c-589b1bb6da55,
    "reportDataLocation": https://<Reporting endpoint Base
    URL>/odata/EvidenceOfReview?ReportId=a337e782-aa81-40fd-a65c-589b1bb6da55
}
```


2 Call the *ReportStatus* API to get the status of asynchronous API report. See "Report Status API" on page 409.

3 Once the report is ready, call the *EvidenceOfReview* API to retrieve the report data from the asynchronous API. See "Evidence of Review API" on page 351.

Evidence of Review API

Supported Operations

EvidenceOfReview - List by filter	Gets the total messages count, captured message count and the marking count, (that is count of messages marked as reviewed/unreviewed/questioned/pending) per monitored employee. The counts are calculated for the specified date range and using the specified filters.

EvidenceOfReview - List by filter

```
GET https://<Reporting endpoint base URL>/odata/EvidenceOfReview
```

Sample requests

```
GET https://<Reporting endpoint Base
URL>/odata/EvidenceOfReview?reportid=<ID of the EvidenceOfReviewAsync
API report>
```

```
GET https://<Reporting endpoint Base
URL>/odata/EvidenceOfReview?reportid=a337e782-aa81-40fd-a65c-589b1bb6da55
```

EvidenceOfReview - URL Parameter/Filters

The following filters can be used with the EvidenceOfReview API when invoked using the GET method. The system uses the **AND** operator between the filters to return the result based on the specified filters.

Name	Type	Description
ReportID	Mandatory	Specify the ID of report you want to view.

Note: This note is intended to those who have used earlier versions of this API.

- There were two separate reporting endpoint APIs: ***EvidenceOfReviewByDept*** and ***EvidenceOfReviewByUsers***. However, from this release, these two APIs have been merged into one API called ***EvidenceOfReview***. This unified API offers the same detailed reports which is conveniently accessible in one place.
- The ***users*** field is changed to ***monitoredemployees***.
- In the response, the ***-1*** value for ***SearchHits*** signifies ***Not Applicable***.

Scenario 1: Return By Department

Sample response

Status code: 200 OK

```
{
    "@odata.context": "https://<Reporting endpoint base
    URL>/odata/$metadata#EvidenceOfReview",
    "value": [
        {
            "departmentId": 2085,
            "departmentName": "dept2",
            "monitoredEmployeeId": -1,
            "monitoredEmployee": "",
            "messageTypeID": 1,
            "messageDirectionID": 0,
            "captureTypeID": 1,
            "totalMessagesForSampling": -1,
            "captured": 0,
            "unReviewed": 0,
            "unreviewedIrrelevant": 0,
            "unreviewedRelevant": 0,
            "pending": 0,
            "questioned": 0,
            "reviewedIrrelevant": 0,
            "reviewedRelevant": 0,
            "messageType": "Exchange",
            "captureType": "Internal",
            "captureTypeDisplayName": "Search",
            "captureTypeDescription": "Indicates that item was
            captured based on immediate or scheduled search",
            "messageDirection": "NotSpecified",
            "messageDirectionDisplayName": "Not Specified",
            "messageDirectionDescription": "Items with a message
            type under the Collab and Transcript categories.",
            "searchId": 0,
            "searchName": null,
            "searchHits": 0
        }
}
```


Scenario 1: Return By Monitored Employees

Sample response

Status code: 200 OK

```
{
    "departmentId": 2095,
    "departmentName": "Dept3",
    "monitoredEmployeeId": 69563,
    "monitoredEmployee": "Krishna Ghodke",
    "messageTypeID": 12,
    "messageDirectionID": 0,
    "captureTypeID": 2,
    "totalMessagesForSampling": 0,
    "captured": 0,
    "unReviewed": 0,
    "unreviewedIrrelevant": 0,
    "unreviewedRelevant": 0,
    "pending": 0,
    "questioned": 0,
    "reviewedIrrelevant": 0,
    "reviewedRelevant": 0,
    "messageType": "Teams Channel",
    "captureType": "Clean",
    "captureTypeDisplayName": "Random Sampling",
    "captureTypeDescription": "Indicates that items were randomly
    sampled",
    "messageDirection": "NotSpecified",
    "messageDirectionDisplayName": "Not Specified",
    "messageDirectionDescription": "Items with a message type
    under the Collab and Transcript categories.",
    "searchId": 0,
    "searchName": null,
    "searchHits": -1
}
```


Supported OData filters

See "Supported OData query options" on page 410.

Supported reporting endpoint API filters and their values

See "Supported reporting endpoint API filters and their values" on page 412.

Responses

See "Responses" on page 415.

Item Classification Metrics Async API

ItemClassificationMetricsAsync	This API submits the report generation request which executes asynchronously. The result of this API contains the identifier for the report, status, and location for retrieving the report data. The report identifier and locations in the result can be used to track the report generation operation.

To use the *ItemClassificationMetricsAsync* API, follow the steps below:

1. Call the *ItemClassificationMetricsAsync* API to submit a report generation request.

   This asynchronous API supports GET and POST query methods. Use any of the following as needed:

   - `GET https://<Reporting endpoint base URL>/OData/ItemClassificationMetricsAsync?ReportName=<Name of the report>&StartDate=<YYYY-MM-DD>&EndDate=<YYYY-MM-DD>`
   - `POST https://<Reporting endpoint base URL>/OData/ItemClassificationMetricsAsync`

   Sample Input

   - `GET https://<Reporting endpoint Base URL>/odata/ItemClassificationMetricsAsync?ReportName=<Name of the report>&StartDate=<YYYY-MM-DD>&EndDate=<YYYY-MM-DD>&Departments=[<DeptID1>,<DeptID2>,...]&Tags=[<tagId1>,<tagId2>...]`
   - `POST https://<Reporting endpoint base URL>/OData/ItemClassificationMetricsAsync`

   ItemClassificationMetricsAsync - URL Parameter/Filters

   The following parameters/filters can be used with the *ItemClassificationMetricsAsync* API when invoked using the GET and POST methods. The system uses the AND operator between the filters to return the result based on the specified filters.

ReportName	Mandatory	Specify the name of the report you want to generate. **Limitations** ■ The report name can be up to a maximum of 256 characters long. ■ Special characters are not allowed; only alphanumeric values are permitted.
StartDate	Mandatory	StartDate refers to the date items are captured or ingested in Insight Surveillance and recorded as their CaptureDate. Specify the start date to return the count of items with a CaptureDate on or after this date. **Data Type** Date in the YYYY-MM-DD format that is StartDate. **Limitations** For the cloud-based application, a maximum of one year duration is allowed.
EndDate	Mandatory	Specify the end date to return the count of items with a CaptureDate on or before this date. **Data Type** Date in the YYYY-MM-DD format that is StartDate. **Limitations** For the cloud-based application, a maximum of one year duration is allowed.

Departments	Optional	Specifies the departments to which the captured item belongs and returns item counts for items within that department. **Data Type** JSON array of integers 'id'(identifier fields) that is Department IDs. **Limitation** As an input, this API can pass maximum of 1000 Departments IDs. ■ To include results for all departments of a specified customer in a report, do not specify any department IDs in a query. ■ To include results for specific departments of a specified customer in a report, specify department IDs in the query. Note: To get the Department IDs, See "Departments API" on page 311. Refer to the **departmentId** field only.
Tags	Optional	Specifies the classification tags of the captured items and returns item counts for those tags. **Data Type** JSON array of integers 'id'(identifier fields) that is Tag IDs. **Limitation** As an input, this API can pass maximum of 1000 Tag IDs. ■ To include results for all the classification tags of a specified customer in a report, do not specify any classification tag ID in a query. ■ To include results for specific classification tag IDs of a specified customer in a report, specify classification tag IDs in the query. Note: To get the Tag IDs, See "Classification Tags API" on page 322. Refer to the **tagID** field only.

Scenario 1: New request to submit a report.

Sample input:

```
POST https://<reporting endpoint base url>/odata/ItemClassificationMetricsAsync
{
  "reportName": "TestReport1",
  "startDate": "2024-01-24T10:39:00.213Z",
  "endDate": "2024-09-23T10:39:00.213Z",
  "departments": [2084,2095],
  "tags": [862]
}
```

Sample response:

```
"@odata.context": "http://<reporting endpoint base URL>/odata/$metadata
#ItemClassificationMetricsAsync/$entity",

"reportId": "7fb3ecac-e94a-4378-8897-1d7d8283f80f",
"reportName": "TestReport1",
"reportType": "Item Classification Metrics",
"reportDate": "2024-10-01T04:25:25.69-05:00",
"reportStatus": "Queued",
"info": "Successfully queued the report request.",
"newReportInstanceQueued": true,

"reportStatusLocation": "http://<reporting endpoint base URL>/odata/ReportStatus?
ReportId=7fb3ecac-e94a-4378-8897-1d7d8283f80f",

"reportDataLocation": "http://<reporting endpoint base
URL>/odata/ItemClassificationMetrics?ReportId=7fb3ecac-e94a-4378-8897-1d7d8283f80f"
```

Name	Description
reportId	Displays report ID. It is generated upon successful execution of API.
reportName	Displays report name. It is generated upon successful execution of API.
reportType	Displays the report type as *Item Classification Metrics*.
reportDate	Displays the date of report generation after successful execution of API.
reportStatus	Displays report status. For more information on statuses, See "Report Status API" on page 409.
info	Displays a message if the report request has queued successfully or not.

Name	Description
newReportInstanceQueued	Specifies whether a new report generation request has been submitted or not. The *Rate Limiting* feature restricts submission of multiple requests with identical input parameters if attempted within one minute. It returns the following values: ***True***: The value is shown as *True*, if the new report request has been queued successfully. ***False***: The value is shown as *False*, if the input parameters of the current request are identical to the parameters of the already submitted request *within one minute*, a new report will not be queued. As a result, the details of the existing report request are returned.
reportStatusLocation	Displays a URL with report ID. To view the status of this report, use the same URL.
reportDataLocation	Displays a URL for the location of report data. To access the report data, use the same URL.

Scenario 2: The same request has been submitted again within one minute.

Sample response:


```
"@odata.context": "http://<reporting endpoint base URL>/odata/$metadata
#ItemClassification MetricsAsync/$entity",

"reportId": "38b38eb9-a0e1-47d4-8026-63146e69009b",
"reportName": "TestReport1",||
"reportType": "Item Classification Metrics",
"reportDate": "2024-09-30T00:21:23.153-05:00",
"reportStatus": "Ready",
"info": "Requested report is already queued with details in this response. In case
you want to generate new instance of this report then please try after some time.",
"newReportInstanceQueued": false,

"reportStatusLocation": "http://<reporting endpoint base URL/odata/ReportStatus?
ReportId=38b38eb9-a0e1-47d4-8026-63146e69009b",

"reportDataLocation": "http://<reporting endpoint base
URL/odata/ItemClassificationMetrics? ReportId=38b38eb9-a0e1-47d4-8026-63146e69009b"
```


2. Call the *ReportStatus* API to get the status of the *ItemClassificationMetricsAsync* API report. See "Report Status API" on page 409.

3. Once the report is ready, call the *ItemClassificationMetrics* API to retrieve the report data from the asynchronous API. See "Item Classification Metrics API" on page 360.

Item Classification Metrics API

ItemClassificationMetrics - List by filter	This report provides the count of messages captured in Arctera Insight Surveillance for all or specified departments and tags for a date, categorized by Message Types (e.g. Exchange, TeamsChat, etc) and Capture types (e.g. Search, Random Sampling, etc). Furthermore, the report shows the count of marked messages (Pending, Questioned, Reviewed Irrelevant, Reviewed Relevant). The counts are calculated for the specified date range and using the specified filters. This report helps tenants/customers to adjust classification tags.

ItemClassificationMetrics - List by filter

```
GET https://<Reporting endpoint base
URL>/odata/ItemClassificationMetrics
```

Sample requests

- `GET https://<Reporting endpoint Base URL>/odata/ItemClassificationMetrics?reportid=<ID of the ItemClassificationMetricsAsync API report>`
- `GET https://<Reporting endpoint Base URL>/odata/ItemClassificationMetrics?reportid=a337e782-aa81-40fd-a65c-589b1bb6da56`

ItemClassificationMetrics - URL Parameter/Filters

The following filters can be used with the ItemClassificationMetrics API when invoked using the GET method only. The system uses the AND operator between the filters to return the result based on the specified filters.

ReportID	Mandatory	Specify the ID of report you want to view.

Scenario 1

```
GET https://<Reporting endpoint base
URL>/odata/ItemClassificationMetrics?

ReportId=a337e782-aa81-40fd-a65c-589b1bb6da56&$count=true
```

Sample response

Status code: 200 OK


```
{
    "@odata.context": "http://<reporting endpoint base URL>/odata/$metadata#ItemClassificationMetrics",
    "@odata.count": 15,
    "value": [
        {
            "itemClassificationMetricsId": 3143,
            "departmentId": 2113,
            "department": "HR Department",
            "tagId": 863,
            "tagName": "extention tag",
            "captureDate": "2024-04-30T00:00:00-05:00",
            "itemsClassified": 20,
            "irrelevant": 0,
            "relevant": 0,
            "pending": 0,
            "questioned": 0,
            "messageTypeId": 11,
            "messageType": "Teams Chat",
            "captureTypeId": 1,
            "captureType": "Search",
            "captureTypeDescription": "Indicates that item was captured based on immediate or scheduled search"
        },
        {
            "itemClassificationMetricsId": 3144,
            "departmentId": 2113,
            "department": "Admin Department",
            "tagId": 863,
            "tagName": "extention tag",
            "captureDate": "2024-04-30T00:00:00-05:00",
            "itemsClassified": 70,
            "irrelevant": 0,
            "relevant": 0,
            "pending": 0,
            "questioned": 0,
            "messageTypeId": 12,
            "messageType": "Teams Channel",
            "captureTypeId": 1,
            "captureType": "Search",
            "captureTypeDescription": "Indicates that item was captured based on immediate or scheduled search"
        },
```


Supported OData Filters

See "Supported OData query options" on page 410.

Responses

See "Responses" on page 415.

Item Label Metrics Async API

ItemLabelMetricsAsync	This API submits the report generation request which executes asynchronously. The result of this API contains the identifier for the report, status, and location for retrieving the report data. The report identifier and locations in the result can be used to track the report generation operation.

To use the *ItemLabelMetricsAsync* API, follow the steps below:

1. Call the *ItemLabelMetricsAsync* API to submit a report generation request.

This asynchronous API supports GET and POST query methods. Use any of the following as needed:

- `GET https://<Reporting endpoint base URL>/OData/ItemLabelMetricsAsync?ReportName=<Name of the report>&StartDate=<YYYY-MM-DD>&EndDate=<YYYY-MM-DD>`
- `POST https://<Reporting endpoint base URL>/OData/ItemLabelMetricsAsync`

Sample Input

- `GET https://<Reporting endpoint Base URL>/odata/ItemLabelMetricsAsync?ReportName=<Name of the report>&StartDate=<YYYY-MM-DD>&EndDate=<YYYY-MM-DD>&Departments=[<DeptID1>,<DeptID2>,...]&Labels=[<LabelId1>,<LabelId2>...]&ReturnByDepartment=<true or false>`
- `POST https://<Reporting endpoint base URL>/OData/ItemLabelMetricsAsync`

ItemLabelMetricsAsync - URL Parameter/Filters

The following parameters/filters can be used with the *ItemLabelMetricsAsync* API when invoked using the GET and POST methods. The system uses the AND operator between the filters to return the result based on the specified filters.

ReportName	Mandatory	Specify the name of the report you want to generate. **Limitations** ■ The report name can be up to a maximum of 256 characters long. ■ Special characters are not allowed; only alphanumeric values are permitted.

StartDate	Mandatory	StartDate refers to the date items are captured or ingested in Insight Surveillance and recorded as their CaptureDate. Specify the start date to return the count of items with a CaptureDate on or after this date. **Data Type** Date in the YYYY-MM-DD format that is StartDate. **Limitations** For the cloud-based application, a maximum of one year duration is allowed.
EndDate	Mandatory	Specify the end date to return the count of items with a CaptureDate on or before this date. **Data Type** Date in the YYYY-MM-DD format that is StartDate. **Limitations** For the cloud-based application, a maximum of one year duration is allowed.
Departments	Optional	Specifies the departments to which the captured item belongs and returns item counts for items within that department. **Data Type** JSON array of integers 'id'(identifier fields) that is Department IDs. **Limitation** As an input, this API can pass maximum of 1000 Departments IDs. ■ To include results for all departments of a specified customer in a report, do not specify any department IDs in a query. ■ To include results for specific departments of a specified customer in a report, specify department IDs in the query. Note: To get the Department IDs, See "Departments API" on page 311. Refer to the **departmentId** field only.

Labels	Optional	Specifies the labels of the captured items and returns item counts for those labels. **Data Type** JSON array of integers 'id'(identifier fields) that is label IDs. **Limitation** As an input, this API can pass maximum of 1000 label IDs. ■ To include results for all the labels of a specified customer in a report, do not specify any label ID in a query. ■ To include results for specific label IDs of a specified customer in a report, specify label IDs in the query. Note: To get the Label IDs, See "Labels API" on page 323. Refer to the **labelID** field only.
ReturnByDepartment	Optional	To generate the Item Label Metrics Report by departments, set this value to ***True***. To generate the Item Label Metrics Report by monitored employees, set this value to ***False***. The default value of this parameter is set to ***False***.

Scenario 1: New request to submit a report.

Sample input:

```
POST : https://<Reporting endpoint Base
URL>/odata/ItemLabelMetricsAsync

{
"ReportName": "LabelMetricsReport",
"StartDate": "2024-01-02",
"EndDate": "2024-12-04",
"Departments":[1038,456],
"Labels":[475],
"ReturnByDepartment": true
}
```

Sample response:

```
{
    "@odata.context": "https://<Reporting endpoint Base
    URL>/odata/$metadata#ItemLabelMetricsAsync/$entity",
    "reportId": "03c0de05-9e7c-4b6e-9729-3ebab9be65fb",
    "reportName": "LabelMetricsReport",
    "reportType": "Item Label Metrics By Department",
    "reportDate": "2024-12-20T04:41:19.45-08:00",
    "reportStatus": "Queued",
    "info": "Successfully queued the report request.",
    "newReportInstanceQueued": true,
    "reportStatusLocation": "https://<Reporting endpoint Base
    URL>/odata/ReportStatus?ReportId=03c0de05-9e7c-4b6e-9729-3ebab
    9be65fb",
    "reportDataLocation": "https://<Reporting endpoint Base
    URL>/odata/ItemLabelMetrics?ReportId=03c0de05-9e7c-4b6e-9729-3
    ebab9be65fb"
}
```


Name	Description
reportId	Displays report ID. It is generated upon successful execution of API.
reportName	Displays report name. It is generated upon successful execution of API.
reportType	Displays the report type as *Item Label Metrics*.
reportDate	Displays the date of report generation after successful execution of API.
reportStatus	Displays report status. For more information on statuses, See "Report Status API" on page 409.
info	Displays a message if the report request has queued successfully or not.

Name	Description
newReportInstanceQueued	Specifies whether a new report generation request has been submitted or not. The *Rate Limiting* feature restricts submission of multiple requests with identical input parameters if attempted within one minute. It returns the following values: ***True***: The value is shown as *True*, if the new report request has been queued successfully. ***False***: The value is shown as *False*, if the input parameters of the current request are identical to the parameters of the already submitted request *within one minute*, a new report will not be queued. As a result, the details of the existing report request are returned.
reportStatusLocation	Displays a URL with report ID. To view the status of this report, use the same URL.
reportDataLocation	Displays a URL for the location of report data. To access the report data, use the same URL.

Scenario 2: The same request has been submitted again within one minute.

Sample response:


```
{
    "@odata.context": "https://<Reporting endpoint Base
    URL>/odata/$metadata#ItemLabelMetricsAsync/$entity",
    "reportId": "03c0de05-9e7c-4b6e-9729-3ebab9be65fb",
    "reportName": "LabelMetricsReport",
    "reportType": "Item Label Metrics By Department",
    "reportDate": "2024-12-20T04:41:19.45-08:00",
    "reportStatus": "Queued",
    "info": "Requested report is already queued with details in
    this response. In case you want to generate new instance of
    this report then please try after some time.",
    "newReportInstanceQueued": false,
    "reportStatusLocation": "https://<Reporting endpoint Base
    URL>/odata/ReportStatus?ReportId=03c0de05-9e7c-4b6e-9729-3ebab
    9be65fb",
    "reportDataLocation": "https://<Reporting endpoint Base
    URL>/odata/ItemLabelMetrics?ReportId=03c0de05-9e7c-4b6e-9729-3
    ebab9be65fb"
}
```

2. Call the *ReportStatus* API to get the status of the *ItemLabelMetricsAsync* API report. See "Report Status API" on page 409.
3. Once the report is ready, call the *ItemLabelMetrics* API to retrieve the report data from the asynchronous API. See "Item Label Metrics API" on page 367.

Item Label Metrics API

ItemLabelMetrics - List by filter

This report provides detailed insights into the labels applied to items for monitored employees within a specific department. This report includes the following key information:

- **Item Counts by Label**: Displays the number of items each label has been applied to for monitored employees in the department.
- **Capture Information**: Displays the capture date along with counts for various marking statuses, categorized by capture types, message types, and directions.
- **Label Details**: Provides additional details about the labels, including label type and label group IDs.
- **Search Support**: If items are captured through a search, the corresponding search ID and name will be displayed for easy identification.

This report helps tenants/customers to adjust item labels and can be generated at the following levels:

Item Label Metrics by Department Report: Displays metrics for items across the department.

Item Label Metrics by Monitored Employee Report: Displays metrics for monitored employees within the department.

ItemLabelMetrics - List by filter

```
GET https://<Reporting endpoint base URL>/odata/ItemLabelMetrics
```

Sample requests

- `GET https://<Reporting endpoint Base URL>/odata/ItemLabelMetrics?reportid=<ID of the ItemLabelMetricsAsync API report>`
- `GET https://<Reporting endpoint Base URL>/odata/ItemLabelMetrics?reportid=a337e782-aa81-40fd-a65c-589b1bb6da56`

ItemLabelMetrics - URL Parameter/Filters

The following filters can be used with the ItemLabelMetrics API when invoked using the GET method only. The system uses the AND operator between the filters to return the result based on the specified filters.

ReportID	Mandatory	Specify the ID of report you want to view.

Scenario 1: Item Label Metric Report by Employee.

```
GET https://<Reporting endpoint Base
URL>/odata/ItemLabelMetrics?ReportId=be1bbfb3-fc7f-4d93-b178-e002afac76d3
```

Sample response

Status code: 200 OK

```
{
    "@odata.context": "https://<Reporting endpoint Base
    URL>/odata/$metadata#ItemLabelMetrics",
    "value": [
        {
            "labelMetricsId": 1,
            "departmentId": 1038,
            "department": "MR2",
            "monitoredEmployeeId": 635,
            "monitoredEmployee": "Admin User",
            "labelId": 42,
            "labelName": "Money Laundering",
            "labelGroupIDs": "1",
            "labelType": "Predicted_And_Applied_Label",
            "captureDate": "2024-06-19T00:00:00-07:00",
            "itemsLabeled": 3,
            "reviewedIrrelevant": 0,
            "reviewedRelevant": 3,
            "pending": 0,
            "questioned": 0,
            "unreviewed": 0,
            "unreviewedIrrelevant": 0,
            "unreviewedRelevant": 0,
            "messageTypeId": 1,
            "messageType": "Exchange",
            "captureTypeId": 2,
            "captureType": "Random Sampling",
            "captureTypeDescription": "Indicates that items were
            randomly sampled",
            "messageDirectionID": 1,
            "messageDirection": "Internal",
            "messageDirectionDisplayName": "Internal",
            "messageDirectionDescription": "The items where the
            author and all recipients are internal to the
            organization.",
            "searchId": 0,
            "searchName": ""
        }
```


Scenario 2: Item Label Metric Report by Department.

Sample response

Status code: 200 OK

```
{
    {
    "@odata.context": "https://<Reporting endpoint Base
    URL>/odata/$metadata#ItemLabelMetrics",
        "labelMetricsId": 1,
        "departmentId": 1038,
        "department": "MR2",
        "monitoredEmployeeId": -1,
        "monitoredEmployee": "",
        "labelId": 23,
        "labelName": "Internal Announcements",
        "labelGroupIDs": "1",
        "labelType": "Predicted_Label",
        "captureDate": "2024-03-01T00:00:00-08:00",
        "itemsLabeled": 20,
        "reviewedIrrelevant": 0,
        "reviewedRelevant": 0,
        "pending": 0,
        "questioned": 0,
        "unreviewed": 20,
        "unreviewedIrrelevant": 0,
        "unreviewedRelevant": 0,
        "messageTypeId": 1,
        "messageType": "Exchange",
        "captureTypeId": 1,
        "captureType": "Search",
        "captureTypeDescription": "Indicates that item was
        captured based on immediate or scheduled search",
        "messageDirectionID": 1,
        "messageDirection": "Internal",
        "messageDirectionDisplayName": "Internal",
        "messageDirectionDescription": "The items where the
        author and all recipients are internal to the
        organization.",
        "searchId": 4908,
        "searchName": "blank"
}
```


Supported OData Filters

See "Supported OData query options" on page 410.

Responses

See "Responses" on page 415.

Item Archived Metrics Async API

ItemArchivedMetricsAsync	This API submits the report generation request which executes asynchronously. The result of this API contains the identifier for the report, status, and location for retrieving the report data. The report identifier and locations in the result can be used to track the report generation operation.

To use the *ItemArchivedMetricsAsync* API, follow the steps below:

1. Call the *ItemArchivedMetricsAsync* API to submit a report generation request.

