# Arctera Enterprise Vault™ Insight Surveillance Installation Guide

15.2

arctera™

# Arctera Enterprise Vault™ Insight Surveillance: Installation 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

# Introducing Insight Surveillance

This chapter includes the following topics:



## About Insight Surveillance desktop application

Before the 15.0 release, the Insight Surveillance desktop application helped organizations perform cost-effective supervisory reviews of employee communications, a requirement for regulatory compliance. The role assigned to a Insight Surveillance desktop application user determined the features they could access. Administrators could manage and customize the application, while reviewers could review the items, add marks and comments to the items they reviewed.

However, during the 15.0 release, the Insight Surveillance desktop application was entirely replaced by the **Insight Surveillance web client**. For more information, See "About Insight Surveillance web application" on page 9.

From the 15.1 release, the Insight Surveillance desktop application was reinstated with limited functionalities. There is no *Reviewer* role and functionalities anymore. The Insight Surveillance administrators can still use the application. Under the **Configuration** tab, only a few functionalities are retained, allowing administrators to configure certain feature settings.

Note: If you do not have administrator permissions, contact your system administrator.

This guide explains the prerequisites and processes involved in the Insight Surveillance desktop application installation process.

# 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.

# 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. |

| Feature | Arctera Insight Surveillance Desktop Application* | Arctera Insight Surveillance Web Application | Details |
|---|---|---|---|
| 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 | |
| Department: Export | Yes | Yes | |
| Department: Hotwords | Yes | Yes | |
| Department: Labels | No | Yes | |

| Feature | Arctera Insight Surveillance Desktop Application* | Arctera Insight Surveillance Web Application | Details |
|---|---|---|---|
| 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 | |
| Review: Filters: Sentiment Score | No | Yes | |
| Review: Delegate review (on behalf of mode) | Yes | No | |

| Feature | Arctera Insight Surveillance Desktop Application* | Arctera Insight Surveillance Web Application | Details |
|---|---|---|---|
| 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 | |
| Configuration: Department partitions, Attributes | Yes | No | |
| Configuration: Message Types | Yes | No | |

| Feature | Arctera Insight Surveillance Desktop Application* | Arctera Insight Surveillance Web Application | Details |
|---|---|---|---|
| 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 | |
| Audio-Video Transcript support | No | Yes | |
| Chinese Wall security | Yes | No | |

| Feature | Arctera Insight Surveillance Desktop Application* | Arctera Insight Surveillance Web Application | Details |
|---|---|---|---|
| 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. |
| 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

# Preparing to install Insight Surveillance

This chapter includes the following topics:

# Configuration options for Insight Surveillance

Insight Surveillance software runs on a Windows server. For optimum performance, we strongly recommend that you install the server software on a dedicated computer rather than your normal Enterprise Vault server. A SQL Server computer stores all the configuration and customer information.

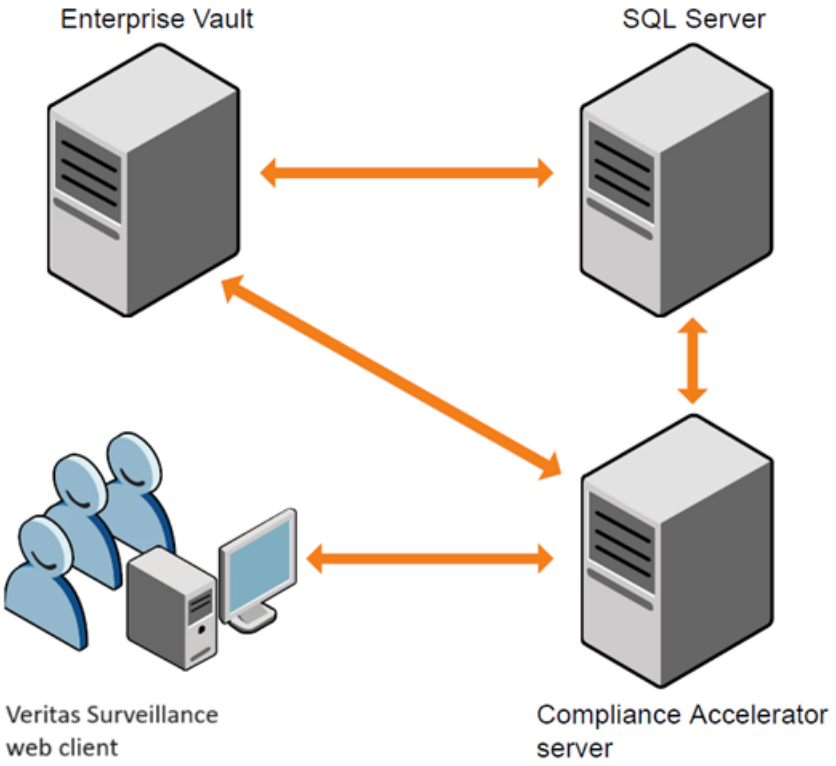
You can choose from several configuration options. If your planned configuration is different and you are unsure of what to configure on the Insight Surveillance computer, contact Arctera for advice.

## Insight Surveillance configuration for large installations

A self-contained installation of Insight Surveillance with a separate SQL Server computer minimizes the effect that intensive Insight Surveillance searches and export runs have on the Enterprise Vault installation. This configuration is likely to suit larger installations.

The Insight Surveillance computer must be in the same domain as the Enterprise Vault server or in a trusted domain.

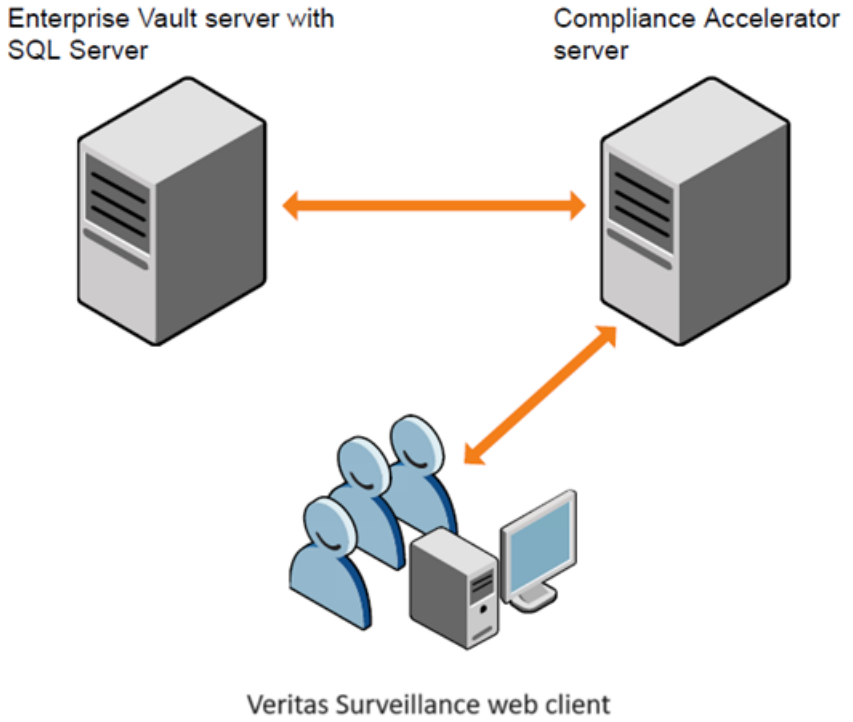
**Figure 2-1** Configuration for large installations




## Insight Surveillance configuration for smaller installations

The only difference between the configuration for smaller installations and the configuration for large installations is that, in smaller installations, Enterprise Vault and SQL Server are on the same computer.

