Arctera Enterprise Vault™ Insight Surveillance Administrator's Guide

Version 15.2

Enterprise Vault™ Insight Surveillance: Administrator's Guide

Last updated: 2025-07-07.

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 on the company website:

https://www.veritas.com/docs/100040095

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 (formerly Veritas) community site:

https://vox.veritas.com/category/arctera-discussions/discussions/enterprise-vault

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.

Contents

Chapter 1

Understanding Arctera Insight Surveillance

This chapter includes the following topics:

About Insight Surveillance web application

Arctera Insight Surveillance manages monitoring, searching, retrieval, and reporting of emails and messages. It is designed to fulfill diverse regulatory requirements for supervising electronic communications.

Arctera Insight Surveillance serves as a web-based alternative for the Insight Surveillance desktop application. It lets organizations perform cost-effective supervisory review of their employees' communications to ensure compliance with regulatory bodies. It greatly reduces audit review time, minimizes compliance risk and increases organizational efficiency for today's global enterprises.

This guide outlines the configuration and management of your Arctera Insight Surveillance environment, ensuring compliance with your organization's supervision needs for archived electronic communications.

Routine operations executed with Arctera Insight Surveillance

This section lists the regularly performed operations by the Arctera Insight Surveillance administrators and reviewers. Access the following link to understand the below-mentioned workflows in detail.

Arctera Insight Surveillance Administrator's Guide

- **Monitoring statistics on dashboard**
  Users can view the status summary of recently reviewed departments, pin or unpin departments to monitor review status, change the order of pinned departments, and access summaries for escalated items and searches and exports.
- **Managing employees and employee groups**
  Users can create and edit individual employee profiles and employee groups.
- **Managing departments**
  Users can search existing departments, create new departments, move existing departments under others, and delete departments. Furthermore, users can monitored employees and groups, edit monitoring policies, department details, and monitoring policy details, manage exception employees, designate exception status to employees, assign exception reviewers, remove exception status and reviewers, and enable or disable departments for monitoring.
- **Managing (configuring) department users**
  Users can assign individuals to departments, remove users from departments, add new roles for users, remove roles, and manage role assignments for a user within departments.
- **Managing department and application-level searches**
  Users can follow guidelines for effective searches, create and execute department-level searches, pause and resume searches, download search details for archives, disable scheduled searches, preview search results, accept or reject search results, and resubmit searches as needed.
- **Managing search schedules**
  Users can set up new search schedules, including both one-time and recurring schedules. Additionally, they can edit and delete existing search schedules as needed.
- **Managing department and application-level hotwords and hotwords sets**
  Users can create new hotwords and hotwords sets, modify the existing ones, and delete them if no longer needed.
- **Managing department and application-level archives**

Users can customize (include and exclude) Enterprise Vault Archives that Arctera Insight Surveillance uses to search for items. Users can set searchable archives for each department and synchronize these archives manually besides the routine synchronization.

- **Managing department and application-level labels**
  Users can create new labels, modify the existing ones, activate them for use, and deactivate them if no longer needed.
- **Managing department and application-level review comments**
  Users can add new review comments, modify the existing ones, and delete them if no longer needed.
- **Managing users, roles, and permissions**
  Users can leverage predefined roles and permissions, add new roles for both individual users and employee groups, edit user roles and permissions, delete user roles, assign roles to users and employee groups, restrict users from using hotwords in searches, and remove assigned user roles.
- **Managing exports**
  Users can export the review items from Arctera Insight Surveillance if you want to review items offline or present them as evidence to a third party.
- **Managing reviews**
  Users can rearrange columns in the item list pane to customize the display based on their preferences.
  They can filter items by selecting the required facets, facilitating focused attention on specific content. Reviewing *Audio-Video Transcript* type items is made efficient, along with checking tags and hotwords statistics for comprehensive analysis.
  Users have the flexibility to add or remove text for machine learning purposes, and they can assign review status to items seamlessly. Furthermore, users can view hotwords highlighting, both within the content and collaboration messages, as well as tags highlighting and tags within collaboration messages.
  The platform allows users to open the full content in a new window, add comments to items, and escalate review items when necessary. The history of items can be easily reviewed, and users have options for printing, downloading items, and their attachments.
  Most importantly, users can access the *intelligent review details* for a comprehensive understanding of the reviewed content.
- **Managing reports**
  Though the SSRS reports support is discontinued, users can access the previously SSRS reports. In addition, users can access OData reports and a few enhanced report by using various APIs.

- **Managing Audit Settings**
  Users can control the configuration settings for the Enhanced Auditing feature. However, it is possible if the Auditing feature is configured and enabled in the system.
- **Working with Audit viewer**
  If the Enhanced Auditing feature is set up and activated for a customer, audit records for that customer are transmitted to the audit server when specific operations and modifications occur in the modules selected in the Audit Settings.
  Logging includes changes made in Arctera Insight Surveillance, Surveillance, or both. The Audit viewer allows users to search and export audit records for various modules and operations at the application, department, and folder levels.

About Arctera Insight Surveillance system security

For enhanced system security, Arctera Insight Surveillance implements the following measures:

- **Temporarily stored data encryption**: Arctera Insight Surveillance encrypts sensitive customer data stored in temporary storage to ensure heightened security.
- **Federal Information Processing Standards (FIPS) compliance**: Arctera Insight Surveillance adheres to the US Federal Information Processing Standards (FIPS) to maintain data security.

Feature comparison: Arctera Insight Surveillance desktop application Vs Arctera Insight Surveillance web application

If you previously used the Arctera Insight Surveillance desktop application and would like to examine the features of both the Insight Surveillance desktop application and the Arctera Insight Surveillance web application, refer to the table provided below.

Feature	Arctera Insight Surveillance Desktop Application*	Arctera Insight Surveillance Web Application	Details
Only server installation required	No	Yes	Accessing Arctera Insight Surveillance does not require application installation; server installation alone is sufficient.
Windows-based Authentication and Authorization	Yes	Yes	

* The features listed in the Enterprise Vault Compliance Accelerator Desktop Client (known as Arctera Insight Surveillance Desktop Application from Enterprise Vault 15.2 onwards) are available only up to Enterprise Vault version 14.5.

Dashboard			
Dashboard: Summary	Yes	Yes	
Dashboard: Summary: Pin/Unpin Departments	No	Yes	
Dashboard: Task	Yes	No	Links are provided to perform some tasks.
Departments			
Department: User Summary	Yes	Yes	
Department: User Action	Yes	Yes	
Department: Department Attributes	Yes	No	
Department: Role assignment	Yes	Yes	
Department: Searches	Yes	Yes	
Department: Searches: Custom Attributes	No	Yes	
Department: Monitoring Employees	Yes	Yes	
Department: Archives	Yes	Yes	

Feature	Arctera Insight Surveillance Desktop Application*	Arctera Insight Surveillance Web Application	Details
Department: Export	Yes	Yes	
Department: Hotwords	Yes	Yes	
Department: Labels	No	Yes	
Department: Review Comments	No	Yes	
Research Folders	Yes	No	
Employees	Yes	Yes	Profile creation and management
Reports	Yes	Partially yes	
Monitor	Yes	Yes	
Application			
Application: Roles	Yes	Yes	
Application: Roles Assignments	Yes	Yes	
Application: Hotwords	Yes	Yes	
Application: Label	No	Yes	
Application: Reviewing Comments	Yes	Yes	
Application: Searches	Yes	Yes	
Application: Archives	Yes	Yes	
Review			
Review: Review Pane Actions	Yes	Yes	Copy action is not available in Arctera Insight Surveillance.
Review: Advanced Filter	No	Yes	Filter on Author/Domain and Subject is provided.
Review: Filters	Yes	Yes	

Feature	Arctera Insight Surveillance Desktop Application*	Arctera Insight Surveillance Web Application	Details
Review: Filters: Sentiment Score	No	Yes	
Review: Delegate review (on behalf of mode)	Yes	No	
Review: Printable View	Yes	No	
Review: Bulk Review	Yes	Yes	
Review: Review Status	Yes	Yes	
Review: Research folder review	Yes	Yes	Some actions, such as Escalate, Commit, and Copy are not available in Arctera Insight Surveillance.
Review: Hit highlight navigation for Hotwords	Yes	Yes	
Review: Labels	No	Yes	
Review: Review Comments	No	Yes	
Review: Hit highlight navigation for Tags	No	Yes	
Configuration			
Configuration: Search Schedules	Yes	Yes	
Configuration: Reviewing status	Yes	No	
Configuration: Import configuration	Yes	No	
Configuration: Account Information	Yes	No	
Configuration: Directory Mappings	Yes	No	

Feature	Arctera Insight Surveillance Desktop Application*	Arctera Insight Surveillance Web Application	Details
Configuration: Department partitions, Attributes	Yes	No	
Configuration: Message Types	Yes	No	
Configuration: Settings	Yes	No	
Configuration: Audit settings	No	Yes	Modules can be enabled or disabled for auditing purposes.
Enhanced Auditing	Yes	Yes	
Audit Viewer	No	Yes	The operations and modifications made to any modules are shown in the **Audit Settings**.
Hotword analysis and statistics	Yes	Yes	Hotword analysis is done, and filters and counts are updated to view the statistics.
Tag (Policy) analysis and statistics	No	Yes	Tag (Policy) analysis is done, and counts are updated to view the statistics.
Custom attributes	Yes	Yes	
Intelligent Review	Yes	Yes	
Advanced Intelligent Review	No	Yes	The relevance score and the reasoning behind classifying the item as Unreviewed Relevant or Unreviewed Irrelevant are provided. Content snippets are added to train the learning model.
Microsoft Teams Chat and Channel support	No	Yes	

Feature	Arctera Insight Surveillance Desktop Application*	Arctera Insight Surveillance Web Application	Details
Audio-Video Transcript support	No	Yes	
Chinese Wall security	Yes	No	
Localization of UI and Documentation	Yes	No	Insight Surveillance user interface and user documentation are translated into Japanese, Chinese Simplified, and Chinese Traditional languages for localization purposes.

Product documentation

Table 1-1 lists the documentation that accompanies Insight Surveillance. This documentation is also available in PDF and HTML format in the Arctera Documentation Library.

Table 1-1 The Insight Surveillance documentation set

Document	Comments
Installation Guide	Outlines how to perform a first-time installation of the Insight Surveillance server and web client.
Upgrade Instructions	Explains how to upgrade an existing installation of Insight Surveillance.
Administrator's Guide	Provides information for Insight Surveillance administrators on how to set up and assign roles, search for items to include in the review set, export items for offline review, create reports, and more.
Online Help	Accompanies all the Insight Surveillance applications and provides extensive information on how to use their facilities.
Release Notes	Provides late-breaking information that you may need to be aware of before you install and use Insight Surveillance.

Table 1-1 The Insight Surveillance documentation set *(continued)*

Document	Comments
Arctera Insight Surveillance User Guide	Provides information on how to use all the key features of Arctera Insight Surveillance.
Arctera Insight Surveillance Reviewer's Guide	Describes the features of Arctera Insight Surveillance that are available to reviewers.

White papers on the Arctera Support website

The following white papers on the Arctera Support website provide more information on some of the features that this guide describes.

Table 1-2 White papers on the Arctera Support website

White paper	Describes
Accelerator Deduplication	The deduplication features in Insight Surveillance.
Best Practices for Enhanced Accelerator Reporting	How to create custom Insight Surveillance reports using the Open Data (OData) protocol.

Chapter 2

Configuring Insight Surveillance: Desktop Client

This chapter includes the following topics:

Customizing the reviewing action statuses

You can customize the status names with which Insight Surveillance shows the status of items in the **Review** pane.

Table 2-1 Default status names and access keys

Action status	Appraisal status	Escalation status
Unreviewed	Not Appraised	Not Escalated
Pending (Alt+P)	Appraised (Alt+A)	Escalated (Alt+E)
Questioned (Alt+Q)		Closed (Alt+C)
Reviewed Relevant (Alt+R)		
Reviewed Irrelevant (Alt+I)		

You can rename these statuses, change their descriptions, and, in most cases, assign different access keys to them. When pressed in combination with the Alt key, an access key lets reviewers assign a specific status mark to an item in the Review pane. For example, the key combination Alt+P typically assigns the Pending mark to an item. You can also change the navigation keys with which reviewers can select the next item or previous item in the pane.

You must have the Modify System Configuration permission to configure the reviewing statuses. By default, users with the role of Compliance System Admin have this permission.

To customize the reviewing action statuses

1 Click the **Configuration** tab in the Insight Surveillance client, and then click the **Reviewing Statuses** tab.

2 In the left pane, click the name of the status mark or navigation key that you want to change.

You cannot mark a message as Unreviewed, Not Appraised, or Not Escalated, so none of these statuses has an access key or a button in the **Review** pane.

3 Enter the new details.

Note that the names appear on the status mark buttons in the **Review** pane. It is therefore advisable to keep them short so that they do not disturb the page display.

4 Click **Save**.

Importing configuration data from an XML file

This section describes how the configuration data can be imported from an XML file.

About importing configuration data

As part of the process of setting up Insight Surveillance, you must enter configuration data on employees, departments, partitions, roles, and so on. If this data already exists outside Insight Surveillance and is convertible to XML format, you can import it into Insight Surveillance from an XML file. Then you can quickly load large amounts of configuration data that might otherwise be time-consuming to enter.

You can also use the import facility to load predefined hotwords and phrases from some XML files that come with Insight Surveillance.

Sample XML files

The Insight Surveillance server software comes with a number of sample XML files. These files are in the `AcceleratorAdminWeb\Installation` subfolder of the Insight Surveillance program folder (typically `C:\Program Files (x86)\Enterprise Vault Business Accelerator`).

Table 2-2 describes the sample XML files.