```
GET https://<Reporting endpoint base
URL>/OData/ItemArchivedMetricsAsync?
IndexStartDate=<YYYY-MM-DD>&IndexEndDate=<YYYY-MM-DD>&ReportName=<Name
of the report>
```

Sample Input

```
GET https://<Reporting endpoint base
URL>/OData/ItemArchivedMetricsAsync?
IndexStartDate=2024-01-01&IndexEndDate=2024-05-31&ReportName=TotalCountReport
```

ItemArchivedMetricsAsync - URL Parameter/Filters

The following parameters/filters can be used with the *ItemArchivedMetricsAsync* API when invoked using the GET method. The system uses the AND operator between the filters to return the result based on the specified filters.

ReportName	Mandatory	Specify the name of the report you want to generate. **Limitations** ■ The report name can be up to a maximum of 256 characters long. ■ Special characters are not allowed; only alphanumeric values are permitted.

IndexStartDate	Mandatory	IndexStartDate refers to the start date on which the items got archived. Specify the start date to return the count of items with archive date on or after this date. **Data Type** Date in the YYYY-MM-DD format that is IndexStartDate. **Limitations** For the cloud-based application, a maximum of one year duration is allowed.
IndexEndDate	Mandatory	IndexEndDate refers to the end date to return the count of archived items with Index End Date on or before this date. Specify the end date to return the count of items with capture date on or before this date. **Data Type** Date in the YYYY-MM-DD format that is IndexEndDate. **Limitations** For the cloud-based application, a maximum of one year duration is allowed.

Scenario 1: New request to submit a report.

Sample input:

```
"@odata.context": https://<Reporting endpoint Base
URL>/odata/ItemArchivedMetricsAsync
"value":
[
    {
        "reportName": "TotalCountReport",
        "IndexStartDate": "2024-01-01",
        "IndexEndDate": "2024-05-31",
    }
]
```

Sample response:

```
{
    "@odata.context": "
    https://api.advancedsupervision.dev.veritas.com/odata/$metadata#ItemArchivedMet
    ricsAsync/$entity",

    "reportId": "accea85a-acd4-479c-acd8-0093d767aa4e",
    "reportName": "TotalCountReport",
    "reportType": "Item Archived Metrics",
    "reportDate": "2024-09-26T00:03:13-07:00",
    "reportStatus": "Queued",
    "info": "Successfully queued the report request.",
    "newReportInstanceQueued": true,

    "reportStatusLocation": "
    https://api.advancedsupervision.dev.veritas.com/odata/ReportStatus?ReportId=acc
    ea85a-acd4-479c-acd8-0093d767aa4e",

    "reportDataLocation": "
    https://api.advancedsupervision.dev.veritas.com/odata/ItemArchivedMetrics?Repor
    tId=accea85a-acd4-479c-acd8-0093d767aa4e"
}
```


Name	Description
reportId	Displays report ID. It is generated upon successful execution of API.
reportName	Displays report name. It is generated upon successful execution of API.
reportType	Displays the report type as *Item Archived Metrics*.
reportDate	Displays the date of report generation after successful execution of API.
reportStatus	Displays report status. For more information on statuses, See "Report Status API" on page 409.
info	Displays a message if the report request has queued successfully or not.

Name	Description
newReportInstanceQueued	Specifies whether a new report generation request has been submitted or not. The *Rate Limiting* feature restricts submission of multiple requests with identical input parameters if attempted within one minute. It returns the following values: ***True***: The value is shown as *True*, if the new report request has been queued successfully. ***False***: The value is shown as *False*, if the input parameters of the current request are identical to the parameters of the already submitted request *within one minute*, a new report will not be queued. As a result, the details of the existing report request are returned.
reportStatusLocation	Displays a URL with report ID. To view the status of this report, use the same URL.
reportDataLocation	Displays a URL for the location of report data. To access the report data, use the same URL.

Scenario 2: The same request has been submitted again within one minute.

Sample response:


```
{
    "@odata.context": "
    https://api.advancedsupervision.dev.veritas.com/odata/$metadata#ItemArchived
    MetricsAsync/$entity",

    "reportId": "accea85a-acd4-479c-acd8-0093d767aa4e",
    "reportName": "TotalCountReport",
    "reportType": "Item Archived Metrics",
    "reportDate": "2024-09-26T00:03:13-07:00",
    "reportStatus": "Queued",
    "info": "Successfully queued the report request.",
    "newReportInstanceQueued": true,

    "reportStatusLocation": "
    https://api.advancedsupervision.dev.veritas.com/odata/ReportStatus?ReportId=
    accea85a-acd4-479c-acd8-0093d767aa4e",

    "reportDataLocation": "
    https://api.advancedsupervision.dev.veritas.com/odata/ItemArchivedMetrics?Re
    portId=accea85a-acd4-479c-acd8-0093d767aa4e"
}
```

2. Call the *ReportStatus* API to get the status of the *ItemArchivedMetricsAsync* API report. See "Report Status API" on page 409.
3. Once the report is ready, call the *ItemArchivedMetrics* API to get the report data from the asynchronous API. See "Item Archived Metrics API" on page 375.

Item Archived Metrics API

ItemArchivedMetrics - List by filter	This report provides the count of archived items, grouped by each MessageType, Employee, and Date.

ItemArchivedMetrics - List by filter

```
GET https://<Reporting endpoint base URL>/odata/ItemArchivedMetrics
```

Sample requests

- `GET https://<Reporting endpoint Base URL>/odata/ItemArchivedMetrics?reportid=<ID of the ItemArchivedMetricsAsync API report>`
- `GET https://<Reporting endpoint Base URL>/odata/ItemArchivedMetrics?reportid=accea85a-acd4-479c-acd8-0093d767aa4e`

Parameter/Filters

The following filter can be used with the ItemArchivedMetrics API when invoked using the GET method only. The system uses the AND operator between the filters to return the result based on the specified filters.

ReportID	Mandatory	Specify the ID of report you want to view.

Scenario 1

```
GET https://<Reporting endpoint base URL>/odata/ItemArchivedMetrics?ReportId=accea85a-acd4-479c-acd8-0093d767aa4e
```

Sample response

Status code: 200 OK

```
"@odata.context": "https://<Reporting endpoint base
URL>/odata/$metadata#ItemArchivedMetrics",
    "value": [
        {
            "id": 46544,
            "indexProcessDate": "2024-01-24T00:00:00-08:00",
            "messageTypeId": 1,
            "messageType": "Exchange",
            "monitoredEmployeeId": 945586,
            "monitoredEmployeeName": "admin ",
            "messageDirectionId": 3,
            "messageDirection": "External Outbound",
            "archivedItemCount": 140
        },
        {
            "id": 46545,
            "indexProcessDate": "2024-01-24T00:00:00-08:00",
            "messageTypeId": 1,
            "messageType": "Exchange",
            "monitoredEmployeeId": 945586,
            "monitoredEmployeeName": "admin ",
            "messageDirectionId": 1,
            "messageDirection": "Internal",
            "archivedItemCount": 30
        },
```


Supported OData Filters

See "Supported OData query options" on page 410.

Responses

See "Responses" on page 415.

Item Hotword Metrics Async API

ItemHotwordMetricsAsync	This API submits the report generation request which executes asynchronously. The result of this API contains the identifier for the report, status, and location for retrieving the report data. The report identifier and locations in the result can be used to track the report generation operation.

To use the *ItemHotwordMetricsAsync* API, follow the steps below:

1. Call the *ItemHotwordMetricsAsync* API to submit a report generation request.

This asynchronous API supports GET and POST query methods. Use any of the following as needed:

- `GET https://<Reporting endpoint base URL>/OData/ItemHotwordMetricsAsync?ReportName=<Name of the report>&StartDate=<YYYY-MM-DD>&EndDate=<YYYY-MM-DD>`
- `POST https://<Reporting endpoint base URL>/OData/ItemHotwordMetricsAsync`

Sample Input

- `GET https://<Reporting endpoint Base URL>/odata/ItemHotwordMetricsAsync?ReportName=<Name of the report>&StartDate=<YYYY-MM-DD>&EndDate=<YYYY-MM-DD>&Departments=[<DeptID1>,<DeptID2>,...]`
- `POST https://<Reporting endpoint base URL>/OData/ItemHotwordMetricsAsync`

ItemHotwordMetricsAsync - URL Parameter/Filters

The following parameters/filters can be used with the *ItemHotwordMetricsAsync* API when invoked using the GET and POST methods. The system uses the AND operator between the filters to return the result based on the specified filters.

ReportName	Mandatory	Specify the name of the report you want to generate. **Limitations** ■ The report name can be up to a maximum of 256 characters long. ■ Special characters are not allowed; only alphanumeric values are permitted.
StartDate	Mandatory	StartDate refers to the date items are captured or ingested in Insight Surveillance and recorded as their capture date. Specify the start date to return the count of items with a capture date on or after this date. **Data Type** Date in the YYYY-MM-DD format that is StartDate. **Limitations** For the cloud-based application, a maximum of one year duration is allowed.

EndDate	Mandatory	Specify the end date to return the count of items with a capture date on or before this date. **Data Type** Date in the YYYY-MM-DD format that is StartDate. **Limitations** For the cloud-based application, a maximum of one year duration is allowed.
Departments	Optional	Specifies the departments to which the captured item belongs and returns item counts for items within that department. **Data Type** JSON array of integers 'id'(identifier fields) that is Department IDs. **Limitation** As an input, this API can pass maximum of 1000 Departments IDs. ■ To include results for all departments of a specified customer in a report, do not specify any department IDs in a query. ■ To include results for specific departments of a specified customer in a report, specify department IDs in the query. Note: To get the Department IDs, See "Departments API" on page 311. Refer to the **departmentId** field only.

Scenario 1: New request to submit a report.

Sample input:

```
POST https://<Reporting endpoint Base
URL>/odata/ItemHotwordMetricsAsync
{
"ReportName":"TestItemHotwordMetricsReport",
"StartDate":"2024-01-01",
"EndDate":"2025-03-18",
"Departments":[101, 102],
}
```

Sample response:

```
{
    "@odata.context": "https://<Reporting endpoint Base
    URL>/odata/$metadata#ItemHotwordMetricsAsync/$entity",
    "reportId": "d0558287-3349-4df3-9528-11168637a83b",
    "reportName": "TestItemHotwordMetricsReport",
    "reportType": "Item Hotword Metrics",
    "reportDate": "2025-03-18T23:49:25.463-07:00",
    "reportStatus": "Queued",
    "info": "Successfully queued the report request.",
    "newReportInstanceQueued": true,
    "reportStatusLocation": "https://<Reporting endpoint Base
    URL>/odata/ReportStatus?ReportId=d0558287-3349-4df3-9528-11168637a83b",
    "reportDataLocation": "https://<Reporting endpoint Base
    URL>/odata/ItemHotwordMetrics?ReportId=d0558287-3349-4df3-9528-11168637a83b"
}
```


Name	Description
reportId	Displays report ID. It is generated upon successful execution of API.
reportName	Displays report name. It is generated upon successful execution of API.
reportType	Displays the report type as *Item Hotword Metrics*.
reportDate	Displays the date of report generation after successful execution of API.
reportStatus	Displays report status. For more information on statuses, See "Report Status API" on page 409..
info	Displays a message if the report request has queued successfully or not.

Name	Description
newReportInstanceQueued	Specifies whether a new report generation request has been submitted or not. The *Rate Limiting* feature restricts submission of multiple requests with identical input parameters if attempted within one minute. It returns the following values: ***True***: The value is shown as *True*, if the new report request has been queued successfully. ***False***: The value is shown as *False*, if the input parameters of the current request are identical to the parameters of the already submitted request *within one minute*, a new report will not be queued. As a result, the details of the existing report request are returned.
reportStatusLocation	Displays a URL with report ID. To view the status of this report, use the same URL.
reportDataLocation	Displays a URL for the location of report data. To access the report data, use the same URL.

Scenario 2: The same request has been submitted again within one minute.

Sample response:


```
{
    "@odata.context": "https://<Reporting endpoint Base
    URL>/odata/$metadata#ItemHotwordMetricsAsync/$entity",
    "reportId": "d0558287-3349-4df3-9528-11168637a83b",
    "reportName": "TestItemHotwordMetricsReport",
    "reportType": "Item Hotword Metrics",
    "reportDate": "2025-03-18T23:49:25.463-07:00",
    "reportStatus": "Queued",
    "info": "Requested report is already queued with details in this response.
    In case you want to generate new instance of this report then please try
    after some time.",
    "newReportInstanceQueued": false,
    "reportStatusLocation": "https://<Reporting endpoint Base
    URL>/odata/ReportStatus?ReportId=d0558287-3349-4df3-9528-11168637a83b",
    "reportDataLocation": "https://<Reporting endpoint Base
    URL>/odata/ItemHotwordMetrics?ReportId=d0558287-3349-4df3-9528-11168637a83b"
}
```


2. Call the *ReportStatus* API to get the status of the *ItemHotwordMetricsAsync* API report. See "Report Status API" on page 409.

3. Once the report is ready, call the *ItemHotwordMetrics* API to retrieve the report data from the asynchronous API. See "Item Hotword Metrics API" on page 381.

Item Hotword Metrics API

ItemHotwordMetrics - List by filter

This report provides detailed insights into the hotwords applied to items within a specific department. This report includes the following key information:

- **Item Counts by hotwords**: Displays the number of items each hotword has been applied to in the department.
- **Capture Information**: Displays the capture date along with counts for various marking statuses.
- **Hotword Details**: Displays additional information about hotwords, including the hotword name, hotword category IDs, and the hotword category name.

This report helps tenants/customers to adjust item hotwords and can be generated at the following level:

ItemHotwordMetrics - List by filter

```
GET https://<Reporting endpoint base URL>/odata/ItemHotwordMetrics
```

Sample requests

- `GET https://<Reporting endpoint Base URL>/odata/ItemHotwordMetrics?reportid=<ID of the ItemHotwordMetricsAsync API report>`
- `GET https://<Reporting endpoint Base URL>/odata/ItemHotwordMetrics?reportid=d0558287-3349-4df3-9528-11168637a83b`

ItemHotwordMetrics - URL Parameter/Filters

The following filter can be used with the ItemHotwordMetrics API when invoked using the GET method only. The system uses the AND operator between the filters to return the result based on the specified filters.

ReportID	Mandatory	Specify the ID of report you want to view.

Scenario 1: Item Hotword Metric Report.

Sample response

Status code: 200 OK

```
{
    "@odata.context": "https://<Reporting endpoint Base
    URL>/odata/$metadata#ItemHotwordMetrics",
    "value": [
        {
            "hotwordStatsID": 73546,
            "departmentId": 6074,
            "department": "HR Department",
            "hotwordID": 73102,
            "hotword": "one",
            "hotwordCategoryID": 50612,
            "hotwordCategory": "For Perf Test",
            "captureDate": "2024-09-17T00:00:00-07:00",
            "itemCount": 2,
            "relevant": 0,
            "irrelevant": 0,
            "unreviewed": 2,
            "unreviewedIrrelevant": 0,
            "unreviewedRelevant": 0
        },
}
```


Supported OData Filters

See "Supported OData query options" on page 410.

Responses

See "Responses" on page 415.

Item Details Async API

ItemDetailsAsync	This API submits the report generation request which executes asynchronously. The result of this API contains the identifier for the report, status, and location for retrieving the report data. This report displays items that have been archived and discovered within the Insight Surveillance application. It includes metadata such as subject and author, as well as a history of actions performed on the item, including label assignment, marking, escalation, appraisal, and commenting. The report identifier and locations in the result can be used to track the report generation operation. Note: If the number of records in the report exceeds 400,000 records, the result will be truncated. The extra records beyond the limit (400,000) are not included in the report. If the result is truncated, refine the filter criteria to narrow down the number of records and retrieve more specific data.

To use the *ItemDetailsAsync* API, follow the steps below:

1. Call the *ItemDetailsAsync* API to submit a report generation request.

   This asynchronous API supports GET and POST query methods. Use any of the following as needed:

   - `GET https://<Reporting endpoint base URL>/OData/ItemDetailsAsync?ReportName=<Name of the report>&StartDate=<YYYY-MM-DD>& EndDate=<YYYY-MM-DD>`
   - `POST https://<Reporting endpoint base URL>/OData/ItemDetailsAsync`

   Sample Input

   - `GET https://<Reporting endpoint Base URL>/odata/ItemDetailsAsync?ReportName=<Name of the report>&StartDate=<YYYY-MM-DD>& EndDate=<YYYY-MM-DD>&DateType=CaptureDate or ItemHistoryDate& Departments=[<DeptID1>,<DeptID2>,...]&MessageTypes=[<MessageType ID1>,< MessageType ID2>,...]&MonitoredEmployees=[<MonitoredEmployees ID1>,<`

```
MonitoredEmployees ID2>,...]&IncludeItemHistory=[True or
False]& ItemHistoryEventType=[1, 2, 3, 4, and/or 5]
```

- `POST https://<Reporting endpoint base URL>/OData/ItemDetailsAsync`

ItemDetailsAsyncAPI - URL Parameter/Filters

The following parameters/filters can be used with the *ItemDetailsAsync* API when invoked using the GET and POST methods. The system uses the AND operator between the filters to return the result based on the specified filters.

ReportName	Mandatory	Specify the name of the report you want to generate. **Limitations** ■ The report name can be up to a maximum of 256 characters long. ■ Special characters are not allowed; only alphanumeric values are permitted.
StartDate	Mandatory	StartDate refers to the beginning of the date range used to filter items in Insight Surveillance. The interpretation of this filter depends on the selected DateType: ■ If DateType = CaptureDate, StartDate refers to the date the items were captured or ingested into Insight Surveillance. ■ If DateType = ItemHistoryDate, StartDate refer to the dates when specific actions—such as commenting, labeling, or escalation—were initially performed on the items. **Data Type** Date in the YYYY-MM-DD format that is StartDate. **Limitations** For the cloud-based application, a maximum of one year duration is allowed.

EndDate	Mandatory	EndDate refers to the end of the date range used to filter items in Insight Surveillance. The interpretation of this filter depends on the selected DateType: ■ If DateType = CaptureDate, EndDate refers to the date the items were captured or ingested into Insight Surveillance. ■ If DateType = ItemHistoryDate, EndDate refer to the date when specific actions—such as commenting, labeling, or escalation—were finally initially performed on the items. **Data Type** Date in the YYYY-MM-DD format that is EndDate. **Limitations** For the cloud-based application, a maximum of one year duration is allowed.

DateType	Optional	Specify the date type to return the count of item IDs based on their capture date or the item history date. Select any of the following options as required: ■ **CaptureDate** ■ This option is selected by default. ■ It is the specific date on which the item is captured into the Insight Surveillance application. ■ If you select this option, the result includes items captured within the specified date range inside surveillance, along with the metadata and complete history of those items. ■ **ItemHistoryDate** ■ Select this option if you want to get item count by the item history date. ■ It is a specific date, falling within the range of the StartDate and EndDate, on which the item's historical event occurred. ■ If you select this option, the result includes items captured within the specified date range inside surveillance, along with the metadata and complete history of those items. **Data Type** String. **Limitations** For the cloud-based application, a maximum of one year duration is allowed.

Departments	Optional	Specifies the departments to which the item belongs and returns item counts for items within that department. **Data Type** JSON array of integers id (identifier fields) that is Department IDs. **Limitation** As an input, this API can pass maximum of 1000 Departments IDs. ■ To include results for all departments of a specified customer in a report, do not specify any department IDs in a query. ■ To include results for specific departments of a specified customer in a report, specify department IDs in the query. Note: To get the Department IDs, See "Departments API" on page 311. Refer to the **departmentId** field only.
MessageTypes	Optional	Specifies the type of captured items and returns item counts for items that have the specified message type. **Data Type**: JSON array of integers 'id'(identifier fields) that is MessageTypes IDs. **Limitation**: As an input, the ItemDetails API can pass maximum 100 MessageTypes IDs on a single page.

MonitoredEmployees	Optional	This field specifies the monitored employee IDs for which the report has to be generated. For example, if a department has 10 monitored employees but only 2 are specified in this filter, the report will include item counts for only those 2 monitored employees. **Note:** ■ The MonitoredEmployee field is available only for items captured through Searches. ■ For items captured through Sampling, this MonitoredEmployee field will remain null. No value is provided in the report. ■ To include all monitored employees in a report, do not specify any monitored employee IDs in a query. ■ To include results for specific monitored employees in a report, specify monitored employee IDs in the query ■ The valid values of monitored employees are the IDs of any monitored employee from the Insight Surveillance MonitoredEmployee ID list. This ID list can be fetched from the MonitoredEmployee API endpoint. See "MonitoredEmployees API" on page 339. Refer to the **MonitoredEmployeeId** field only. **Data Type**: Integer ID of the user. **Limitation** As an input, this API can pass maximum of 1000 MonitoredEmployee IDs.
IncludeItemHistory	Optional	Determines whether the history of items is included or excluded in the output. ■ Set this value as ***False*** to exclude history of items from the output. By default this value is set to *False*. ■ Set this value as ***True*** to include history of items in the output.
ItemHistoryEventType	Optional	Includes or excludes the item history event type in the output based on the value set for the *IncludeItemHistory* field.

- If the **DateType** = **CapturedDate** (default) and **IncludeItemHistory** = **False**, then, the report compares dates with the item's CaptureDate and does not include item history in the results. Refer to the sample scenario below.

```
Input for Minimum parameters
{
    "ReportName":"ItemDetails",
    "StartDate":"2025-01-01",
    "EndDate":"2025-03-02"
}
```

- If the **DateType** = **CapturedDate** (default) and **ItemHistoryEventType** is set to 1 (Appraisal), 2 (Comment), or 4 (Action Status – Mark)), then, the report returns:
  - Items are captured within a specified date range.
  - From the captured items, results are further filtered based on event type (e.g., *Appraisal*, *Comment*, *Mark*).
  - For the filtered items, full metadata and history are returned. Refer to the sample scenario below.

```
Input for DateType is CapturedDate

{
    "ReportName":"ItemDetailsBasedOnCaptureDate",
    "StartDate":"2025-01-01",
    "EndDate":"2025-03-02",
    "DateType":"CapturedDate",
    "IncludeItemHistory":true,
    "Departments":[106,635],
    "MessageTypes":[1,4,7],
    "ItemHistoryEventType":[1,2,4],
    "MonitoredEmployees":[2,3,4,5]
}
```

- If the **DateType** = **ItemHistoryDate** and **ItemHistoryEventType** is set to 2 (Comment), 3 (Escalation), or 5 (Action Status – Label), the report returns:
  - Items with comment, escalation, or label actions performed between the specified start and end dates are retrieved.
  - From these results, full metadata and history are returned for each item.

    Refer to the sample scenario below.

