Enterprise Vault™ Compliance Accelerator Administrator's Guide

15.0

VERITAS™

Enterprise Vault™ Compliance Accelerator: Administrator's Guide

Last updated: 2024-03-04.

Legal Notice

Veritas Technologies LLC, 2625 Augustine Drive, Santa Clara, CA 95054

https://www.veritas.com

Technical Support

Technical Support maintains support centers globally. All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policies. For information about our support offerings and how to contact Technical Support, visit our website:

https://www.veritas.com/support

You can manage your Veritas account information at the following URL:

https://my.veritas.com

If you have questions regarding an existing support agreement, please email the support agreement administration team for your region as follows:

Worldwide (except Japan)	CustomerCare@veritas.com
Japan	CustomerCare_Japan@veritas.com

Before you contact Technical Support, run the Veritas Quick Assist (VQA) tool to make sure that you have satisfied the system requirements that are listed in your product documentation. You can download VQA from the following article on the Veritas Support website:

https://www.veritas.com/support/en_US/vqa

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 Veritas 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:

evdocs@veritas.com

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

https://www.veritas.com/community

Contents

Chapter 1

Introducing Compliance Accelerator

This chapter includes the following topics:

Key features of Compliance Accelerator

Compliance Accelerator enables organizations to perform cost-effective supervisory reviews (required to follow regulatory compliance) of employee communications. Some important key features are listed below:

- **The Compliance Accelerator desktop client is replaced with the Veritas Surveillance web client**
  The Compliance Accelerator desktop client, used until the 14.5 release, is discontinued. It has been entirely replaced by the more efficient web-based alternative, Veritas Surveillance. Compared to the desktop client, Veritas Surveillance, being a web-based client, offers more convenient workflows for managing departments, employees, item searches, intelligent reviews, exporting search results, and various other operations.
  See “About Veritas Surveillance” on page 12.
  See “Feature comparison: Compliance Accelerator desktop client Vs Veritas Surveillance web client” on page 15.
- **Efficient items sampling modes**

The Veritas Surveillance web client captures items that are archived from the Microsoft Exchange, Domino journal mailboxes, SMTP, and Shared Compliance Accelerator archives. Users can select their preferred any of the below-mentioned sampling mode during configuring monitoring policy when creating a department.

- ***Guaranteed sampling***: This is the default mode. In this mode, the application captures all items for each monitored employee throughout the day. There is no option to restrict or limit the number of items that are added to the review set.
- ***Random sampling***: In this mode, the application randomly selects items from each monitored employees according to the specified monitoring policy and adds these sampled items to the review set.
- ***Statistical sampling***: In this mode, the application selects the items that are randomly sampled in the previous 24-hours period and adds these sampled items to the review set. As a result, certain employees may have fewer captured items compared to others.

- **Deduplication of items**

  This feature empowers organizations to identify and eliminate duplicates from search results, preventing their inclusion in the review set. The fingerprint mechanism is used to determine whether one item is a duplicate of another. Deduplication works within individual searches only, and does not work across multiple searches, even when conducted within the same department.

  During sampling, the duplicate items in all search types (immediate, scheduled, and guaranteed sample searches) are removed. In guaranteed sample searches, it includes randomly sampled items in the review set to make up for any shortage caused by the deduplication process.
- **Effective review process**: Messages from specific employees who are exceptions can be kept apart and checked by assigned reviewers.
- **Intelligent Review**

  This feature helps application to learn from the reviewer's actions of marking items as relevant or irrelevant, allowing it to intelligently capture and sample items the next time and categorize items as relevant or irrelevant before presenting then to reviewers. This way, reviewers can efficiently spend their review time by focusing more on the relevant items over irrelevant ones.
- **Secured database**

  A secured SQL database stores details about monitored employees, captured items, and the review processes applied to those items.
- **Enhanced Reporting**: This feature empowers organizations to enhance their reporting and analytics capabilities.

- ***SSRS reports***: Though the support for SSRS reports is discontinued, users can still access the previously generated SSRS reports from database.
- ***OData reports***: The Open Data (OData) web service enables users to retrive information from the configuration and customer databases using OData-compatible reporting tools like Microsoft Excel and PowerQuery.
- ***Enhanced reports***: New reporting endpoint APIs, such as *Departments*, *Users*, *UserRoles*, *Roles*, *ItemMetrics*, *EvidenceOfReviewByDept*, and *EvidenceOfReviewByUser* are introduced.