Table 2-2 Sample XML files

File	Function
`Dataload.xml`	Explains how to load department and employee data to create a flat department structure.
`Dataload_tree.xml`	Gives an example of how to load the data to create a structured organization with nested departments.
`DataLoadCaptureExclusions.xml`	Gives some examples of how to exclude certain file types from review sets.

Format of the Dataload.xml file

You can use the `Dataload.xml` file with both Surveillance and eDiscovery, so it contains some information that applies to both applications. However, the file is well documented and shows which sections apply to which application.

Table 2-3 Primary Insight Surveillance sections in Dataload.xml file

Section	Defines
ApplicationVaultStore	Vault stores that the application uses. This section is mandatory.

Table 2-3 Primary Insight Surveillance sections in Dataload.xml file *(continued)*

Section	Defines
CaptureExclusions	Types of items, such as non-delivery reports and out-of-office replies, that Insight Surveillance is not to capture and add to the review set.
Employee	Employees to add to the system, their email addresses, and any application roles to assign to them. Employees are identified using the EmployeeID field, which equates to the **Employee ID** box in the employee properties page of the Insight Surveillance client. If you create some profiles using the Insight Surveillance client and later want to update them using an XML file, ensure that each employee has a unique ID.
EmployeeGroup	Employee groups, their members, and any application roles that are assigned to each group.
HotWordCategory	Global hotwords sets.
Attribute_n_Definition	Identity attributes that, when used in combination with the filter options in the Departments pane, let you hide or show selected departments in that pane.
Department	Departments. This section includes definitions of the following: ■ Department members and exception employees ■ The required review percentage for the department, groups, and individuals ■ Department roles that are assigned to individuals or groups ■ Vault stores for the department ■ Department hotword sets
Partition	Partitions, and the departments in them.
Proxy	Delegates for reviewers and compliance supervisors.
StandardReviewComment	Common comments that reviewers can add to the items that they review.

The second part of the file describes each XML entry. The last part of the file provides sample entries for a Insight Surveillance system.

If you use any non-ASCII characters in a dataload file, you must specify the appropriate encoding. For example, you can save a file that contains accented European characters in Unicode format or add the following at the start of the file:

```
<?xml version="1.0" encoding="iso-8859-1" ?>
```

Importing the configuration data

You must have the Import Configuration Data permission to import configuration data from an XML file. By default, users with the application role of Compliance System Admin have this permission.

To import configuration data from an XML file

1. Click the **Configuration** tab in the Insight Surveillance client, and then click the **Import Configuration** tab.
2. In the **Configuration file** box, type the full path to the XML file that you want to import, or click **Browse** and then choose the file to import.

   The path can contain up to 250 characters.

   You can specify a UNC path or NTFS path to the file if it is stored on a remote computer. For example:

   ```
   \\server2\EVBA\import.xml
   ```
3. If you want to clear the import information from previous imports before you proceed, select **Clear log before import**.
4. Click **Import**.

Specifying the Windows domains with which to synchronize employee details

You can specify multiple Windows domains with which Insight Surveillance synchronizes the details of employees and employee groups. The domains also appear in the list from which you can choose when you add a new employee and browse for the corresponding Windows account.

You must have the Modify System Configuration permission to specify the Windows domains. By default, users with the application role of Compliance System Admin have this permission.

To specify the Windows domains with which to synchronize employee details

1. Click the **Configuration** tab in the Insight Surveillance client, and then click the **Account Information** tab.
2. Click **New** at the top of the window.
3. In the **Domain Name (NETBIOS)** box, type the NetBIOS name of the Active Directory domain.
4. In the **Enter the fully qualified domain names** box, type any DNS fully qualified domain names that you want to map to the NetBIOS name.
5. If you want to use a specific account when you connect to the domain, type the name and password of the account in the **Account Information** area.

   By default, when synchronizing with Active Directory, Insight Surveillance uses the service account under which the eDiscovery Manager service is running.
6. To force Insight Surveillance to use a specific server instead of attempting to find the global catalog automatically, select **Use the following Global Catalog server** and then specify the required server.
7. Click **Save**.

Mapping employee properties to Active Directory or Domino directory attributes

Each employee profile in Insight Surveillance comprises a number of properties, some of which correspond to Active Directory or Domino directory attributes.

Table 2-4 lists the employee properties that Insight Surveillance maps to the directory attributes by default.

Table 2-4 How employee properties map to Active Directory or Domino directory attributes

Employee property	Active Directory attribute	Domino directory attribute
Department	department	department
Display Name	displayName	cn
First Name	givenName	Givenname
Middle Name	initials	middleinitial

Table 2-4 How employee properties map to Active Directory or Domino directory attributes *(continued)*

Employee property	Active Directory attribute	Domino directory attribute
Surname	sn	sn
Title	title	Personaltitle

When configuring an employee profile, you can choose whether Insight Surveillance should automatically synchronize these properties with the corresponding attributes.

You can also set up mappings for the following optional properties: Start Date, End Date, and Employee ID. The Employee ID property is mandatory if you want to import department and employee data by using XML files.

See "About importing configuration data" on page 20.

You must have the View System Configuration permission to view the existing mappings, and the Modify System Configuration permission to change them. By default, users with the role of Compliance System Admin have both permissions.

To view and modify an existing directory mapping

1 Click the **Configuration** tab in the Insight Surveillance client, and then click the **Directory Mappings** tab.

2 In the left pane, click the employee property whose mapping you want to modify.

3 In the right pane, choose whether to synchronize the employee property with Active Directory, Domino directory, or both.

4 Type the names of the Active Directory and Domino directory attributes with which to synchronize the employee property.

5 If you want to synchronize with both Active Directory and Domino directory, nominate one of them as the preferred source.

6 Click **Save**.

7 Restart the Enterprise Vault eDiscovery Manager service on the Insight Surveillance server to put the new mapping or changed mapping into effect.

Grouping departments into partitions

You can group departments into partitions to restrict the scope of searches. For example, you may find this facility useful if you want to restrict searching in some departments to items to and from certain other departments.

If you do not define any department partitions, the searches that you initiate in one department can include the items of employees in other departments. When you define partitions, searches are restricted to items to and from monitored employees in departments in the same partition.

You can also create department partitions by specifying the details in an XML configuration file. Then you can import this file into the Insight Surveillance database.

See "Importing the configuration data" on page 22.

Creating department partitions

You must have the Manage Department Partitions permission to create a partition. By default, users with the application role of App User Admin have this permission.

To create a department partition

1. Click the **Configuration** tab in the Insight Surveillance client, and then click the **Department Partitions** tab.
2. Click **New** at the top of the window.
3. Type a name and description for the partition.
4. Click **Add** to select the departments that you want to include in the partition.
5. Click **Save**.

Editing department partitions

You can change the name and description of a partition and add or remove departments.

You must have the Manage Department Partitions permission to edit a partition. By default, users with the application role of App User Admin have this permission.

To edit a department partition

1. Click the **Configuration** tab in the Insight Surveillance client, and then click the **Department Partitions** tab.
2. In the left pane, click the name of the partition that you want to edit.

3 In the right pane, change the details of the partition as necessary.

4 Click **Save**.

Deleting department partitions

When you have no further use for a partition, you can delete it. Deleting the partition does not delete the departments that belong to it.

You must have the Manage Department Partitions permission to delete a partition. By default, users with the application role of App User Admin have this permission.

To delete a department partition

1 Click the **Configuration** tab in the Insight Surveillance client, and then click the **Department Partitions** tab.

2 In the left pane, click the name of the partition that you want to delete.

3 Click **Delete** at the top of the window.

Setting up department attributes

A standard Insight Surveillance system comes with the following attributes that you can apply to your departments: Country, City, and Division. You can rename these attributes, supply values from which department administrators can choose when they assign the attributes to their departments, and more.

You must have the View System Configuration permission to view the properties of each attribute, and the Modify System Configuration permission to change them. By default, users with the application role of Compliance System Admin have these permissions.

To set up department attributes

1 Click the **Configuration** tab in the Insight Surveillance client, and then click the **Department Attributes** tab.

2 In the left pane, click the name of the attribute that you want to set up.

3 In the right pane, type the name and an optional description for the attribute.

The name cannot contain the following characters:

*** ? < > |**

4 If you want to make the attribute available for selection when you define the properties of a department, select **Visible**.

5 If you want to permit users to enter a free-text value for the attribute instead of choosing from a predefined list, select **Allow free text values to be entered**.

6 If you have nested departments, choose the required behavior in child departments when you change the attribute value assigned to a parent department. The options are as follows:

Do nothing	No change is made to the values that are assigned to associated child departments.
Copy value to child departments if not set	The same value is only set for the child departments that do not have a value set for this attribute.
Overwrite value on all child departments	The same value is set for all child departments, regardless of any value that is set for this attribute.

7 If you want to change the values from which users can choose when they set the attribute in department properties pages, do the following:

- To add a new value, click **New** and then type the required name and description.
- To edit an existing value, click it and then click **Edit**. Insight Surveillance automatically updates the properties of any department to which you assigned the value.
- To delete an existing value, click it and then click **Delete**. Insight Surveillance automatically removes the value from the properties of any department to which you assigned it.

8 Click **Save**.

Setting up custom message types

Insight Surveillance lets you search, filter, and export items for message types Bloomberg, Domino Mail, Exchange Mail, Fax, File, Instant Messaging, SharePoint, SMTP Mail, Microsoft Teams chat, Microsoft Teams channel, Audio-Video transcript, and Social. Other than these message types, you can set up custom message types such as Facebook, Twitter and so on.

The **Configuration** tab in the Surveillance client includes a new tab that is called **Message Types** that lets you add custom message types. These custom message type names appear in the following places in the Insight Surveillance client:

- In the **Review** tab, under the **Type** facet in the Filter pane.

- In the **Application** tab, under the **Message type** option in the Miscellaneous section of the **Searches** pane.
- In the **Departments** tab, under the **Message type** option in the Items Selection box of the **Export Details** pane.

You must have the Manage Message Types permission to view the **Message Type** tab in the **Configuration** tab. By default, only users with the role of App Rule Admin, App User Admin and Compliance System Admin have this permission.

To set up custom message types

1. Click the **Configuration** tab in the Insight Surveillance client, and then click the **Message Types** tab.
2. Click **New**.
3. In the **Message Type Details** pane type a name and value for the message type.

   The name cannot contain any of the following characters:

   \ / : * ? " < > |
4. Click **Save**.

Setting Insight Surveillance system configuration options

Insight Surveillance provides hundreds of configuration options with which you can customize the appearance and performance of the application. These configuration options are grouped into categories, as Table 2-5 explains.

Table 2-5 Configuration settings by category

Category	Function
Ad Hoc Searches	Configure the searches that users can initiate from their research folders.
Auditing	Specify the Audit Server URL and enable or disable the Enhanced Auditing feature. If enabled, the modifications made in the audit modules will be recorded and can be viewed or exported later in &ProductNameLong;.
Diagnostics	Enable or disable the Insight Surveillance troubleshooting facilities.

Table 2-5 Configuration settings by category *(continued)*

Category	Function
Document Conversion	Customize the error messages that Insight Surveillance displays in the Review pane when it cannot open an item in the preview window of that pane.
Export/production	Configure the output when users export or produce items from Insight Surveillance for offline review.
General	Configure general Insight Surveillance options.
Home Page	Control the appearance of the Home page of Insight Surveillance.
Hotword Analysis	Enable or disable the analysis of hotwords in Insight Surveillance.
Item Prefetch Cache	Configure the primary settings for the Insight Surveillance prefetch cache mechanism. This mechanism is designed to speed up the rendering of items in the Review pane.
Item Prefetch Cache (Advanced)	Configure advanced settings for the prefetch cache mechanism.
Policy Integration	Integrate Insight Surveillance with your policy management software to better flag items for inclusion in or exclusion from the review set.
Profile Synchronization	Control how Insight Surveillance synchronizes user profiles with the corresponding Active Directory or Domino directory accounts.
Random Capture	Configure the random sampling of messages.
Reviewing	Customize the appearance and functionality of the Review pane.
Search	Optimize the search features in Insight Surveillance.
Security	Implement Chinese walls security restrictions on what users can access in Insight Surveillance. You can also choose whether to make the SQL Server sysadmin logon the creator and owner of Insight Surveillance search schedules.
System	Record the dates on which you installed Enterprise Vault and began to archive data, and more.
Vault Directory Synchronization	Configure when Insight Surveillance synchronizes with the Enterprise Vault archives.

You must have the Modify System Configuration permission to change the configuration settings. By default, only users with the role of Compliance System Admin have this permission.

To set Insight Surveillance system configuration options

1. Click the **Configuration** tab in the Insight Surveillance client, and then click the **Settings** tab.
2. Click the plus sign at the left of a section name to list the associated settings.

   Alternatively, type some characters in the filter box at the top of the window to search for the configuration options that contain those characters. For example, type **Colour** to find all the options that contain this word in their names.
3. For each setting whose value you want to change, do the following in the order listed:
   - Click the value in the **Value** column.
   - Set the required value.
   - Click outside the **Value** column.
4. When you have set all the required options, click **Save**.
5. If you have changed any setting that has a tick in its **Restart Required** column, restart the Enterprise Vault eDiscovery Manager service on the Insight Surveillance server to put your changes into effect.

Ad Hoc Searches configuration options

Use these settings to configure the searches that users can initiate from the research folders that they have created.

Ad-hoc search Pre-fix	Specifies the prefix to add to the names of ad-hoc searches that users save to the review set.
Allow hits to be deleted from an Ad-Hoc search result	Specifies whether users can delete the items from a folder search before they accept the search into the review set. By default, Insight Surveillance lets users delete the items.
Allow users to commit items without committing audit history	Specifies whether reviewers can commit items from their research folders to the review set without also committing the associated review marks and comments. This option is only used if you select "Commit All Audit History When Committing An Item". By default, Insight Surveillance expects users to commit the marks and comments when they commit items to the review set.