Figure 2-2 Configuration for smaller installations




For test purposes, you can run Insight Surveillance, SQL Server, and Enterprise Vault on the same computer.

# Supported versions of Enterprise Vault in Insight Surveillance environments

You must install 15.2 version of one of the following on the Insight Surveillance server:

- Enterprise Vault Services
- Enterprise Vault API Runtime

Note the following important points:

- All Enterprise Vault servers in all Enterprise Vault sites in a Insight Surveillance environment must run the same version of Enterprise Vault.

For example, when using Insight Surveillance with two Enterprise Vault installations, you cannot have one site that runs Enterprise Vault 14.5 and another that runs Enterprise Vault 15.2.

- When upgrading both Insight Surveillance and Enterprise Vault, you must first upgrade Enterprise Vault on all Enterprise Vault servers, then Enterprise Vault on all Insight Surveillance servers, and finally Insight Surveillance itself.

See the Compatibility Charts for more information on supported versions of Enterprise Vault.

# Prerequisites for Arctera Insight Surveillance

For the latest information on supported devices and versions of software, see the Enterprise Vault Compatibility Charts.

## Prerequisites for the SQL Server computer

The SQL Server computer must be running one of the following:

- SQL Server 2016 SP3 x64 Edition, Original Release or later
- SQL Server 2017 x64 Edition, Original Release
- SQL Server 2019 x64 edition, Enterprise and Standard
- SQL Server 2022 x64 edition, Enterprise and Standard

---

Note: The sort order/collation of the SQL Server installation must be case-insensitive to match the Enterprise Vault installation. Case-sensitive installations are not supported.

---

Arctera Insight Surveillance supports SQL Server Always On availability groups and failover cluster instances for high availability and disaster recovery.

- The *Always On availability group* feature maximizes availability at the database level. An availability group provides a failover environment for a discrete set of user databases, known as *availability databases*, which failover together.
- The *Always On failover cluster instance* feature provides availability for the entire instance—a failover cluster instance (FCI). On the network, an FCI appears to be an instance of SQL Server running on a single computer, but it provides failover from one node to another.

Both of these Always On features require that the SQL Server instances reside on Windows Server Failover Clustering nodes.

For the best results when deploying Arctera Insight Surveillance in an Always On environment, we recommend that you ensure the following:

- All the server instances that host availability replicas for an Always On availability group are using the same SQL Server collation. For more information, see the following Microsoft article:
  https://msdn.microsoft.com/library/ff878487.aspx
- For the account under which the Enterprise Vault eDiscovery Manager service will run (typically the Vault Service account), you have created the same login on all the server instances that host availability replicas. For more information, see the following Microsoft article:
  https://msdn.microsoft.com/hh270282.aspx
  Note that for non-contained availability databases, you must explicitly create logins on the server instances that host the availability replicas.
- All the availability replicas have the same service primary key. You can do this by exporting the service primary key of the primary replica to a backup file, with which you can then import the key into each secondary replica. See the following Microsoft articles for instructions on how to perform these activities:
  https://msdn.microsoft.com/library/ms190337.aspx
  https://msdn.microsoft.com/library/ms187972.aspx

## Prerequisites for the Arctera Insight Surveillance server computer

Table 2-1 lists the software items that you must install and configure on the computer that is to run the Arctera Insight Surveillance server software.

Table 2-1 Required software for Arctera Insight Surveillance server installation

| Item | Notes |
|---|---|
| .NET Core | You require the following versions:<br>■ **For Surveillance**: Microsoft ASP.Net Core Runtime Windows Hosting Bundle 8.0.x. The minimum supported version is 8.0.16.<br>■ **For Reporting website**: Microsoft ASP.Net Core Runtime Windows Hosting Bundle 8.0.x. The minimum supported version is 8.0.16.<br>■ Microsoft .Net Desktop Runtime 8.0.x. The minimum supported version is 8.0.16.<br>See the `Links To Related Software` folder in the distribution media. |

Table 2-1 Required software for Arctera Insight Surveillance server installation *(continued)*

| Item | Notes |
|---|---|
| .NET Framework | You require .NET Framework 4.7.2.<br>See the `Links To Related Software` folder in the distribution media. |
| Enterprise Vault | If Arctera Insight Surveillance is installed on a separate computer from Enterprise Vault, you must install the Enterprise Vault software on the Arctera Insight Surveillance computer.<br>You require an 15.2 version of one of the following:<br>■ Enterprise Vault Services.<br>■ Enterprise Vault API Runtime.<br>See "Supported versions of Enterprise Vault in Insight Surveillance environments" on page 19.<br>There is no need to configure Enterprise Vault after you have installed it on your Arctera Insight Surveillance server computer; do not run the Enterprise Vault configuration wizard. In addition, if the Enterprise Vault Admin service is running on your Arctera Insight Surveillance server computer, we recommend that you stop it and set its startup type to Disabled.<br>To search on content with Arctera Insight Surveillance, set indexing on the Enterprise Vault archives to full. |
| Internet Information Services (IIS) | You require IIS 8.0 or later with ASP.NET, IIS 6.0 Management Compatibility, and IP and domain restrictions (for the Auditing Websites). |
| Node.js | You require Node.js (x64) version 14.17.3 or later.<br>See the `Links To Related Software` folder in the distribution media. |
| Notes client | You require version 9.0 or later of the Notes client so that client users can export Domino items.<br>Install the client in single-user mode, using the account under which the eDiscovery Manager service runs. |

Table 2-1 Required software for Arctera Insight Surveillance server installation *(continued)*

| Item | Notes |
|---|---|
| Outlook | You require Microsoft Outlook 2016, 2019, 2021, and Outlook for M365.<br><br>Outlook for M365 (32-bit supported on Enterprise Vault/Insight Surveillance Server)<br><br>Outlook for M365 (64-bit supported on Windows 10/11 Clients)<br><br>Add the AttachmentMax and RecipientMax values to the registry on the Arctera Insight Surveillance server to avoid problems when processing items that have many attachments or many recipients.<br><br>See "Configuring Outlook to enable the processing of items with many attachments or many recipients" on page 27. |
| Visual C++ Redistributable | You require the Microsoft Visual C++ 2015-2019 or later Redistributable (x86).<br><br>See the `Links To Related Software` folder in the distribution media. |
| Web browser | You require any of the following browsers:<br><br>■ Mozilla Firefox<br>■ Microsoft Edge<br>■ Google Chrome<br><br>For optimum results, do the following:<br><br>■ Configure the privacy settings in the browser to allow cookies.<br>■ Turn off any pop-up blockers.<br>■ Ensure that the advanced option **Play animations in webpages** is selected.<br>In Internet Explorer, click **Internet Options** on the **Tools** menu. Then, on the **Advanced** tab, locate the required option in the **Multimedia** category. |