```
Input for DateType is ItemHistoryDate

{
    "ReportName":"ItemDetailsBasedOnItemHistoryDate",
    "StartDate":"2025-01-01",
    "EndDate":"2025-03-02",
    "DateType":"ItemHistoryDate",
    "IncludeItemHistory":true,
    "Departments":[106,635],
    "MessageTypes":[1,4,7],
    "ItemHistoryEventType":[3,2,5],
    "MonitoredEmployees":[2,3,4,5]
}
```

- Items that have comment, escalation, or label actions performed between the specified start and end dates.
- From that result, full metadata and history is returned for those items.

Possible values of item history event type are:

- 1 - Appraisal
- 2 - Comment
- *3 - Escalation*
- 4 - Action Status - Mark
- 5 - Action Status - Label
- 6 - Action Status – Preview

Data Type: Integer ID of the item.

Limitation

As an input, this API can pass maximum of 10 ItemHistoryEventType IDs.

Scenario 1: A new request to submit the report when DateType = CaptureDate

Sample input:

```
POST https://<Reporting endpoint base URL>/OData/ItemDetailsAsync
{
    "StartDate":"2024-04-15",
    "EndDate":"2025-04-15",
    "ReportName":"ItemDetailsBasedOnCaptureDate",
    "DateType":"CaptureDate",
    "IncludeItemHistory":true,
    "Departments":[19366,19449],
    "MessageTypes":[114,5],
    "ItemHistoryEventType":[1,2,3,4,5],
    "MonitoredEmployees":[945697,945698]
}
```

Sample response:

```
{
    "@odata.context": https://<Reporting endpoint base
    URL>/OData/$metadata#ItemDetailsAsync/$entity,
    "reportId": "516a992d-45ce-4ec7-9595-9d1106e7c405",
    "reportName": "ItemDetailsBasedOnCaptureDate",
    "reportType": "Item Details",
    "reportDate": "2025-04-24T05:05:20.66-07:00",
    "reportStatus": "Queued",
    "info": "Successfully queued the report request.",
    "newReportInstanceQueued": true,
    "reportStatusLocation":
    https://api.advancedsupervision.qa.veritas.com/odata/ReportStat
    us?ReportId=516a992d-45ce-4ec7-9595-9d1106e7c405,
    "reportDataLocation":
    https://api.advancedsupervision.qa.veritas.com/odata/ItemDetail
    s?ReportId=516a992d-45ce-4ec7-9595-9d1106e7c405
}
```


Scenario 2: A new request to submit the report when DateType = ItemHistoryDate

Sample input

```
POST https://<Reporting endpoint base URL>/OData/ItemDetailsAsync
{
    "StartDate":"2024-04-15",
    "EndDate":"2025-04-15",
    "ReportName":"ItemDetailsBasedOnItemHistoryDate",
    "DateType":"ItemHistoryDate",
    "IncludeItemHistory":true,
    "Departments":[19366,19449],
    "MessageTypes":[114,5],
    "ItemHistoryEventType":[1,2,3,4,5],
    "MonitoredEmployees":[945697,945698]
}
```

Sample response:

```
{
    "@odata.context": https://<Reporting endpoint base
    URL>/OData/odata/$metadata#ItemDetailsAsync/$entity,
    "reportId": "00a5b2d9-fa75-4909-bbfa-2bf295b489b5",
    "reportName": "ItemDetailsBasedOnItemHistoryDate",
    "reportType": "Item Details",
    "reportDate": "2025-04-24T05:10:37.87-07:00",
    "reportStatus": "Queued",
    "info": "Successfully queued the report request.",
    "newReportInstanceQueued": true,
    "reportStatusLocation":
    https://api.advancedsupervision.qa.veritas.com/odata/ReportStat
    us?ReportId=00a5b2d9-fa75-4909-bbfa-2bf295b489b5,
    "reportDataLocation":
    https://api.advancedsupervision.qa.veritas.com/odata/ItemDetail
    s?ReportId=00a5b2d9-fa75-4909-bbfa-2bf295b489b5
}
```

Scenario 3: A new request to submit the report when IncludeItemHistory = False. ItemHistoryEventType is ignored/excluded from the report.

Sample request:

```
POST https://<Reporting endpoint base URL>/OData/ItemDetailsAsync
{
    "StartDate":"2024-04-15",
    "EndDate":"2025-04-15",
    "ReportName":"ItemDetailsWithoutItemHistory",
    "DateType":"CaptureDate",
    "IncludeItemHistory":false,
    "Departments":[19366,19449],
    "MessageTypes":[114,5],
    "MonitoredEmployees":[945697,945698]
}
```

Sample response:

```
{
    "@odata.context": https://<Reporting endpoint base
    URL>/OData/$metadata#ItemDetailsAsync/$entity,
    "reportId": "f3e05a85-38bd-4c20-8d10-9d4b87ef3852",
    "reportName": "ItemDetailsWithoutItemHistory",
    "reportType": "Item Details",
    "reportDate": "2025-04-24T06:44:19.283-07:00",
    "reportStatus": "Queued",
    "info": "Successfully queued the report request.",
    "newReportInstanceQueued": true,
    "reportStatusLocation":
    https://api.advancedsupervision.qa.veritas.com/odata/ReportStat
    us?ReportId=f3e05a85-38bd-4c20-8d10-9d4b87ef3852,
    "reportDataLocation":
    https://api.advancedsupervision.qa.veritas.com/odata/ItemDetail
    s?ReportId=f3e05a85-38bd-4c20-8d10-9d4b87ef3852
}
```


Name	Description
reportId	Displays report ID. It is generated upon successful execution of API.
reportName	Displays report name. It is generated upon successful execution of API.
reportType	Displays the report type as *Item Details*.
reportDate	Displays the date of report generation after successful execution of API.
reportStatus	Displays report status. For more information on statuses, See "Report Status API" on page 409.
info	Displays a message if the report request has queued successfully or not.

Name	Description
newReportInstanceQueued	Specifies whether a new report generation request has been submitted or not. The *Rate Limiting* feature restricts submission of multiple requests with identical input parameters if attempted within one minute. It returns the following values: ***True***: The value is shown as *True*, if the new report request has been queued successfully. ***False***: The value is shown as *False*, if the input parameters of the current request are identical to the parameters of the already submitted request *within one minute*, a new report will not be queued. As a result, the details of the existing report request are returned.
reportStatusLocation	Displays a URL with report ID. To view the status of this report, use the same URL.
reportDataLocation	Displays a URL for the location of report data. To access the report data, use the same URL.

2. Call the *ReportStatus* API to get the status of the *ItemDetailsAsync* API report. See "Report Status API" on page 409.
3. Once the report is ready, call the *ItemDetails* API to retrieve the report data from the asynchronous API. See "Item Details API" on page 396.

Item Details API

ItemDetails - List by filter

This report displays items that have been archived and discovered within the Insight Surveillance application. It includes metadata such as subject and author, as well as a history of actions performed on the item, including label assignment, marking, escalation, appraisal, and commenting.

This report provides detailed insights into the items and the history of events associated with those items.

This report provides the following additional parameters:

- **itemId**: Copy this ID and use it in the advanced filter in Insight Surveillance to preview the item.
- **itemIdentifier**: This is a unique identifier for an item.

Note:

- If the number of records in the report exceeds 400,000 records, the result will be truncated. The extra records beyond the limit (400,000) are not included in the report.
- If the result is truncated, refine the filter criteria to narrow down the number of records and retrieve more specific data.

ItemDetails - List by filter

```
GET https://<Reporting endpoint base URL>/odata/ItemDetails
```

Sample requests

- `GET https://<Reporting endpoint Base URL>/odata/ItemDetails?reportid=<ID of the ItemDetailsAsync API report>`
- `GET https://<Reporting endpoint Base URL>/odata/ItemDetails?reportid=dd437b60-32cc-459b-a60d-8acd413c3aeb`

ItemDetailsAPI - URL Parameter/Filters

The following filters can be used with the ItemDetails API when invoked using the GET method only. The system uses the AND operator between the filters to return the result based on the specified filters.

ReportID	Mandatory	Specify the ID of ItemDetails API report you want to view.

Scenario 1: Item Details Report when DateType = CaptureDate

```
GET https://<Reporting endpoint Base
URL>/odata/ItemDetails?ReportId=dd437b60-32cc-459b-a60d-8acd413c3aeb
```

Sample response:

Status code: 200 OK


```
{
"@odata.context":
https://api.advancedsupervision.qa.veritas.com/odata/$metadata#ItemDetails,
"value":[
        {
        "itemDetailsId": 10038095,
        "itemIdentifier": 33234734,
        "itemId":
        "d4zl28UXkL5B_GtWGgXUzKMF9q-DYU6n81ft_mRjNzdjODczZjJkYTQzNzFhMmYyZmQ5NG
        UyMTgwNTA5w0xk1SOaKsBDAJ2fmE8YCjByzQmKWzouewY",
        "departmentId": 19449,
        "departmentName": "AutoTagIR1-271224022951",
        "captureDate": "2024-12-27T11:04:26.903-08:00",
        "subject": "271224022951-T-24-Domino first none email",
        "author": user1-bhagirathi-group5@vas-bhagirathi-group5.com,
        "recipient": user2-bhagirathi-group5@vas-bhagirathi-group5.com,
        "mailDate": "2024-12-27T10:42:38-08:00",
        "messageType": 5,
        "messageTypeName": "Domino",
        "monitoredEmployees": "[User1-Bhagirathi-group5] | [User2-Bhagirathi-group5]",
        "itemHistory": [
            {
             "eventName": "Action Status-Mark",
             "description": "Pending",
             "eventTimestamp": "2025-01-08T04:16:09.47-08:00",
             "userId": 216,
             "userName": "admin ",
             "type": "Mark",
             "subType": "None"
            },
            {
             "eventName": "Action Status-Mark",
             "description": "Questioned",
             "eventTimestamp": "2025-01-08T04:16:14.803-08:00",
             "userId": 216,
             "userName": "admin ",
             "type": "Mark",
             "subType": "None"
            },
},],}
```

Scenario 2: Item Details Report when DateType = ItemHistoryDate

Sample response:


```
{
 "@odata.context":
 https://api.advancedsupervision.qa.veritas.com/odata/$metadata#ItemDetails,
    "value": [
        {
            "itemDetailsId": 10038119,
            "itemIdentifier": 33234746,
            "itemId":
            "rYVmTiE6NCHh9mDr6FD-DWkyda7kE95d_3ZvH2RjNzdjODczZjJkYTQzNzFhMmYyZmQ5NGU
            yMTgwNTA5bV1T7Ybje-Ey856TmJKk06Ceq0kpYcJrZE8",
            "departmentId": 19449,
            "departmentName": "AutoTagIR1-271224022951",
            "captureDate": "2024-12-27T11:04:26.963-08:00",
            "subject": "271224022951-T-24-Domino cake at my desk",
            "author": user1-bhagirathi-group5@vas-bhagirathi-group5.com,
            "recipient": outside@out.com,
            "mailDate": "2024-12-27T10:42:39-08:00",
            "messageType": 5,
            "messageTypeName": "Domino",
            "monitoredEmployees": "[User1-Bhagirathi-group5]",
            "itemHistory": [
                {
                "eventName": "Action Status-Mark",
                "description": "Reviewed Relevant",
                "eventTimestamp": "2025-01-08T05:53:59.937-08:00",
                "userId": 216,
                "userName": "admin ",
                "type": "Mark",
                "subType": "None"
                }
            ]
        },
}
```


Scenario 3: Item Details Report when IncludeItemHistory = False

Sample response:

```
{
 "@odata.context":
 https://api.advancedsupervision.qa.veritas.com/odata/$metadata#ItemDetails,
 "value": [
    {
     "itemDetailsId": 10038142,
     "itemIdentifier": 40518782,
     "itemId":
     "DV9OIus5_AIr1ijYyS7ZiI6dss_TNtQXet04nzBiZTQxOGNjZjE5OTQyN2ZiZjgxMWJiNDgzNjFiY2
     U4DKrfwhHcbhsNzZD9dT9sLt9OfWZR3U7xs80",
     "departmentId": 19366,
     "departmentName": "0_TestAutoHHN-11224204924",
     "captureDate": "2025-04-14T11:25:32.937-07:00",
     "subject": "101224030559-T0-CellTrust internal odata-gss",
     "author": user1-bhagirathi-group5@vas-bhagirathi-group5.com,
     "recipient": user2-bhagirathi-group5@vas-bhagirathi-group5.com,
     "mailDate": "2024-12-10T11:15:20-08:00",
     "messageType": 114,
     "messageTypeName": "CellTrust",
     "monitoredEmployees": "[User1-Bhagirathi-group5] | [User2-Bhagirathi-group5]",
     "itemHistory": []
        },
}
```


Scenario 4: Limiting a report when records are more than 400000

Sample response:

```
{
    "IsResultTruncated": true,
    "ResultTruncationReason": "The result set has been truncated to 400000 records.
    Please refine your filter criteria to narrow down the results and retrieve more
    specific data.",
    "@odata.context":
    https://api.advancedsupervision.qa.veritas.com/odata/$metadata#ItemDetails,
    "value": [
        {
            "itemDetailsId": 9485429,
            "itemIdentifier": 15344126,
            "itemId":
            "TdQNkn7H-VRUl75LtDtJkOPQpv1PvZpuoJe5EGRjNzdjODczZjJkYTQzNzFhMmYyZmQ5NGU
            yMTgwNTA5rheVFCi8DxvHWZB9nQmcvZVuyd8nmvaVGz0",
            "departmentId": 5834,
            "departmentName": "50Tenant5Dept4",
            "captureDate": "2024-05-02T10:11:06.973-07:00",
            "subject": "sunday for regression random testing 11",
            "author": admin@vas-bhagirathi-group5.com,
            "recipient":
            user1-bhagirathi-group5@vas-bhagirathi-group5.com;user2-bhagirathi-group
            5@vas-bhagirathi-group5.com;user3-bhagirathi-group5@vas-bhagirathi-group
            5.com;user4-bhagirathi-group5@vas-bhagirathi-group5.com;user5-bhagirathi
            -group5@vas-bhagirathi-group5.com,
            "mailDate": "2024-03-06T05:45:23-08:00",
            "messageType": 1,
            "messageTypeName": "Exchange",
            "monitoredEmployees": null,
            "itemHistory": []
        },
}
```


Supported OData Filters

See "Supported OData query options" on page 410.

Responses

See "Responses" on page 415.

Reviewer Assessment Metrics Async API

Reviewer Assessment Metrics Async	This API submits the report generation request which executes asynchronously. The result of this API contains the identifier for the report, status, and location for retrieving the report data. This report displays metrics for actions performed by reviewers within the Insight Surveillance application. These actions include marking, labeling, escalating, and appraising items. The report is intended to assess reviewer performance based on the accuracy of their reviews. The report identifier and locations in the result can be used to track the report generation operation.

To use the *Reviewer Assessment Metrics Async* API, follow the steps below:

1. Call the *Reviewer Assessment Metrics Async* API to submit a report generation request.

   This asynchronous API supports GET and POST query methods. Use any of the following as needed:

   - `GET https://<Reporting endpoint base URL>/OData/ReviewerAssessmentMetricsAsync?ReportName=<Name of the report>&StartDate=<YYYY-MM-DD>& EndDate=<YYYY-MM-DD>`
   - `POST https://<Reporting endpoint base URL>/OData/ReviewerAssessmentMetricsAsync`

   Sample Request

   - `GET https://<Reporting endpoint Base URL>/odata/ReviewerAssessmentMetricsAsync?StartDate=2025-04-23&EndDate=2025-05-31&ReportName=SampleReviewerAssessReport`
   - `POST https://<Reporting endpoint base URL>/OData/ReviewerAssessmentMetricsAsync`

   Reviewer Assessment Metrics Async API - URL Parameter/Filters

   The following parameters/filters can be used with the *Reviewer Assessment Metrics Async* API when invoked using the GET and POST methods. The system uses the AND operator between the filters to return the result based on the specified filters.

ReportName	Mandatory	Specify the name of the report you want to generate. **Data Type**: String **Limitations** ■ The report name can be up to a maximum of 256 characters long. ■ Special characters are not allowed; only alphanumeric values are permitted.
StartDate	Mandatory	StartDate refers to the beginning of the datetime used to filter items in Insight Surveillance. It specifies emails with a 'sent date' greater than or equal to the specified value. **Data Type**: DateTime **Notes**: 1. Format is YYYY-MM-DDThh:mm:ss. The time component is optional. If you prefer not to include the time, you can simply use the YYYY-MM-DD format. 2. StartDate must be earlier than EndDate. **Limitations** For the cloud-based application, a maximum of one year duration is allowed.
EndDate	Mandatory	EndDate refers to the end of the datetime used to filter items in Insight Surveillance. It specifies emails with a 'sent date' less than or equal to the specified value. **Data Type**: DateTime **Notes**: 1. Format is YYYY-MM-DDThh:mm:ss. The time component is optional. If you prefer not to include the time, you can simply use the YYYY-MM-DD format. 2. EndDate must be later than StartDate. **Limitations** For the cloud-based application, a maximum of one year duration is allowed.

Departments	Optional	Specifies the departments to which the item belongs and returns item counts for items within that department. **Data Type**: JSON array of integers id (identifier fields) that is Department IDs. **Limitation** As an input, this API can pass maximum of 1000 Departments IDs. ■ To include results for all departments of a specified customer in a report, do not specify any department IDs in a query. ■ To include results for specific departments of a specified customer in a report, specify department IDs in the query. Note: To get the Department IDs, See "Departments API" on page 311. Refer to the **departmentId** field only.
Reviewers	Optional	Specify a list of UserIDs for the reviewers whose details you want to retrieve. **Data Type**: JSON array of integers 'id'(identifier fields) that is Reviewer IDs **Limitation** As an input, this API can pass maximum of 100 reviewers. Note: The valid value of the Reviewer is an ID of any user from the Insight Surveillance User ID list. The User ID list can be fetched from the Users API endpoint. See "Users API" on page 312. Refer to the **userId** field only.
MessageTypes	Optional	Specifies the type of captured items and returns item counts for items that have the specified message type. **Data Type**: JSON array of integers 'id' (identifier fields) that is MessageTypes IDs. **Limitation** As an input, the Reviewer Assessment Metrics API can pass maximum 100 MessageTypes IDs on a single page.

Note: If no optional parameters are specified (such as in the GET request), the Reviewer Assessment Metrics API returns counts for all Departments, Reviewers, and MessageTypes.

Primary actions and corresponding API behavior

- **Marking**: All marking actions, such as ReviewedRelevant, ReviewedIrrelevant, Questioned, Pending, are counted against the reviewer who performed the action. However, if a reviewer performs multiple markings on the same item, only the last marking action is considered. For example, if an item is first marked as Questioned and later changed to Pending, only the Pending action is counted. Each item retains only one marking at a time, based on the most recent action.
- **Escalation**: When a reviewer escalates an item, the escalation count is attributed solely to that reviewer. However, an item can be escalated multiple times, but for reporting purposes, only the first escalation is considered. The escalation count is attributed solely to the initial reviewer who triggered it. Subsequent re-escalations by other reviewers are not included in the report.
- **Appraise** and **Label**: For Appraise and Label actions, the count is attributed to the first reviewer who took any action on the item (marking, escalating, appraising, labeling), not the reviewer who performed the appraise or label action. This differs from Mark and Escalate, where the count goes to the reviewer who actually performed the action. Even if Reviewer X appraises or labels an item, the count will reflect under the original reviewer who first interacted with the item.

Scenario 1: A new request to submit the report

Sample request:

```
POST https://<Reporting endpoint base URL>/OData/ReviewerAssessmentMetricsAsync
{
"ReportName":"Test",
"StartDate":"2025-01-01",
"EndDate":"2025-12-31",
"Departments":[237,17604],
"Reviewers":[4095],
"MessageTypes":[1]
}
```

Sample response:


```
{
    "@odata.context": "https://api.advancedsupervision.qa.veritas.com/odata/$metadata#ReviewerAssessmentMetricsAsync/$entity",
    "reportId": "b429f566-f44d-4b68-a637-a8e9490a511b",
    "reportName": "test",
    "reportType": "Reviewer Assessment",
    "reportDate": "2025-07-15T19:28:44.613-07:00",
    "reportStatus": "Queued",
    "info": "Successfully queued the report request.",
    "newReportInstanceQueued": true,
    "reportStatusLocation": "https://api.advancedsupervision.qa.veritas.com/odata/ReportStatus?
        ReportId=b429f566-f44d-4b68-a637-a8e9490a511b",
    "reportDataLocation": "https://api.advancedsupervision.qa.veritas.com/odata/ReviewerAssessmentMetrics?
        ReportId=b429f566-f44d-4b68-a637-a8e9490a511b"
}
```

Refer to the table below for details on the attributes included in the ReviewerAssessmentMetricsAsync API response.

Name	Description
reportId	Displays report ID. It is generated upon successful execution of API.
reportName	Displays report name. It is generated upon successful execution of API.
reportType	Displays the report type as *Item Details*.
reportDate	Displays the date of report generation after successful execution of API.
reportStatus	Displays report status. For more information on statuses, See "Report Status API" on page 409.
info	Displays a message if the report request has queued successfully or not.
newReportInstanceQueued	Specifies whether a new report generation request has been submitted or not. The *Rate Limiting* feature restricts submission of multiple requests with identical input parameters if attempted within one minute. It returns the following values: ***True***: The value is shown as *True*, if the new report request has been queued successfully. ***False***: The value is shown as *False*, if the input parameters of the current request are identical to the parameters of the already submitted request *within one minute*, a new report will not be queued. As a result, the details of the existing report request are returned.
reportStatusLocation	Displays a URL with report ID. To view the status of this report, use the same URL.
reportDataLocation	Displays a URL for the location of report data. To access the report data, use the same URL.

Scenario 2: A new request to submit the report when optional parameters are omitted

Sample request:

```
POST https://<Reporting endpoint base URL>/OData/ReviewerAssessmentMetricsAsync
{
"ReportName":"Test",
"StartDate":"2025-01-01",
"EndDate":"2025-12-31"
}
```

Sample response:


```
{
    "@odata.context": "https://api.advancedsupervision.qa.veritas.com/odata/$metadata#ReviewerAssessmentMetricsAsync/$entity",
    "reportId": "a62124ec-f711-43a5-a64c-2f269c231a4d",
    "reportName": "test",
    "reportType": "Reviewer Assessment",
    "reportDate": "2025-07-15T19:44:25.717-07:00",
    "reportStatus": "Queued",
    "info": "Successfully queued the report request.",
    "newReportInstanceQueued": true,
    "reportStatusLocation": "https://api.advancedsupervision.qa.veritas.com/odata/ReportStatus?
        ReportId=a62124ec-f711-43a5-a64c-2f269c231a4d",
    "reportDataLocation": "https://api.advancedsupervision.qa.veritas.com/odata/ReviewerAssessmentMetrics?
        ReportId=a62124ec-f711-43a5-a64c-2f269c231a4d"
}
```


Scenario 3: A new request to submit the report when ReportName parameter is ignored

Sample request:

```
POST https://<Reporting endpoint base URL>/OData/ReviewerAssessmentMetricsAsync
{
"StartDate":"2025-01-01",
"EndDate":"2025-12-31",
"Departments":[237,17604],
"Reviewers":[4095],
"MessageTypes":[1]
}
```

Sample response:


```
{
    "error": {
        "code": "BadParameter",
        "message": "Parameter(s): ReportName either need to be specified or have an incorrect name, value or format.For details regarding
            API parameters, refer to the documentation."
    }
}
```


Scenario 4: A new request to submit the report when one of the dates parameter is ignored

Sample request:

```
POST https://<Reporting endpoint base URL>/OData/ReviewerAssessmentMetricsAsync
{
"ReportName":"Test",
"EndDate":"2025-12-31",
"Departments":[237,17604],
"Reviewers":[4095],
"MessageTypes":[1]
}
```

Sample response:

```
{
    "error": {
        "code": "Dates are invalid. Reasons: 1)StartDate and EndDate are mandatory, 2)StartDate and EndDate must be within one year.",
        "message": "InvalidDateRange"
    }
}
```

2. Call the *ReportStatus* API to get the status of the *Reviewer Assessment Metrics Async* API report. See "Report Status API" on page 409.
3. Once the report is ready, call the *Reviewer Assessment Metrics* API to retrieve the report data from the asynchronous API. See "Reviewer Assessment Metrics API" on page 407.

Reviewer Assessment Metrics API

Reviewer Assessment Metrics- List by filter	This report displays metrics for actions performed by reviewers within the Insight Surveillance application. These actions include marking, labeling, escalating, and appraising items. The report is intended to assess reviewer performance based on the accuracy of their reviews.

Reviewer Assessment Metrics- List by filter

`GET https://<Reporting endpoint base URL>/odata/ReviewerAssessmentMetrics`

Sample request

- `GET https://<Reporting endpoint Base URL>/odata/ReviewerAssessmentMetrics?reportid=<ID of the ReviewerAssessmentMetricsAsync API report>`

ReviewerAssessmentMetricsAPI - URL Parameter/Filters

The following filters can be used with the ReviewerAssessmentMetrics API when invoked using the GET method only. The system uses the AND operator between the filters to return the result based on the specified filters.

ReportID	Mandatory	Specify the ID of ReviewerAssessmentMetrics API report you want to view.

Scenario 1

```
GET https://<Reporting endpoint Base
URL>/odata/ReviewerAssessmentMetrics?

ReportId=752cd9c0-c93f-4be3-b4fd-04d1b2747b0e
```

Sample response:

Status code: 200 OK


```
{
    "@odata.context": "https://api.advancedsupervision.qa.veritas.com/odata/$metadata#ReviewerAssessmentMetrics",
    "@odata.count": 11,
    "value": [
        {
            "reviewerAssessmentMetricsID": 1296,
            "departmentID": 6073,
            "departmentName": "Teams-UJ1 ",
            "reviewerID": 3821,
            "reviewer": "admin@teamsqa.com",
            "messageType": 1,
            "messageTypeName": "Exchange",
            "captured": 1,
            "unReviewed": 0,
            "unreviewedIrrelevant": 0,
            "unreviewedRelevant": 0,
            "pending": 0,
            "questioned": 0,
            "reviewedIrrelevant": 0,
            "reviewedRelevant": 0,
            "escalated": 0,
            "appraised": 0,
            "reportDateRange": "Apr 23 2025 12:00PM-May 31 2025 12:00PM",
            "labelledItemMetrics": [
                {
                    "labelID": 2570,
                    "labelName": "Pass",
                    "labelled": 1
                },
                {
                    "labelID": 3224,
                    "labelName": "Needs change",
                    "labelled": 1
                }
            ]
```


Supported OData Filters

See “Supported OData query options” on page 410.

Responses

See “Responses” on page 415.

Report Status API

ReportStatus	■ Returns the status of all reports, when a specific *ReportId* is not mentioned in a query. ■ Returns the status of a specific report when a *ReportId* is mentioned in a query.

ReportStatus API - List by filter

```
GET https://<Reporting endpoint Base URL>/odata/ReportStatus
```

Sample Request

- **To view status of all the Async reports, execute the following query:**

  ```
  GET https://<Reporting endpoint Base URL>/odata/ReportStatus
  ```

  Besides the ReportStatus parameter, this API supports all the OData query options (See "Supported OData query options" on page 410.). See an example below.

  ```
  GET https://<Reporting endpoint Base
  URL>/odata/ReportStatus?$Count=true&$Skip=100&$Top=200
  ```

- **To view status of a specific Async report, execute the following query:**

  ```
  GET https://<Reporting endpoint Base
  URL>/odata/ReportStatus?ReportId=a337e782-aa81-40fd-a65c-589b1bb6da55
  ```

Sample response

Status code: 200 OK

For single report ID


```
{
    "@odata.context": https://<Reporting endpoint Base
    URL>/odata/ReportStatus?ReportId=a337e782-aa81-40fd-a65c-589b1bb6da55

    "value": [
        {
            "reportId": "a337e782-aa81-40fd-a65c-589b1bb6da55",
            "reportName": "a0 9AdD",
            "reportType": "Evidence Of Review",
            "reportDate": "2024-07-05T14:07:20.503+05:30",
            "reportStatus": "Queued",
            "info": "Successfully queued the report request."
        }
    ]
}
```


For multiple report IDs

```
{
    "@odata.context": "https://<Reporting endpoint Base
    URL>/odata/$metadata#ReportStatus",
    "@odata.count": 33,
    "value": [
        {
            "reportId": "137c0384-ccf7-4099-8efe-0e143a3f4c50",
            "reportName": "ReportStatus_1",
            "reportType": "Evidence Of Review",
            "reportDate": "2024-07-01T12:37:07.06+05:30",
            "reportStatus": "Processing",
            "info": "Report generation is in progress."
        },
        {
            "reportId": "5c95349f-225f-4a32-8370-1845e1fe5567",
            "reportName": "ReportRequest_2",
            "reportType": "Evidence Of Review",
            "reportDate": "2024-07-01T13:58:23.153+05:30",
            "reportStatus": "Ready",
            "The report is ready."
        }
    ]
}
```


Report statuses and description

Status	Description
Queued	The report is currently queued for generation.
Processing	The report generation is currently in progress.
Ready	The report is generated and available for review and utilization.
RetryQueued	The report generation failed and has been queued for retry.
Failed	The report generation has failed even after retrying.

Supported OData query options

The currently supported OData query options that can be used for query composition to customize responses are mentioned below.

- **$select**
  : Use the $select query parameter to return a set of properties that are different than the default set for an individual resource or a collection of resources. With $select, you can specify a subset of the default properties.

Example: In the example below, the query returns only two properties, Department name and Department status in the result.