Commit All Audit History When Committing An Item	Specifies whether reviewers must commit the full audit history when committing items from their personal folders to the review set. By default, Insight Surveillance lets users choose the elements that they want to commit.
Require Export permission in Department for Export permission in Folder	Specifies whether to limit the export facility in a folder to those users who have export permissions in the associated department. By default, Insight Surveillance does not require users to have this permission.
Require Review permission in Department for Review permission in Folder	Specifies whether to limit the review facility in a folder to those users who have review permissions in the associated department. By default, Insight Surveillance does not require users to have this permission.
Require Search permission in Department for Search permission in Folder	Specifies whether to limit the search facility in a folder to those users who have search permissions in the associated department. By default, Insight Surveillance does not require users to have this permission.
Show shared folders to Delegates	Controls the extent to which delegates can access the folders to which their principal reviewers have access. By default, all folders that a principal owns are automatically available to delegates. However, any other folders to which the principal has access are not available. If you want delegates to have access to these shared folders, change this setting.

Diagnostics configuration options

Use these settings to enable or disable the Insight Surveillance troubleshooting facilities.

Enable performance monitor	Specifies whether to report Insight Surveillance performance data, which you can view with the Windows Performance Monitor utility.
Enable tracing	Specifies whether to record every server action in the event log. Tracing to the event log applies to information events only, as Insight Surveillance always records all error messages and warning messages in the log.

Save deduplication information	Specifies whether to generate deduplication information files in a `DeduplicationInfo` subfolder of your Insight Surveillance program folder on the Insight Surveillance server (typically, `C:\Program Files (x86)\Enterprise Vault Business Accelerator\DeduplicationInfo`). These deduplication information files, which are in plain text and XML format, may assist the Arctera Support team when dealing with deduplication-related problems. By default, this setting is cleared; Insight Surveillance does not create the files.
Save Search Criteria	Specifies whether to generate search criteria files in a `SearchCriterias` subfolder of your Insight Surveillance program folder on the Insight Surveillance server. These files, which are in plain text and XML format, may assist the Arctera Support team when dealing with search-related problems. By default, Insight Surveillance does not create the files.
Save XML Search Items To Commit	Specifies whether to save the XML files of the items to commit to the database under a subfolder of the server. By default, Insight Surveillance does not save the XML files.
Save XML Search Results	Specifies whether to generate search results files (one for each Enterprise Vault archive that is searched) in a `SearchResults` subfolder of your Insight Surveillance program folder on the Insight Surveillance server. By default, Insight Surveillance does not create the files.

Document Conversion configuration options

Use these settings to customize the error messages that the Review pane of the Insight Surveillance client may display.

Conversion Errors	Specify the error messages to display if Insight Surveillance cannot display an item in the preview window of the Review pane. Each message can contain up to 200 characters.

Export/production configuration options

Use these settings to configure the output when users export items from Insight Surveillance for offline review.

Add Bate identifier to File System exports	Specifies whether to add an identifying Bates number to the file name of each exported item that Enterprise Vault has archived through File System Archiving (FSA). The options are as follows: ■ 0. Omit the Bates number. ■ 1. Add the Bates number to the start of the file name. This option is the default option. ■ 2. Append the Bates number to the end of the file name.
Always date stamp exported File System items	Specifies whether to append a last-modified date stamp to the file name of each exported item that Enterprise Vault has archived through File System Archiving (FSA). By default, Insight Surveillance appends the date stamp.
Automatic retry: Maximum retries	Specifies the maximum number of attempts that Insight Surveillance makes to repeat an export run that failed for any reason. Set the value to 0 to stop Insight Surveillance from retrying the run.
Automatic retry: Minimum time between retries (minutes)	Specifies the minimum delay in minutes between automatic attempts to repeat a failed export or production run. By default, Insight Surveillance waits five minutes between retries. Note that Insight Surveillance multiplies this value by the number of retries. So, if this value is 5, the delay between retries starts at five minutes and increases to 10, 15, and so on with subsequent retries.
Custom conversion extension	Specifies the file name extension of the files to create when exporting items for viewing outside Insight Surveillance. For example, you would specify `.xls` as the extension for export files in Microsoft Excel format.

Custom conversion file	Specifies the name of the template file to use when exporting files in their custom format. For example, if you have created a template file for exporting items in Microsoft Excel format, you can enter `ExcelReport.xslt` as the file name.
Default export folder	Specifies the default folder on the Insight Surveillance server to use for exported items. If you do not specify a default export folder, Insight Surveillance uses the folder `c:\Insight Surveillance Export\`*`customer_name`*. The folder path can contain up to 100 characters.
Default Production status	Specifies the status that you want to set as the default current status when you perform an export run. Type one of the following values: ■ 0. N/A ■ 1. Pending ■ 2. Reviewed ■ 3. Questioned
Default to Unicode for PST and MSG	Specifies whether to export PST and MSG files in Unicode (Outlook 2003 and later) format or ANSI (Outlook 97 through 2002) format. By default, Insight Surveillance exports the items in Unicode format.
Domino Export Template	Specifies the name of the file to use as a template when exporting files to a Notes Database Template (NTF) file. The default file name is `accelexp.ntf`.
Domino ID File	Specifies the name of the `.id` file that is used for local Domino authentication when exporting files to an NTF file. The default file name is `Accelerator.id`.
Domino Password	Specifies the password that is used for local Domino authentication when exporting files to an NTF file.
Enable Production threads	Specifies whether to enable or disable all exporting and production facilities. By default, Insight Surveillance enables these facilities.

HTML conversion file	Lets you download, edit, and then upload an XSL style sheet. This style sheet serves as the template for all the export reports that Insight Surveillance generates in HTML format.
Maximum production retry for items stored on slow devices	Specifies the number of attempts that Insight Surveillance makes to retrieve an item from an offline device, such as a tape drive, before giving up. Enter a value between 1 and 1000, where the default is 120.
Minimum number of minutes between retries for items stored on slow devices (min)	Specifies the number of minutes that Insight Surveillance waits between retry attempts when trying to retrieve an item from an offline device. Enter a value between 1 and 300, where the default is 5.
Number of production report threads	Specifies the number of threads that Insight Surveillance assigns to generating reports of export runs. The default is 5.
Number of production threads per production run	Specifies the number of threads in the SQL connection pool that Insight Surveillance assigns to each export or production run. Enter a value in the range 1 to 25, where the default is 25. See also the configuration setting "Total number of production threads per customer". To determine the maximum number of export or production runs that you can conduct simultaneously, divide the "Total number of production threads per customer" by the "Number of production threads per production run". For example, if you specify 100 for the first setting and 25 for the second setting, you can conduct up to four export or production runs simultaneously. If you try to conduct further export or production runs, Insight Surveillance holds them in a queue until the required number of threads is available.
Production order Search by RunDate	Sets the order in which Insight Surveillance lists the searches when you set the criteria for an export run. You can choose to sort the searches by name or by run date. By default, Insight Surveillance sorts the searches by name.

PST ExportID Column Name	In Microsoft Outlook, specifies the label for the column in which to show Insight Surveillance export IDs. The default label is "Bate Number". When you export items from Insight Surveillance as a Personal Folders (`.pst`) file, and then import this file into Outlook, the export IDs of the items appear in this column.
PST Folder Name	Specifies the Outlook folder in which to place the items after you import a Personal Folders (`.pst`) file that you exported from Insight Surveillance.
Report chunk size	Specifies the number of exported items to list in each report file. The default is 25000.
Show PST version option on export run	Specifies whether, when you undertake an export run, Insight Surveillance prompts you to select a PST version: Outlook 97-2002 (ANSI) or Outlook 2003 (Unicode). By default, Insight Surveillance does not display the prompt.
TAB Conversion file	Lets you download, edit, and then upload an XSL style sheet. This style sheet serves as the template for all the export reports that Insight Surveillance generates in tab-separated format.
Total number of production threads per customer	Specifies the maximum number of threads per customer that Insight Surveillance assigns when it conducts export or production runs. Enter a value between 50 and 1000, where the default is 100. See also the configuration setting "Number of production threads per production run".

General configuration options

Use these settings to configure general Insight Surveillance options.

Add User page refresh time	Specifies the frequency in seconds with which Insight Surveillance refreshes the Select User dialog box. This dialog box lets you select a user account to add to Insight Surveillance. It appears when you click **Browse** in the properties page for an employee. Specify a value between 1 and 300, where the default is 10.

Display warning in Archives pane when number of archives to load exceeds this threshold	Specifies a threshold count for the number of archives to load in the Archives To Search pane of the Insight Surveillance client. If the number of archives that match the current selection and filter criteria exceeds this threshold, a warning message prompts you to change the criteria and reduce the number of archives. Specify a value in the range 50,000 to 200,000. The default is 50,000.
Enable deduplication in search	Specifies whether to deduplicate the items in search results. By default, with this setting selected, Insight Surveillance deduplicates the items. Note that Insight Surveillance does not deduplicate randomly-sampled items.
Hide Active Directory accounts ending with '$' in account selector	In areas of Insight Surveillance where you select an Active Directory account, specifies whether to show any accounts whose names end with the character $. By default, Insight Surveillance shows these accounts.
List searches without sampled hits in filters	When you filter items by search, specifies whether to omit from the list those searches that failed to capture any items. By default, Insight Surveillance shows these searches.
Show First Name followed by Last Name	Specifies the order in which to display the first and last names of employees. By default, the first name precedes the last name. You may want to clear this option when working in countries where the names are typically reversed, such as Japan.
Show search sample counts in filters	In areas of Insight Surveillance such as the Review pane, specifies whether to append the sample size to the name of each listed search. So, if a search has 200 hits, and your monitoring policy requires you to add 10% of captured items to the review set, Insight Surveillance shows the search as "My Search [20]". By default, Insight Surveillance shows the sample size.

Home Page configuration options

Use these settings to control the appearance of the Home page of Insight Surveillance.

List Exceptions On Home page	Specifies whether to hide or show the list of individual exceptions on the Insight Surveillance home page. By default, Insight Surveillance lists the exceptions.
Maximum number of exports to show on home page	Sets a limit on the number of export runs that Insight Surveillance can list in the home page of the application. The default is 30.
Maximum number of searches to show on home page	Sets a limit on the number of searches that Insight Surveillance can list in the home page of the application. The default is 30.
Maximum task age (days) to show on home page	Specifies the maximum age of the data that Insight Surveillance can display for tasks in the home page of the application. The default is 30 days.
Show Department 'All Container' Review Link	Specifies whether to display an **All Departments** link at the top of the **Review Messages** column on the Insight Surveillance home page. By default, Insight Surveillance displays the link.
Show Escalation 'All Container' Review Link	Specifies whether to display an **All Departments** link at the top of the **Escalated Messages** column on the Insight Surveillance home page. By default, Insight Surveillance displays the link.
Show Folders on Home Page	Specifies whether to list individual research folders on the Insight Surveillance home page. By default, Insight Surveillance lists the folders.
Show Reviewers' statistics to reviewers	Specifies whether reviewers can see the statistics for other reviewers on the home page of the application. By default, all reviewers can see these statistics.

Hotword Analysis configuration options

Enable or disable the analysis of hotwords in Insight Surveillance.

Enable analysis of hotwords	Specifies whether to enable the analysis of hotwords for items in review. By default, Insight Surveillance analyses and displays the statistics of hotwords that are found in each item.

Item Prefetch Cache configuration options

Use these settings to configure the Insight Surveillance prefetch cache mechanism. This mechanism retrieves and caches items from the vault store during a scheduled window every night, instead of retrieving each item when the user chooses to review it. The cache therefore helps to speed up the rendering of items in the Review pane. You can specify the size, location, and other characteristics of the cache.

To optimize performance in an environment where you review items very intensively, we recommend the following:

- Use the fastest storage available and set aside a full partition so that there is no competition for I/O.
- Set the maximum size within the cache to match the partition size.
- Set the cache to 365 days before expiry.
- Set the cache to retrieve the full items with HTML and MSG. If you do not need to export the items, you can choose to retrieve the items with HTML only.

The Item Prefetch Cache options are the more commonly used cache options. You can also set the Item Prefetch Cache (Advanced) options.

Cache enabled	Specifies whether to enable or disable the prefetch cache. By default, Insight Surveillance disables the cache. Therefore, prefetching does not occur and the cache is not used for item retrieval, even if there are items in the cache. Only enable the cache for a Insight Surveillance database in which you actively review items or where you connect to slow storage for export runs. Note that the cache is either enabled or disabled for an entire database.

Cache location	Specifies the local path or network share path to the folder in which to store the cache. Within this folder, Insight Surveillance stores the prefetched files in a subfolder that is called `AcceleratorPrefetch_`*`CustomerId`*. Note the following: ■ We recommend that you specify a local path, where possible. If you must specify a network share path, always use the UNC path rather than a mapped drive. ■ The folder must already exist; Insight Surveillance does not create it. ■ In a hosting environment, multiple customers must not share the same folder.
Cache maximum item age (days)	Specifies the number of days for which items can remain in the cache before Insight Surveillance automatically deletes them. The item age is based on the creation time of the file in the cache, and not the time that Insight Surveillance captured the item or the time that the item was originally sent. The default age is 5 days. Insight Surveillance may remove an item from the cache earlier than the maximum item age if the cache becomes full.
Cache maximum size (Mbytes)	Specifies the maximum size of the cache in megabytes (MB). The default is 1000 MB. The larger the value of the "Cache maximum item age (days)" setting, the higher the cache maximum size must be to accommodate the items.
End prefetching time of day (server local time)	Specifies the time of day at which Insight Surveillance stops prefetching items. The default is 05:00 A.M. Use this setting with "Start prefetching time of day" to determine the hours of the day that prefetching is active. Configuring a period during which caching does not occur lets you undertake other maintenance activities during this period, such as performing Enterprise Vault backups. To make prefetching active at all times, set this option and "Start prefetching time of day" to the same time.