Table 2-1 Required software for Arctera Insight Surveillance server installation *(continued)*

| Item | Notes |
|---|---|
| Windows | You require any of the Windows 2016, 2019, 2022, or 2025 server.<br>We recommend that you do the following:<br>■ Before you install the Arctera Insight Surveillance server software, ensure that the Windows Server service is running.<br>See "Ensuring that the Windows Server service is running on the Insight Surveillance server" on page 31.<br>■ Disable the Windows Search Service to stop it from interfering with the progress of Arctera Insight Surveillance export runs.<br>See "Disabling the Windows Search Service on the Insight Surveillance server" on page 31. |

For the best results, we recommend that you install the Arctera Insight Surveillance server software on a computer that has the following:

- At least 16 GB of memory.
- Minimum 10 GB space must be available on the hard disk where the Intelligent Review Holding Folder is located.
- Sufficient hard drive space to accommodate the searches and export runs that you expect to undertake.
  All transaction requests from Insight Surveillance web application to the Enterprise Vault and Arctera Insight Surveillance servers use the Temp folder of the Vault Service account for temporary storage. Therefore, you must ensure that this folder has sufficient free space to handle large Arctera Insight Surveillance searches and export runs. On both the Arctera Insight Surveillance and Enterprise Vault servers, the Vault Service account's Temp folder must be on a drive that has a minimum of 40 GB of free space. However, 80 GB of free space is preferable.
  Exclude the Vault Service account's Temp folders from antivirus scanning.
- Multiple hard drives. For example, you might use drive C for the operating system, drive D for the CD or DVD drive, drive E for the Temp folder of the Vault Service account, and drive F for the export output folder. You might split the Windows paging file across drives E and F.

- Configure Intelligent Review API Authentication and Authorization. See "Configuring Intelligent Review API Authentication and Authorization" on page 34.

## Prerequisites for the Enterprise Vault server computer

It is recommended to refer to the Enterprise Vault installation guide for the latest updates on prerequisites. However, the general information is as below:

You require Outlook 2016, 2019, 2021, Outlook for M365[(32-bit supported on EV/CA/DA Server) (64-bit supported on Windows 10/11 Clients)] on the Enterprise Vault server if you want to enable Insight Surveillance users to export SMTP (`.eml`) items in PST format.

The export-to-PST feature requires a 32-bit version of Outlook 2016 SP1; it does not work with the 64-bit version.

If the Storage service that manages the archived items is hosted on a separate Enterprise Vault server, you must install Outlook on that server.

## Prerequisites for Insight Surveillance

If you want to install and use Arctera Insight Surveillance, you must install and configure the following software items on the computer that is to run the Arctera Insight Surveillance server. These are in addition to the prerequisites for Arctera Insight Surveillance.

---

Note: While installing the prerequisites, you must use the domain administrator account.

---

- ASP .NET Core Runtime 8.0.x Hosting Bundle. The minimum supported version is 8.0.16.
- IIS Security feature - IP and Domain Restrictions feature must be installed using the Roles and Features option of the System Configuration application.

---

Note: Arctera Insight Surveillance can be best viewed with Mozilla Firefox or Google Chrome. Internet Explorer is not supported.

---

### Additional requirements for Arctera Insight Surveillance

**IIS setting for processes on a single server**

The default value **1** for the **Maximum Worker Processes** setting of Application Pool of the **SupervisionWeb** web application must not be changed so that Arctera Insight Surveillance functions properly while authenticating users.

**About Security Certificates**

Surveillance generates self-signed certificates for Arctera Insight Surveillance web application during configuration time to ensure all endpoints are encrypted. It is encouraged to replace these with certificates signed by well-known authorities. For details, see the following article for details on how Enterprise Vault configures an SSL Certificate.

https://www.veritas.com/support/en_US/doc/85434533-129299639-0/index

If you are accessing Arctera Insight Surveillance from a computer other than your Surveillance server, you need to import the certificate on that computer and add it to the Trusted Root Certification Authorities store. You also need to configure HTTPS.

**Disabling unsafe cryptographic protocols and cipher suites**

It is recommended to disable unsafe cryptographic protocols and cipher suites on the server to let users access Arctera Insight Surveillance without exposing your proxy server.

When a application device uses HTTPS to connect to Arctera Insight Surveillance on a proxy server, the application and server negotiate a common cryptographic protocol to secure the channel. If the application and server have multiple protocols in common, Internet Information Services (IIS) tries to secure the channel with one of the protocols that IIS supports. However, some protocols are stronger than others; to maximize the security of your environment, you may therefore want to disable the weak protocols in favor of stronger, Arctera-approved alternatives.

You can comply with Arctera recommendations by configuring the cryptographic protocols and cipher suites on your proxy server as follows:

- Enable the TLS 1.2 protocols.
- Disable the TLS 1.0 and 1.1, SSL 2.0 and 3.0 protocols.
- Disable the RC2, RC4, and DES cipher suites.

The following article in the Microsoft Knowledge Base provides guidelines on how to implement these changes:

http://support.microsoft.com/kb/245030

### Set Kerberos Trusted Delegation

For the enhanced Intelligent Review feature, you need to set the Kerberos trusted delegation between the Surveillance Server and the Surveillance Database Server. For more information on configuring the Kerberos trusted delegation, See "Configuring Intelligent Review API Authentication and Authorization" on page 34.

# Configuring Outlook to enable the processing of items with many attachments or many recipients

You must install a supported version of Outlook on the Insight Surveillance server so that application users can export Exchange Server items in PST format and download the original versions of the items.

See "Prerequisites for the Arctera Insight Surveillance server computer" on page 21.

By default, Outlook does not allow any items that have more than 2048 attachments or 2048 recipients to be opened. To avoid problems when application users try to export or download any items that have a larger number of attachments or recipients, set the registry values AttachmentMax and RecipientMax on the Insight Surveillance server.

To configure Outlook to enable the processing of items with many attachments or many recipients

1. On the Insight Surveillance server, start the Registry Editor.
2. Do one of the following:
   - If you do not use policies, locate and then click the following registry subkey:
     `HKEY_CURRENT_USER\Software\Microsoft\Office\`*`version`*`\Outlook\Options\Mail`
   - If you use policies, locate and then click the following registry subkey:
     `HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\`*`version`*`\Outlook\Options\Mail`

   Where *`version`* is `16.0` for Outlook 2016, `19.0` for Outlook 2019, and `22.0` for Outlook 2022.
3. On the **Edit** menu, point to **New**, and then click **DWORD Value**.
4. Type **AttachmentMax**, and then press Enter.
5. Right-click **AttachmentMax**, and then click **Modify**.