```
https://<Reporting endpoint base
URL>/odata/departments?$select=DepartmentName,Status
```

- **$count**

  Use the $count query parameter to retrieve the total count of matching resources.

  In the example below, the query returns a total count of roles in the system irrespective of any other filters.

  ```
  https://<Reporting endpoint Base URL>/odata/roles?$count=true
  ```

- **$top**

  Use the $top query parameter to limits the number of records returned.

  In the example below, the query returns the top 10 records in the result.

  ```
  https://<Reporting endpoint Base URL>/odata/departments?$top=10
  ```

- **$skip**

  Use the $skip query parameter to skips a specified number of records before returning results.

  In the example below, the query returns the records skipping the first 60 records in the result.

  ```
  https://<Reporting endpoint Base URL>/odata/departments?$skip=60
  ```

- **$skipToken**

  Use the $skipToken query parameter to retrieve the next page of results from result sets that span multiple pages.

  Some requests return multiple pages of data due to server-side paging to limit the page size of the response. Reporting APIs use the $skipToken query parameter to reference subsequent pages of the result. The $skipToken parameter contains an opaque token that references the next page of results and is returned in the URL provided in the `@odata.nextLink` property in the response.

  For example, if you call the Roles API that have more than 1000 records in the result, then the response will return only 1000 records with `@odata.nextLink` property as shown below.