- **Enhanced Auditing**: This feature enables users to search and export audit records for different modules and operations within Veritas Surveillance.

About the Compliance Accelerator components

Table 1-1 lists the primary Compliance Accelerator components.

Table 1-1 The Compliance Accelerator components

Component	Notes
Enterprise Vault Business Accelerator Administration (EVBAA) website	This website lets you set up multiple Compliance Accelerator databases in which to store your data.
Enterprise Vault Accelerator Manager service	This service handles the requests from the Veritas Surveillance web client and works with the Enterprise Vault components to access archives, perform searches, and so on.
Enterprise Vault IR Classifier service	This service is a component of Intelligent Review that classifies the items as *Relevant* and *Irrelevant*.
Enterprise Vault IR ModuleBuilder service	This service is a component of Intelligent Review that builds machine learning models for departments.
IRAPIEndPoint web application	Enterprise Vault calls this API to process each indexable item for Intelligent Review.
Customer database	The customer database is a SQL database in which Compliance Accelerator stores details of departments, user roles, search results, and more. You can set up multiple customer databases.
Configuration database	The configuration database is a SQL database that specifies the location of the customer databases and stores details of the SQL Server, database files, and log files to use.

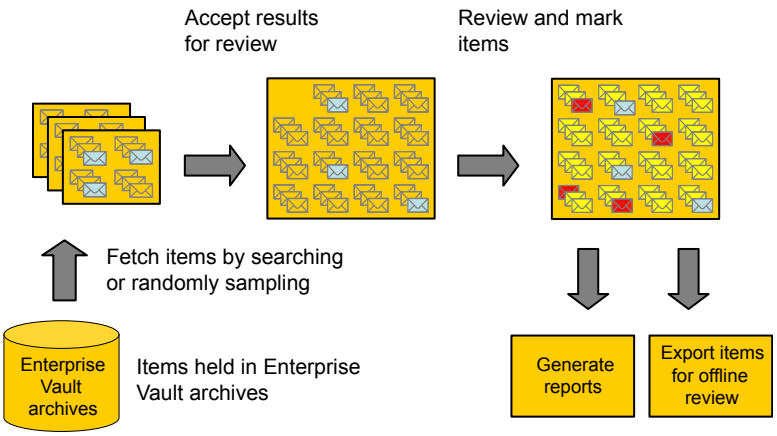
Table 1-1 The Compliance Accelerator components *(continued)*

Component	Notes
Compliance Accelerator website	This website provides functionality for some of the Compliance Accelerator reports.
Veritas Surveillance	A Web-based replacement for the Compliance Accelerator desktop client.
Enhanced Auditing	A website that offers the capability to search and export audit records for different modules and operations within Veritas Surveillance.
Enhanced Reporting	This feature increases reporting and analytics capabilities by providing reporting endpoint APIs, such as *Departments, Users, UserRoles, Roles, ItemMetrics, EvidenceOfReviewByDept, and EvidenceOfReviewByUser*.

The Compliance Accelerator process

Figure 1-1 provides an overview of the steps in the compliance process.

Figure 1-1 Steps in the Compliance Accelerator process



You typically perform the steps in the Compliance Accelerator process in the following order:

- Create an employee profile for every user who is to access Compliance Accelerator as an administrator, supervisor, or reviewer. You must also create a profile for every employee whose communications you want to monitor. You

can enter a few employee details and then populate the rest by synchronizing with the corresponding Active Directory or Domino directory account.

- Assign roles to those users or groups of users who are to perform administrative tasks in Compliance Accelerator.
  In a default Compliance Accelerator system, there are a number of predefined application and department roles. You can modify most of these as necessary, and you can create new roles. Each role has a number of permissions that are associated with it. Application roles let users perform system-wide tasks, whereas department roles let them perform certain tasks within a specific department only.
- Select the archives that you want to make available to all departments for searches. If necessary, department administrators can further customize this set of archives in their departments.
- Create one or more departments.
- In each department, do the following:
  - Assign roles to other users so that they can perform administrative, supervisor, and reviewer tasks in the department.
  - Add employees to the departments in which they are to be monitored.
  - If required, customize the archives that you want to include in your department searches.