6 In the **Value data** box, type the required value, and then click **OK**.

The recommended value is FFFFFFFF in hexadecimal.

7 Repeat steps 3 through 6 to add the RecipientMax registry entry.

8 Exit the Registry Editor.

# Setting the Windows and ASP.NET Temp folder permissions

To enable users to access any of the Insight Surveillance websites, such as the eDiscovery Manager site, you must ensure that the Authenticated Users group has Full Control permissions in the following folders:

- The Windows Temp folder on the Insight Surveillance server. This folder is typically `%windir%\Temp`.
- The ASP.NET Temp folder on the IIS computer. This folder is typically:
  `%windir%\Microsoft.NET\Framework\version\Temporary ASP.NET Files`
  64-bit versions of Windows also have the following ASP.NET Temp folder:
  `%windir%\Microsoft.NET\Framework64\version\Temporary ASP.NET Files`

To set the Temp folder permissions

1 In Windows Explorer, right-click the folder whose permissions you want to change, and then click **Properties**.

2 Click the **Security** tab.

3 Add **Authenticated Users** and give them **Full Control**.

4 Click **Advanced**.

5 In the **Advanced Security Settings** dialog box, click **Enable inheritance**.

# Security requirements for temporary folders

---

Note: The following article on the Arctera Support website provides comprehensive information on the security requirements:

https://www.veritas.com/docs/100014060

---

On Insight Surveillance server and applications, Insight Surveillance makes occasional use of various folders for temporary storage. To protect against unauthorized access to these folders, which can contain sensitive data, Insight

Surveillance checks access to them on startup and periodically thereafter. If the security check fails on the Insight Surveillance server, the Enterprise Vault eDiscovery Manager service stops and an error event is recorded in the Arctera Enterprise Vault event log. If the security check fails on a application computer, the user must choose to rerun the check or close the application.

On server computers, Insight Surveillance checks the security of these folders:

- The temporary folder of the user who is running the Enterprise Vault eDiscovery Manager service.
- The folder that you specify as the "ECM Temporary Storage Area" through the Reviewing configuration options in the client. By default, this folder is the Windows `%TEMP%` folder.

On client computers, Insight Surveillance checks the security of the temporary folder that belongs to the user who is running the client.

In both cases, Insight Surveillance considers the following to be authorized users:

- Members of the Built-in groups Administrators, Backup Operators, Domain Administrators, and System Operators
- The user to whom the temporary folder belongs
- The Local System account

## Granting additional users and groups access to the temporary folders

On both Insight Surveillance server and application, you can set registry entries to exempt selected users or groups from the security checks or turn the checks off altogether.

To use registry entries to configure the security checks

1. On the Insight Surveillance server or application computer where you want to set the registry entries, open the Registry Editor.
2. Do one of the following:
   - On a server computer, browse to the following subkey:
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KVS
   - On a application computer, browse to the following subkey:
     HKEY_CURRENT_USER\Software\KVS
     If this subkey does not exist, you must create it. This is typically the case if you have performed a per-machine installation of the application, rather than a per-user installation.

3 Set one of the following registry entries:

| | |
|---|---|
| TempFolderExceptions | String. Specifies the names of one or more users or groups to exempt from the security check. Enter the credentials in the form *domain**user_name*, or BUILTIN*user_name* for built-in users, and separate them with semicolons. For example:<br><br>OurDomain\Marie.Lopez;BUILTIN\Server Operators |
| SkipTempFolderCheck | DWORD. Specifies whether to perform the security check (0, the default) or turn it off (1). |

4 If you set the registry entry on a server computer, restart the Enterprise Vault eDiscovery Manager service. If you set it on a application computer, restart the application.

# Disabling networking facilities that can disrupt a Insight Surveillance environment

The Windows networking subsystem provides a number of facilities that can cause issues in a Insight Surveillance environment. We recommend that you disable these facilities.

To disable networking facilities that can disrupt a Insight Surveillance environment

1 Disable the following features on your designated Insight Surveillance server, Enterprise Vault servers, and all SQL Servers that host an Enterprise Vault database:

- Receive-Side Scaling
- TCP Chimney
- TCP Segmentation Offloading
- TCP/IP Offload Engine

The following article on the Arctera Support website provides instructions on how to disable these features:

https://www.veritas.com/docs/100019120

2 Disable any network interface card (NIC) Teaming that may be present on the Enterprise Vault and Insight Surveillance servers.

For guidelines on how to disable NIC Teaming, consult the documentation that your hardware vendor provides.

# Disabling the Windows Search Service on the Insight Surveillance server

If the Windows Search Service is running on the Insight Surveillance server, it can sometimes prevent Insight Surveillance from exporting items for offline review. We therefore recommend that you disable the service, as described in the following article on the Arctera Support website:

https://www.veritas.com/docs/100028814

You can disable the service altogether or you can partially disable it by excluding selected folders from indexing, such as the Windows Temp and Insight Surveillance export folders.

# Ensuring that the Windows Server service is running on the Insight Surveillance server

When you run the installation program for the Insight Surveillance server software, it tries to assign a number of user rights to the Vault Service account, such as "Log on as a service". The installation program uses the Windows Server service to assign these rights. So, before you run the installation program, it is important to ensure that the Server service is enabled and running on your designated Insight Surveillance server.

To ensure that the Windows Server service is running on the Insight Surveillance server

1. On the Insight Surveillance server, double-click the **Administrative Tools** applet in Control Panel.
2. Double-click **Services**.
3. Start the Server service, if it is not already running.

# Configuring the SQL Server Agent service

Insight Surveillance provides the facility to create schedules with which you can conduct recurrent or future searches for items. As these schedules are SQL Server Agent jobs, you must ensure that the SQL Server Agent service is running on your SQL Server computer.

We recommend that you configure the SQL Server Agent service to start automatically when the SQL Server computer starts.

To configure the SQL Server Agent service to start automatically

1. On your SQL Server computer, double-click the **Administrative Tools** applet in Control Panel.
2. Double-click **Services**.
3. Right-click **SQL Server Agent**, and then click **Properties**.
4. Change the startup type to **Automatic**, and then click **OK**.

# Assigning SQL Server roles to the Vault Service account

The Vault Service account is the account that Enterprise Vault services and tasks use when accessing Enterprise Vault databases. You must assign a number of SQL Server roles to this account to perform various activities with Insight Surveillance. The two required roles are as follows:

- dbcreator (database creator). The facility to create configuration and customer databases with Insight Surveillance is dependent on the Vault Service account having this role.
- sysadmin (system administrator). Insight Surveillance provides the facility to create schedules with which you can conduct searches repeatedly or at some future time. These schedules are SQL Server Agent jobs and, by default, Insight Surveillance assumes that you want to make a user with the sysadmin role the creator and owner of them.