Start prefetching time of day (server local time)	Specifies the time of day at which Insight Surveillance starts to prefetch items. The default is 20:00 P.M. Use this setting with "End prefetching time of day" to determine the hours of the day that prefetching is active. Configuring a period during which caching does not occur lets you undertake other maintenance activities during this period, such as performing Enterprise Vault backups. To make prefetching active at all times, set this option and "End prefetching time of day" to the same time.

Item Prefetch Cache (Advanced) configuration options

These settings provide additional, advanced options for configuring the Insight Surveillance prefetch cache functionality. Use these settings with the Item Prefetch Cache options.

Cache encrypted	Specifies whether to encrypt files before they are stored in the cache. By default, Insight Surveillance does not encrypt the cache.
Cache purge time of day (server local time)	Specifies the time of day at which Insight Surveillance performs cache housekeeping (primarily removing old items). The default time is 19:00 PM.
Maximum capture age (days)	Excludes from the cache those captured items that are older than the specified number of days. The default is 3 days. This setting only has an effect when prefetching is first turned on, or if it has been disabled for some time and is then reenabled.
Maximum item fetch attempts	Specifies the maximum number of times that Insight Surveillance tries to prefetch an item before giving up. The default is 10.

Maximum item size to store in cache (bytes)	Sets a limit on the size of items and parts of items that Insight Surveillance can prefetch. If an item or part of an item exceeds this limit, it is ignored. The default is 10 MB. For example, Insight Surveillance still prefetches an item that has multiple attachments, none of which is bigger than 10 MB, even though the combined size of the attachments may greatly exceed the 10 MB limit.
Minimum time between item fetch retries (minutes)	Specifies the number of minutes that Insight Surveillance waits between attempts to prefetch items. The default is 30 minutes. Use this setting with "Maximum item fetch attempts" to configure retry behavior for failed fetches.
Prefetch attachments	Specifies whether to prefetch the attachments to items. By default, Insight Surveillance prefetches attachments. Note that attachments of nested items are not prefetched.
Prefetch attachments as HTML	Specifies whether to render attachments as HTML when prefetching them. By default, Insight Surveillance prefetches attachments as HTML.
Prefetch guaranteed sample search items	Specifies whether the results of guaranteed sample searches are eligible for prefetching. By default, they are.
Prefetch immediate search items	Specifies whether to prefetch the items that users have captured with an immediate, unscheduled search. By default, Insight Surveillance does not prefetch these items.
Prefetch Native format	Specifies whether to prefetch items in their original, native format. By default, Insight Surveillance does not prefetch the items in their native format. However, if your policy is to review items in their original format then you should enable this feature.
Prefetch Random Sampling items	Specifies whether the items that you have captured through random sampling are eligible for prefetching. By default, they are. For best results, ensure that prefetching is active for a suitable period after the nightly random sampling tasks are expected to complete.

Prefetch research items	Specifies whether to prefetch the items that users have placed in personal folders through ad-hoc searches. By default, Insight Surveillance prefetches these items.
Prefetch scheduled search items	Specifies whether to prefetch the items that users have captured with a scheduled search. By default, Insight Surveillance prefetches the items. Note that items are only prefetched when the search is accepted, so this option works best when scheduled searches are set to auto-accept.
Prefetch search items	Specifies whether to prefetch the items that users have captured with a search. You can further control this facility with the "Prefetch immediate search items" and "Prefetch scheduled search items" options. By default, Insight Surveillance prefetches the items.
Prefetch XML structure	Specifies whether to prefetch the XML structure of an item. This structure defines the parts of the item and includes a list of attachments (but not the attachments themselves). The XML structure is used for the preview pane in the Review pane. An XSL transform is applied to the XML to convert it to HTML. By default, Insight Surveillance prefetches the XML structure.
Render HTML for message review	Specifies whether to prefetch the items for review in HTML format. By default, Insight Surveillance prefetches the items in this format. Prefetching the items improves review performance because Insight Surveillance does not need to perform the rendering from XML to HTML at review time. The benefits of this are most likely to be noticeable on a system where many reviewers work concurrently.
Render printable HTML	Specifies whether to prefetch the printable versions of items in HTML format. By default, Insight Surveillance does not prefetch the items in HTML format. However, it is advisable to change the setting if you expect to use the printable view functionality regularly.

Retry record retention period (days)	Specifies how long Insight Surveillance keeps records of repeated, failed attempts to prefetch items. The default is 30 days.

Policy Integration configuration options

Use these settings to integrate Insight Surveillance with your policy management software to better flag items for inclusion in or exclusion from the review set.

Always show policy display in review grid	When you preview an item that has no associated policies in the Review pane, specifies whether to show the Policy field above the item. By default, Insight Surveillance hides this field when there are no associated policies.
Sort Policies within type	When you preview an item in the Review pane, specifies the order in which to list the associated policies in the banner above the item. Enter one of the following values: ■ 0. The policies are not sorted. ■ 1 (default). Insight Surveillance first groups the policies by policy type (inclusion, exclusion, and category) and then sorts them alphabetically within each type. ■ 2. The policies are sorted alphabetically, regardless of policy type. Changing the sort order does not affect the items that are already in the Accelerator database; only newly-added items are affected.

Profile Synchronization configuration options

Use these settings to control how Insight Surveillance synchronizes employee profiles with the corresponding Active Directory or Domino directory accounts.

Automatically detect deleted profiles and mark them as deactivated	Specifies whether Insight Surveillance should automatically deactivate those employee profiles for which it cannot find a corresponding Active Directory or Domino directory account. Deactivating a profile removes all permissions, group memberships, and department memberships from it.

Default Domino domain when creating profiles	Specifies a domain to add to a user name automatically when synchronizing employees with Domino accounts.
Default Domino server when browsing for users	Specifies the name of the default Domino LDAP server to use when you browse for new users to add to your Insight Surveillance system.
Force users to use the default Domino server when browsing for users	Stops you from choosing any Domino LDAP server other than the default server when you browse for new users to your Insight Surveillance system. By default, Insight Surveillance lets you nominate any Domino server.
Minimum days to wait before profiles are deactivated	Specifies the number of days after which Insight Surveillance should automatically deactivate those employee profiles for which it cannot find a matching Active Directory or Domino directory account.
Minimum number of failed synchronizations before deactivating profiles	Specifies the number of times that Insight Surveillance should fail to synchronize an employee profile with the corresponding Active Directory or Domino directory account before it deactivates the profile.
Number of synchronization threads	Specifies the number of threads that Insight Surveillance employs when it synchronizes employee profiles with the corresponding Active Directory or Domino directory accounts. Enter a value in the range 1 through 5, where the default is 1.
Remove addresses that do not exist in Domino or Active Directory	Specifies whether Insight Surveillance deletes the email addresses in an employee profile before it synchronizes the profile with Active Directory or a Domino directory. By default, Insight Surveillance does not delete the addresses. This is because you may still want to perform searches that use old email addresses, or you may have entered some additional email addresses manually. Insight Surveillance does not delete the email addresses in the profile if synchronization fails for any reason.

Synchronization interval (hours)	Specifies the frequency in hours with which Insight Surveillance synchronizes employee profiles with the corresponding Active Directory or Domino directory accounts. Enter a value in the range 1 through 24. The default is every eight hours and every time the eDiscovery Manager service starts.
Synchronize profiles	Specifies whether Insight Surveillance should attempt to synchronize employees and groups with the corresponding Active Directory or Domino directory accounts. The default is to do so.
When service starts wait before synchronizing (minutes)	Specifies the number of minutes to wait after the eDiscovery Manager service starts before synchronizing employees and groups with Active Directory or a Domino directory. Enter a value in the range 0 through 720. By default, the service does not wait before synchronizing.

Random Capture configuration options

Use these settings to configure the random sampling of items.

Cache backup location	When cache safety mode is enabled, specifies a location for the cache folder. It is better to enter a local path for performance reasons, but you can also enter a network share path. The account that runs the Enterprise Vault eDiscovery Manager service must have full access to this folder. If the folder does not exist and the service has the appropriate permissions, the folder is created.

First Pass Sampling time (server local time)	Reduces the burden of resolving the transactions at the sample time by letting the server resolve some of them before the main sampling time is reached. At this time, transactions of items that are captured are resolved. The default time is 20:00. This setting applies only to the items that older versions of Insight Surveillance have captured but have yet to process and sample. In Insight Surveillance 11.0.1 and later, transaction resolution no longer occurs; Insight Surveillance adds the items to the database with the saveset ID (SSID) already populated.
Maximum age of unresolved items (hours)	Specifies the number of hours after which Insight Surveillance purges from temporary storage any sampled items that it has yet to move into the review set. Enter a value in the range 1 through 672, where the default is 96. This setting is used with "Maximum resolve attempts". Both conditions must be reached for the purging to take place.
Maximum resolve attempts	Specifies the maximum number of attempts that Insight Surveillance should make to move an item into the review set before it purges the item. Enter a value in the range 1 through 500, where the default is 5. This setting is used with "Maximum age of unresolved items". Both conditions must be reached for the purging to take place.
Record extra statistics for evidence of review reports	Causes Insight Surveillance to collect additional data for use in Evidence of Review reports. Insight Surveillance holds the extra data in the tblMessageAddress database table, which can grow large as a result.

Sampling mode	Specifies whether to use guaranteed sampling or statistical sampling of items. With guaranteed sampling (1, the default), Insight Surveillance captures all items for every monitored employee throughout the day. After midnight, it picks a random sample from each employee's items and adds them to the review set. If you choose guaranteed sampling, you cannot cap the number of items that Insight Surveillance adds to the review set. With statistical sampling (0), Insight Surveillance takes a random sample of the items that it has captured during the previous 24-hour period and adds them to the review set. This means that some employees may have fewer items captured than others with an identical monitoring percentage.
Sampling time (server local time)	Specifies the time at which Insight Surveillance puts sampled items from the previous 24 hours in the review set. The default time is 01:00. This means that sampled items from the previous 24 hours become visible in the review set after 1 A.M. local time when the processing is complete.
Stale config timeout (mins)	Specifies the frequency with which the Compliance Sampling process on the Enterprise Vault storage server should synchronize with the configuration data from the Insight Surveillance customer databases. Enter a value in the range 1 through 300, where the default is 60.
Stale config use period (hours)	Specifies how long the Compliance Sampling process on the Enterprise Vault storage server should continue to sample items after it has failed to synchronize with the configuration data from the Insight Surveillance customer databases. After a failed synchronization attempt, sampling is based on cached customer configuration data. Enter a value in the range 0 through 168, where the default is 6.

Reviewing configuration options

Use these settings to configure the Review pane.

Default Page Size	Specifies the default number of items to show in the Review pane. Enter a value in the range 1 through 1000, where the default is 100.
Display Marking List	Specifies how to show the available marks in the Review pane: as clickable options across the bottom of the page, or in a drop-down list. By default, Insight Surveillance shows the marks as clickable options rather than as options in a drop-down list.
ECM Temporary Storage Area	Specifies the path to the folder in which temporarily to store the items that you retrieve by using the Enterprise Vault Content Management API. By default, Insight Surveillance uses the Windows `%TEMP%` folder. Note the following: ■ We recommend that you specify a local path, where possible. If you must specify a network share path, always use the UNC path rather than a mapped drive. ■ The folder must already exist; Insight Surveillance does not create it. ■ In a hosting environment, multiple customers must not share the same folder.
ECM Temporary Storage Area Cleanup Interval (Minutes)	Specifies the frequency in minutes with which to purge stale data from the temporary storage area. The default value is five minutes.
Facets To Hide	Provides a comma-separated list of the filter options that are not available to users in the Review pane. The available options are as follows: appraisalid, appraiserid, author, capturedate, capturetype, commentid, direction, escalatedbyid, escalationid, escalationownerid, maildate, numattachments, policyaction, policyid, reviewerid, scheduledsearchid, searchid, size, type.
Folder item colour when it exists in the review set	Specifies the color with which to identify the items in a research folder that already exist in the associated review set. The default color is blue.

Highlight Background Colour	Specifies the background color with which to highlight instances of search terms in HTML renderings of items. You can enter a color name, such as “Yellow” (the default color), or a red-green-blue color value, such as “#FFFF00”.
Highlight Foreground Colour	Specifies the foreground color with which to highlight instances of search terms in HTML renderings of items. You can enter a color name, such as “Black” (the default color), or a red-green-blue color value, such as “#000000”.
Hit Highlighting Type	Specifies whether to enable or disable search highlighting in HTML renderings of items. Set the value to 1 (the default) if you want to highlight instances of search terms in items, or to 0 to disable highlighting.
Item Unlocking Thread	Specifies whether to turn on or off the lock cleanup thread, which unlocks any items that have been accidentally left locked. For example, this may be the case if a reviewer's computer or Insight Surveillance client stops working during a reviewing session. By default, the thread is turned on.
Label for messages without a subject	Specifies the subject line to assign to those items that do not have a subject line. The default is “No Title”.
Log preview actions in item history	If set to true then, when a reviewer previews an item in the Review pane, displays a printable version of it, or downloads the original version of the item, causes Insight Surveillance to log the action in the item history. By default, Insight Surveillance does not log these actions. Even if you choose to log these actions for items in the Review pane, the Searches pane still allows users to preview the results of searches that they have conducted in a research folder without their actions being logged. If you want to prevent this, set the configuration option “Disable search results preview". See “Search configuration options” on page 52.