  Compliance Accelerator is now ready to monitor employees and add items to the department review sets for reviewers to work on.
- In each department review set, review each item and add a review status mark and comment, as appropriate.
- If you want to review items offline or send them to a third party, export them in a suitable format. The export formats include PST, Domino NSF database, HTML, MSG, and ZIP.
- Use the reporting facilities to generate reports on various aspects of Compliance Accelerator, including the progress of reviewers and their roles and responsibilities.

Product documentation

Table 1-2 lists the documentation that accompanies Compliance Accelerator. This documentation is also available in PDF and HTML format in the Veritas Documentation Library.

Table 1-2 The Compliance Accelerator documentation set

Document	Comments
Installation Guide	Outlines how to perform a first-time installation of the Compliance Accelerator server and Veritas Surveillance web client.
Upgrade Instructions	Explains how to upgrade an existing installation of Compliance Accelerator.
Administrator's Guide	Provides information for Compliance Accelerator 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.
Reviewer's Guide	Describes the features of the Veritas Surveillance web client, which is a replacement of Compliance Accelerator desktop client, that are available to reviewers.
Online Help	Accompanies all the Compliance Accelerator 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 Compliance Accelerator.
Veritas Surveillance User Guide	Provides information on how to use all the key features of Veritas Surveillance.
Veritas Surveillance Reviewer's Guide	Describes the features of Veritas Surveillance that are available to reviewers.

White papers on the Veritas Support website

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

Table 1-3 White papers on the Veritas Support website

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

Chapter 2

Introducing Veritas Surveillance

This chapter includes the following topics:

About Veritas Surveillance

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

Veritas Surveillance serves as a web-based alternative for the Compliance Accelerator client. 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 Veritas Surveillance environment, ensuring compliance with your organization's supervision needs for archived electronic communications.

Routine operations executed with Veritas Surveillance

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

Veritas 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 Veritas 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 Veritas 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 Veritas Surveillance, Compliance Accelerator, 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 Veritas Surveillance system security

For enhanced system security, Veritas Surveillance implements the following measures:

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

Feature comparison: Compliance Accelerator desktop client Vs Veritas Surveillance web client

If you previously used the Compliance Accelerator desktop client and would like to examine the features of both the Compliance Accelerator desktop client and the Veritas Surveillance web client, refer to the table provided below.

Feature	Compliance Accelerator	Veritas Surveillance	Details
Only server installation required	No	Yes	Accessing Veritas Surveillance does not require client installation; server installation alone is sufficient.
Windows-based Authentication and Authorization	Yes	Yes	

Feature	Compliance Accelerator	Veritas Surveillance	Details
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	
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	

Feature	Compliance Accelerator	Veritas Surveillance	Details
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 Veritas Surveillance.
Review: Advanced Filter	No	Yes	Filter on Author/Domain and Subject is provided.
Review: Filters	Yes	Yes	
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 Veritas Surveillance.
Review: Hit highlight navigation for Hotwords	Yes	Yes	

Feature	Compliance Accelerator	Veritas Surveillance	Details
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	
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**.

Feature	Compliance Accelerator	Veritas Surveillance	Details
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	
Audio-Video Transcript support	No	Yes	
Chinese Wall security	Yes	No	
Localization of UI and Documentation	Yes	No	Compliance Accelerator user interface and user documentation are translated into Japanese, Chinese Simplified, and Chinese Traditional languages for localization purposes.

Chapter 3

Creating and viewing reports

This chapter includes the following topics:

About the Compliance Accelerator 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 21.

Enhanced reporting

Compliance Accelerator 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 22.

OData Reports

With Compliance Accelerator, 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 52.

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

   For example, in Compliance Accelerator, 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 > Compliance Accelerator Reports > ABC-Finance > MyDomain User1

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

Enhanced reporting

Compliance Accelerator 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 Compliance Accelerator. Upon successful configuration, Compliance Accelerator

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 23.

See “Departments API” on page 28.

See “Users API” on page 32.

See “UserRoles API” on page 33.

See “Roles API” on page 29.

See “ItemMetrics API” on page 37.

See “Evidence of Review by Department API” on page 42.

See “Evidence of Review by User API” on page 46.