---

Note: The dbcreator and sysadmin roles are server-wide roles that may grant more security privileges to the Vault Service account than you are comfortable with. If this is the case, you can give the Vault Service account the minimum required permissions by following the instructions in this article on the Arctera Support website:

https://www.veritas.com/docs/100038151

After the Insight Surveillance is installed, you must change the value of the security configuration option "Use SQL Server SysAdmin Server Role for Schedules". For instructions on how to do this, see the *Administrator's Guide*.

---

To assign SQL Server roles to the Vault Service account

1. On the SQL Server computer, start SQL Server Management Studio.
2. In the left pane of the SQL Server Management Studio window, expand the tree to display first the required SQL Server and then the **Security** folder.

3 Under the **Security** folder, double-click **Logins** to display the users in the right pane.

4 In the **Logins** list, right-click the Vault Service account, and then click **Properties**.

5 In the **Login Properties** dialog box, select the **Server Roles** page.

6 In the **Server roles** box, make sure that **dbcreator** and **sysadmin** are selected.

7 Click **OK**.

# Installing and configuring the SQL full-text search indexing service

Insight Surveillance provides the facility to search within the review set using analytics. This facility only works when the "Full Text and Semantic Extractions for Search" feature is installed on SQL Server. Ensure that you select this feature when you install SQL Server. If SQL Server is already installed, you can add this feature by running the SQL Server setup and then selecting the option to add this feature.

You must also ensure that the SQL Full-text Filter Daemon Launcher service is running if you want to use the analytics facilities in Insight Surveillance to run analytics searches. For more information on these facilities, see the *Administrator's Guide*.

You can configure the SQL Full-text Filter Daemon Launcher service to start automatically when the SQL Server computer starts.

To configure the SQL Server Agent service to start automatically

1 On your SQL Server computer, double-click the **Administrative Tools** applet in Control Panel.

2 Double-click **Services**.

3 Right-click **SQL Full-text Filter Daemon Launcher**, and then click **Properties**.

4 Change the startup type to **Automatic**, and then click **OK**.

# Verifying that Enterprise Vault expands distribution lists

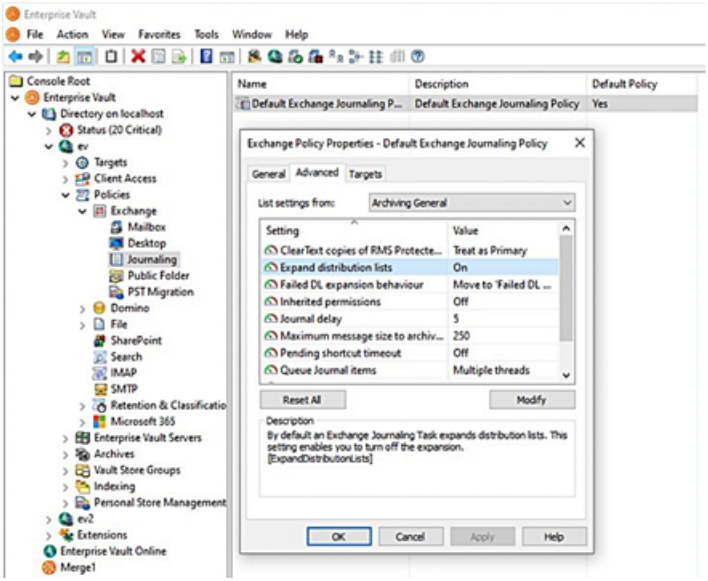
In Microsoft Exchange environments, you must ensure that the Enterprise Vault Exchange Journaling Task expands distribution lists in the To, CC, and BCC fields of items.

To verify that Enterprise Vault expands distribution lists

1 Open the Enterprise Vault Administration Console.

2 Expand the contents of the left pane until the journaling policies are visible.

3 Right-click the required policy, and then click **Properties**. For example:




4 Click the **Advanced** tab, and then check the value for the **Expand distribution lists** setting.

5 If you need to change the value for the setting, do the following:

- Click **Modify**.
- Change the value to **On**.
- Click **OK** in each dialog box to save the change that you have made.
- Restart the Journaling task to put the change into effect.

# Configuring Intelligent Review API Authentication and Authorization

In the multi-domain setup, the Surveillance server and the Surveillance Database Server reside in different domains with a trusted relationship. For the

multi-domain setup of Kerberos trusted delegation between the above-mentioned servers, follow the Microsoft documentation.

In the single-domain setup, the Surveillance server and the Surveillance Database Server reside in the same domain. For the single-domain setup, follow the procedures below.

Setting Kerberos trusted delegation between Surveillance Servers and Surveillance Database Servers

Setting Kerberos trusted delegation between Surveillance Servers and Surveillance Database Servers on IP address

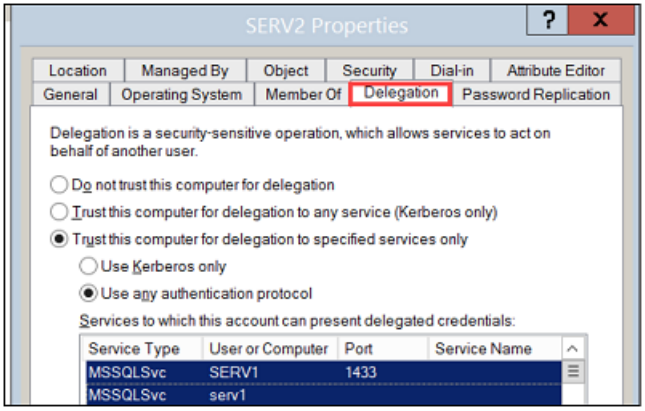
## Setting Kerberos trusted delegation between Surveillance Servers and Surveillance Database Servers

To set the Kerberos trusted delegation based on hostnames

1 Open **Active Directory Users and Computers**.

2 Click on the **Computers** node under the **Domain** node.

3 Locate the Surveillance Server. Right-click and select **Properties**.




4 On the **Delegation** tab, select **Trust this computer for delegation to specified services only** and select **Use any authentication protocol**.

5 Click **Add**.

6 In the **Users or Computers** column, enter the Surveillance Database Server Name.

7 Select the **MSSQLSvc** Services.

---

Note: If the MSSQLSvc service does not appear, instead of entering the Surveillance Database Server Name in Step 6, add the name of the Surveillance Database Service Account associated with **MSSQLSvc**. Right-click on the Surveillance Database Server (MSSQLSvc) server in Services. Right-click to select **Properties**. Click the **Log On** tab. This will identify the service account. Repeat steps 6-8.