Maximum Page Size	Specifies the maximum number of items to list on a page within a review set. Enter a value between 1 and 300, where the default is 300.
Maximum items user can temporarily self-assign	Sets a limit on the number of items that users can temporarily assign to themselves while they review. The default is 10000.
Prevent self-review	(Application-wide option that applies to all Insight Surveillance customers.) For those reviewers whom you have also designated as exception employees, specifies whether to prevent them from reviewing the items that they themselves have sent and received. By default, Insight Surveillance allows such users to self-review their items. This can give rise to the situation where, for example, an item that an exception employee has sent to a non-exception employee can appear in both of the following review sets: ■ The exception reviewer's review set, because the sender is an exception employee. The exception employee does not have access to this review set. ■ The department review set, because the recipient is not an exception employee. The exception employee who sent the item may be able to access this review set through the Department Reviewer role, and so assign a review mark to the item. Setting this option to true prevents self-reviews in these circumstances. This option does not apply to escalation reviewers. They can potentially self-review their items, even if you set this option to true.
Require comment when escalating or assigning items	Specifies whether a reviewer must add a mandatory comment when escalating or assigning items.
Review Grid File	Lets you download and upload an XML file with which to define the column layout in the Review pane for all users.
Review Set Expiry Time (Minutes)	Specifies the number of minutes of inactivity after which a user's review set expires. The default value is 120 minutes.

Sanitize HTML for review	Specifies whether to preprocess HTML items before review to remove any script that may cause navigation problems. By default, Insight Surveillance preprocesses the items.
Show Appraisal UI	For users with the Apply Appraisal Status permission, specifies whether to hide or show the appraisal system features in the Review pane and Export pane.
Timeout for building or sorting review set (seconds)	Specifies the number of seconds within which Insight Surveillance must build a review set or sort a review set before the process times out. The default is 300.

Search configuration options

Use these settings to optimize the search features in Insight Surveillance.

Allow search and capture of existing items	Specifies whether, when you set the criteria for a new search, you can choose to include previously-captured items in the search results. By default, you have the option to do so.
Buffer Since Last Run	When you select a schedule to use when you define the criteria for a new search, you can select **Since last run** in the **Date range** section. This option instructs Insight Surveillance to search new items that have arrived since you last ran this scheduled search. In the **Start** box, you enter the date to be taken as a starting point for the first run of the search. By default, **Since last run** 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). If required, you can change this interval to search to the current day minus *n* days. To use **Since last run** with any searches that run more than once a day, set the interval to 0.
Combine subject and content fields with OR	When you search for words in both the subject of an item and its content, specifies whether to find only those items that meet one or both criteria. By default, Insight Surveillance finds only those items that meet both criteria.

Disable Search against Other Departments	Specifies whether, when you define the criteria for a new search, the **Other Depts** option in the **Author & Recipients** area is available. By default, Insight Surveillance does let you conduct searches against other departments.
Disable search results preview	If set to true, prevents users who conduct a search in a research folder from previewing the search results. By default, Insight Surveillance does not stop users from previewing these items.
Enable automatic synchronization of index volumes	Specifies whether Insight Surveillance should automatically synchronize the index volumes for an archive when it encounters any unknown index volumes during a search. By default, Insight Surveillance synchronizes the index volumes automatically.
Enable Search Threads	Specifies whether to enable or disable all search facilities. By default, Insight Surveillance enables these facilities.
Error search if index is rebuilding or failed	Specifies whether the search of a particular archive returns an error if its index is offline, rebuilding, or failed. By default, Insight Surveillance returns an error in these circumstances.
Error search if missing items or content	Specifies whether the search of a particular archive returns an error if its index has failed to index either an indexable archived item or the content of the item. The default setting is false (not enabled).
Error search if index requires width normalization	Specifies whether the search of a particular archive returns an error if its index must be rebuilt to handle full-width characters correctly. The default setting is Off.
Fail search of archive if archive has been copied or moved	Specifies whether to mark as failed a search of a moved or copied archive, if the destination archive is not included in the search. The default is False, which means that Insight Surveillance produces a warning when searching such archives, but it does not mark them as failed.

Guaranteed Sample search timeout (mins)	Specifies the number of minutes for which guaranteed sample searches run before Insight Surveillance automatically accepts them and uses the results for sampling. The default is 240 minutes.
Hotword Set Tag	Specifies the tag with which Insight Surveillance prefixes hotword sets when you enter them in the criteria for a new search. The default is HWS.
Hotword Tag	Specifies the tag with which Insight Surveillance prefixes hotwords when you enter them in the criteria for a new search. The default is HW.
Maximum number of searches listed in filters	For areas of Insight Surveillance that list searches from which you can choose, specifies the maximum number of searches to include in the list. The default is 250.
Maximum Search Retries	Specifies the number of times that Insight Surveillance tries to search an archive before giving up. Enter a value in the range 1 through 50, where the default is 5.
Number of acceptance search Threads	Specifies the number of threads that are assigned to accepting search result sets. For example, the default setting of 5 means that no more than five search results sets are accepted at a time. Enter a value in the range 1 through 10.
Number of delete search Threads	Specifies the number of threads that are assigned to deleting search result sets. For example, the default setting of 2 means that no more than two search results sets are deleted at a time. Enter a value in the range 1 through 10.
Number of sampling search Threads	Specifies the number of threads that are assigned to sampling search result sets. For example, the default setting of 5 means that no more than five search results sets are sampled at a time. Enter a value in the range 1 through 10.
Number of Vault search Threads	Specifies the number of threads that are assigned to searching archives per index server. For example, the default setting of 10 means that no more than 10 archives are searched per Enterprise Vault server at a time. Enter a value in the range 1 through 10.

Only allow 'Research this message' on the first selected message	Specifies whether, when you click multiple items in the Review pane and then click Search, Insight Surveillance lets you specify the search criteria for each of the selected items or only for the first of the selected items.
Optimize search based on oldest and youngest items	When set to True, improves performance by excluding from a search those archives that Insight Surveillance has determined do not contain any items in the date range that you have specified in your search criteria. The default setting is False, which means that Insight Surveillance searches all the available archives, regardless of whether their contents fall within your specified date range or not. Use this setting with "Synchronize thread checking period (sec)", which is one of the Vault Directory Synchronization configuration options. If you set "Optimize search based on oldest and youngest items" to True, you must lower the setting for "Synchronize thread checking period (sec)" to ensure that Insight Surveillance does not run searches against out-of-date data. For example, you can lower the setting to 3600 seconds (one hour).
Perform Guaranteed Sample searches against sampling-eligible archives only	Specifies whether to limit guaranteed sample searches to the types of archives that are eligible for random sampling: Exchange Journal, Domino Journal, SMTP, and Shared. By default, Insight Surveillance limits guaranteed sample searches to these archive types to improve search performance. However, you may want to include other types of archives in guaranteed sample searches if, for example, Enterprise Vault is archiving SMTP items to them. This setting replaces the setting that was called "Ignore non journal archives for Guaranteed Sample searches" in earlier versions of Insight Surveillance.

Require 'Author' / 'Content' / 'From Date' / 'Recipients' / 'Subject' / 'To Date' to be specified	Specifies whether it is mandatory to enter the designated criteria before you can perform a search. By default, these criteria are optional. You may want to make them mandatory to prevent searches from returning an overwhelming number of results.
Retry time when index service is busy (min)	Specifies the frequency in minutes with which Insight Surveillance tries to access an Enterprise Vault Indexing service that is too busy to perform a search. Enter a value in the range 1 through 300, where the default is 5.
Retry time when index service not running (min)	Specifies the frequency in minutes with which Insight Surveillance tries to access an Enterprise Vault Indexing service that is unavailable. Enter a value in the range 1 through 300, where the default is 5.
Return only top messages in search results	Specifies whether searches return the top-level items only. Setting this option to Off means that all files attached to the top-level items are displayed in search results.
Save SMTP subject rather than filename	For items that were archived using File System Archiving (FSA), specifies whether to show the SMTP message subject rather than the FSA file name in the Review pane.
Search result page refresh time	Specifies the frequency in seconds with which Insight Surveillance refreshes the results summary page during a running search. Enter a value in the range 1 through 300, where the default is 10.
Search timeout (hours)	Specifies the maximum time in hours that Insight Surveillance allows for searches to complete. The default is four hours.
Searches page refresh time	Specifies the frequency in seconds with which Insight Surveillance refreshes the Searches pane for a department. Enter a value in the range 1 through 300, where the default is 20.

Show Application Search Tree 'Constrain Tree Height' option	When you define the criteria for a new search, specifies whether a **Constrain tree height** option is available in the Authors & Recipients area. When selected, this option fixes the height of the department tree view in the Authors & Recipients area. By default, Insight Surveillance hides the option.
Show Application Search Tree 'Expand All' option	When you define the criteria for a new search, specifies whether an **Expand All** link is available in the Authors & Recipients area. Clicking this link expands all the departments in the tree view. By default, Insight Surveillance hides the link.
Show 'Guaranteed Sample' option for new searches	Specifies whether you can create Guaranteed Sample searches. By default, you can.
Show Search Result In Progress	Specifies whether users can access the Review pane while a search is in progress, so that they can immediately start to review the items that Insight Surveillance has found. By default, Insight Surveillance permits this.
Total number of search results worker threads	Specifies the maximum number of search results worker threads that are allowed to run on the system. These threads handle the processing of search results returned from the archive. The maximum value is 5, and the default is 2.
Total number of search threads	Specifies the maximum number of search threads that are allowed to run on the system across all index volumes. The maximum value is 500, and the default is 100.
Use sequence number for searches	Optimizes performance for searches that return more than 50,000 results. By default, this option is enabled.
When service starts, wait before synchronizing Index Services (minutes)	Specifies the number of minutes that Insight Surveillance waits at startup before synchronizing with available index services. Enter a value in the range 0 through 300, where the default is 0.
When service starts, wait before starting Vault Searches (minutes)	Specifies the number of minutes that Insight Surveillance waits at startup before searching the archives for items. Enter a value in the range 0 through 300, where the default is 0.

Security configuration options

Use these settings to implement *Chinese walls* security restrictions on what users can access in Insight Surveillance.

A Chinese wall is a metaphor used to refer to the practice of ensuring that different parts of an organization are kept apart so that information does not circulate freely and to prevent conflicts of interest. By implementing Chinese walls, you can stop users in one part of your organization from giving access to departments and folders to users in another part of the organization.

Bypass Department Users Permissions check when removing all roles	Lets users who do not have the Manage Department User permission remove Department Users from departments.
Enable Chinese Wall Department Users	Prevents users from being assigned to roles in a department unless they have first been assigned to the Department User role in that department.
Use SQL Server SysAdmin Server Role for Schedules	When selected, makes the SQL Server sysadmin logon the creator and owner of Insight Surveillance search schedules. If you want to lock down your SQL Server instance, clear this setting and consult the following article on the Arctera Support website for further instructions: https://www.veritas.com/docs/100038151

System configuration options

Use these options to record the dates on which you installed Enterprise Vault and began to archive data, configure the threads that Insight Surveillance uses to pause searches, and more.

Enterprise Vault Oldest Archived Item Date	Specifies the date on which Enterprise Vault archived the oldest available data. If the oldest archived item date and "Enterprise Vault V5 Installation Date" are the same then, when entering the criteria for a search, you can specify the message type without also specifying a start date. (Insight Surveillance does not return any pre-5.0 data.) However, if the oldest archived item date is earlier than the V5 installation date, you can only specify the message type if you specify a start date that is on or after the V5 installation date.
Enterprise Vault V5 Installation Date	Specifies the date on which you first installed or upgraded Enterprise Vault 5.0 or later.
IIS Application Pool	Identifies the application pool in which the Accelerator web applications are grouped. Application pools allow specific configuration settings to be applied to groups of applications and to the worker processes that service those applications. The default application pool is EVAcceleratorAppPool.
Initial Pausing Queue Size	Specifies the maximum number of searches that you can pause instantly. The default is 2.
Number Of Pause Search Threads	Specifies the number of threads that are assigned to pausing searches. Enter a value in the range 1 through 10, where 1 is the default value.
Pause queue threshold	Specifies the total number of pause search requests that can be queued at once. Enter a value in the range 10 through 100, where 10 is the default value.
Pause Threads Delay	Specifies the number of minutes that Insight Surveillance waits at startup before it initializes the threads that are assigned to pausing searches. By default, Insight Surveillance does not delay before it initializes the threads.
Search Pause Thread Checking Period (Sec)	Specifies the number of seconds to wait before starting pause threads. The default is 5.

Show Vault Management Option	Does not serve any function in the current version of Insight Surveillance. The option will be removed from Insight Surveillance in a later release.

Vault Directory Synchronization configuration options

Use these settings to configure when Insight Surveillance synchronizes with the Enterprise Vault archives.

Archive registration/deregistration task period (minutes)	Specifies the frequency in minutes with which to run the archive registration/deregistration task. The default is 60 minutes. To prevent the accidental deletion of Enterprise Vault archives whose contents appear in the Insight Surveillance review set or search results, this task registers an interest in the archives. The task also discards existing archive registrations when they are no longer required. See also the options "Enable archive registration task" and "Discard existing archive registrations after you turn off 'Enable archive registration task'".
Archive selection page size	Specifies the maximum number of Enterprise Vault archives to display on a single page during archive selection. By default, Insight Surveillance lists a maximum of 100 archives. If the number of available archives exceeds the value that you specify here, Insight Surveillance displays some extra hyperlinks so that you can page through the archives.