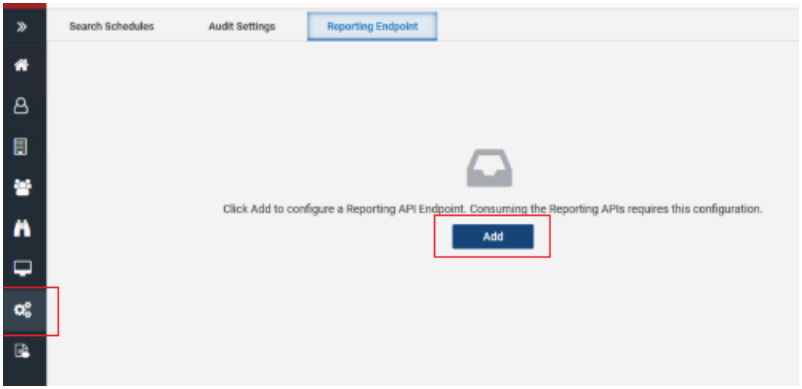
Configuring a reporting endpoint

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.

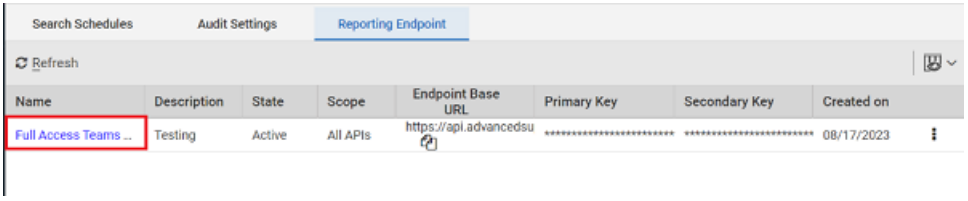


2 Click **Add**.

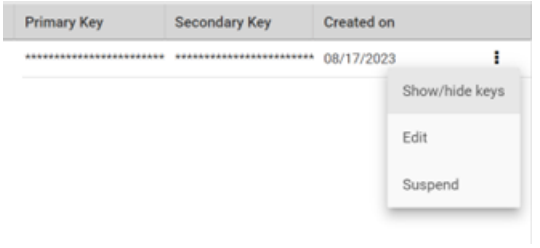
3 On the **Add New Endpoint Configuration** page, specify the following details and click **Save**.

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.



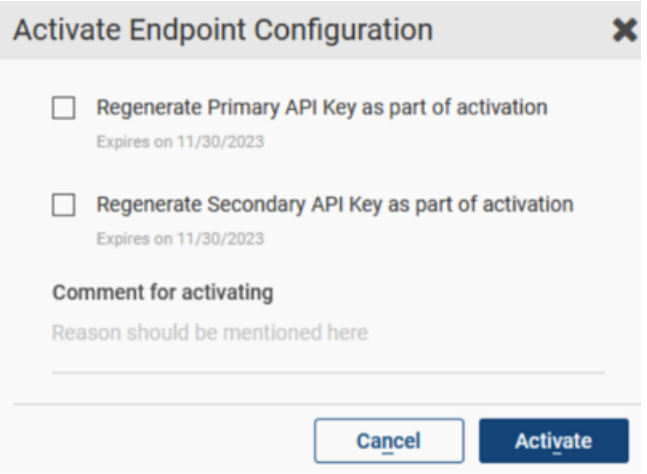
4 Click the kebab icon (three vertical dots) in the same row to perform the following actions:



- 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 49.

Responses

See “Responses” on page 51.

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 49.

Responses

See “Responses” on page 51.

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 49.

Responses

See “Responses” on page 51.

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 49.

Responses

See “Responses” on page 51.

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 49.

Responses

See “Responses” on page 51.

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 Compliance Accelerator 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 Compliance Accelerator 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 49.

Supported reporting endpoint API filters and their values

See “Supported reporting endpoint API filters and their values” on page 50.

Responses

See “Responses” on page 51.

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 Compliance Accelerator 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 Compliance Accelerator 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 Compliance Accelerator 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 49.

Supported reporting endpoint API filters and their values

See “Supported reporting endpoint API filters and their values” on page 50.

Responses

See “Responses” on page 51.