  ```
  "@odata.nextLink": "https://<Reporting endpoint Base
  URL>/odata/roles?$skipToken=29310"
  ```

  To fetch the next page of records, the value of the `@odata.nextLink` can be used as the endpoint URL which has a `skipToken` value.

Supported reporting endpoint API filters and their values

This section provides information about the reporting endpoint API filters and their possible values. Refer to the following tables if you are using the reporting APIs.

CaptureTypes filter

Table 25-1 CaptureTypes filters and respective IDs

CaptureTypes ID	Value	Description
0	NotSpecified	Items with a capture types under the *Collaboration* and *Transcript* categories.
1	Search	Indicates that item was captured based on immediate or scheduled search
2	Clean	Indicates that items were randomly sampled
3	Alert	
4	Adhoc	
6	GuaranteedSearch	If guaranteed sampling was configured for the department, indicates that the item was sampled and captured based on guaranteed sample search.
10	SearchDuplicate	Indicates that the item was sampled and considered as a duplicate during guaranteed sample search results deduplication
99	Policy	Indicates that the item was captured based on classification inclusion rules.

MessageDirections filter

Table 25-2 MessageDirections filters and respective IDs

MessageDirections ID	Value	Description
0	NotSpecified	Items with a message directions under the *Collaboration* and *Transcript* categories..
1	Internal	The items where the author and all recipients are internal to the organization.

Table 25-2 MessageDirections filters and respective IDs *(continued)*

MessageDirections ID	Value	Description
2	ExternalInbound	The items where the author is external to the organization and at least one recipient is internal.
3	ExternalOutbound	The items where the author is internal to the organization and at least one recipient is external.

MessageTypes filters (Email-specific)

Table 25-3 Email-specific MessageTypes filters and respective IDs

MessageType ID	Filter Name	MessageTypes ID	Filter Name
1	Exchange	129	ImportedEmails
2	Instant Messaging	130	MS Teams (EML)
4	Fax	131	Slack (EML)
7	SMTP	132	Citrix Workspace and ShareFile (EML)
9	Social	133	Sharepoint (EML)
16	Rackspace Mail	134	IceChat (EML)
18	GroupWise	135	Twitter (EML)
19	SFChatter	136	Youtube (EML)
20	Office 365 - PA Collection	137	ZoomChat (EML)
21	DoNotUse	138	Box (EML)
22	Zimbra	139	GoogleDrive (EML)
23	Exchange Hosted Archive Ingestion	140	Dropbox (EML)
25	Lync OnPrem	141	AmazonsS3 (EML)

Table 25-3 Email-specific MessageTypes filters and respective IDs *(continued)*

MessageType ID	Filter Name	MessageTypes ID	Filter Name
27	Google Journal	142	JSON (EML)
101	EML	143	CiscoWebex (EML)
114	CellTrust	181	Carbon
115	LSEG	182	ENMACC Energy
116	Symphony	183	Legato Chat
117	Workplace from Facebook	184	LiquidNet
118	Salesforce Chatter	185	Markets Manager
119	FXConnect	186	Saphyre
120	XIP	187	Skytel-Pager
121	Yieldbroker	188	Social
122	Webpage Capture	189	Web CHAT
123	Redtail Speak	190	WeChat
124	ServiceNow	191	FXT
125	RingCentral		

MessageTypes filters (Collaboration-specific)

Table 25-4 Collaboration-specific MessageTypes filters and respective IDs

MessageTypes ID	Filter Name	MessageType ID	Filter Name
11	Teams Chat	37	Zoom Chat
12	Teams Channel	38	Zoom Meetings Chats
32	Slack	39	SMS Collaboration
34	IceChat	40	WhatsApp Collaboration
35	Twitter	41	IMessage Collaboration

Table 25-4 Collaboration-specific MessageTypes filters and respective IDs *(continued)*

MessageTypes ID	Filter Name	MessageType ID	Filter Name
36	Chatter Cipher Cloud	42	Viva Engage

Transcript-specific (Transcript-specific)

Table 25-5 Transcript-specific MessageTypes filters and respective IDs

MessageType ID	Filter Name	MessageType ID	Filter Name
150	Zoom	157	Vodafone
151	Cisco Webex Teams	158	IPC
152	YouTube	159	Cisco
153	Audio File	160	Avaya
154	Video File	161	Dubber Media
155	Microsoft Teams Meeting	162	Mobile Phone
156	Audio Video		

Responses

The application provides following responses:

Name	Description
200 OK	The request is successful.
401 Unauthorized	Access is denied due to invalid credentials.
Other Status Codes	Error response describing reason for the failed operation.

Managing Power BI templates for reporting APIs

Insight Surveillance provides predefined Power BI templates that consume Reporting API endpoints to view interactive reports. Power BI templates are

pre-defined, reusable report designs or blueprints created within Power BI for analytics purposes. These templates serve as starting points for creating consistent and visually appealing reports and dashboards.

All control elements within the Power BI report are interactive, allowing for clicking to filter, highlight, and drill-down into the report. When any element of the report is clicked, all other graphs, tiles, and more, dynamically update to display data relevant to the clicked element. The clickable elements encompass a variety of components, including (but not limited to):

- Filters (for example, Departments lists)
- Check boxes
- Tiles
- Data bars/columns on charts
- Data labels on charts
- Axis labels on charts

Prerequisite

Before you begin working with the Power BI Templates in Insight Surveillance, ensure that you have the Microsoft Power BI desktop application installed on your computer.

Accessing Insight Surveillance reports and datasets through the OData web service

Accessing reports

You can expose information from the Insight Surveillance configuration and customer databases through the Open Data (OData) web service. You can use this information with any OData-compatible reporting tool to create reports as required. Examples of such reporting tools include Excel/PowerQuery and Microsoft SQL Server Reporting Services (SSRS).

For extensive information on this facility, see the white paper Best Practices for Enhanced Accelerator Reporting.

Accessing datasets

You can access the datasets by typing the following addresses in the address bar of your web browser. In each case, *server_name* is the name of the server on which you have installed the Insight Surveillance server software.

- To access a list of all the available datasets, type
  `http://server_name/CAReporting/OData`

- To access a list of all the available datasets together with all the fields included in each dataset, type `http://server_name/CAReporting/OData/$metadata`
- To access a particular dataset, type `http://server_name/CAReporting/OData/dataset_name`

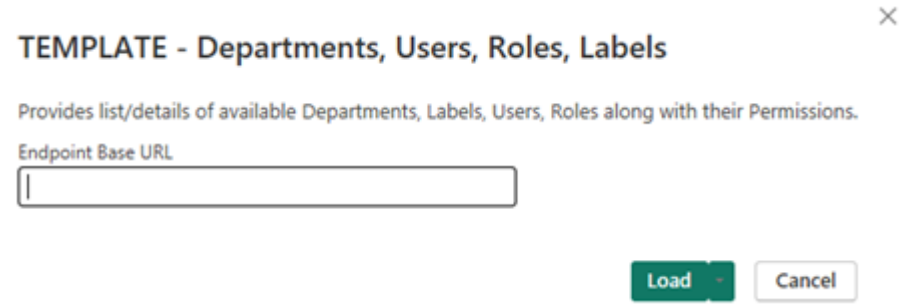
Guidelines for using Insight Surveillance templates with Microsoft Power BI Desktop

Here are the guidelines you must follow when using Reporting API Templates in Microsoft Power BI:

- Ensure that the correct credentials are used for Power BI template.
  When loading Reporting API templates in Microsoft Power BI Desktop, select **Basic Authentication** when prompted, and enter the Username as **ReportingApiUser** and the Password as either a **primary or secondary API Key** that are generated after configuring the reporting endpoint
- Ensure that the Power BI Desktop privacy levels are appropriate.
  Some Insight Surveillance Power BI templates combine data from multiple Reporting API endpoints and visualize the data. To achieve this, multiple PowerQueries are created within the template and the resulting data from one reporting API endpoint is shared with reporting API endpoint.
  In Microsoft Power BI Desktop application, the **Privacy Level** feature employs policies for sharing data of API across other API. For more details, refer to Power BI Desktop privacy levels.
  Since the Reporting APIs of Insight Surveillance operate externally (outside the organization calling it), you must specify the Privacy Level as **Public** for each Data Source. Occasionally, you may need to globally ignore the Privacy Levels so that the Reporting API Templates function properly.
- Ensure that the cached credentials are correct.
  Microsoft Power BI Desktop caches credentials entered when connecting to the Reporting API. Upon reloading the Power BI template, it does not prompt for credentials again. If credentials change, such as due to an expired Access Key, you must clear the cached credentials.
  To clear them, navigate to **File** > **Options and settings** > **Data source settings**, and clear the credentials for all data sources. This is one of the troubleshooting steps if the template cannot connect.

TEMPLATE - Departments, Users, Roles, Labels

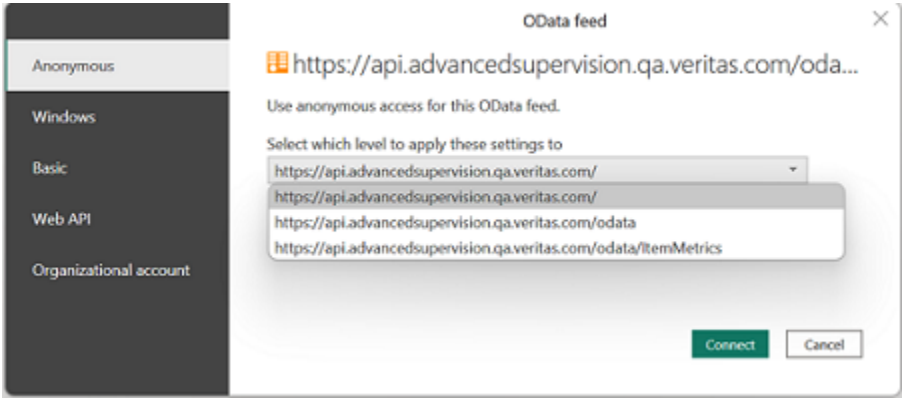
1 Open the *TEMPLATE - Departments, Users, Roles, Labels.pbit* file, and specify the following details.



Endpoint Base URL	Enter the REST API endpoint URL. For example, `https://<Reporting endpoint Base URL>`

2 Click **Load**.

3 Select the required OData Feed.



4 Click **Connect** and choose *Basic Authentication* mechanism to access Reporting API.

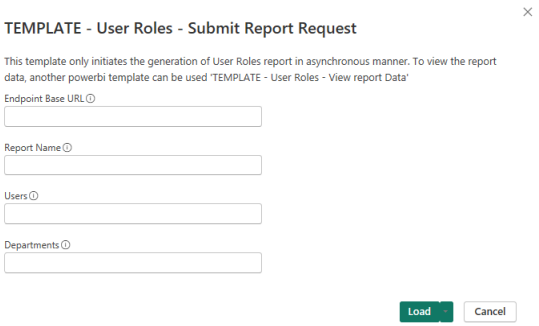
The application prompts you several times to provide appropriate credentials when querying Reporting API for each report.

5 Wait while Microsoft Power BI Desktop uses the provided filter values to generate queries and fetch OData reports from the specified Insight Surveillance Server. This process may take some time depending on the amount of data being retrieved from the server.

Upon successful processing, the application displays a report for the retrieved data of the corresponding API endpoint. To help you better visualize and understand the API Endpoint reports, refer to sample images of reports.

TEMPLATE - User Roles - Submit Report Request

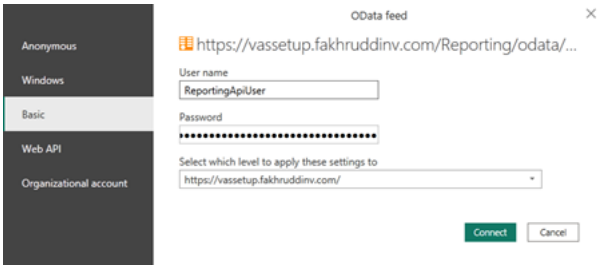
1 Open the *TEMPLATE- User Roles - Submit Report Request.pbit* file, and specify the following details.



Endpoint Base URL	Enter the REST API endpoint URL. For example, `https://<Reporting endpoint Base URL>`
Report Name	Specify a unique name for the report.
Users	Specify IDs of the users. **Limitations** This API can pass a maximum of 100 User IDs as input. **Data Type**: JSON array of integers 'id'(identifier fields) that is Users.
Departments	Specify IDs of the departments. **Limitations** This API can pass a maximum of 100 Departments IDs as input. **Data Type** JSON array of integers 'id'(identifier fields) that is Departments.

2 Click **Load**.

3 Select the required OData Feed.

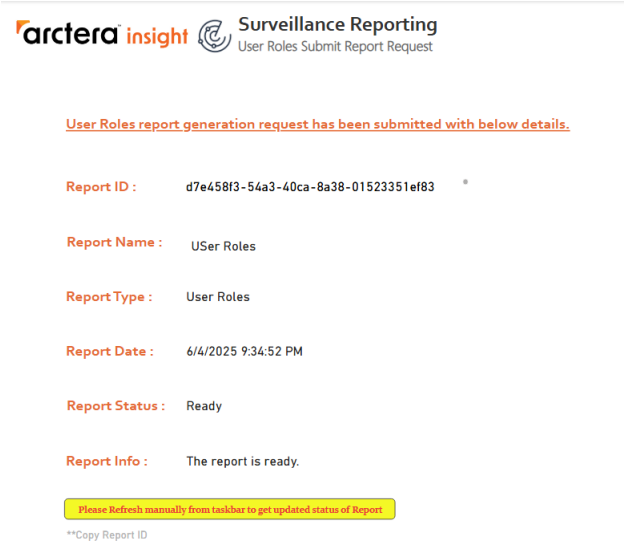


The application submits the report generation request and shows the details.

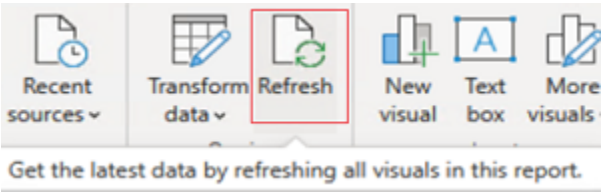
4 Click **Connect** and choose *Basic Authentication* mechanism to access Reporting API.

The application prompts you several times to provide appropriate credentials when querying Reporting API for each report.

5 Manually refresh the page to view the details such as Report ID, Report Name, Report Type, Report Date, Report Status, and Report Information.



If still the entire details are not displayed, click **Refresh** again as shown in the sample image below.



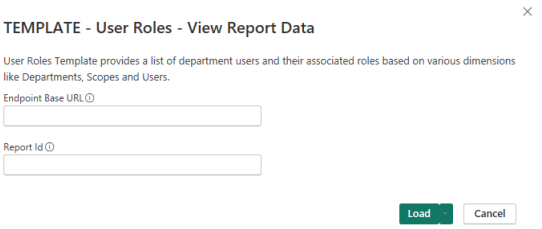
6 When all the details are available and *Report Status: Ready* is displayed, copy the report ID.

Use this Report ID in the *TEMPLATE- User Roles - View Report Data* template to view the report. Click **Refresh** to view the updated status of report generation.

Upon successful processing, the application displays a report for the retrieved data of the corresponding API endpoint. To help you better visualize and understand the API Endpoint reports, refer to sample images of reports.

TEMPLATE - User Roles - View Report Data

1 Open the *TEMPLATE- User Roles - View report Data.pbit* file, and specify the following details.

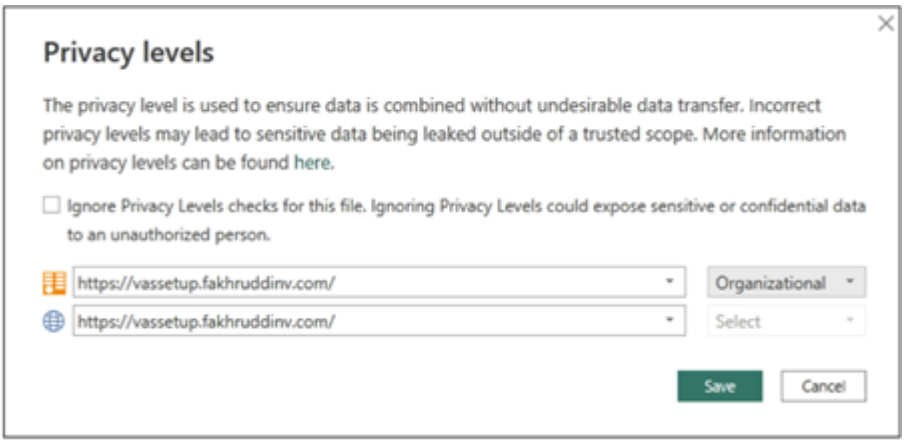


Endpoint Base URL	Enter the REST API endpoint URL. For example, `https://<Reporting endpoint Base URL>`
Report ID	Enter the *Report ID* that is generated during execution of *UserRolesAsync* API report or the *TEMPLATE- User Roles - Submit Report Request* template.

2 Click **Load**.

3 Set the privacy organizational or public for each selected data source.

For more information, See "Guidelines for using Insight Surveillance templates with Microsoft Power BI Desktop" on page 417.



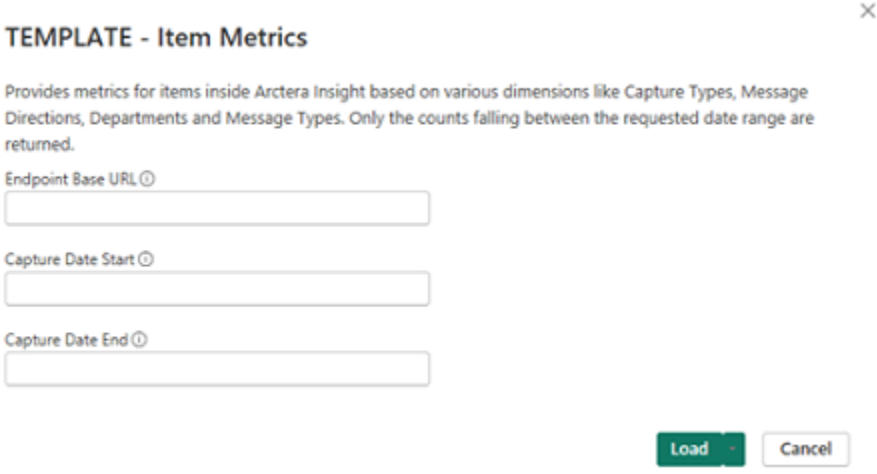
4 Click **Save**.

Upon successful processing, the application displays a report for the retrieved data of the corresponding API endpoint.

To help you better visualize and understand the API Endpoint reports, refer to sample images of reports.

TEMPLATE - Item Metrics

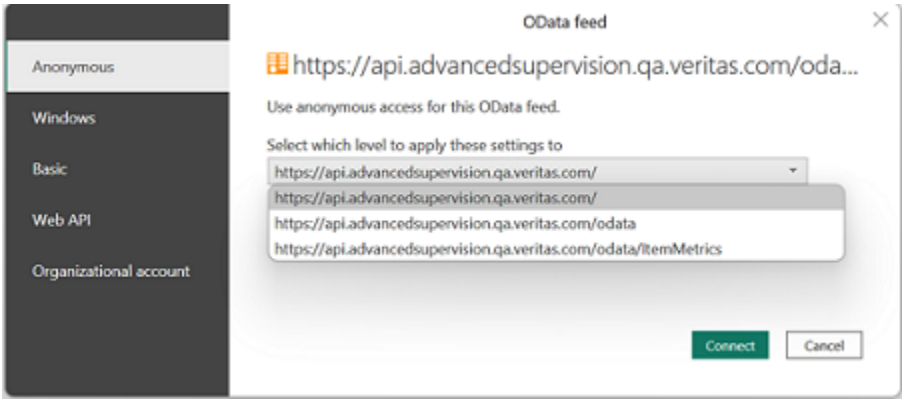
1 Open the *TEMPLATE - Item Metrics.pbit* file, and specify the following details.



Endpoint Base URL	Enter the REST API endpoint URL. For example, `https://<Reporting endpoint Base URL>`
CaptureDateStart	CaptureDateStart is the date on which items are captured or ingested in Insight Surveillance is recorded as the CaptureDateStart for that item. This filter specifies the start date for returning count of items whose CaptureDateStart is greater than or equal to this start date. **Data Type**: Date in the *YYYY-MM-DD* format that is CaptureDateStart.
CaptureDateEnd	This filter specifies the end date for returning count of items whose CaptureDateEnd is greater than or equal to this date. **Data Type**: Date in the *YYYY-MM-DD* format that is CaptureDateEnd.

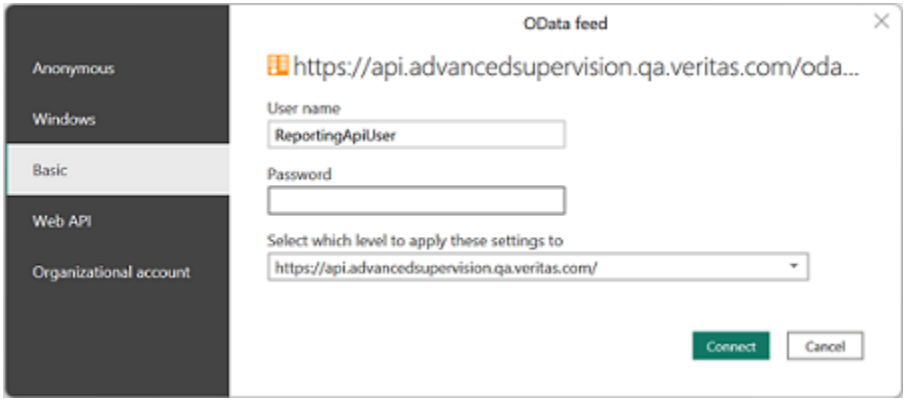
2 Click **Load**.

3 Select the required OData Feed.



4 Click **Connect** and choose *Basic Authentication* mechanism to access Reporting API.

The application prompts you several times to provide appropriate credentials when querying Reporting API for each report.

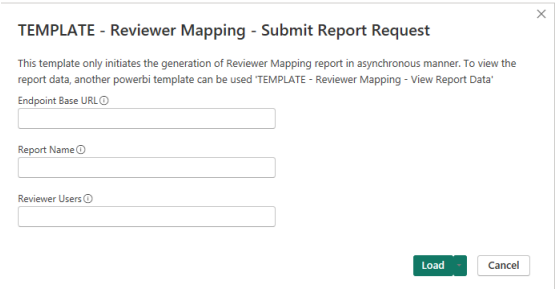


5 Wait while Microsoft Power BI Desktop uses the provided filter values to generate queries and fetch OData reports from the specified Insight Surveillance Server. This process may take some time depending on the amount of data being retrieved from the server.

Upon successful processing, the application displays a report for the retrieved data of the corresponding API endpoint. To help you better visualize and understand the API Endpoint reports, refer to sample images of reports.