Automatically enable new Vault Stores in departments/cases	Specifies whether, when a new vault store is created, Insight Surveillance automatically includes it in searches. The options are as follows: ■ 1. New vault stores are never automatically enabled. ■ 2. New vault stores are always automatically enabled. ■ 3 (default value). New vault stores are automatically enabled when all the other vault stores in the same site are already enabled.
Discard existing archive registrations after you turn off 'Enable archive registration task'	Specifies whether to keep or discard any existing archive registrations if you choose to disable the archive registration task. By default, Enterprise Vault keeps the existing archive registrations after you disable the task. See also the options "Archive Registration task period (minutes)" and "Archive registration/ deregistration task period (minutes)".
Enable archive registration task	Specifies whether to enable or disable the archive registration task. By default, the task is enabled. If you disable it, a message prompts you to choose the required setting for the option "Discard existing archive registrations after you turn off 'Enable archive registration task'". See also the option "Archive Registration task period (minutes)".
Synchronize archives on search	Specifies whether to synchronize all the archives when running a new search. By default, Insight Surveillance does not synchronize all the archives.
Synchronize Retention Categories on search	Specifies whether to synchronize all the retention categories when running a new search. By default, Insight Surveillance does not synchronize all the retention categories.

Synchronize thread checking period (sec)	Specifies the frequency in seconds with which Insight Surveillance synchronizes with the Enterprise Vault archives. The default is 21600 (six hours). For best results, you may want to change the synchronization period to 3600 (one hour). The more frequently synchronization occurs, the greater the load on the Insight Surveillance database. However, if the synchronization is not frequent enough, Insight Surveillance may take a long time to recognize new archives, vault stores, and retention categories.
Synchronize Vault Stores when viewing Department/Case properties	Specifies whether to synchronize the vault stores when displaying the properties page for a department. By default, Insight Surveillance does not synchronize the vault stores.

Chapter 3

Creating and viewing reports

This chapter includes the following topics:

About the Insight Surveillance reports

SSRS Reports

The SSRS reports are discontinued, however, the previously generated reports are saved and organized in a folder provided on the SSRS database server. Contact your database administrator if needed. Either the administrator can grant you access to the SSRS reports by providing you with individual report links or by assigning the ***My Reports*** permission on the SSRS Database server or the folder itself. You can then access the entire folder on the ***SQL Server Reporting Services*** web portal.

See "Accessing data through the Microsoft SQL Server Reporting Services (SSRS)" on page 64.

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 Alta Surveillance. Upon successful configuration, Alta 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

See "Enhanced reporting" on page 65.

OData Reports

With Insight Surveillance, you can access information from the configuration and customer databases using the Open Data (OData) web service. Use any OData-compatible reporting tool, for example Excel/PowerQuery, to generate reports.

See "Accessing reports through the OData web service" on page 94.

Besides printing the reports, you can export them in a number of formats, including XML, comma-separated values (CSV), Acrobat (PDF), web archive (MHTML), Excel, and TIFF.

Accessing data through the Microsoft SQL Server Reporting Services (SSRS)

The SSRS reports are discontinued, however, the previously generated reports are saved and organized in a folder provided on the SSRS database server. Contact your database administrator if needed. Either the administrator can grant you access to the SSRS reports by providing you with individual report links or by assigning the ***My Reports*** permission on the SSRS Database server or the folder itself. You can then access the entire folder on the ***SQL Server Reporting Services*** web portal.

To access the SSRS reports

1 Ensure that you have the ***My Reports*** permission that is mandatory for accessing the SSRS reports.

Note: If you do not have the ***My Reports*** permission, contact your database administrator. Either the database administrator can directly grant you access to the SSRS reports by providing you with individual report links or assign this permission to the SSRS Database server or the folder itself.

---

2 Specify the below-mentioned information in the following URL and then launch it.

Home > Surveillance Reports > Folder with name as Surveillance Customer's name > Folder with name as Windows username who has generated the reports in the " <Domain><space character><username>" format.

For example, in Surveillance, if there is a customer named ABC-Finance, and a user with the login name MyDomain\User1 has generated reports, the folder structure will be:

Home > Surveillance Reports > ABC-Finance > MyDomain User1

The application will navigate you to the folder containing SSRS reports.

Enhanced reporting

Insight Surveillance has introduced reporting endpoint APIs to improve reporting and analytics capabilities.

The currently available reporting endpoint APIs are:

- Departments
- Users
- UserRoles
- Roles
- ItemMetrics
- EvidenceOfReviewByDept
- EvidenceOfReviewByUser

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 66.

See "Departments API" on page 70.

See "Users API" on page 74.

See "UserRoles API" on page 75.

See "Roles API" on page 71.

See "ItemMetrics API" on page 79.

See "Evidence of Review by Department API" on page 84.

See "Evidence of Review by User API" on page 88.

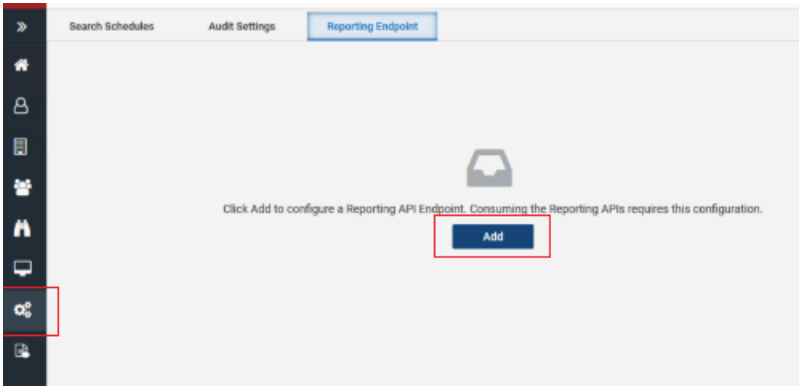
Configuring a reporting endpoint

To configure a reporting endpoint, you must have a *Compliance System Administrator* 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.

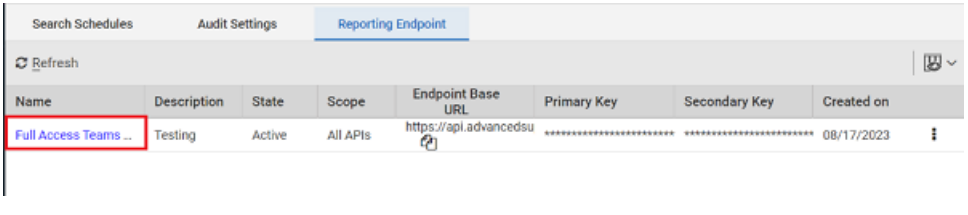


2 Click **Add**.

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.
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.

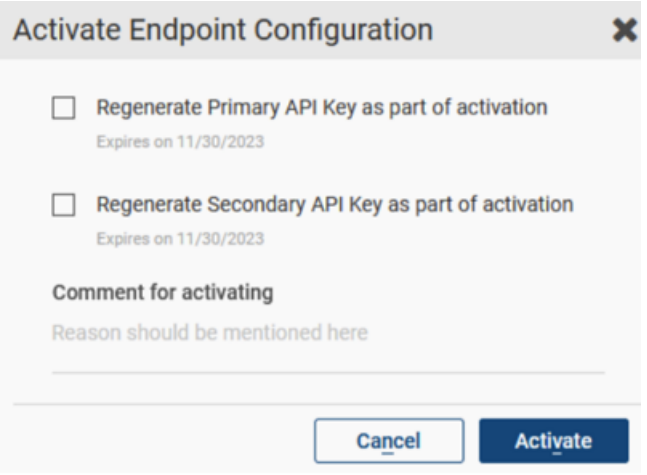


4 Click the kebab icon (three vertical dots) in the same row to perform the following actions:

- 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 must 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 requests

```
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 91.

Responses

See "Responses" on page 93.

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 91.

Responses

See "Responses" on page 93.

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


```
{
    "@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": []
        }
    ]
}
```


Supported OData Filters

See "Supported OData query options" on page 91.

Responses

See "Responses" on page 93.

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://<server>/odata/$metadata#Users",
    "@odata.count": 10,
    "value": [
        {
            "userId": 1,
            "userName": "User1"
        },
        {
            "userId": 2,
            "userName": "VSA"
        },
        {
            "userId": 3,
            "userName": "User3"
        },
        {
            "userId": 5,
            "userName": "User5"
        },
        {
            "userId": 6,
            "userName": "User6"
        },
        {
            "userId": 1004,
            "userName": "User1004"
        }
    ],
"@odata.nextLink": "https://<Server>/odata/users?$count=true&$skiptoken=1"
}
```

Supported OData Filters

See "Supported OData query options" on page 91.

Responses

See "Responses" on page 93.

UserRoles API

Supported Operations

UserRoles - List by filters	Gets a list of department users and their associated roles. The users filter gets all the roles associated with the specified users. It includes all the department-level and application-level roles for the users.

UserRoles - List by filters

```
POST https://<Reporting endpoint Base URL>/odata/userroles
```

Request body

Specify the following filters to obtain refined and selective results from this report.

Note: Either *Departments* or *Users* is a mandatory parameter. The *Scope* is an optional parameter.

Name	Type	Description
Departments	Mandatory (if the Users parameter is not provided) Optional (if the Users parameter is provided)	Specifies IDs of the departments to which users and their roles belongs to. **Limitations**: The Users roles API can pass a maximum of 100 Departments IDs as input. **Data Type**: JSON array of integers 'id'(identifier fields) that is Departments.

Name	Type	Description
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	Mandatory (if the Departments parameter is not provided) Optional (if the Departments parameter is provided)	Specifies IDs of the users. **Limitations** The Users roles API can pass a maximum of 100 User IDs as input. **Data Type**: JSON array of integers 'id'(identifier fields) that is Users.

Scenario 1

To get the item counts only for Users when the Users are mentioned, but the Departments and the Scopes are not mentioned.

Sample request

```
POST https://<Reporting endpoint Base URL>/odata/Userroles

{

"Departments": [],

"Scopes" :[]

"Users" :[3821]

}
```

Scenario 2

To get the item counts only for users when Departments are mentioned, but the Scopes and Users are mentioned.

Sample request

```
POST https://<Reporting endpoint Base URL>/odata/Userroles

{

"Departments": [23],

"Scopes" :[]

"Users" :[]
```

```
}
```

Scenario 3

To get the item counts only for users when Departments and Scopes are mentioned, but Users are not mentioned.

Sample request

```
POST https://<Reporting endpoint Base URL>/odata/Userroles

{

"Departments": [23],

"Scopes" :[161]

"Users" :[]

}
```

Scenario 4

To get the item counts only for users when Departments are not mentioned, but the Scopes and Users are mentioned.

Sample request

```
POST https://<Reporting endpoint Base URL>/odata/Userroles

{

"Departments": []

"Scopes" :[160]

"Users" :[3821]

}
```

Scenario 5

To get the item counts only for users when the Departments, Scopes, and Users are mentioned.

Sample request

```
POST https://<Reporting endpoint Base URL>/odata/Userroles

{

"Departments": [23],

"Scopes" :[160,161]

"Users" :[55,67]
```

```
}
```

Sample response

(For scenario 1 to 5) Status code: 200 OK


```
{
    "@odata.context": "https://<Server>/odata/$metadata#UserRoles",
    "@odata.count": 4,
    "value": [
        {
            "userId": 3821,
            "roleId": 6780,
            "department": 10963,
            "scope": "Department"
        },
        {
            "userId": 3821,
            "roleId": 6780,
            "department": 7127,
            "scope": "Department"
        }
],
 "@odata.nextLink": "https://<Server>/odata/userRoles?$count=true&$skiptoken=1"
}
```


Scenario 6

Invalid Inputs. Either the Department or the User parameter must be specified as input.

Sample request

```
POST https://<Reporting endpoint Base URL>/odata/Userroles

{

"Departments": [],

"Scopes" :[160]

"Users" :[]

}
```

Sample response

Status code: 400 Bad Request Error Code: InvalidOdataQuery

Supported OData Filters

See "Supported OData query options" on page 91.

Responses

See "Responses" on page 93.

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. **Date format**: YYYY-MM-DD **Data Type**: JSON array of integers 'id'(identifier fields) 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. **Date format**: YYYY-MM-DD **Data Type**: JSON array of integers 'id'(identifier fields) 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
```

Supported OData Filters

See "Supported OData query options" on page 91.

Supported reporting endpoint API filters and their values

See "Supported reporting endpoint API filters and their values" on page 92.

Responses

See "Responses" on page 93.

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.

Name	Type	Description
CaptureType	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 CaptureType IDs. **Limitation**: As an input, the ItemMetrics API can pass maximum 10 CaptureType 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. **Date format**: yyyy-mm-dd **Data Type**: JSON array of integers 'id'(identifier fields) that is CaptureDateStart.
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. **Date format**: yyyy-mm-dd **Data Type**: JSON array of integers 'id'(identifier fields) that is CaptureDateEnd.

Name	Type	Description
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.
MessageType	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, the ItemMetrics API can pass maximum 100 MessageType IDs on a single page.

Scenario 1:

To get the item counts for *Departments IDs* 7622, between *CaptureDates* 2023-11-24 and 2023-12-24 and having *CaptureType* as 1 or 3.

Sample Requests

```
POST https://<Reporting endpoint Base URL>/odata/ItemMetrics

{

{"CaptureDateStart": "2023-11-24",

"CaptureDateEnd": "2023-12-24",

"Departments": [7622],

"CaptureType": [1,3]

}
```

Sample response

Status code: 200 OK

```
"@odata.context": "https://<Reporting endpoint Base
URL>/odata/$metadata#ItemMetrics",
"value": [
        {
            "capturedItemCountId": 6,
            "captureDate": "2023-11-24T00:00:00-08:00",
            "departmentId": 7622,
            "department": "ParentHW",
           "messageTypeId": 1,
            "messageType": "Exchange",
            "captureType": "Search",
            "captureTypeId": 1,
            "messageDirectionId": 1,
            "messageDirection": "Internal",
            "capturedItemsCount": 125
        }
    ]
}
```


Scenario 2

To get item counts for *Department IDs* 9 and 5, between *CaptureDates* 2023-06-01 and 2023-08-02 and having *MessageType IDs* 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],

"MessageType": [7,8]

}
```

Scenario 3:

To get item counts for *Departments IDs* 9 and 5 , between *CaptureDates* 2023-06-01 and 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 *CaptureDates* 2023-06-01 and 2023-08-02 and having *MessageType IDs* as 7 or 8.

```
POST https://<Reporting endpoint Base URL>/odata/ItemMetrics

{

"CaptureDateStart": "2023-06-01",

"CaptureDateEnd": "2023-06-02",

"Departments": [9,5],

"MessageType": [7,8]

}
```

Supported OData Filters

See "Supported OData query options" on page 91.