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 Compliance Accelerator 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

```
{
    {
    "@odata.context": "http://<Reporting endpoint base URL>/odata/$metadata#EvidenceOfReviewByDept",
    "value": [
        {
            "departmentId": 5,
            "departmentName": "Finance ",
            "principalID": 8,
            "monitoredEmployee": "VAS-User2",
            "totalMessages": 12,
            "captured": 3,
            "unReviewed": 3,
            "pending": 0,
            "questioned": 0,
            "reviewed": 0
        },
        {
            "departmentId": 5,
            "departmentName": "Finance ",
            "principalID": 10,
            "monitoredEmployee": "vas-user1",
            "totalMessages": 10,
            "captured": 1,
            "unReviewed": 1,
            "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 49.

Supported reporting endpoint API filters and their values

See “Supported reporting endpoint API filters and their values” on page 50.

Responses

See “Responses” on page 51.

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 Compliance Accelerator 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 VeritasidVeritas(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 Compliance Accelerator 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 49.

Supported reporting endpoint API filters and their values

See “Supported reporting endpoint API filters and their values” on page 50.

Responses

See "Responses" on page 51.

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 Compliance Accelerator 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 Compliance Accelerator datasets

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

Table 3-4 Available Compliance Accelerator 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 Compliance Accelerator 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 Compliance Accelerator.
`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 Compliance Accelerator 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 Compliance Accelerator 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 Compliance Accelerator.
`StatisticalSamplingSummary`	Information on statistical sampling data that was sent by Enterprise Vault to Compliance Accelerator.

Accessing the Compliance Accelerator 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 Compliance Accelerator 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

Compliance Accelerator 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 Compliance Accelerator, 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 Compliance Accelerator 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 Compliance Accelerator 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**.

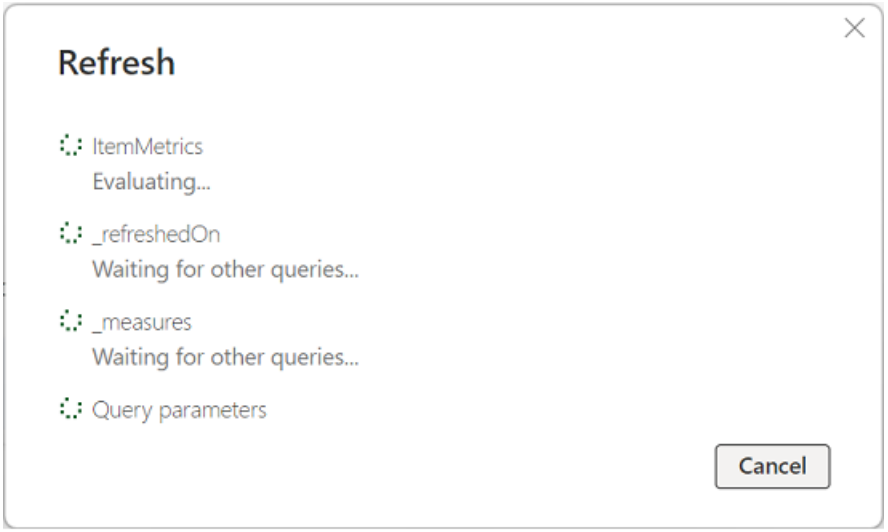
   The application prompts you several times to provide appropriate credentials when querying Reporting API for each report.

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 Compliance Accelerator 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:

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

If the Veritas 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 Veritas 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 Compliance Accelerator against the correct Enterprise Vault site. ■ The Accelerator Manager service is running. ■ In the Enterprise Vault directory database, the AcceleratorConfigEntry table contains a configuration entry for the Compliance Accelerator 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 Compliance Accelerator correctly, with monitored employees configured for sampling. ■ If you have only just configured Compliance Accelerator, 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 Compliance Accelerator configuration and customer databases is online and accessible from the Enterprise Vault server. ■ If you have explicitly mapped archives to Compliance Accelerator customers, ensure each target archive is mapped to a customer. ■ You have enabled the customer background tasks for the appropriate Compliance Accelerator 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 Compliance Accelerator customer and configuration databases are online and accessible from the Compliance Accelerator server. ■ In the Enterprise Vault directory database, the AcceleratorConfigEntry table does not contain any entries for Compliance Accelerator servers that are no longer in use.

Display issues when you open a Compliance Accelerator website in Internet Explorer 10 or later

The Accelerator 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 Veritas Surveillance web client

In those areas of the Veritas 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 Veritas Surveillance and Enterprise Vault servers.
- In the Accelerator Manager website, check that the Directory DNS alias information for the Veritas 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 Compliance Accelerator server when the Compliance Accelerator 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 Accelerator Manager service starts

When the Enterprise Vault Accelerator Manager service starts, the following error messages may appear in the event log of the Compliance Accelerator server:

```
Event Type:     Error
Event Source:   Accelerator 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:Accelerator 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 Compliance Accelerator 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 Compliance Accelerator Server and the Compliance Accelerator Database Server.