---

8 Click **Apply** and then click **OK**.

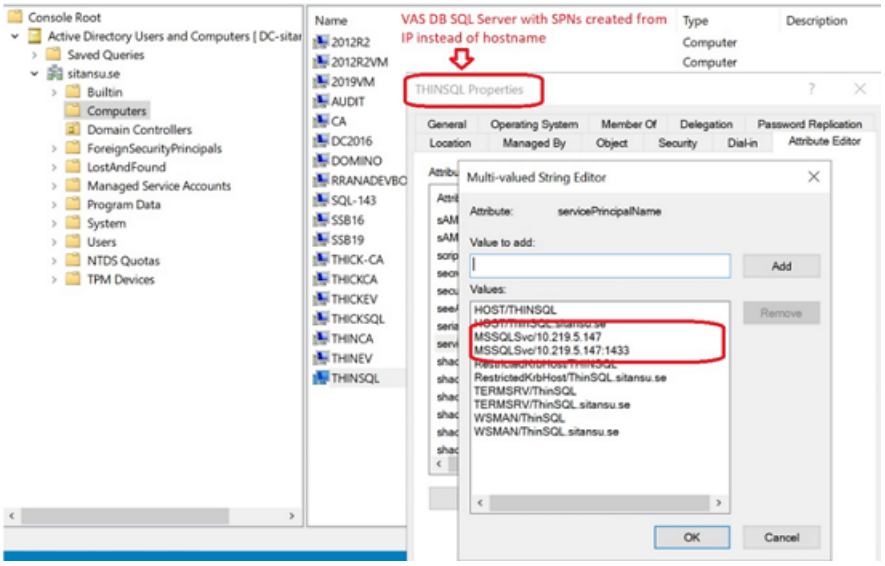
## Setting Kerberos trusted delegation between Surveillance Servers and Surveillance Database Servers on IP address

Kerberos constrained trusted delegation works with FQDNs. Since Surveillance Server has a provision to allow IP addresses instead of hostnames/FQDNs while creating or upgrading Surveillance databases, customer can configure the Surveillance database connection strings using the IP address instead of FQDN. The IP Address based delegation is restricted to some Windows Operating Systems for which Microsoft has started providing trusted delegation based on IP address.

To set the Kerberos trusted delegation based on IP address

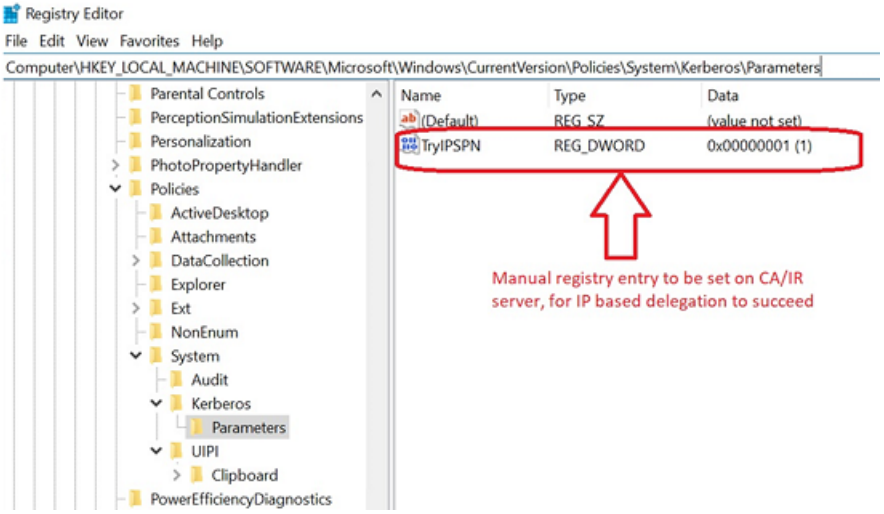
1 Check whether the Surveillance Server and the SQL Server are enabled for the IP address-based delegation support. Refer to the Kerberos trusted delegation article: Configuring Kerberos for IP Address | Microsoft Docs)

2 Configure the Surveillance SQL Server service with an SPN based on IP address, instead of hostname/FQDN.



3 Set the following registry key on the Surveillance server.

*reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\Kerberos\Parameters" /v TryIPSPN /t REG_DWORD /d 1 /f*



Chapter 3

# Installing Insight Surveillance

This chapter includes the following topics:



## Installing the Insight Surveillance server software

Follow the instructions in this section to perform a first-time installation of the Insight Surveillance server software. If you want to upgrade an existing Insight Surveillance installation, see the `CAUpgradeInstructions` file.

Before you proceed, note the following:

- You must install this software as the Vault Service account.
- Installing this software on a computer on which you have also installed the eDiscovery server software is not supported.
- You can configure Insight Surveillance for use in a Network Load Balancing cluster. However, installing the software on the nodes in other types of clusters is not supported.
  See "Installing Insight Surveillance in a clustered environment" on page 54.

To install the Insight Surveillance server software

1. Load the release media, and then do one of the following:
   - When the Install Launcher starts, follow the links to install the Insight Surveillance server software.
   - In Windows Explorer, browse to the `Arctera Enterprise Vault Insight Surveillance\Server` folder, and then run `setup.exe`.

The `setup.exe` program launches the Windows Installer (`.msi`) package that is in the same folder with elevated privileges. This is necessary to enable the installation to complete all of its processes.

2 On the **Welcome** screen, click **Next**.

The installer navigates you to the **Settings** section, where you can configure the values required for the Surveillance and the Arctera Insight Surveillance installation.

3 On the **Prerequisites** screen, scroll up and down to view the list of hardware and software required for the Surveillance and the Arctera Insight Surveillance installation.

If you meet the listed prerequisites, select the **I have read and met the above prerequisites** check box and then click **Next**.

4 On the **Prerequisite Status** screen, the installer performs a check for all required software. When the prerequisite check is completed, click **Next**.

5 On the **End-User License Agreement** screen, read the Arctera Software License Agreement. If you agree the terms, select the **I accept the terms in the License Agreement** check box and then click **Next**.

6 On the **Choose Setup Type** screen, choose between the following setup types:

| | |
|---|---|
| **Typical** | Lets you install all the components. This option is recommended for most users.<br><br>After you click **Typical**, The default path is displayed. Ensure that the path to the folder where you want to install Surveillance is appropriate. If not, click **Browse** to select path of the appropriate folder. |
| **Custom** | Lets you select or remove the components as per your requirement.<br><br>Note: It is recommended to install the Surveillance website, as it provides functionality for some of the Surveillance reports. |

---

Note: While configuring Insight Surveillance, specify details, such as **Server Alias**, **Internal Port**, and **Website Port** and ensure that you meet the additional prerequisites as needed.

---

7 On the **Accelerator Service Account Login** screen, provide the accelerator service account details such as Domain, Username, and Password. Click **Next**.

8 On the **Intelligent Review Configuration** screen, specify the following details, and click **Next**.

| | |
|---|---|
| **Server Alias** | DNS Alias name or machine name for the Surveillance server. |
| **Port** | Port for the IRAPIEndPoint Website. By default, its value is 449. If required, user can change it to valid available port number. |
| **Holding Folder path** | A directory where files of the Intelligent Review features will be stored temporarily. |

9 Click **Next**.

10 On the **Ready to install** screen, click **Install** to start Surveillance installation.

11 If you have chosen to install the eDiscovery Manager service then, when the installation program has finished, select the option to display the Enterprise Vault eDiscovery Manager website. Then you can create the configuration database and customer databases.