Supported reporting endpoint API filters and their values

See "Supported reporting endpoint API filters and their values" on page 92.

Responses

See "Responses" on page 93.

Evidence of Review by Department API

Supported Operations

EvidenceOfReviewByDept - List by filter	For the specified departments, 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 of that department. The counts are calculated for the specified date range and using the specified filters.

EvidenceOfReviewByDept - List by filter

```
POST https://<Reporting endpoint base
URL>/odata/EvidenceOfReviewByDept
```

Sample requests

```
POST https://<Reporting endpoint base
URL>/odata/EvidenceOfReviewByDept
```

EvidenceOfReviewByDept - URL Parameter/Filters

The following filters can be used with the EvidenceOfReviewByDept 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
StartDate	Mandatory	StartDate is the date on which items are captured or ingested in 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. **Date format**: YYYY-MM-DD **Data Type**: JSON array of integers 'id'(identifier fields) that is StartDate.
EndDate	Mandatory	This filter specifies the end date for returning count of items whose CaptureDate is greater than or equal to this date. **Date format**: YYYY-MM-DD **Data Type**: JSON array of integers 'id'(identifier fields) that is EndDate.
MessageType	Mandatory	Specifies the type of captured items and returns item counts for items that have the specified message type. **Data Type**: Integer 'id' (identifier fields) that is MessageType ID.

Name	Type	Description
Departments	Mandatory	Specifies the departments to which the captured item belongs and returns item counts for items within that department. **Data Type**: JSON string containing integer IDs (identifier field) that is department IDs. **Limitation**: As an input, this API can pass maximum of 1000 Departments IDs.
MessageDirection	Mandatory	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**: Integer id (identifier field) that is MessageDirection ID

Scenario 1

To get the item counts for *Department IDs* 5 and 6, between *StartDate* 2023-01-01 and *EndDate* 2024-01-01 and having *MessageType* as 7, and *MessageDirection* as 1.

```
POST http://<Reporting endpoint base URL>/odata/EvidenceOfReviewByDept

Input:
{
    "StartDate": "2023-01-01",
    "EndDate": "2024-01-01",
    "MessageType":7,   //SMTP messages
    "Departments":[5,6],    //Finance, Human Resources
    "MessageDirection":1 //Messages exchanged between employees of same organization
}
```

Sample response

Status code: 200 OK

Supported OData filters

See "Supported OData query options" on page 91.

Supported reporting endpoint API filters and their values

See "Supported reporting endpoint API filters and their values" on page 92.

Responses

See "Responses" on page 93.

Evidence of Review by User API

Supported Operations

EvidenceOfReviewByUser - List by filter	For the specified users, gets the total messages count, captured message count and the marking count, (that is count of messages marked as reviewed/unreviewed/questioned/pending) for that user. The counts are calculated for the specified date range and using the specified filters.

EvidenceOfReviewByUser - List by filter

```
POST https://<Reporting endpoint base
URL>/odata/EvidenceOfReviewByUser
```

Sample requests

```
POST https://<Reporting endpoint base
URL>/odata/EvidenceOfReviewByUser
```

EvidenceOfReviewByUser - URL Parameter/Filters

The following filters can be used with the EvidenceOfReviewByUser 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
StartDate	Mandatory	StartDate is the date on which items are captured or ingested in 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. **Date format**: YYYY-MM-DD **Data Type**: JSON array of integers 'id'(identifier fields) that is StartDate.

Name	Type	Description
EndDate	Mandatory	This filter specifies the end date for returning count of items whose CaptureDate is greater than or equal to this date. **Date format**: YYYY-MM-DD **Data Type**: JSON array of integers 'id'(identifier fields) that is EndDate.
MessageType	Mandatory	Specifies the type of captured items and returns item counts for items that have the specified message type. **Data Type**: Integer 'id' (identifier fields) that is MessageType ID.
User	Mandatory	Specifies the user 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 User IDs. **Limitation**: As an input, the ItemMetrics API can pass maximum of 1000 User IDs.
MessageDirection	Mandatory	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**: Integer id (identifier field) that is MessageDirection ID
ContextUserID	Mandatory	Specifies the User ID authorized to generate the evidence of review report. This user possesses permissions across all relevant departments for which the counts need to be generated. This user, typically an administrator, is comparable to the logged-in user in the Surveillance thick client who is responsible to generate the *Evidence of Review* report. **Data Type**: Integer ID of the user.

Scenario 1

To get the item counts for *MonitoredEmployee* VAS-User2, between *StartDate* 2023-01-01 and *EndDate* 2024-01-01 and having *MessageType* as 7, and *MessageDirection* as 1.

```
{
    "StartDate": "2023-01-01",
    "EndDate": "2024-01-01",
    "MessageType":7,
    "Users":[8]  ,
    "ContextUserID":7,
    "MessageDirection":1
}
```

Sample response

Status code: 200 OK


```
{
    {
    "@odata.context": "http://<Reporting endpoint base URL>/odata/$metadata#EvidenceOfReviewByUser",
    "value": [
        {
            "departmentId": 5,
            "departmentName": "Finance ",
            "principalID": 8,
            "monitoredEmployee": "VAS-User2",
            "totalMessages": 12,
            "captured": 3,
            "unReviewed": 3,
            "pending": 0,
            "questioned": 0,
            "reviewed": 0
        },
        {
            "departmentId": 6,
            "departmentName": "Human Resources",
            "principalID": 8,
            "monitoredEmployee": "VAS-User2",
            "totalMessages": 10,
            "captured": 1,
            "unReviewed": 1,
            "pending": 0,
            "questioned": 0,
            "reviewed": 0
        }
    }
}
```


Supported OData Filters

See "Supported OData query options" on page 91.

Supported reporting endpoint API filters and their values

See "Supported reporting endpoint API filters and their values" on page 92.

Responses

See "Responses" on page 93.

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 *ItemMetrics* API, *Evidence of Review by Department* API, and *Evidence of Review by User* API.

CaptureType filter

Table 3-1 Possible values of the CaptureType filter

ID	Value	Description
0	NotSpecified	
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 3-2 Possible values of the MessageDirections filter

ID	Value	Description
0	NotSpecified	
1	Internal	The items where the author and all recipients are internal to the organization.
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.

MessageType filter

Table 3-3 Possible values of the MessageType filter

ID	Filter	ID	Filter
1	Exchange	6	File System
2	Instant Messaging	7	SMTP
3	Bloomberg	8	Sharepoint
4	Fax	9	Social
5	Domino	10	10 IMAP

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.

Accessing reports through the OData web service

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.

Available Insight Surveillance datasets

Table 3-4 describes the Insight Surveillance datasets that you can view through the OData web service.

Table 3-4 Available Insight Surveillance datasets

This dataset	Shows
`ActionStatusDetail`	The history of actions that reviewers have taken on the items in one or more departments.
`ClassificationSummaryByDepartment`	The count of items in the specified department based on the classification policy applied.
`Customers`	Information about the SQL Server database in which Insight Surveillance stores details of departments, user server roles, search results, and more.
`Departments`	Information on one or more departments associated with the specified customer.
`DifferentialSamplingSummaryByDepartment`	The sampling activity for the monitored employees in selected departments.
`EscalationHistory`	The escalation history for a specific item.
`GuaranteedSamplingSummary`	Information on guaranteed sampling statistics data that was sent by Enterprise Vault to Insight Surveillance.
`HotwordHitsSummary`	Information on hotword statistics for items that were flagged by hotword hits.
`ItemAgingByDepartment`	The number of items that are either still unreviewed or pending review.

Table 3-4 Available Insight Surveillance datasets *(continued)*

This dataset	Shows
`QuestionedItems ByDepartment`	A summary of the suspect items (those items that reviewers have marked as Questioned).
`ReviewActivitySummary`	The total number of items of each type that Insight Surveillance has captured in the selected reporting period. The report also shows the review status of these items.
`ReviewerActivity ByDepartment`	The status of review set items, including how many items have been escalated, questioned, reviewed, and unreviewed.
`ReviewerActivityBy DepartmentDetailed`	Details of review set items such as the status, direction, message type, author and so on.
`ReviewerActivityByReviewer`	The status of the review set items for each reviewer and information about the reviewer.
`ReviewerActivityDetail`	The status of the review set items for each reviewer for one or more departments.
`ReviewerActivityItemDetailed`	Information on the reviewers who have worked on the review set along with details of each message.
`ReviewerNotes`	Information on the notes that reviewers have assigned to the items in the review set for a specified department.
`SamplingSummary`	Information on sampling statistics data that was sent by Enterprise Vault to Insight Surveillance.
`StatisticalSamplingSummary`	Information on statistical sampling data that was sent by Enterprise Vault to Insight Surveillance.

Accessing the Insight Surveillance 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 the following:
  http://*server_name*/CAReporting/OData
- To access a list of all the available datasets together with all the fields included in each dataset, type the following:

http://*server_name*/CAReporting/OData/$metadata

- To access a particular dataset, type the following:
  http://*server_name*/CAReporting/OData/*dataset_name*

Using the OData service with Microsoft Excel

The following instructions are for using the OData service with the following Microsoft Excel versions:

- Microsoft Excel 2010 and 2013
  Make sure that you have installed the Microsoft Power Query add-in for Excel. You can download the add-in from the following page of the Microsoft website:
  https://www.microsoft.com/download/details.aspx?id=39379
- Microsoft Excel 2016, 2019 and O365

To use the OData service with Microsoft Excel 2010 and 2013

1. Open Microsoft Excel.
2. Create a new, blank workbook.
3. On the **Power Query** tab, in the **Get External Data** group, click **From Other Sources**, and then click **From OData Data Feed**.
4. In the **OData Feed** dialog box page, in the **URL** box, specify the website address for the data feed as follows:

   http://*server_name*/CAReporting/OData/*dataset_name*(*parameter=value*)

   For example:

   http://ca.mycompany.com/CAReporting/OData/ActionStatusDetail(customerID=2,departmentID=8,itemID=32)

   Note: Take care to specify the mandatory parameters that are required to view the dataset. Except for the Customers dataset, all the datasets have mandatory parameters. For information on them, see the online Help for each dataset.

   ---

5. If you are prompted for your credentials, enter them and then log in. The Query Editor opens.

6 In the Query Editor, view the records available for the dataset. Edit the queries as required.

7 Click **Close & Load** to import the dataset information in Excel in tabular format.

To use the OData service with Microsoft Excel 2016, 2019 and O365

1 Open Microsoft Excel.

2 Create a new, blank workbook.

3 On the **Data** tab, in the **Get External Data** group, click **Get Data**, click **From Other Sources**, and then click **From OData Data Feed**.

4 In the **OData Feed** dialog box page, in the **URL** box, specify the website address for the data feed as follows:

http://*server_name*/CAReporting/OData/*dataset_name*(*parameter=value*)

For example:

http://ca.mycompany.com/CAReporting/OData/ActionStatusDetail (customerID=2,departmentID=8,itemID=32)

Note: Take care to specify the mandatory parameters that are required to view the dataset. Except for the Customers dataset, all the datasets have mandatory parameters. For information on them, see the online Help for each dataset.

---

5 If you are prompted for your credentials, enter them and then log in. The Query Editor opens.

6 In the Query Editor, view the records available for the dataset.

7 Transform the records by clicking on the **Transform Data** button. This will open the Power Query Editor where you can edit the data to meet your needs. Note that the original source remains unchanged.

8 Click **Close & Load** to import the dataset information in Excel in tabular format.

Using the OData service with Microsoft SQL Server Reporting Services (SSRS)

The following instructions are for Microsoft SQL Server Reporting Services (SSRS).

To use the OData service with Microsoft SQL Server Reporting Services (SSRS)

1. Open Report Builder.
2. Add a new datasource as an XML connection type.
3. In the **Connection string** box, specify the URL for the data feed as follows:

   http://*server_name*/CAReporting/OData/*dataset_name(parameter=value)*
   ?$format=application/atom+xml

   For example:

   http://ca.mycompany.com/CAReporting/OData/Customers(customerID=1)
   ?$format=application/atom+xml
4. Provide credentials to connect to the data source.
5. Click **OK**.
6. Add the dataset using the above mentioned datasource.
7. Select **Use a dataset embedded in my report**.
8. Select the dataset from the list.
9. Set the query as follows:

```
<Query>
  <ElementPath IgnoreNamespaces="true">
    feed{}/entry{}/content{}/properties
  </ElementPath>
</Query>
```

10. Click **Refresh Fields**.
11. Use the new dataset as reporting data for the SSRS report.

Configuring a Power BI template for reporting

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.

To configure a Power BI Template

1 In the left navigation pane of Insight Surveillance console, select **Configuration** > **Reporting Endpoint** tab.

2 Click **PowerBI Templates** to download the *PowerBITemplates.zip* file that contains PowerBI templates.

3 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>`
Capture Date Start	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. **Date format**: yyyy-mm-dd **Data Type**: JSON array of integers 'id'(identifier fields) that is CaptureDateStart.
Capture Date End	This filter specifies the end date for returning count of items whose CaptureDate is greater than or equal to this date. **Date format**: yyyy-mm-dd **Data Type**: JSON array of integers 'id'(identifier fields) that is CaptureDateEnd.