TEMPLATE - Reviewer Mapping - Submit Report Request

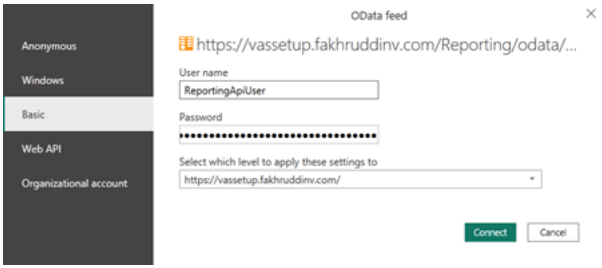
1 Open the *TEMPLATE- Reviewer Mapping - Submit Report Request.pbit* file, and specify the following details.



Endpoint Base URL	Enter the REST API endpoint URL. For example, `https://<Reporting endpoint Base URL>`
Report Name	Specify a unique name for the report.
Reviewer Users	Specify a list of reviewer User IDs to retrieve their details. Refer to the **userid** field of the Users API for the value of reviewer users. **Data Type**: JSON array of integers 'id'(identifier fields) that is ReviewerUsers.

2 Click **Load**.

3 Select the required OData Feed.

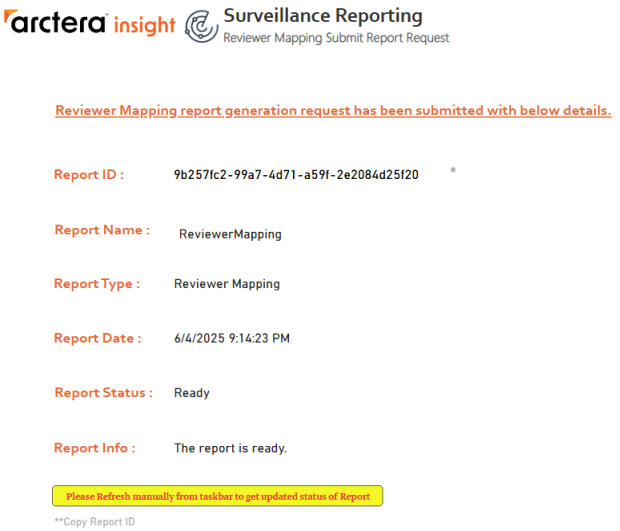


The application submits the report generation request and shows the details.

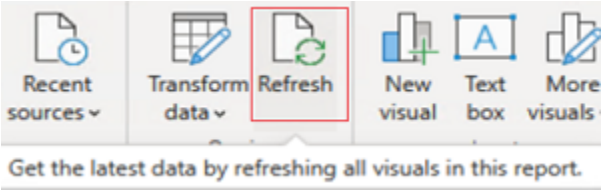
4 Click **Connect** and choose *Basic Authentication* mechanism to access Reporting API.

The application prompts you several times to provide appropriate credentials when querying Reporting API for each report.

5 Manually refresh the page to view the details such as Report ID, Report Name, Report Type, Report Date, Report Status, and Report Information.



If still the entire details are not displayed, click **Refresh** again as shown in the sample image below.



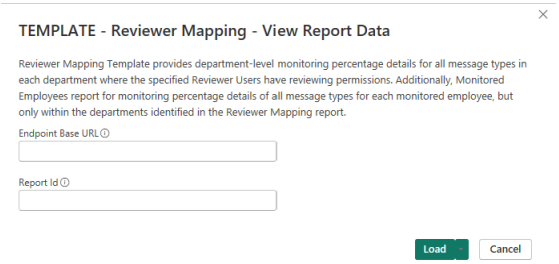
6 When all the details are available and *Report Status: Ready* is displayed, copy the report ID.

Use this Report ID in the *TEMPLATE- Reviewer Mapping - View Report Data* template to view the report. Click **Refresh** to view the updated status of report generation.

Upon successful processing, the application displays a report for the retrieved data of the corresponding API endpoint. To help you better visualize and understand the API Endpoint reports, refer to sample images of reports.

TEMPLATE - Reviewer Mapping - View Report Data

1 Open the *TEMPLATE- Reviewer Mapping - View report Data.pbit* file, and specify the following details.

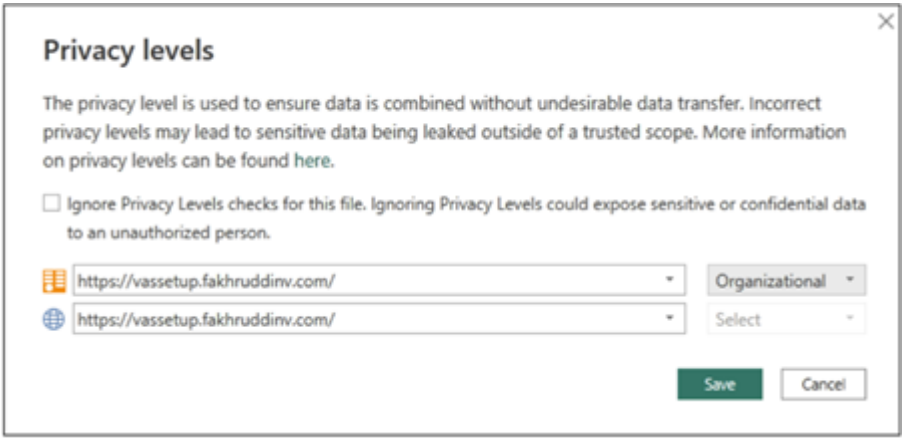


Endpoint Base URL	Enter the REST API endpoint URL. For example, `https://<Reporting endpoint Base URL>`
Report ID	Enter the *Report ID* that is generated during execution of *ReviewerMappingAsync* API report or the *TEMPLATE- Reviewer Mapping - Submit Report Request* template.

2 Click **Load**.

3 Set the privacy organizational or public for each selected data source.

For more information, See "Guidelines for using Insight Surveillance templates with Microsoft Power BI Desktop" on page 417.



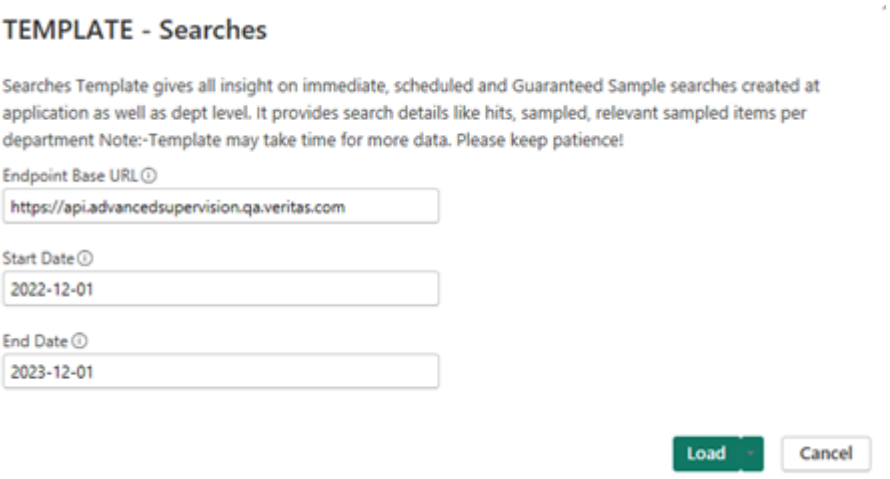
4 Click **Save**.

Upon successful processing, the application displays a report for the retrieved data of the corresponding API endpoint.

To help you better visualize and understand the API Endpoint reports, refer to sample images of reports.

TEMPLATE - Searches

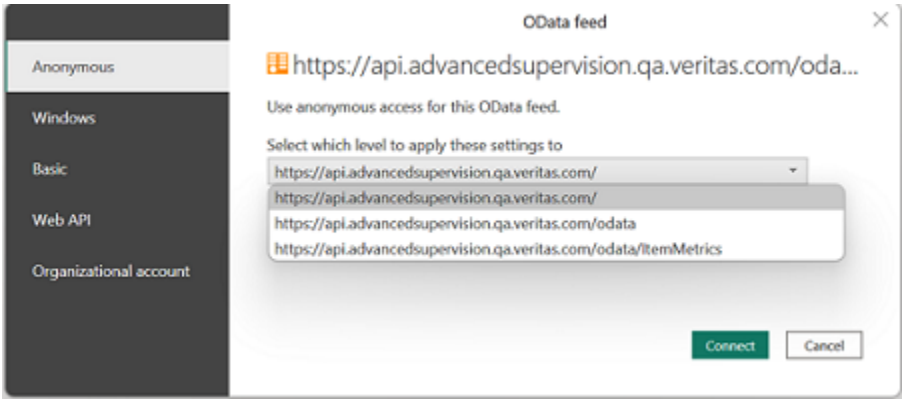
1 Open the *TEMPLATE - Searches.pbit* file, and specify the following details.



Endpoint Base URL	Enter the REST API endpoint URL. For example, `https://<Reporting endpoint Base URL>`
Start Date	This filter specifies the start date for returning count of searches whose creation date is greater than or equal to this start date. **Data Type**: Date in the *YYYY-MM-DD* format that is StartDate.
End Date	This filter specifies the end date for returning count of searches whose creation date is less than or equal to this date. **Data Type**: Date in the *YYYY-MM-DD* format that is EndDate.

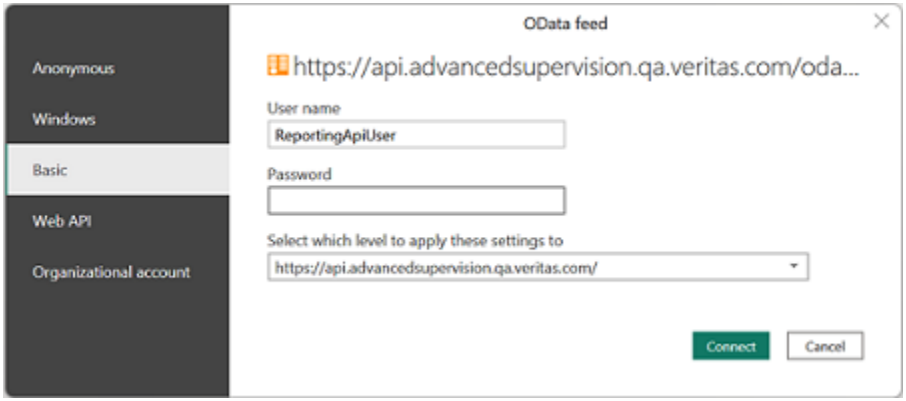
2 Click **Load**.

3 Select the required OData Feed.



4 Click **Connect** and choose *Basic Authentication* mechanism to access Reporting API.

The application prompts you several times to provide appropriate credentials when querying Reporting API for each report.

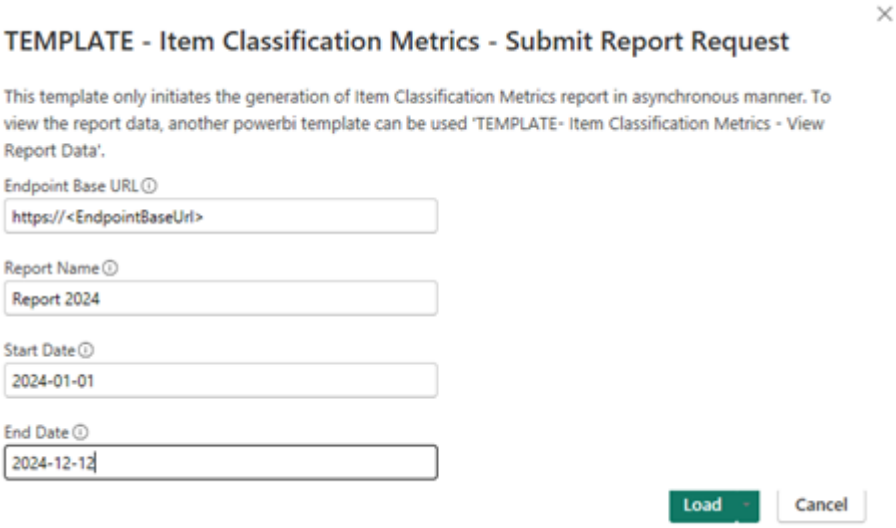


5 Wait while Microsoft Power BI Desktop uses the provided filter values to generate queries and fetch OData reports from the specified Insight Surveillance Server. This process may take some time depending on the amount of data being retrieved from the server.

Upon successful processing, the application displays a report for the retrieved data of the corresponding API endpoint. To help you better visualize and understand the API Endpoint reports, refer to sample images of reports.

TEMPLATE- Item Classification Metrics - Submit Report Request

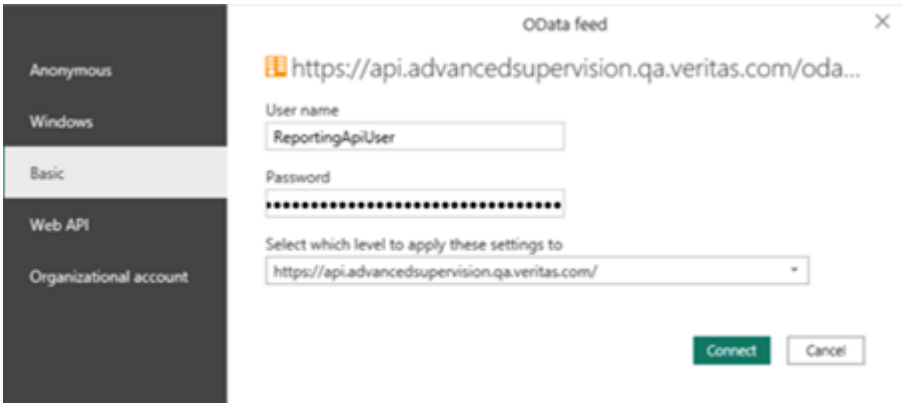
1 Open the *TEMPLATE- Item Classification Metrics - Submit Report Request.pbit* file, and specify the following details.



Endpoint Base URL	Enter the REST API endpoint URL. For example, `https://<Reporting endpoint Base URL>`
Report Name	Specify a unique name for the report.
Start Date	Specify the earliest date from which you want to gather data captured or ingested in Insight Surveillance for your report.
End Date	Specify the end date until which you want to gather data captured or ingested in Insight Surveillance for your report.

2 Click **Load**.

3 Select the required OData Feed.

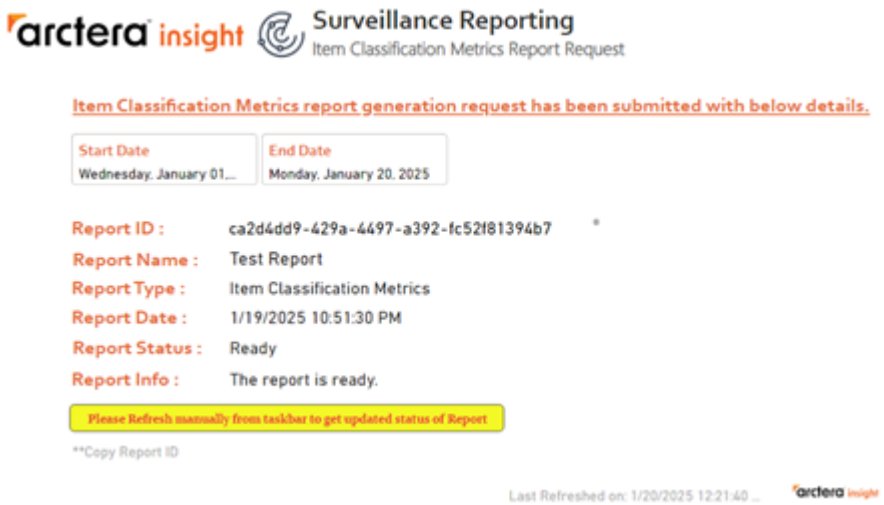


The application submits the report generation request and shows the details.

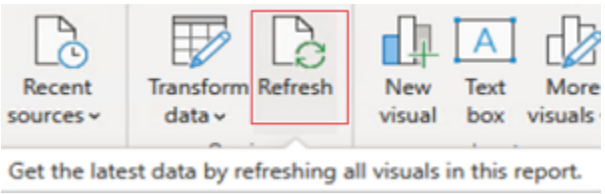
4 Click **Connect** and choose *Basic Authentication* mechanism to access Reporting API.

The application prompts you several times to provide appropriate credentials when querying Reporting API for each report.

5 Manually refresh the page to view the details such as Report ID, Report Name, Report Type, Report Date, Report Status, and Report Information.



If still the entire details are not displayed, Click **Refresh** again as shown in the sample image below.



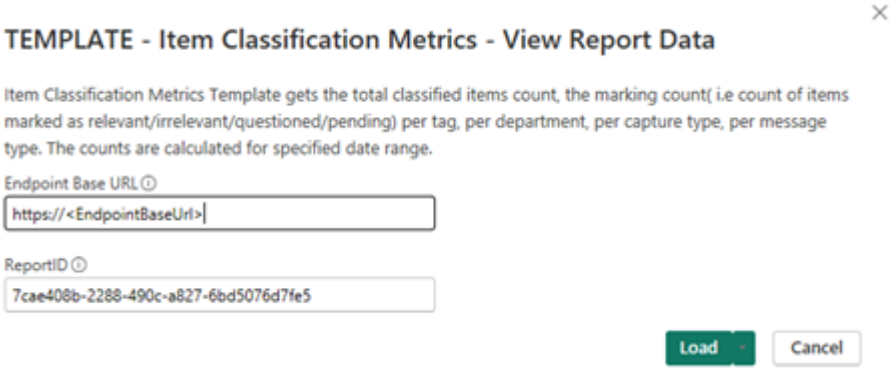
6 When all the details are available, copy the report ID.

Copy the Report ID to retrieve report data once the report is ready. Use this Report ID in the *TEMPLATE- Item Classification Metrics - View Report Data* template. Click **Refresh** to view the updated status of report generation.

Upon successful processing, the application displays a report for the retrieved data of the corresponding API endpoint. To help you better visualize and understand the API Endpoint reports, refer to sample images of reports.

TEMPLATE- Item Classification Metrics - View Report Data

1 Open the *TEMPLATE- Item Classification Metrics - View report Data.pbit* file, and specify the following details.

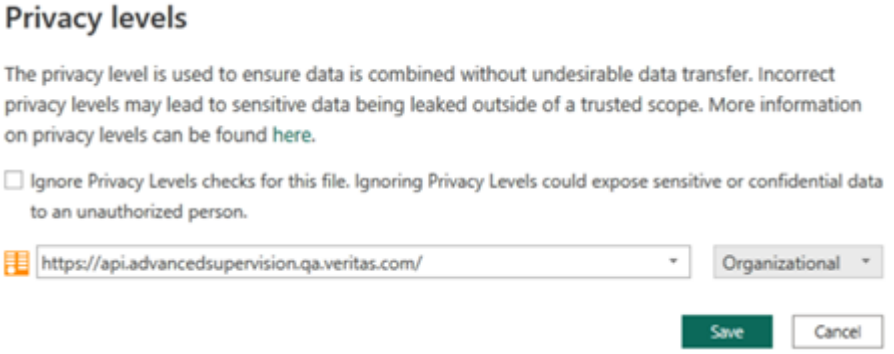


Endpoint Base URL	Enter the REST API endpoint URL. For example, `https://<Reporting endpoint Base URL>`
Report ID	Enter the *Report ID* that is generated during execution of *ItemClassificationMetricsAsync* API report or the *TEMPLATE- Item Classification Metrics - Submit Report Request* template.

2 Click **Load**.

3 Set the privacy organizational or public for each selected data source.

For more information, See "Guidelines for using Insight Surveillance templates with Microsoft Power BI Desktop" on page 417.

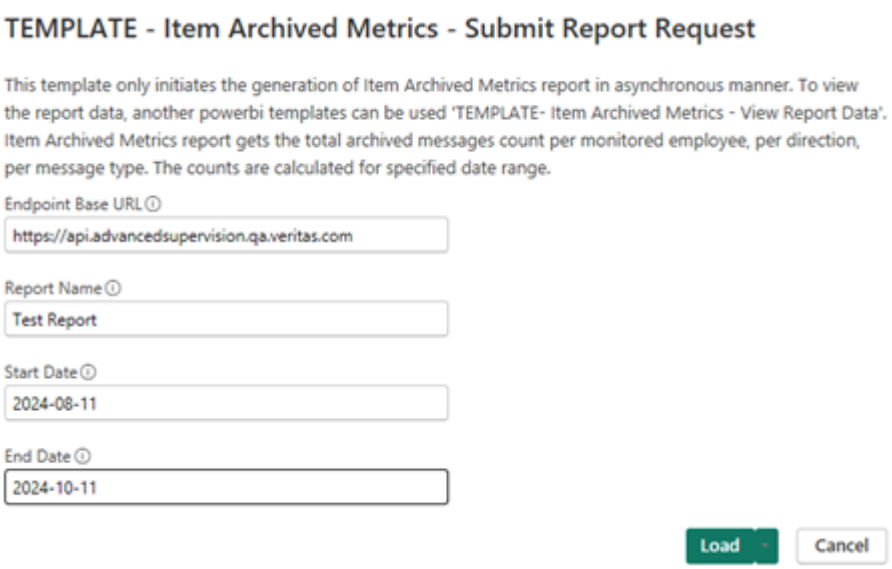


4 Click **Save**.

Upon successful processing, the application displays a report for the retrieved data of the corresponding API endpoint. To help you better visualize and understand the API Endpoint reports, refer to sample images of reports.

TEMPLATE- Item Archived Metrics - Submit Report Request

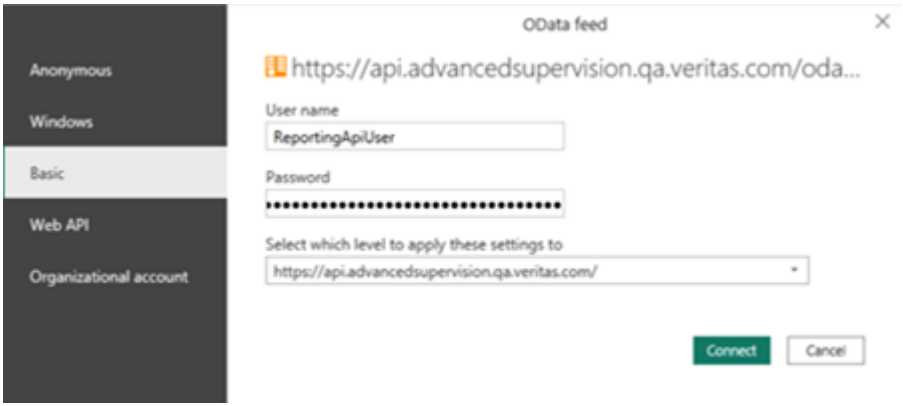
1 Open the *TEMPLATE- Item Archived Metrics - Submit Report Request.pbit* file, and specify the following details.



Endpoint Base URL	Enter the REST API endpoint URL. For example, `https://<Reporting endpoint Base URL>`
Report Name	Specify a unique name for the report.
Start Date	Specify the earliest date from which you want to gather data captured or ingested in Insight Surveillance for your report.
End Date	Specify the end date until which you want to gather data captured or ingested in Insight Surveillance for your report.

2 Click **Load**.

3 Select the required OData Feed.

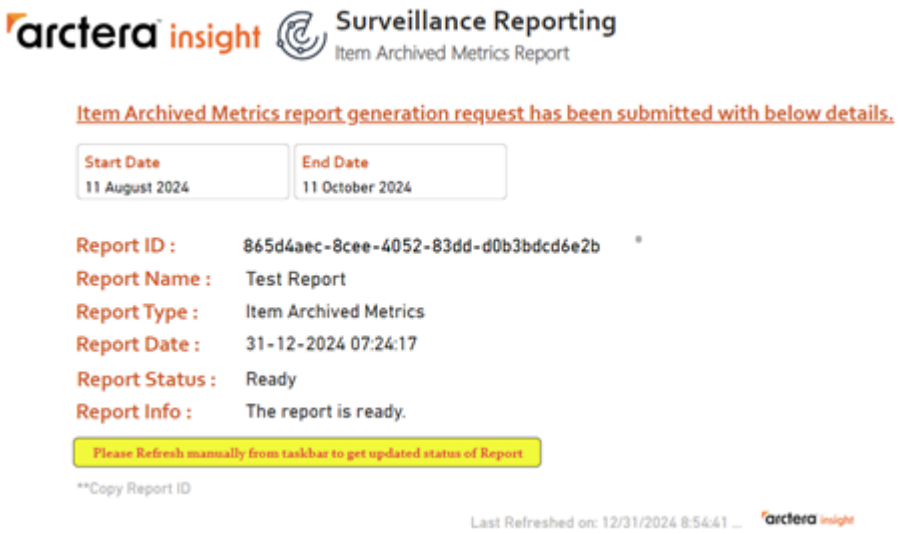


The application submits the report generation request and shows the details.

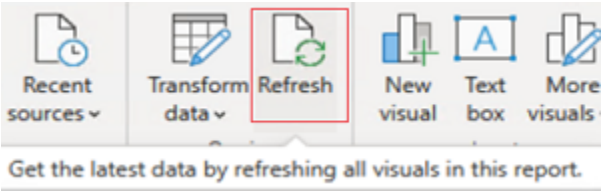
4 Click **Connect** and choose *Basic Authentication* mechanism to access Reporting API.

The application prompts you several times to provide appropriate credentials when querying Reporting API for each report

5 Manually refresh the page to view the details such as Report ID, Report Name, Report Type, Report Date, Report Status, and Report Information.



If still the entire details are not displayed, Click **Refresh** again as shown in the sample image below.



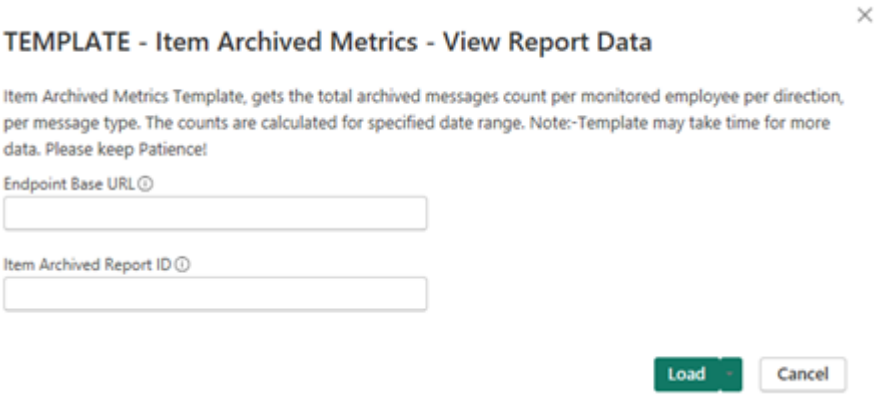
6 When all the details are available, copy the report ID.

Copy the Report ID to retrieve report data once the report is ready. Use this Report ID in the *TEMPLATE- Item Archived Metrics - View Report Data* template. Click **Refresh** to view the updated status of report generation.

Upon successful processing, the application displays a report for the retrieved data of the corresponding API endpoint. To help you better visualize and understand the API Endpoint reports, refer to sample images of reports.

TEMPLATE- Item Archived Metrics - View Report Data

1 Open the *TEMPLATE- Item Archived Metrics - View Report Data.pbit* file, and specify the following details.

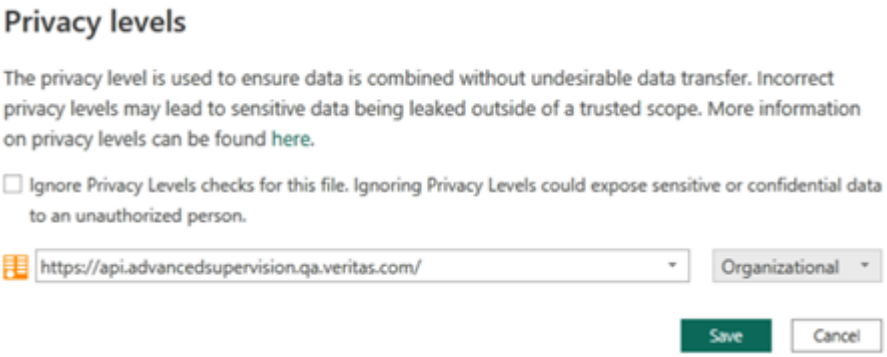


Endpoint Base URL	Enter the REST API endpoint URL. For example, `https://<Reporting endpoint Base URL>`
Report ID	Enter the *Report ID* that is generated during execution of *ItemArchivedMetricsAsync* API report or the *TEMPLATE- Item Archived Metrics - Submit Report Request* template.

2 Click **Load**.

3 Set the privacy organizational or public for each selected data source.

For more information, See "Guidelines for using Insight Surveillance templates with Microsoft Power BI Desktop" on page 417.

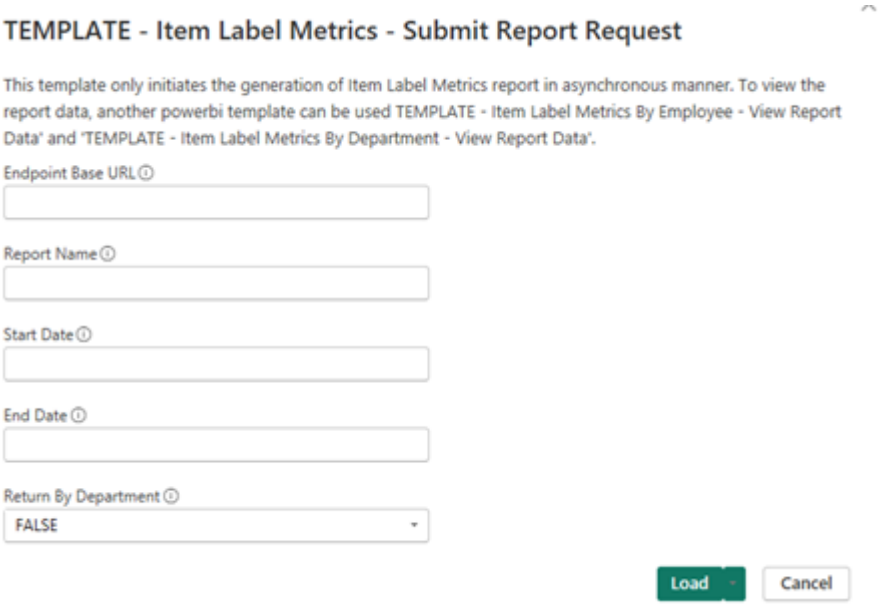


4 Click **Save**.

Upon successful processing, the application displays a report for the retrieved data of the corresponding API endpoint. To help you better visualize and understand the API Endpoint reports, refer to sample images of reports.

TEMPLATE- Item Label Metrics - Submit Report Request

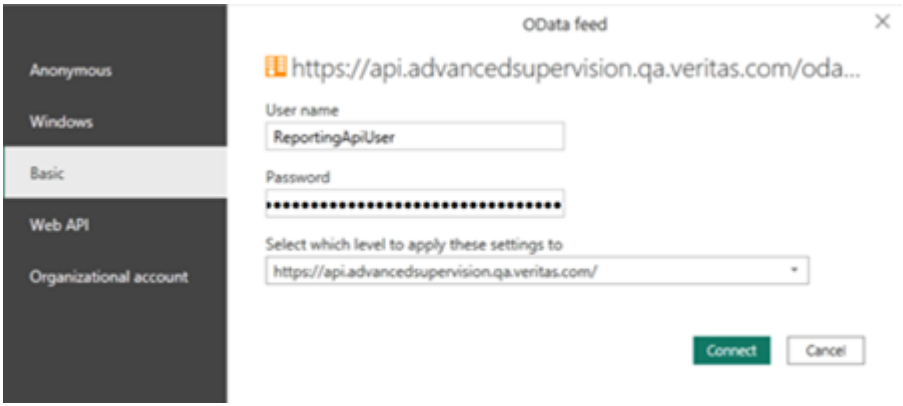
1 Open the *TEMPLATE- Item Label Metrics - Submit Report Request.pbit* file, and specify the following details.



Endpoint Base URL	Enter the REST API endpoint URL. For example, `https://<Reporting endpoint Base URL>`
Report Name	Specify a unique name for the report.
Start Date	Specify the earliest date from which you want to gather data captured or ingested in Insight Surveillance for your report.
End Date	Specify the end date until which you want to gather data captured or ingested in Insight Surveillance for your report.
Return By Department	By default this value is set to ***False***. ■ To get the result of all labels according to monitored employees, set this value as ***False*** ■ To get the result of all labels according to department, set this value as ***True***

2 Click **Load**.

3 Select the required OData Feed.



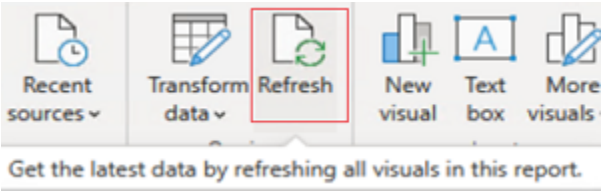
The application submits the report generation request and shows the details.

4 Click **Connect** and choose *Basic Authentication* mechanism to access Reporting API.

The application prompts you several times to provide appropriate credentials when querying Reporting API for each report

5 Manually refresh the page to view the details such as Report ID, Report Name, Report Type, Report Date, Report Status, and Report Information.

If still the entire details are not displayed, Click **Refresh** again as shown in the sample image below.



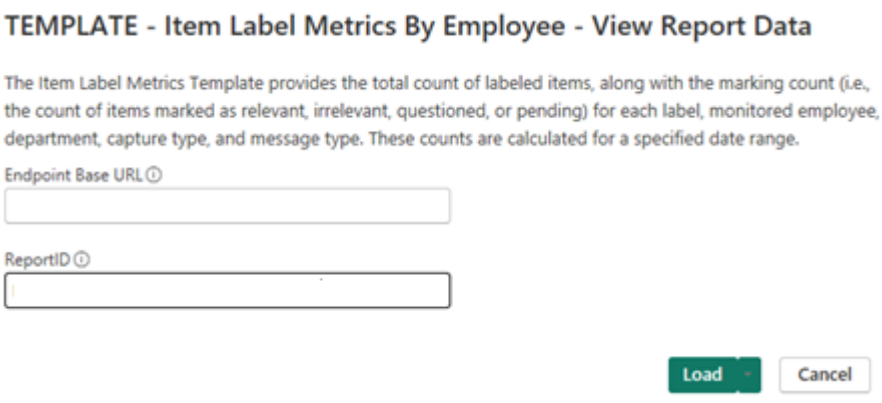
6 When all the details are available, copy the report ID.

Copy the Report ID to retrieve report data once the report is ready. Use this Report ID in the *TEMPLATE- Item Label Metrics By Employee - View Report Data* template to view monitored employees-specific report and *TEMPLATE- Item Label Metrics By Department - View Report Data* template to view department-specific report. Click **Refresh** to view the updated status of report generation.

Upon successful processing, the application displays a report for the retrieved data of the corresponding API endpoint. To help you better visualize and understand the API Endpoint reports, refer to sample images of reports.

TEMPLATE- Item Label Metrics By Employee - View Report Data

1 Open the *TEMPLATE- Item Label Metrics By Employee - View report Data.pbit* file, and specify the following details.

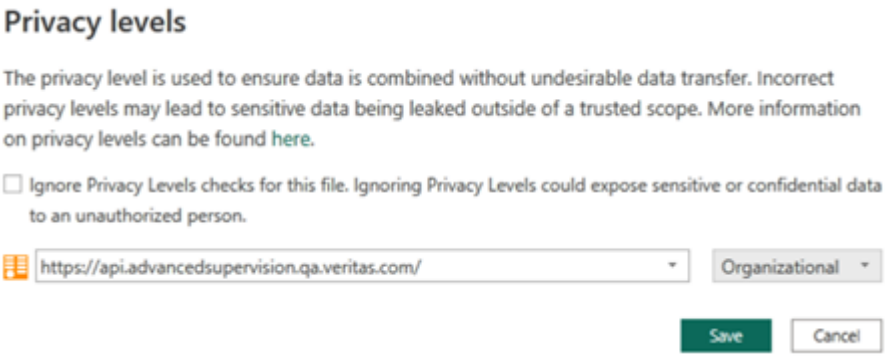


Endpoint Base URL	Enter the REST API endpoint URL. For example, `https://<Reporting endpoint Base URL>`
Report ID	Enter the *Report ID* that is generated during execution of *ItemLabelMetricsAsync* API report or the *TEMPLATE- Item Label Metrics - Submit Report Request* template.

2 Click **Load**.

3 Set the privacy organizational or public for each selected data source.

For more information, See "Guidelines for using Insight Surveillance templates with Microsoft Power BI Desktop" on page 417.

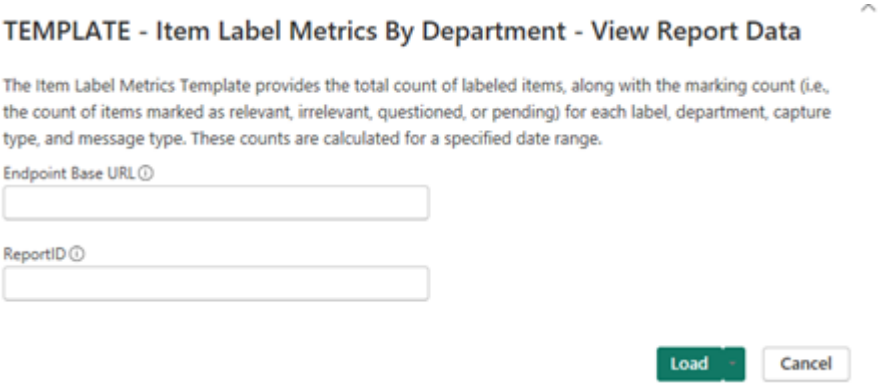


4 Click **Save**.

Upon successful processing, the application displays a report for the retrieved data of the corresponding API endpoint. To help you better visualize and understand the API Endpoint reports, refer to sample images of reports.

TEMPLATE- Item Label Metrics By Department - View Report Data

1 Open the *TEMPLATE- Item Label Metrics By Department - View Report Data.pbit* file, and specify the following details.

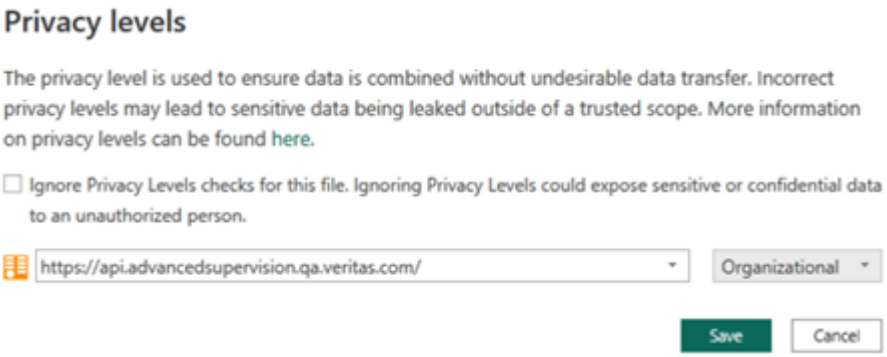


Endpoint Base URL	Enter the REST API endpoint URL. For example, `https://<Reporting endpoint Base URL>`
Report ID	Enter the *Report ID* that is generated during execution of *ItemLabelMetricsAsync* API report or the *TEMPLATE- Item Label Metrics - Submit Report Request* template.

2 Click **Load**.

3 Set the privacy organizational or public for each selected data source.