The installation program automatically opens the eDiscovery Manager website with administrator privileges if you have installed Insight Surveillance on a server in which User Account Control (UAC) is enabled. (This is a requirement when accessing the website in such environments.) If UAC is not enabled, a Run As dialog box may prompt you for the name and password of the user account under which to access the website. Enter the details of the Vault Service account with which you manage your Enterprise Vault server.

See "Creating the configuration database and customer databases" on page 42.

12 If you have chosen to install the Arctera Insight Surveillance, then after installation, select the option to restart the Enterprise Vault eDiscovery Manager service (EVAMS) and Internet Information Services (IIS). You can use the Services snap-in to Microsoft Management Console to restart the Enterprise Vault eDiscovery Manager service. For IIS, you should first stop EVAMS, run the `iisreset` command in an Administration Command Prompt, and then start EVAMS.

13 To ensure that all the endpoints are encrypted, Surveillance generates self-signed certificates for the IRAPIEndPoint web application during configuration. It is recommended to replace such self-signed certificates with certificates signed by well-known authorities. Import these certificates into all Enterprise Vault Storage servers and then add these certificates to the

Trusted Root Certification Authorities store. If there are multiple Surveillance servers, import the certificates from all these servers.

14 To ensure that all the endpoints are encrypted, Surveillance generates self-signed certificates for the default websites during configuration. It is recommended to replace such self-signed certificates with certificates signed by well-known authorities.

## Allowing Enterprise Vault to communicate with Insight Surveillance through the Windows firewall

You must configure the Windows firewall on the Insight Surveillance server to permit Enterprise Vault to communicate with Insight Surveillance through it. Certain interactions between the Enterprise Vault server and the Insight Surveillance server require unrestricted communication. You can allow Enterprise Vault to communicate with Insight Surveillance through the Windows firewall by adding the Accelerator service process to the exceptions list for the firewall.

You must be logged on to the computer as an administrator to complete this procedure.

To allow Enterprise Vault to communicate with Insight Surveillance through the Windows firewall

1 In Control Panel, click **System and Security**, and then click **Windows Firewall**.

2 Click **Allow a program or feature through Windows Firewall**.

3 Click **Change settings**, and then click **Allow another program**.

4 Click **Browse**, and then browse to the Insight Surveillance program folder (typically, `C:\Program Files (x86)\Enterprise Vault Business Accelerator`).

5 Click `AcceleratorService.exe`, and then click **Open**.

6 Click **Add**, and then click **OK**.

## Creating the configuration database and customer databases

After you have installed the Insight Surveillance server software, you must set up the required configuration and customer databases with the eDiscovery Manager website.

The configuration database specifies the locations of the customer databases, and it stores details of the SQL Server, database files, and log files to use. Each customer database stores details of departments, user roles, search results, and more.

You can set up one configuration database only, but you can set up multiple customer databases. The configuration database can reside on one SQL Server, and the customer databases can reside on a different SQL Server. You may find it useful to set up multiple customer databases if, for example, you want to separate the groups who are to perform searches in Insight Surveillance. Suppose that your legal department and human resources department both need to perform searches. These two departments may not be able to share roles in a Insight Surveillance system. Setting up two customers lets both departments use Insight Surveillance without needing access to the same Insight Surveillance setup.

Before you proceed, note the following:

- If you have installed Insight Surveillance on a server in which User Account Control (UAC) is enabled, you must open the eDiscovery Manager website with administrator privileges.
- If Symantec Endpoint Protection is running on your Insight Surveillance server, we recommend that you shut it down temporarily.
  See "Cannot create or upgrade Insight Surveillance customer databases when Symantec Endpoint Protection is running" on page 63.
- For database safety reasons, you must back up the configuration database on a regular basis.

To create the configuration database

1. If you have yet to display the eDiscovery Manager website, browse to the following location:

   http://*server_name*/EVBAAdmin

   Where *server_name* is the name of the server on which you installed the Insight Surveillance server software.

2. In the **Configuration Database Details** page, enter your preferred details, and then click **OK**.

| | |
|---|---|
| SQL Server | Specifies the name or IP address of the SQL Server computer. You can specify the IP address in either IPv4 or IPv6 format. SQL instances are supported.<br><br>Alternatively, in SQL Server environments where the database is part of an Always On availability group or failover cluster instance (FCI), you can specify the virtual network name or IP address of the availability group listener or FCI. For guidelines on deploying databases in Always On environments, see the following article on the Microsoft website:<br><br>https://msdn.microsoft.com/library/ff878487.aspx<br><br>You must append the port number if you have chosen to use a non-default port. For example, **SQLServer,1234**. |
| Database name | Specifies the name of the configuration database. The name cannot contain any of the following characters:<br><br>**\ / : * ? " < > \| '**<br><br>**Note**: Surveillance and eDiscovery cannot share the same configuration database. So, if you previously created the configuration database for one application, you must create a new database with a different name when setting up the other application. |
| Use Existing Database | Instructs Insight Surveillance to use the specified existing database instead of creating a new one. If you choose this option, the remaining boxes in the page are unavailable. |
| Data File Folder | Specifies a location for the configuration database file. This location should be a valid, existing path on the SQL Server computer. A minimum of 300 MB is required for the default configuration database.<br><br>You can specify a local path or a UNC path. For example, you might specify the path as `E:\SQLData` or `\\my_computer\SQLData`. |
| Log File Folder | Specifies a location for the database log files. This location should be a valid, existing path on the SQL Server computer. A minimum of 300 MB is required for the database log files.<br><br>You can specify a local path or a UNC path. For example, you might specify the path as `E:\SQLLogs` or `\\my_computer\SQLLogs`. |

| | |
|---|---|
| Initial Database Size | Sets the initial size in megabytes of the configuration database file. In the **Growth %** box, you can specify as a percentage of the file size the amount of space that is automatically added to the file each time more is needed. |
| Initial Log Size | Sets the initial size in megabytes of the database log files. In the **Growth %** box, you can specify as a percentage of the file size the amount of space that is automatically added to a file each time more is needed. |
| Windows Authentication | Specifies whether to use a Microsoft Windows user account to connect to the configuration database. If you clear this option, you must set the SQL logon name and password to use for the database connection. |
| Connection Time Out | Specifies the amount of time in seconds to wait for connections to the configuration database to complete before terminating the attempt and generating an error. |
| Connection Life Time | Specifies the time in seconds that a connection to the configuration database is considered valid. When the time has elapsed, the connection is disposed of. |
| Max Pool Size | Specifies the maximum number of database connections that can be simultaneously opened to the configuration database. |

3 Under **Database Master Key Configuration**, specify the following:

| | |
|---|---|
| Database Master Key Password | Enter Database Master Key Password.<br><br>To encrypt the data of the Configuration Database, type the password to create the SQL Server Database Master Key. Note down this password as it is required while migrating or restoring the configuration database to another SQL server instance.<br><br>This password must comply with the Windows Password Policy of the computer that is running the instance of SQL Server.<br><br>While using the existing database, if the selected database already has the database master key, the application ignores this password and proceeds to the next step. If the selected database does not have the database master key, the application uses the same password to create a new database.<br><br>Note: If you are upgrading the database, providing this password is a one-time activity only. You do not need to provide this password during the next upgrade, click **Update** to start the configuration. |
| Confirm Password | Enter the same Database Master Key Password again for confirmation. The Confirm Password must match the Database Master Key Password. |

4 When Insight Surveillance prompts you to do so, restart the Enterprise Vault eDiscovery Manager service by using the Services snap-in to Microsoft Management Console.