4 Click **Load**.

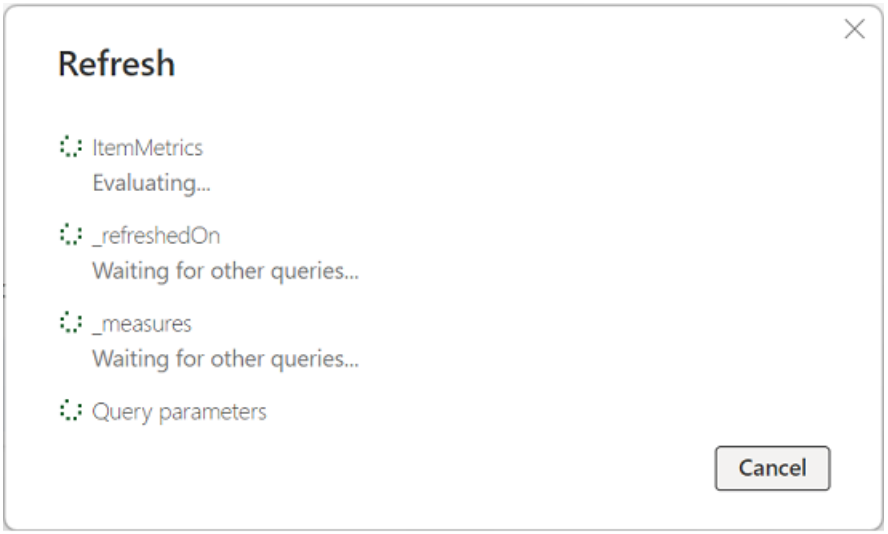
The application prompts you several times to provide appropriate credentials when querying Reporting API for each report.

5 Select the appropriate authentication mechanism to access Reporting API.

Note: These authentication credentials are cached by Power BI for future use and can be managed by clicking **File** > **Options and settings** > **Data source settings**.

---

6 Wait till the Power BI Desktop uses the provided filter values to generate queries and fetch OData reports from the Insight Surveillance Server specified. This step may take a while depending on the amount of data that is being retrieved from the server.



Upon successful processing, the application displays a report for the retrieved data.

Appendix A

Troubleshooting

This appendix includes the following topics:

Insight Surveillance user interface user interface is not displayed properly in non-English environment

If the Insight Surveillance user interface is not displaying correctly, experiencing issues with texts and table column names, please check your browser language. It is recommended to set the browser language to English, then attempt to log in

again. If the problem persists, consider reaching out to Arctera support for assistance.

Issues with the random sampling of items

Table A-1 describes how to resolve some issues that you may encounter when you install, configure, and use the Compliance Sampling feature.

Table A-1 Potential Compliance Sampling issues

Issue	What to check
The Compliance Sampling process (EVCompliance.exe) fails to launch on Enterprise Vault storage servers.	■ You have set up at least one customer database. ■ You have upgraded the customer databases to the latest version. ■ You have configured Insight Surveillance against the correct Enterprise Vault site. ■ The eDiscovery Manager service is running. ■ In the Enterprise Vault directory database, the AcceleratorConfigEntry table contains a configuration entry for the Insight Surveillance server. ■ The SQL connection string in the AcceleratorConfigEntry table is correct. ■ There are no issues launching the Compliance Sampling process. (Run DTrace against StorageServer and filter on "EVComplianceLauncher" to observe any issues with the launching of the process.)

Table A-1 Potential Compliance Sampling issues *(continued)*

Issue	What to check
Items are not randomly sampled.	■ You have set up the department structure in Insight Surveillance correctly, with monitored employees configured for sampling. ■ If you have only just configured Insight Surveillance, ensure that the configuration has been updated in Enterprise Vault. Updates are applied on the next refresh of the cached configuration data. By default, this happens every hour and when the Storage service starts. ■ The SQL server that hosts the Insight Surveillance configuration and customer databases is online and accessible from the Enterprise Vault server. ■ If you have explicitly mapped archives to Insight Surveillance customers, ensure each target archive is mapped to a customer. ■ You have enabled the customer background tasks for the appropriate Insight Surveillance customer. ■ The archived items are suitable for sampling (for example, they must have sender/recipient information). ■ The items are stored in an archive that is eligible for sampling.
The Storage service is automatically shut down.	■ The Insight Surveillance customer and configuration databases are online and accessible from the Insight Surveillance server. ■ In the Enterprise Vault directory database, the AcceleratorConfigEntry table does not contain any entries for Insight Surveillance servers that are no longer in use.

Display issues when you open a Insight Surveillance website in Internet Explorer 10 or later

The eDiscovery Manager website may not display correctly when you open it in Internet Explorer 10 or later. If you experience this issue, you can work around it by adding the website address to the Local Intranet security zone. See the online Help for Internet Explorer for instructions.

Vault stores not displayed in the Insight Surveillance web client

In those areas of the Insight Surveillance where you can select the vault stores in which to conduct searches, the absence of vault stores may indicate that the Enterprise Vault Directory service is not running. If this is the case, try the following:

- Start the Enterprise Vault Directory service, if it is not running.
- Ensure that the same version of Enterprise Vault is running on the Insight Surveillance and Enterprise Vault servers.
- In the eDiscovery Manager website, check that the Directory DNS alias information for the Insight Surveillance customer database is correct.

TNEF-encoded attachments to Internet Mail (.eml) messages may not be readable after you export the messages from a review set

After you export Internet Mail (.eml) messages in their original form from a case review set, the contents of any TNEF-encoded attachments to the messages may not be readable.

TNEF-encoded attachments are commonly created by dragging and dropping a file into an Outlook mailbox folder. They are usually named `winmail.dat`.

Synchronization errors after you rename the SQL Server computer

If you rename the SQL Server computer, the following message may appear in the event log of the Insight Surveillance server when the Insight Surveillance database synchronizes with SQL Server:

```
Cannot add, update, or delete a job (or its steps or schedules)
that originated from an MSX server. The job was not saved.
```

For more information on this problem and guidelines on how to resolve it, see the following article in the Microsoft Knowledge Base:

http://support.microsoft.com/?kbid=281642

You may also be able to fix the problem by running a script on the SQL Server computer.

To fix synchronization errors by running a SQL script

1 Connect to your SQL Server with Query Analyzer.

2 Type the following command to access the msdb database:

```
USE msdb
```

3 Run the following script:

```
DECLARE @srv sysname SET @srv = CAST(SERVERPROPERTY('server_name')
AS sysname) UPDATE sysjobs SET originating_server = @srv
```

Where you must replace *server_name* with the new name of your SQL Server computer.

Performance counter errors when the eDiscovery Manager service starts

When the Enterprise Vault eDiscovery Manager service starts, the following error messages may appear in the event log of the Insight Surveillance server:

```
Event Type:     Error
Event Source:   eDiscovery Manager
Event Category: None
Event ID:       41978
Description:    APP ATM - Error: deleting Performance Counters
Description:    Input string was not in a correct format.

Event           Type:Error
Event           Source:eDiscovery Manager
Event Category: None
Event ID:       41980
Description:    APP ATM - Error: Creating Performance Counters
Description:    Input string was not in a correct format.
```

For more information on this problem and guidelines on how to resolve it, see the following article in the Microsoft Knowledge Base:

http://support.microsoft.com/?kbid=300956

SQL Service Broker warning when restoring a customer database to a different server

SQL Server may record the following warning message in the event log if you restore a Insight Surveillance customer database to a different server than that on which it originally resided:

```
Service Broker needs to access the primary key in the database
'database_name'. Error code:25. The primary key
has to exist and the service primary key encryption is required.
```

You can suppress this warning message by using the following SQL Server command to create a primary key for the database:

```
CREATE PRIMARY KEY ENCRYPTION BY PASSWORD = 'password'
```

For more information, see the following article on the Microsoft website:

https://msdn.microsoft.com/library/aa337551.aspx

Error messages when the Intelligent Review (IR) API authentication and authorization fails

Error: Login failed for user NT AUTHORITY\ANONYMOUS LOGON

This is a Kerberos double hop error. This error appears if the Kerberos constrained trusted delegation is not set correctly between the Surveillance Server and the Surveillance Database Server.

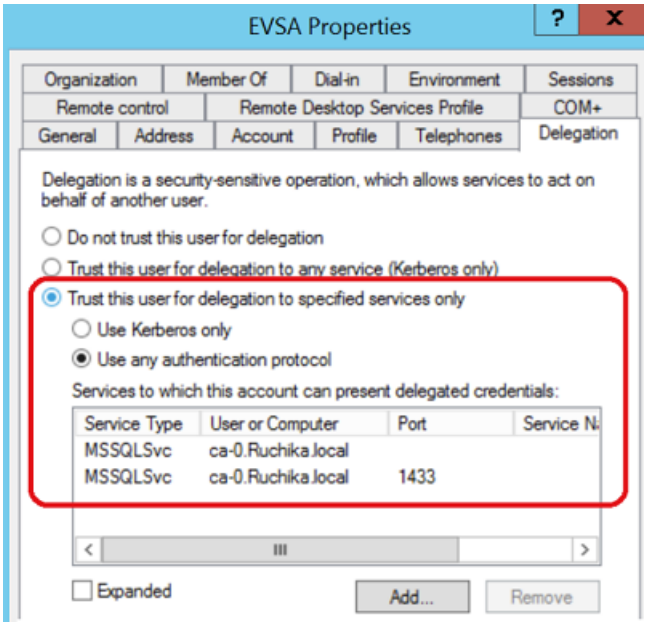
To fix this error, perform the following steps:

- Verify if the Surveillance Server is trusted for delegation.
- Check if the installation setup/environment has Kerberos constrained trusted delegation is set properly. Verify the SQL Service Service Principal Names (SPNs) for correctness, duplication, and missing SPNs. Use the Kerberos Configuration Manager tool.
- Verify if the Surveillance Server is using Fully Qualified Domain Name (FQDN) and not IP Addresses for connecting to the Surveillance Configuration and the customer databases. For configuration database, verify if the <install dir \Arctera Intelligent Review\IR.APIEndPoint \appsettings.json-> ConfigDBConnection key is using the FQDN and not IPAddress for connection string. For the customer database, verify if the configuration

database->tblCustomer table for the 'Server' field for that customer is using FQDN and not IPAddress.

- Verify if the SQL Server service account is a user, then that user is trusted for delegation, and various properties like the user is allowed for the delegation are set correctly.

Refer to the sample screen below.



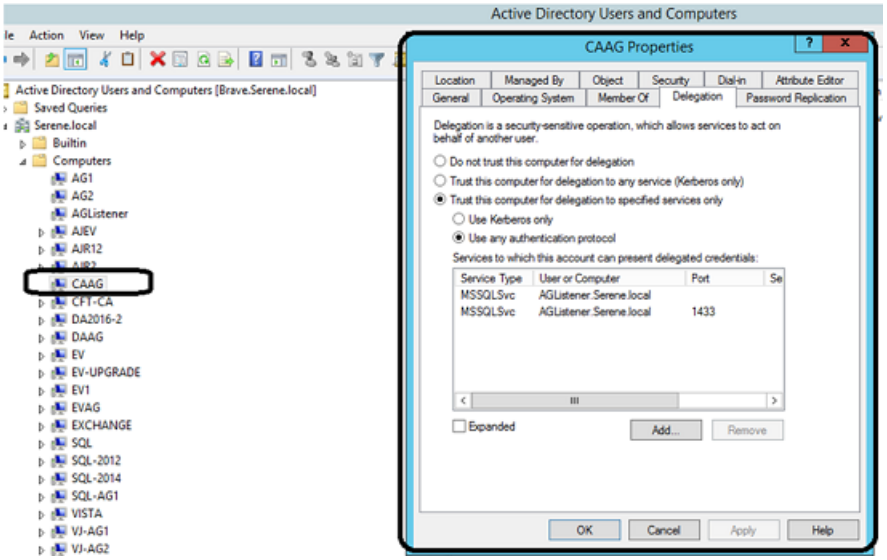
SQL Always On Setup > Kerberos delegation issues

To fix this issue, perform the following procedure:

1 Create the correct SPNs. For example, If the SQL Service is running as a Vault Service account (VSA) user, create or check if proper SPNs exist for VSA.

2 Create SPNs for the availability group listener as well as the actual SQL nodes.

3 Enable the Surveillance Server to trust for delegation (only the listener). Refer to the sample image below.

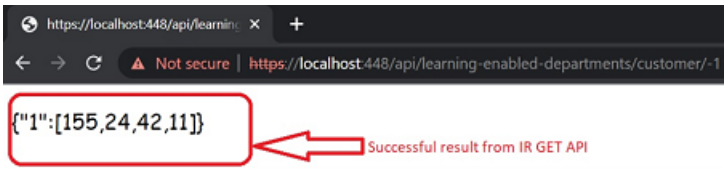


Note: Choose **Add...** while trusting for delegation and choose the SQL Service account (VSA) on which the SPNs are configured.

4 Restart the Active Directory Domain service on the Domain Controller.

5 Restart Internet Information Services (IIS) on the Surveillance Server.

6 Call the Intelligent Review (IR) API directly or via Enterprise Vault. Refer to the sample image below.



Known issues after enabling FIPS

After enabling FIPS, if you encounter any issues, refer to the following articles:

- EVBAAdmin web page fails to open correctly after enabling FIPS compliant algorithms
- Enterprise Vault Reporting's reports fail to open after you enable FIPS compliant algorithms in Windows Local Security Policy