For more information, See "Guidelines for using Insight Surveillance templates with Microsoft Power BI Desktop" on page 417.

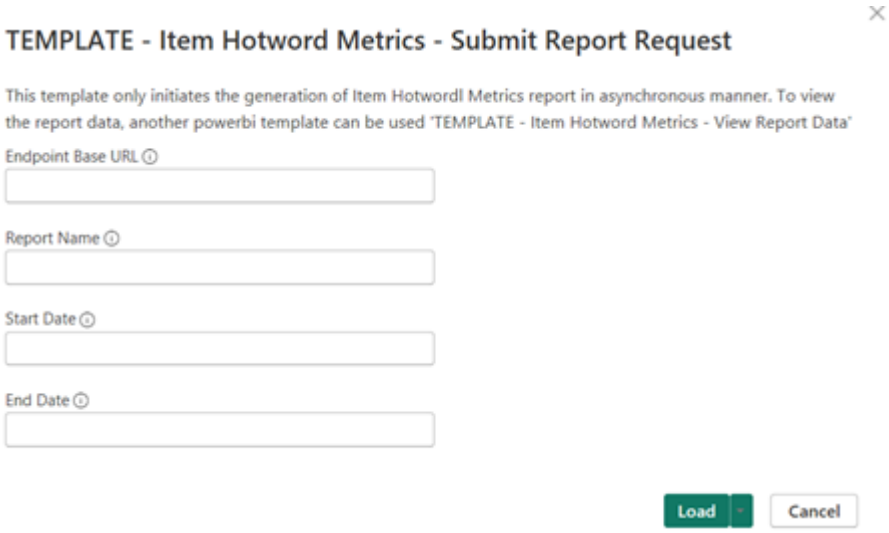


4 Click **Save**.

Upon successful processing, the application displays a report for the retrieved data of the corresponding API endpoint. To help you better visualize and understand the API Endpoint reports, refer to sample images of reports.

TEMPLATE- Item Hotword Metrics - Submit Report Request

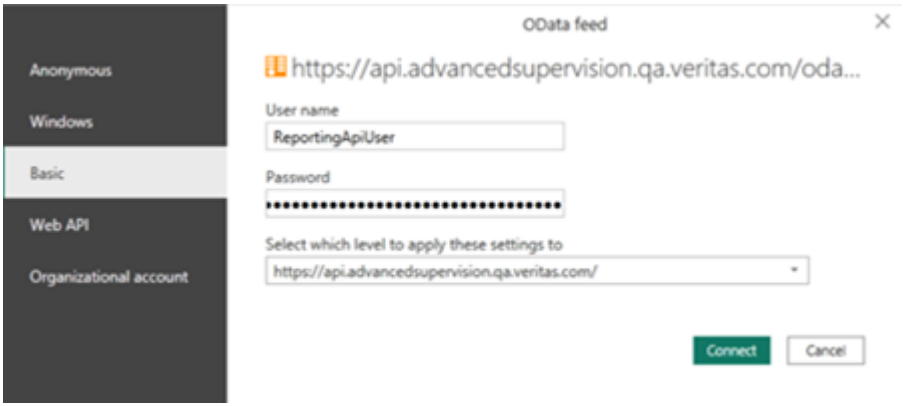
1 Open the *TEMPLATE- Item Hotword Metrics - Submit Report Request.pbit* file, and specify the following details.



Endpoint Base URL	Enter the REST API endpoint URL. For example, `https://<Reporting endpoint Base URL>`
Report Name	Specify a unique name for the report.
Start Date	Specify the earliest date from which you want to gather data captured or ingested in Insight Surveillance for your report.
End Date	Specify the end date until which you want to gather data captured or ingested in Insight Surveillance for your report.

2 Click **Load**.

3 Select the required OData Feed.



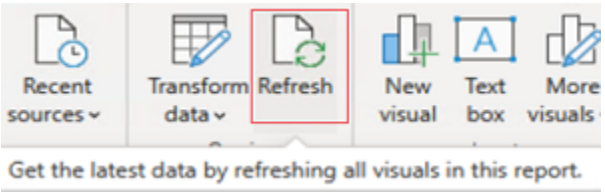
The application submits the report generation request and shows the details.

4 Click **Connect** and choose *Basic Authentication* mechanism to access Reporting API.

The application prompts you several times to provide appropriate credentials when querying Reporting API for each report

5 Manually refresh the page to view the details such as Report ID, Report Name, Report Type, Report Date, Report Status, and Report Information.

If still the entire details are not displayed, click **Refresh** again as shown in the sample image below.



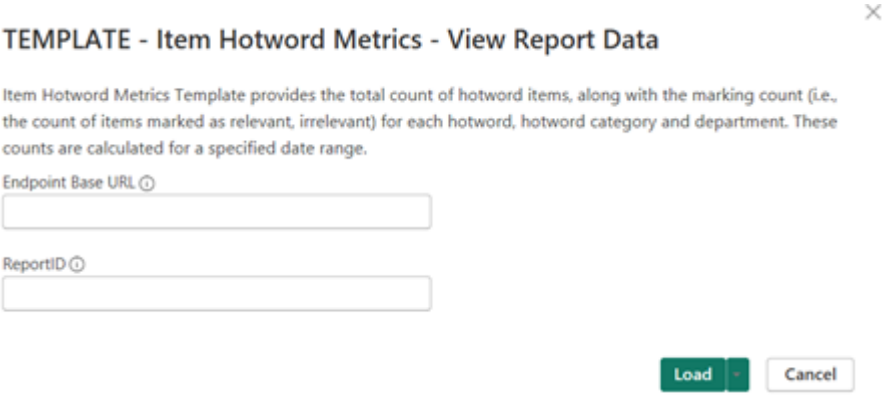
6 When all the details are available, copy the report ID.

Copy the Report ID to retrieve report data once the report is ready. Use this Report ID in the *TEMPLATE- Item Hotword Metrics - View Report Data* template to view the report. Click **Refresh** to view the updated status of report generation.

Upon successful processing, the application displays a report for the retrieved data of the corresponding API endpoint. To help you better visualize and understand the API Endpoint reports, refer to sample images of reports.

TEMPLATE- Item Hotword Metrics - View Report Data

1 Open the *TEMPLATE- Item Hotword Metrics - View report Data.pbit* file, and specify the following details.

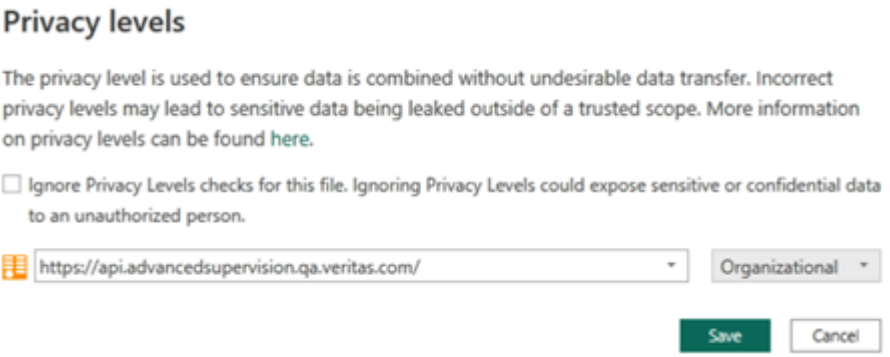


Endpoint Base URL	Enter the REST API endpoint URL. For example, `https://<Reporting endpoint Base URL>`
Report ID	Enter the *Report ID* that is generated during execution of *ItemHotwordMetricsAsync* API report or the *TEMPLATE- Item Hotword Metrics - Submit Report Request* template.

2 Click **Load**.

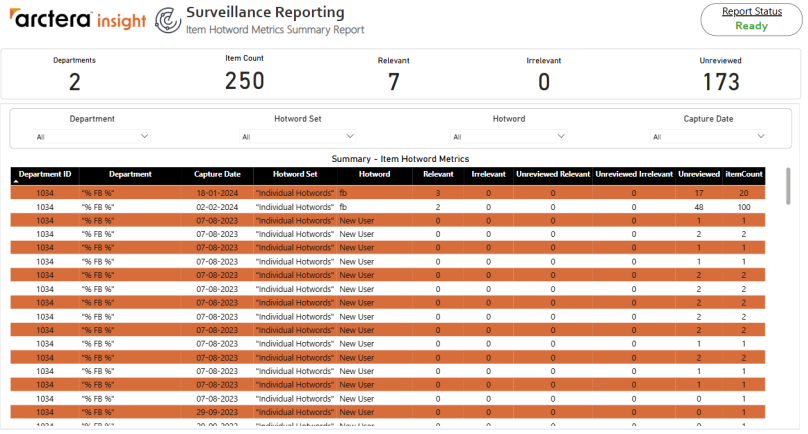
3 Set the privacy organizational or public for each selected data source.

For more information, See "Guidelines for using Insight Surveillance templates with Microsoft Power BI Desktop" on page 417.



4 Click **Save**.

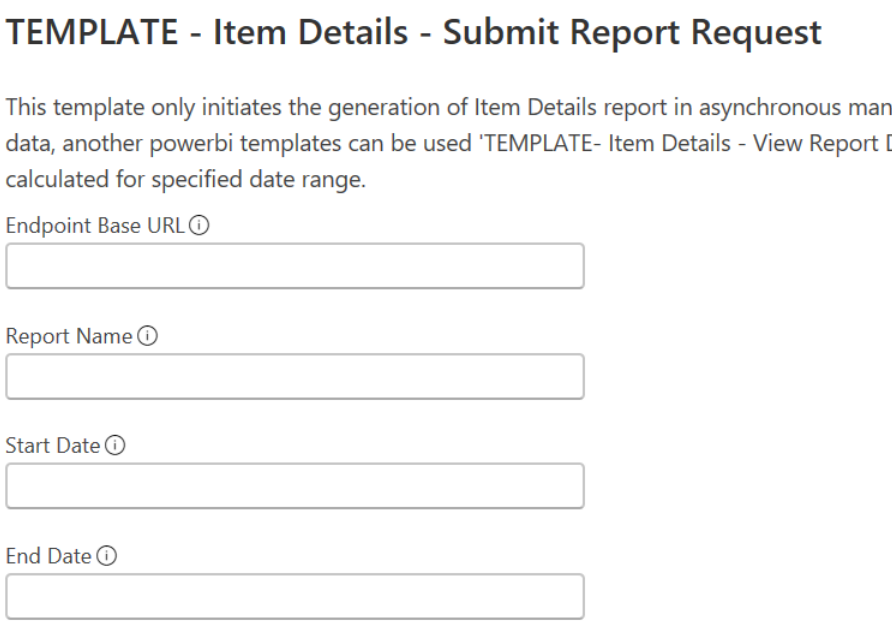
Upon successful processing, the application displays a report for the retrieved data of the corresponding API endpoint.



To help you better visualize and understand the API Endpoint reports, refer to sample images of reports.

TEMPLATE- Item Details - Submit Report Request

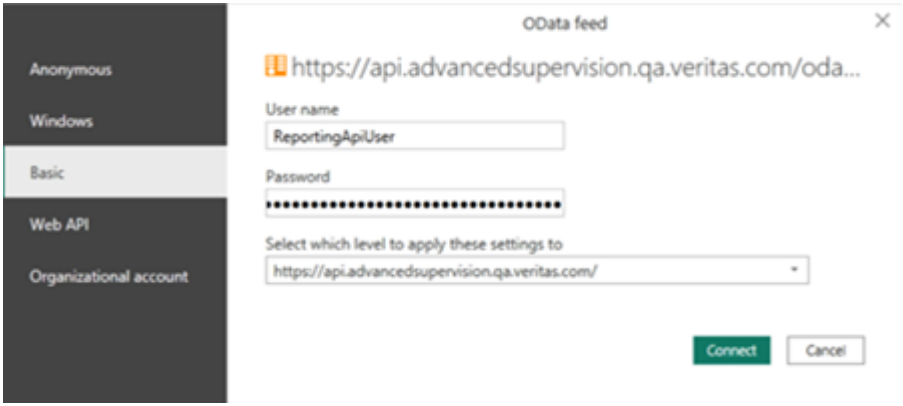
1 Open the *TEMPLATE- Item Details - Submit Report Request.pbit* file, and specify the following details.



Endpoint Base URL	Enter the REST API endpoint URL. For example, `https://<Reporting endpoint Base URL>`
Report Name	Specify a unique name for the report.
Start Date	Specify the earliest date from which you want to gather data captured or ingested in Insight Surveillance for your report.
End Date	Specify the end date until which you want to gather data captured or ingested in Insight Surveillance for your report.

2 Click **Load**.

3 Select the required OData Feed.



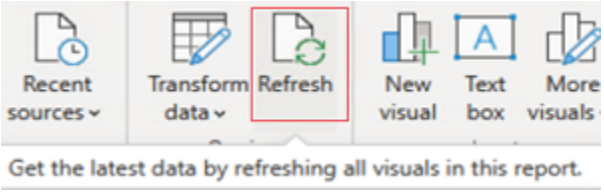
The application submits the report generation request and shows the details.

4 Click **Connect** and choose *Basic Authentication* mechanism to access Reporting API.

The application prompts you several times to provide appropriate credentials when querying Reporting API for each report.

5 Manually refresh the page to view the details such as Report ID, Report Name, Report Type, Report Date, Report Status, and Report Information.

If still the entire details are not displayed, click **Refresh** again as shown in the following sample image.



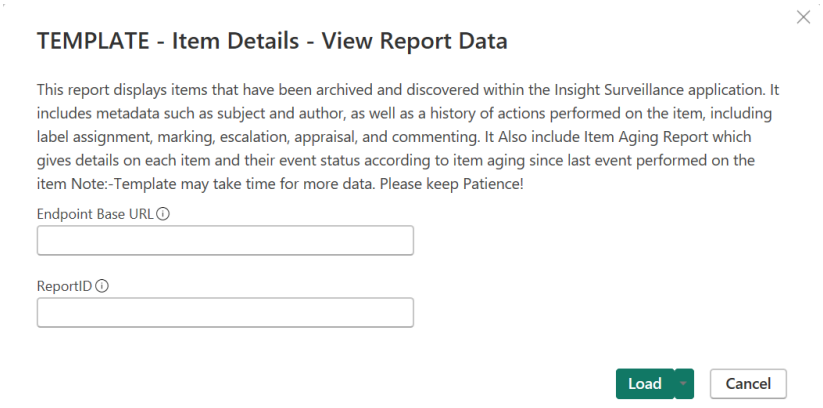
6 When all the details are available and *Report Status: Ready* is displayed, copy the report ID.

Use this Report ID in the *TEMPLATE- Item Details - View Report Data* template. Click **Refresh** to view the updated status of report generation.

Upon successful processing, the application displays a report for the retrieved data of the corresponding API endpoint. To help you better visualize and understand the API Endpoint reports, refer to sample images of reports.

TEMPLATE- Item Details - View Report Data

1 Open the *TEMPLATE- Item Details - View report Data.pbit* file, and specify the following details.

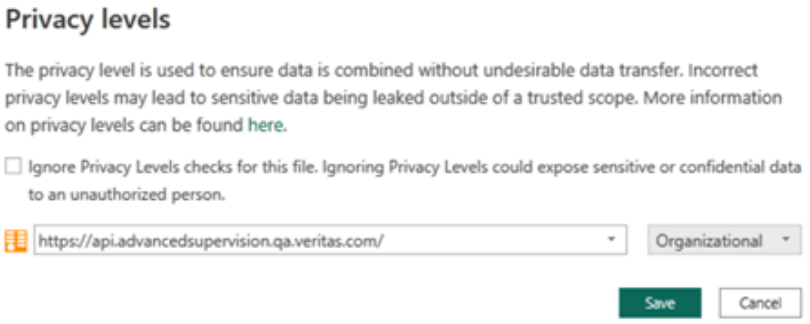


Endpoint Base URL	Enter the REST API endpoint URL. For example, `https://<Reporting endpoint Base URL>`
Report ID	Enter the *Report ID* that is generated during execution of *ItemDetailsAsync* API report or the *TEMPLATE- Item Details - Submit Report Request* template.

2 Click **Load**.

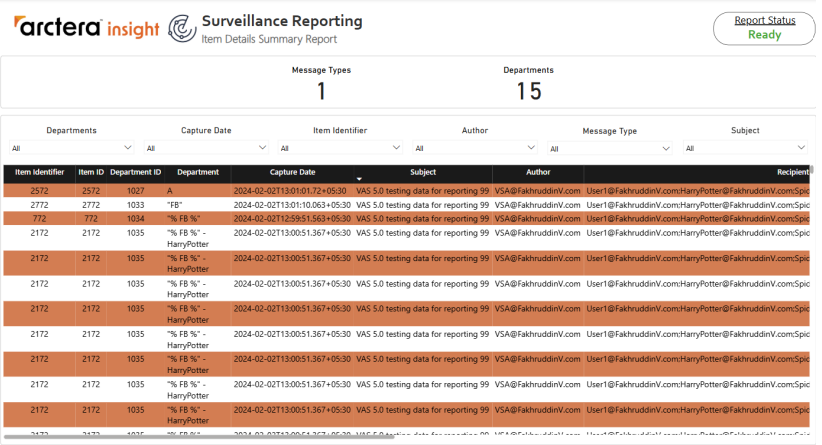
3 Set the privacy organizational or public for each selected data source.

For more information, See "Guidelines for using Insight Surveillance templates with Microsoft Power BI Desktop" on page 417.

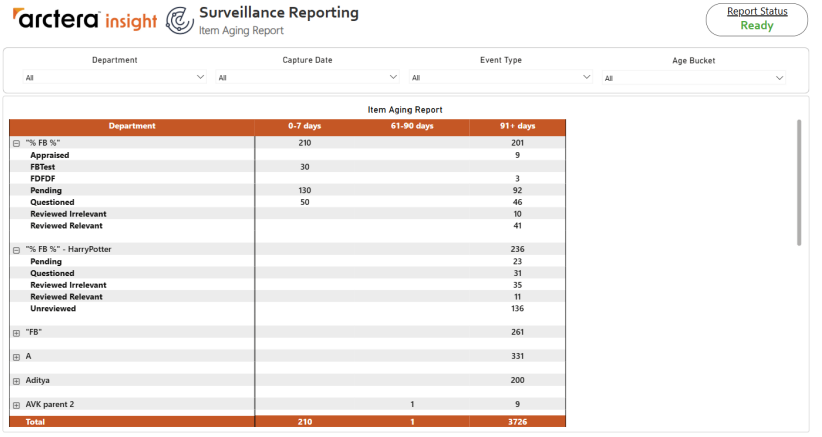


4 Click **Save**.

Upon successful processing, the application displays a report for the retrieved data of the corresponding API endpoint.

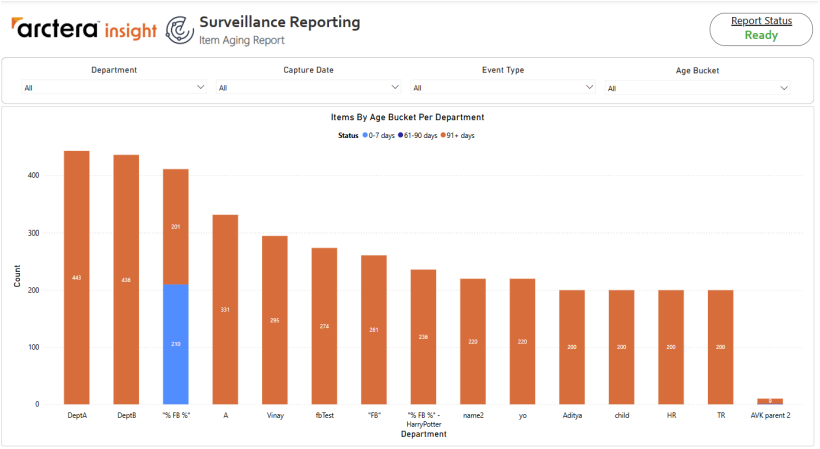


Arctera Insight Surveillance integrates Item Aging Report into the Item Details Power BI report for extended visibility, though it is not backed by a separate API endpoint. Refer the following images:



This report shows the number of messages that are either still unreviewed, pending review, or other event type within the given departments, along with organizational roll-up totals. Item Age bucket gives an indication of how long a message has remained pending, unreviewed or any other event type state from when it was captured for review.

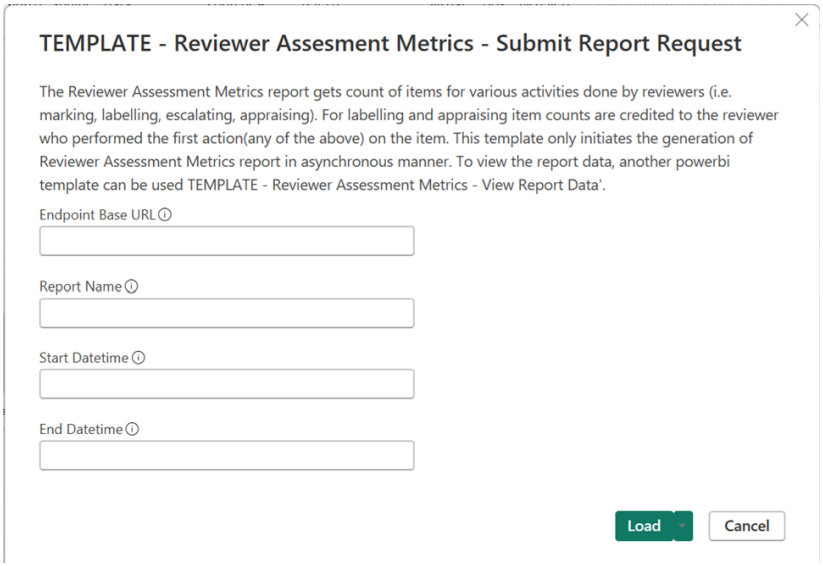
The graphical representation of the same data can also be seen with the help of Item Aging Report template.



To help you better visualize and understand the API Endpoint reports, refer to sample images of reports.

TEMPLATE- Reviewer Assessment Metrics - Submit Report Request

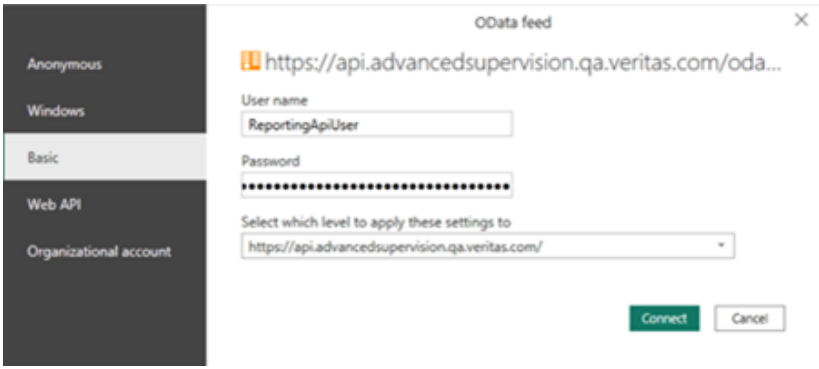
1 Open the *TEMPLATE- Reviewer Assessment Metrics - Submit Report Request.pbit* file, and specify the following details.



Endpoint Base URL	Enter the REST API endpoint URL. For example, `https://<Reporting endpoint Base URL>`
Report Name	Specify a unique name for the report.
Start Datetime	Specify the earliest date from which you want to gather data captured or ingested in Insight Surveillance for your report. Format: YYYY-MM-DDThh:mm:ss **Note**: The time component is optional. If you prefer not to include the time, you can simply use the YYYY-MM-DD format.
End Datetime	Specify the end date until which you want to gather data captured or ingested in Insight Surveillance for your report. Format: YYYY-MM-DDThh:mm:ss **Note**: The time component is optional. If you prefer not to include the time, you can simply use the YYYY-MM-DD format.

2 Click **Load**.

3 Select the required OData Feed.

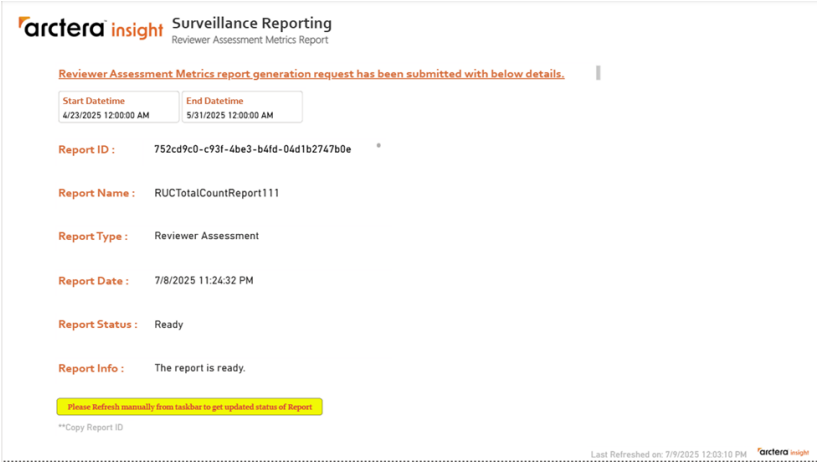


The application submits the report generation request and shows the details.

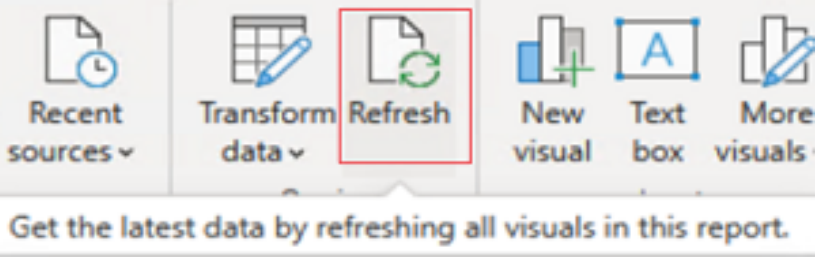
4 Click **Connect** and choose *Basic Authentication* mechanism to access Reporting API.

The application prompts you several times to provide appropriate credentials when querying Reporting API for each report.

5 Manually refresh the page to view the details such as Report ID, Report Name, Report Type, Report Date, Report Status, and Report Information.



If still the entire details are not displayed, click **Refresh** again as shown in the following sample image.



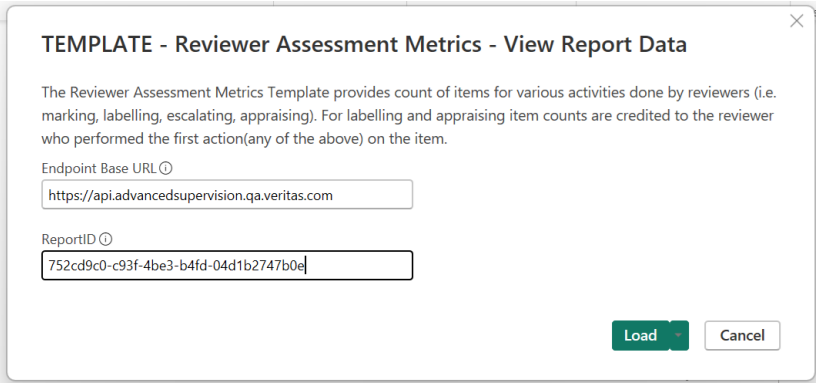
6 When all the details are available and *Report Status: Ready* is displayed, copy the report ID.

Use this Report ID in the *TEMPLATE- Reviewer Assessment Metrics - View Report Data* template. Click **Refresh** to view the updated status of report generation.

Upon successful processing, the application displays a report for the retrieved data of the corresponding API endpoint. To help you better visualize and understand the API Endpoint reports, refer to sample images of reports.

TEMPLATE- Reviewer Assessment Metrics - View Report Data

1 Open the *TEMPLATE- Reviewer Assessment Metrics - View report Data.pbit* file, and specify the following details.

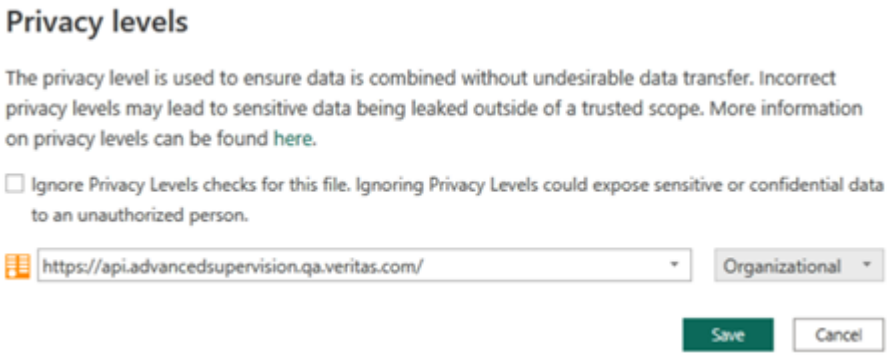


Endpoint Base URL	Enter the REST API endpoint URL. For example, `https://<Reporting endpoint Base URL>`
Report ID	Enter the *Report ID* that is generated during execution of *ReviewerAssessmentMetricsAsync* API report or the *TEMPLATE- Reviewer Assessment Metrics - Submit Report Request* template.

2 Click **Load**.

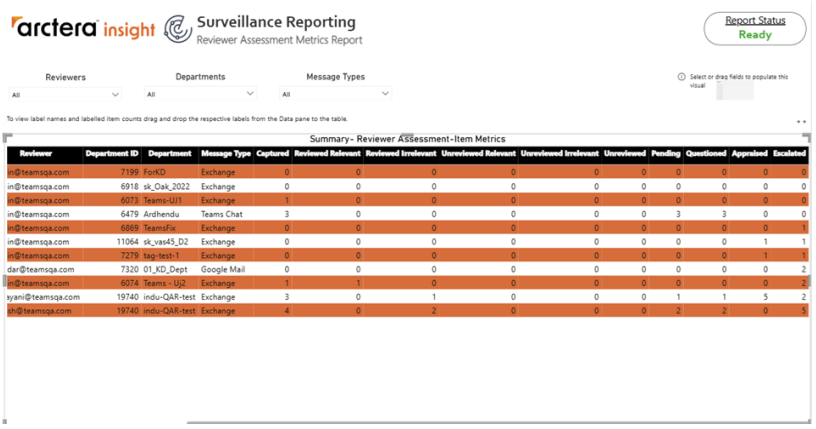
3 Set the privacy organizational or public for each selected data source.

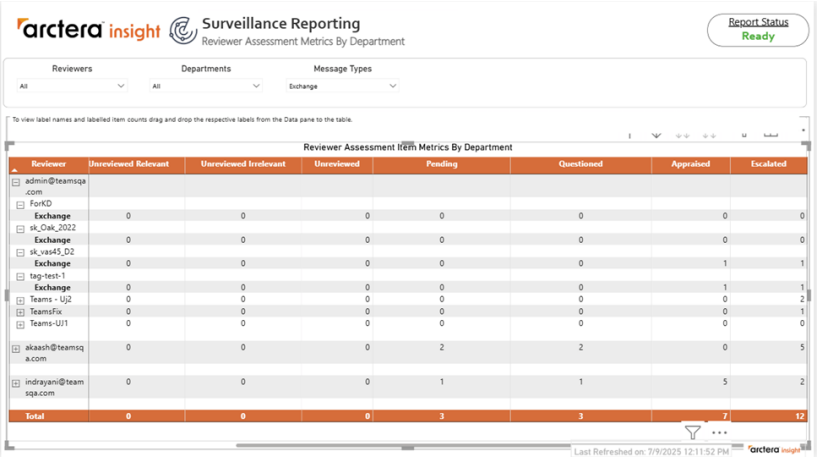
For more information, See "Guidelines for using Insight Surveillance templates with Microsoft Power BI Desktop" on page 417.



4 Click **Save**.

Upon successful processing, the application displays a report for the retrieved data of the corresponding API endpoint.





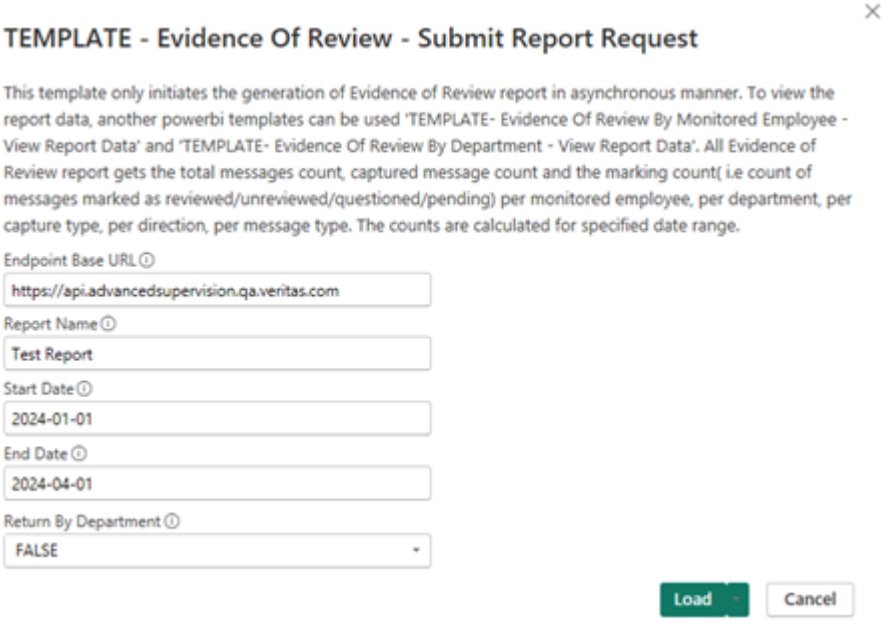
To help you better visualize and understand the API Endpoint reports, refer to sample images of reports.

Note: Since labels are custom-created and not predefined, the Power BI UI cannot automatically select them to display corresponding item counts. Customers need to manually drag and drop the label fields, remove summarization, and then add them to the Power BI table after the data is loaded.

Alternatively, if customers do not intend to use the Power BI UI and simply want the complete dataset, they can export the ReviewerAssessmentMetrics table to Excel.

TEMPLATE- Evidence Of Review - Submit Report Request

1 Open the *TEMPLATE- Evidence Of Review - Submit Report Request.pbit* file, and specify the following details.

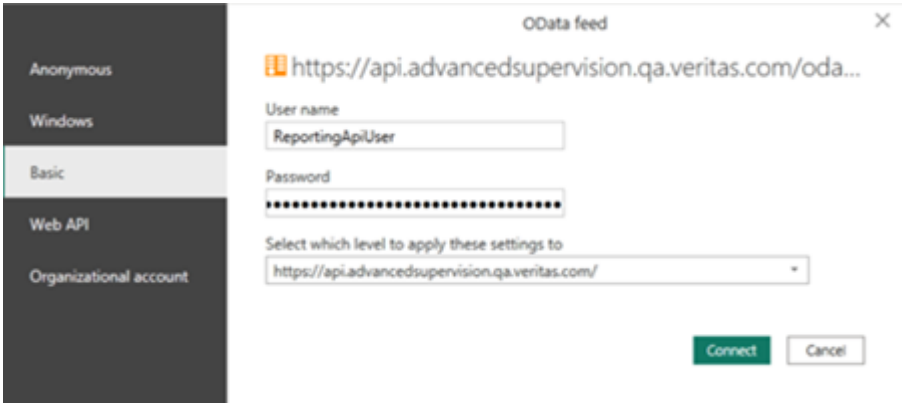


Endpoint Base URL	Enter the REST API endpoint URL. For example, `https://<Reporting endpoint Base URL>`
Report Name	Specify a unique name for the report.
Start Date	Specify the earliest date from which you want to gather data captured or ingested in Insight Surveillance for your report.
End Date	Specify the end date until which you want to gather data captured or ingested in Insight Surveillance for your report.

Return By Department	By default this value is set to ***False***. ■ To get the result according to monitored employees, set this value as ***False***. ■ To get the result according to departments, set this value as ***True***

2 Click **Load**.

3 Select the required OData Feed.

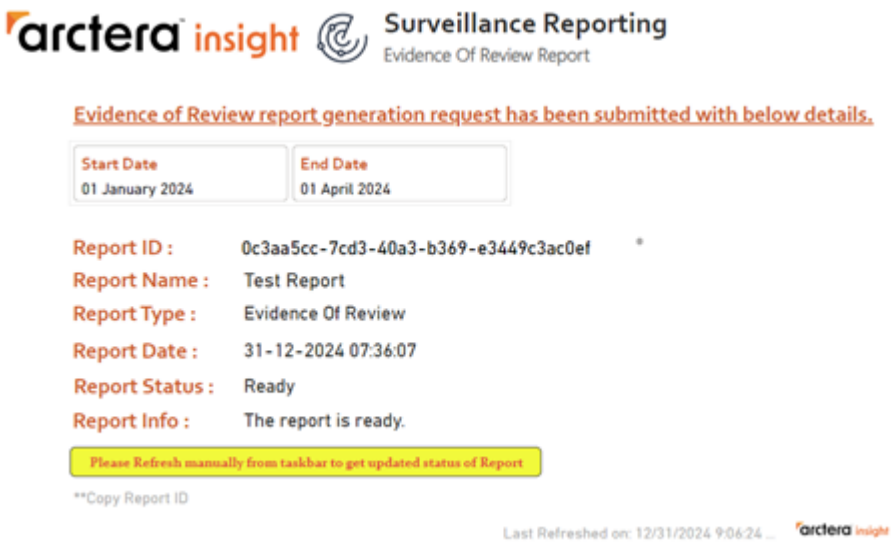


The application submits the report generation request and shows the details.

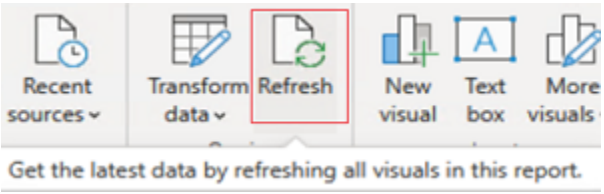
4 Click **Connect** and choose *Basic Authentication* mechanism to access Reporting API.

The application prompts you several times to provide appropriate credentials when querying Reporting API for each report

5 Manually refresh the page to view the details such as Report ID, Report Name, Report Type, Report Date, Report Status, and Report Information.



If still the entire details are not displayed, Click **Refresh** again as shown in the sample image below.



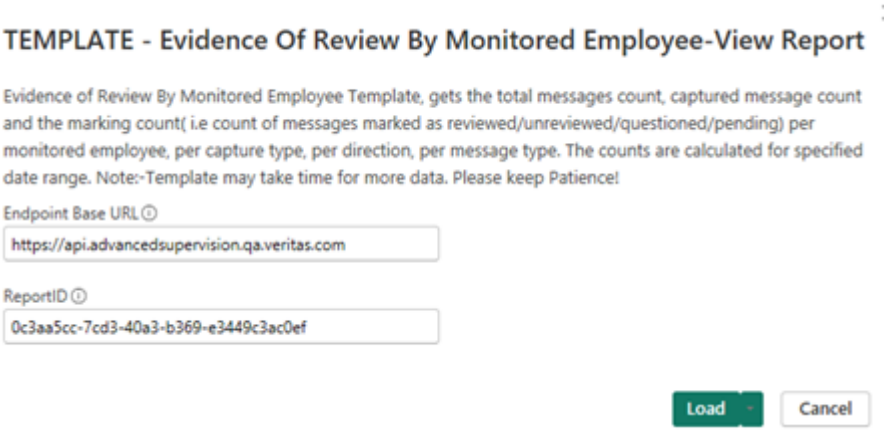
6 When all the details are available, copy the report ID.

Copy the Report ID to retrieve report data once the report is ready. Use this Report ID in the *TEMPLATE- Evidence Of Review By Monitored Employee - View Report Data* template to view monitored employees-specific report or in the *TEMPLATE- Evidence Of Review By Department - View Report Data* template to view departments-specific report. Click **Refresh** to view the updated status of report generation.

Upon successful processing, the application displays a report for the retrieved data of the corresponding API endpoint. To help you better visualize and understand the API Endpoint reports, refer to sample images of reports.

TEMPLATE- Evidence Of Review By Monitored Employee - View Report Data

1 Open the *TEMPLATE- Evidence Of Review By Monitored Employee - View Report Data.pbit* file, and specify the following details.

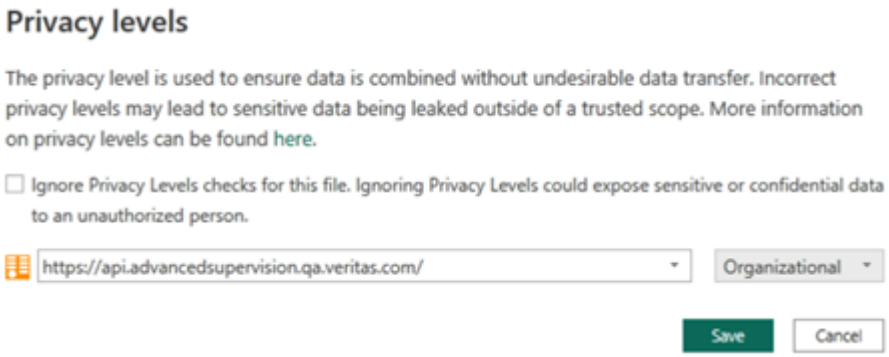


Endpoint Base URL	Enter the REST API endpoint URL. For example, `https://<Reporting endpoint Base URL>`
Report ID	Enter the *Report ID* that is generated during execution of the *TEMPLATE- Evidence Of Review - Submit Report Request* template.

2 Click **Load**.

3 Set the privacy organizational or public for each selected data source.

For more information, See "Guidelines for using Insight Surveillance templates with Microsoft Power BI Desktop" on page 417.

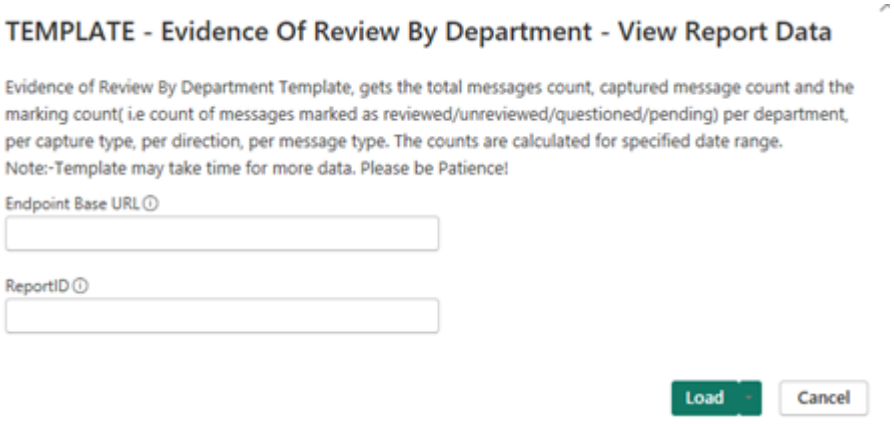


4 Click **Save**.

Upon successful processing, the application displays a report for the retrieved data of the corresponding API endpoint. To help you better visualize and understand the API Endpoint reports, refer to sample images of reports.

TEMPLATE- Evidence Of Review By Department - View Report Data

1 Open the *TEMPLATE- Evidence Of Review By Department - View Report Data.pbit* file, and specify the following details.

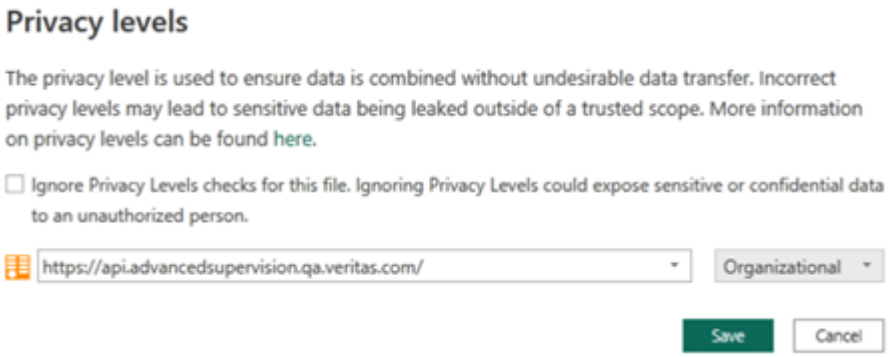