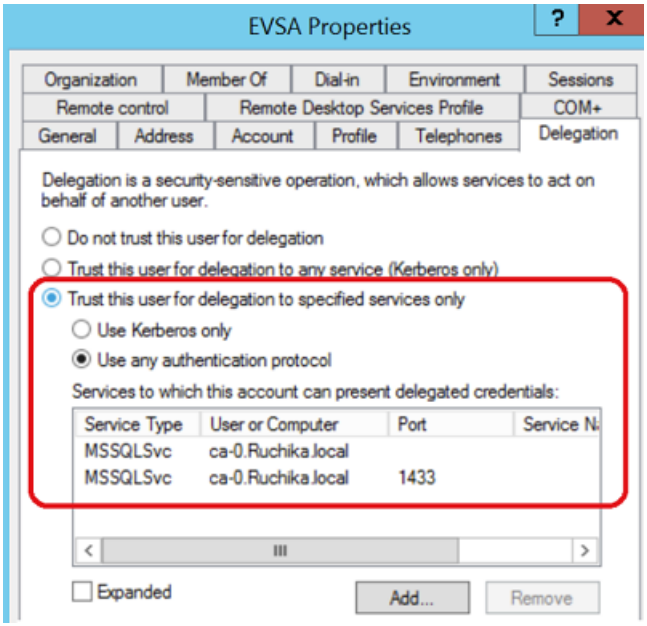
To fix this error, perform the following steps:

- Verify if the Compliance Accelerator 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 Compliance Accelerator Server is using Fully Qualified Domain Name (FQDN) and not IP Addresses for connecting to the Compliance Accelerator Configuration and the customer databases. For configuration database, verify if the <install dir \Veritas 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.

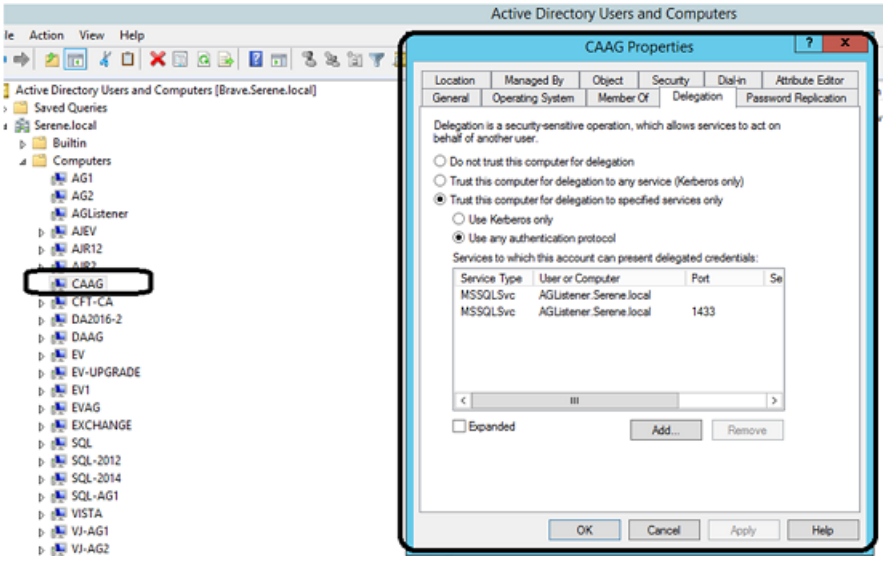


SQL Always On Setup > Kerberos delegation issues

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 Compliance Accelerator Server to trust for delegation (only the listener). Refer to the sample image below.

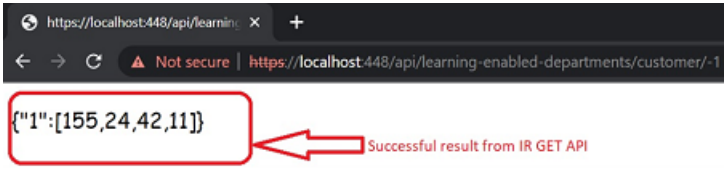


Note: Choose **Add…** while trusting for delegation and choose the SQL Service account (VSA) on which the SPNs are configured.

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

5 Restart Internet Information Services (IIS) on the Compliance Accelerator 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