Endpoint Base URL	Enter the REST API endpoint URL. For example, `https://<Reporting endpoint Base URL>`
Report ID	Enter the *Report ID* that is generated during execution of the *TEMPLATE- Evidence Of Review - Submit Report Request* template.

2 Click **Load**.

3 Set the privacy organizational or public for each selected data source.

For more information, See "Guidelines for using Insight Surveillance templates with Microsoft Power BI Desktop" on page 417.

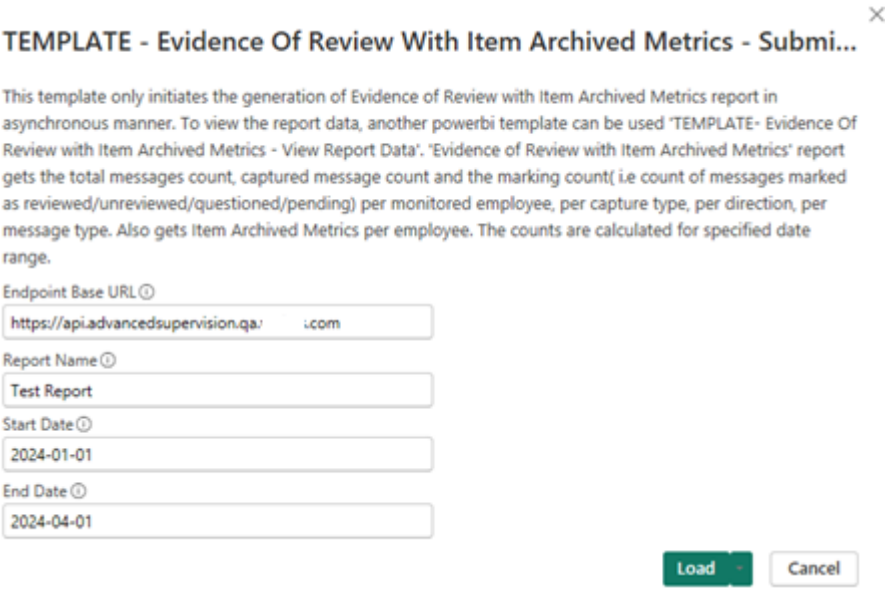


4 Click **Save**.

Upon successful processing, the application displays a report for the retrieved data of the corresponding API endpoint. To help you better visualize and understand the API Endpoint reports, refer to sample images of reports.

TEMPLATE- Evidence Of Review With Item Archived Metrics - Submit Report Request

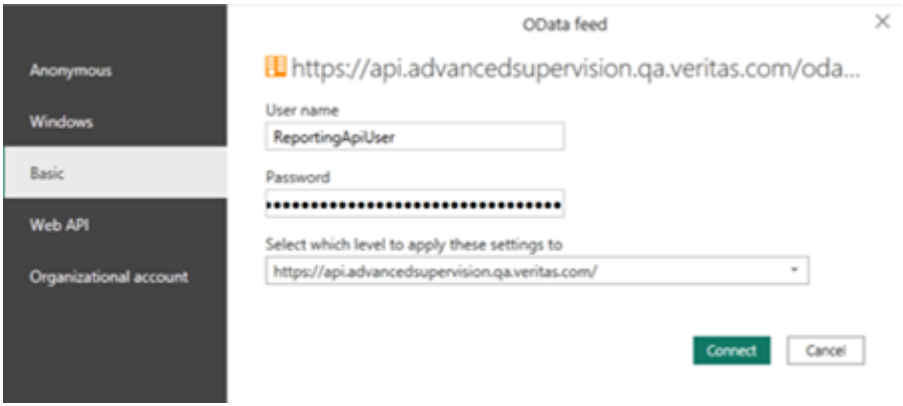
1 Open the *TEMPLATE- Evidence Of Review With Item Archived Metrics - Submit Report Request.pbit* file, and specify the following details.



Endpoint Base URL	Enter the REST API endpoint URL. For example, `https://<Reporting endpoint Base URL>`
Report Name	Specify a unique name for the report.
Start Date	Specify the earliest date from which you want to gather data captured or ingested in Insight Surveillance for your report.
End Date	Specify the end date until which you want to gather data captured or ingested in Insight Surveillance for your report.

2 Click **Load**.

3 Select the required OData Feed.

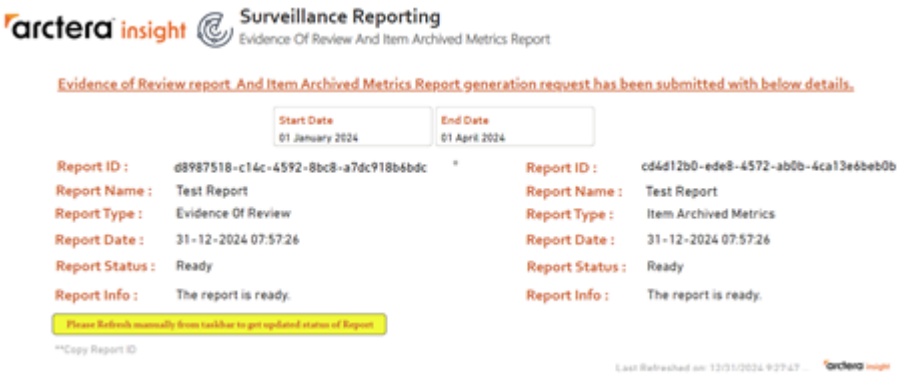


The application submits the report generation request and shows the details.

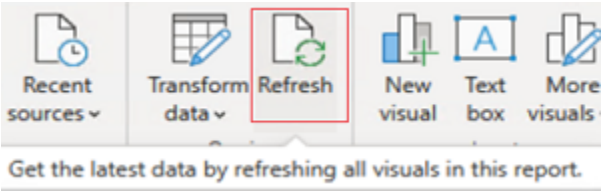
4 Click **Connect** and choose *Basic Authentication* mechanism to access Reporting API.

The application prompts you several times to provide appropriate credentials when querying Reporting API for each report

5 Manually refresh the page to view the details such as Report ID, Report Name, Report Type, Report Date, Report Status, and Report Information.



If still the entire details are not displayed, Click **Refresh** again as shown in the sample image below.



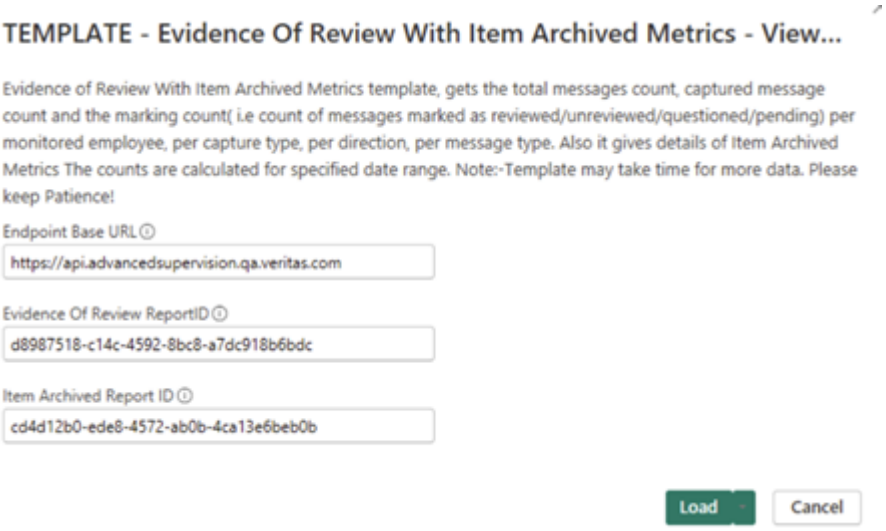
6 When all the details are available, copy the report ID.

Copy the Report ID to retrieve report data once the report is ready. Use this Report ID in the *TEMPLATE- Evidence Of Review With Item Archived Metrics - View Report Data* template. Click **Refresh** to view the updated status of report generation.

Upon successful processing, the application displays a report for the retrieved data of the corresponding API endpoint. To help you better visualize and understand the API Endpoint reports, refer to sample images of reports.

TEMPLATE- Evidence Of Review With Item Archived Metrics - View Report Data

1 Open the *TEMPLATE- Evidence Of Review With Item Archived Metrics - View Report Data.pbit* file, and specify the following details.

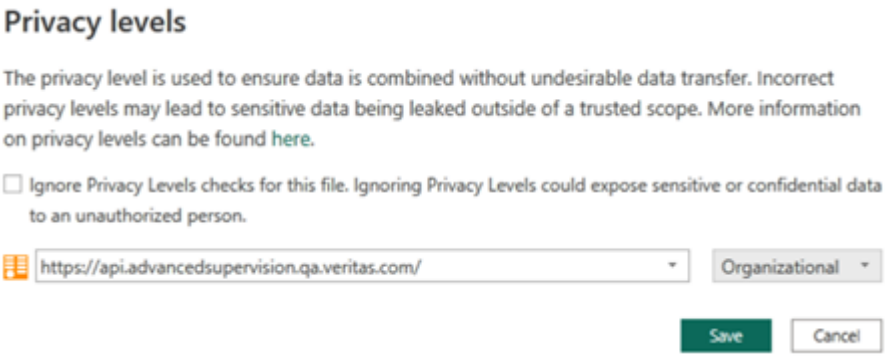


Endpoint Base URL	Enter the REST API endpoint URL. For example, `https://<Reporting endpoint Base URL>`
Evidence Of Review Report ID	Enter the *Report ID* (**when the selected *Report Type* is *Evidence Of Report***) generated during the execution of the *TEMPLATE - Evidence Of Review With Item Archived Metrics - Submit Report Request* template.
Item Archived Report ID	Enter the *Report ID* (**when the selected *Report Type* is *Item Archived Metrics***) generated during the execution of the *TEMPLATE - Evidence Of Review With Item Archived Metrics - Submit Report Request* template.

2 Click **Load**.

3 Set the privacy organizational or public for each selected data source.

For more information, See "Guidelines for using Insight Surveillance templates with Microsoft Power BI Desktop" on page 417.



4 Click **Save**.

Upon successful processing, the application displays a report for the retrieved data of the corresponding API endpoint. To help you better visualize and understand the API Endpoint reports, refer to sample images of reports.

Saving, editing, and refreshing the Power BI reports

To save Power BI reports	After generating and customizing the Power BI reports, you can save these reports as PBIX files for sharing with the concerned members in the organization.	On Power BI Dashboard, select **File** > **Save As**.
To edit Power BI reports	The organization members, who have access to the OData endpoints, can edit parameters if required. The application fetches the latest data from the OData endpoints and updates reports accordingly.	On Power BI Dashboard, select **Home** > **Edit Queries** > **Edit Parameters**. Click **Apply Changes**.
To refresh Power BI reports	The organization members, who have access to the OData endpoints, can often refresh the report to get the latest data. Refreshing the data reruns all the queries and ensures that all the data is up to date and ready for analysis and visualization.	On Power BI Dashboard, select **Home** > **Refresh**.

Chapter 26

Managing Audit Settings

This chapter includes the following topics:

Audit Settings Overview

The **Audit settings** tab lets you control the configuration settings for the Enhanced Auditing feature. Users with the *View Audit Settings* permission can view the Audit settings. Users must have the *Modify Audit Settings* permissions to configure and change the audit settings. Users can configure the Audit settings if the Auditing feature is configured and enabled.

Administrators can control the availability of the Auditing feature at the department and application level for the following modules:

Module	Description	Application	Department
Departments	Logs audit records for the Department specific operations: create and modify departments	NA	Yes
Hotwords	Logs audit records for the Hotwords specific operation: create, modify, or delete hotword and hotword sets	Yes	Yes
Monitored Employees	Logs audit records for all Monitored Employees operations	NA	Yes

Module	Description	Application	Department
Role Assignments	Logs audit records for the Role Assignment specific operations: assign roles to users, remove roles for a user	Yes	Yes
Roles	Logs audit records for the Roles specific operations: create, modify, and delete roles	Yes	Yes
Searches	Logs audit records for all Search specific operations	NA	Yes

Editing the Audit Settings

To edit the Audit Settings

1 In the left navigation pane, click **Configuration**.

2 Click **Audit Settings**.

Insight Surveillance lists all the modules and shows if the Enhanced Auditing feature is enabled at the Application and Department level. You can filter or search for a specific module.

3 Click **Edit**.

The **Edit audit settings** dialog box appears.

4 Select the check boxes under Application and Department columns of those modules for which you want to enable the Auditing feature.

5 Clear the check boxes under Application and Department columns of those modules for which you want to disable the Auditing feature.

6 Click **Save**.

The changes are displayed on the Audit Settings screen.

Chapter 27

Working with Audit viewer

This chapter includes the following topics:

About Audit viewer

If the Enhanced Auditing feature is configured and enabled for a customer, the audit records for that customer are sent to the audit server whenever certain operations and modifications are made to modules as selected in the Audit Settings. The Audit viewer lets you search and export audit records for various modules and operations at the department and application level. See "Audit Settings Overview" on page 481.

The **Audit viewer** tab is only displayed when the user is assigned to an application or department role having the *View Audit Information* permission.

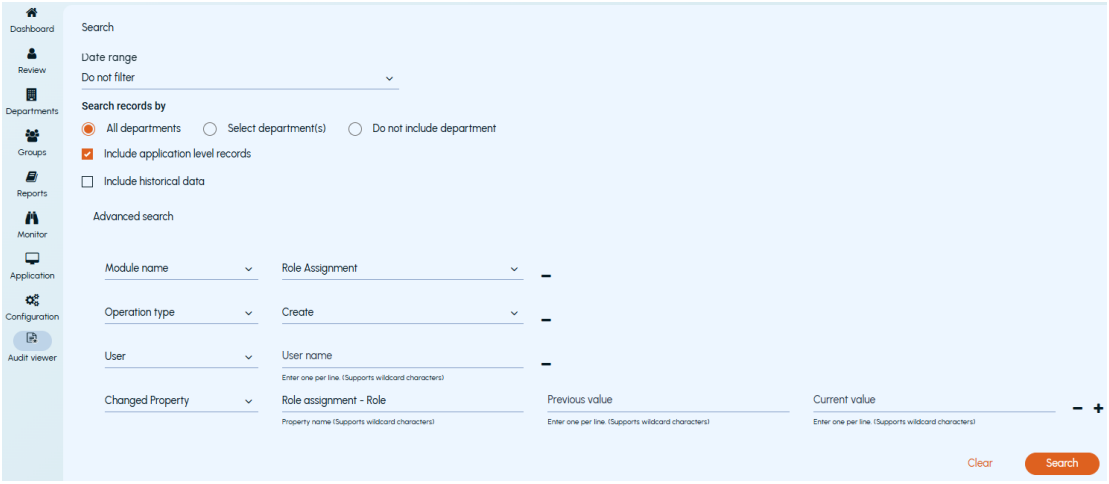
Note: It takes approximately 90 seconds to get the audit logs available for search in Audit viewer. It is recommended to wait for a few minutes after any modification is made in the modules before searching for the audit logs using the Audit viewer.

Performing a search for audit records

To run a search for audit records

1 In the left navigation pane, click **Audit viewer**.

The Audit Viewer screen is displayed.



2 In the **Date range** section, specify the date range for the audit records that fall in this duration.

The options are as follows:

- **Specific date range** - Specify the date and time duration to search audit records that were sent or received during the selected period.
- **Today / Yesterday / Last 7 days / Last 14 days / Last 28 days** - Search audit records that are created today, yesterday, or in last 7/14/28 days.
- **Do not filter** - Do not search for audit records based on date range.

3 To search by departments, select the appropriate option:

- **All departments** - Search for audit records generated at the department level for all departments where the logged-in user has permission to view audit information
- **Select department(s)** - Search for audit records for specific departments or exception departments. If you select this option, the **Selected departments** section appears. Only those departments where the logged-in user has permission to view audit information are displayed. Click **Add**

to search and add departments. You can remove the listed departments from the list using the **Remove** link.

- **Do not include departments** - Select this option if you do not want to search for audit information generated at the department level. If this option is selected, you must select either **Include application level records** or **Include historical data** option.

4 Select the **Include application level records** check box if you want to search for audit records generated at the application level.

5 Select the **Include historical data** check box if you want to include audit information at the following level:

- Deleted department/Folder
- Closed department
- Monitored employees whose exception status is removed

Note: You can select the **Include application level records** and **Include historical records** if you have the *View Audit information* permission at the application level.

---

6 Use **Advanced search** options to narrow the search for audit records. The following additional options, such as operation type, user, and property, are available. You can add a new search row by clicking the + icon.

Search option	Description
Module name	Select the modules for which you want to search the audit records. For details on the available modules and their supported operations for audit records, See "Audit Settings Overview" on page 481. Note: You can search for multiple modules in a single search; however, you cannot search for the module name twice.
Operation type	Select operations such as Create, Update, and Delete.

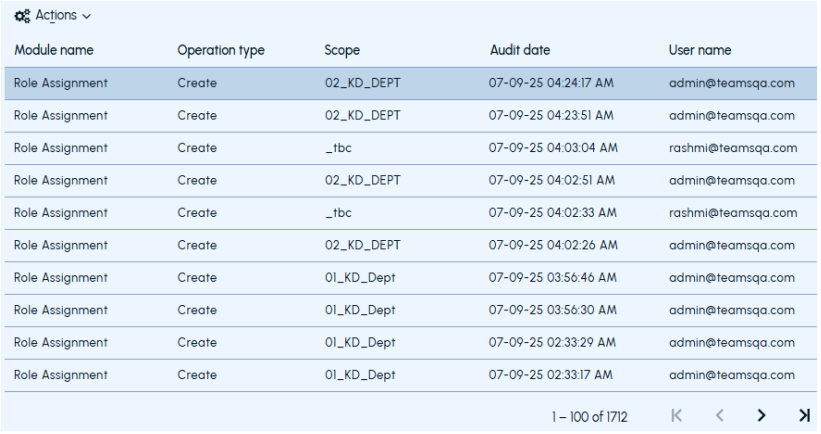
Search option	Description
User	Select audit records based on users. You can enter one user per line. Press the **Enter** key to add another user on next line. Audit records having any of these usernames are returned. The **Username** field supports wildcards * and ?. You can use an asterisk (*) wildcard to represent zero or more characters in your search. Use a question mark (?) wildcard to represent any single character. Wildcards can be escaped using \. Therefore, * represents the character * whereas * represents the wildcard. All the provided values are matched if the search is present anywhere in the data. You cannot use special characters in the **Username** field. Also, special characters which appear in the middle of the text using wildcard cannot be matched. For example, a search term **MyDomain*vsa** will not match the data **MyDomain\user1**, but will match the below search terms: ■ Mydomain\user1 ■ Mydomain user1 ■ Mydomain ■ user

Search option	Description
Changed Property	Search for a property changed in an audit event using the following options. Press the **Enter** key to add another entry on next line. ■ **Property name**: The name of the changed property whose value you want to search. For example, Department parent or Role name. You can use a wildcard to match multiple properties. ■ **Previous value**: The previous value (before modification) of an audit record's changed property. This field supports wildcards and partial matches. ■ **Current value**: The current value of an audit record's changed property. This field supports wildcards and partial matches. Note: You can search for multiple changed properties in a single search; however, you cannot search for the same changed property twice. All the provided values are matched if the search is present anywhere in the data. You can use special characters in your search. These fields support the use of wildcard characters * and ?. You can use an asterisk (*) wildcard to represent zero or more characters in your search. Use a question mark (?) wildcard to represent any single character. Wildcards can be escaped using \. Therefore, * represents the character * and not wildcard *. Since \ is an escape sequence, you can escape \ by using \\. For example, if a username in the **Current value** or **Previous value** fields of the property is **Acme\John Doe**. To search for this, you can provide any of the following search terms: ■ Acme* ■ Acme\\John Doe ■ Acme*John Doe ■ *John Note that wildcards present in the middle of search terms can match special characters. For example, in the above example, **Acme*John Doe** search terms match **Acme\John**.

7 Click **Search** to perform the search for audit records.

When the search is executed, the search results are displayed. A maximum of 10000 audit records can be displayed.

In the left panel, the audit records matching the search criteria are displayed. The newest audit records are displayed first. You can sort the records in ascending or descending order by using the sort arrow icon in the header of the columns. When you select an audit record in the left panel, its changed properties are displayed in the right pane.



8 From the **Actions** menu, click **Export as CSV** if you want to export the search results.