---

Note: Restarting the service causes Insight Surveillance to check the security of various temporary folders that the application uses. If this security check fails, an error event with an ID of 585 is recorded in the Arctera Enterprise Vault event log, and the service does not start.

See "Security requirements for temporary folders" on page 28.

---

5 In the eDiscovery Manager website, click **Upload License** to import your license key file into Insight Surveillance.

To create the customer databases

1 In the left pane of the eDiscovery Manager website, right-click the server node, and then click **New Customer**.

2 Complete the details in the **Create Customer** page, and then click **OK**.

| | |
|---|---|
| Customer Type | Indicates that this database is a customer database for Insight Surveillance. |
| Name | Specifies a unique name for the customer. The name cannot contain any of the following characters:<br>**\ / : * ? " < > \| '** |
| VaultID(s) | Identifies the journal mailbox archive that the customer uses. You can obtain the ID by looking at the archive's property page in the Vault Administration Console.<br>One customer must have a blank **VaultID(s)** field to designate that it is the default customer. All other customers must have a unique entry in the field, such as the required ID or a statement such as "Do_Not_Use". |
| Directory DNS aliases | Specifies the DNS alias, server name, or IP address of the Enterprise Vault Directory service computer. You can specify IP addresses in either IPv4 or IPv6 format.<br>Take care to specify the correct DNS alias information. If the information is wrong, no vault stores will be visible in any area of the client. |
| Administrator User or Group | Optionally nominates an Active Directory user account or group account as an administrator for the Insight Surveillance customer database. This user or group has full administrative permissions in the customer database and typically assigns application-wide roles to other users. Specify the account details in the form *domain\user_or_group_name*; for example, "OurDomain\Marie.Lopez".<br>The Vault Service account already has full administrative permissions in the customer database, so there is usually no need to nominate another user or group. However, you may want to do this if your company policy restricts the use of service accounts.<br>Note: If you choose to nominate an administrator user or group then, using the Insight Surveillance web application, you must also create an employee profile for the user or group in the customer database. For instructions on how to do this, see the *Administrator's Guide*. By creating an employee profile, you allow the user or group to perform administrative tasks in the customer database, such as deleting departments. |

| | |
|---|---|
| Enable Customer's tasks | Enables users to perform activities in the Insight Surveillance web application. If you clear this option, only automatic tasks like scheduled searches are permissible. |

**IIS section**

| | |
|---|---|
| Virtual Directory | Specifies the name of the IIS virtual directory that the Insight Surveillance reporting functionality uses.<br><br>No two customers can share the same virtual directory name. The directory name must not include space characters or any of the following characters:<br><br>*** ? \ / % ' "**<br><br>Note that you cannot name the virtual directory for any Insight Surveillance customer as "EVBAAdmin" because this name is reserved for the eDiscovery Manager website. |
| IIS Server | Specifies the name or IP address of the IIS server that is to host the Insight Surveillance site. You can type the IP address in either IPv4 or IPv6 format. However, you cannot type an IPv6 address that includes colons (:) or is enclosed in square brackets ([]).<br><br>The default entry for this field is the server on which you are running the eDiscovery Manager website. |
| Manage Virtual Directory | Lets you administer the virtual directory by using the Insight Surveillance application. By default, the option is selected. |

**Database Details section**

| | |
|---|---|
| SQL Server | Specifies the name or IP address of the SQL Server computer on which the customer database is to reside. You can specify the IP address in either IPv4 or IPv6 format. SQL instances are supported.<br><br>Alternatively, if the database is part of an Always On availability group or failover cluster instance (FCI), you can specify the virtual network name or IP address of the availability group listener or FCI.<br><br>For guidelines on deploying databases in Always On environments, see the following article on the Microsoft website:<br><br>https://msdn.microsoft.com/library/ff878487.aspx<br><br>You must append the port number if you have chosen to use a non-default port. For example, **SQLServer,1234**. |
| Database | Specifies the name of the customer database. The name cannot contain any of the following characters:<br><br>**\ / : * ? " < > \| '** |
| Use Existing Database | Instructs Insight Surveillance to use the specified existing database instead of creating a new one. If you select this option, many of the remaining boxes in the page become unavailable. By default, the option is not selected. |
| Data File Folder | Specifies a location for the configuration database file. This location should be a valid, existing path on the SQL Server computer.<br><br>You can specify a local path or a UNC path. For example, you might specify the path as `E:\SQLData` or `\\my_computer\SQLData`. |
| Log File Folder | Specifies a location for the database log files. This location should be a valid, existing path on the SQL Server computer.<br><br>You can specify a local path or a UNC path. For example, you might specify the path as `E:\SQLLogs` or `\\my_computer\SQLLogs`. |

| | |
|---|---|
| Initial Database Size | Sets the initial size in megabytes of the customer database file. In the **Growth %** box, you can specify as a percentage of the file size the amount of space that is automatically added to the file each time more is needed. |
| Initial Log Size | Sets the initial size in megabytes of the database log files. In the **Growth %** box, you can specify as a percentage of the file size the amount of space that is automatically added to a file each time more is needed. |
| Windows Authentication | Specifies whether to use a Microsoft Windows user account to connect to the customer database. If you clear this option, you must set the SQL logon name and password to use for the database connection. |
| Connection Time Out | Specifies the amount of time in seconds to wait for connections to the customer database to complete before terminating the attempt and generating an error. |
| Connection Life Time | Specifies the time in seconds that a connection to the customer database is considered valid. When the time has elapsed, the connection is disposed of. |
| Max Pool Size | Specifies the maximum number of database connections that can be simultaneously opened to the customer database. |
| DSN | Specifies the full connection string, or Data Source Name (DSN), to use when connecting to the customer database. The process of creating and connecting to the database automatically fills in this field. Do not modify the details unless Arctera Support advises you to do so. |
| Reporting FileGroup Location | During the fresh Surveillance installation or upgrade, the new Enhanced Reporting feature presents a mandatory field to specify the 'FileGroup' location. This specified FileGroup location serves as the storage for reports-specific data. It is recommended to select storage location other than the CA database location with sufficient storage. |

3 Wait for Insight Surveillance to create the customer database. This process can take several minutes to complete.

4 Repeat steps 1 through 3 for each customer database that you want to create.

# Configuring a dedicated server for Intelligent Review processing (optional deployment configuration)

Surveillance supports the installation of multiple Surveillance Servers in a single Surveillance environment. The Intelligent Review (IR) services get installed along with the installation of each Surveillance Server. Every IR component, by default, processes the customers for its own Surveillance Server.

The **Dedicated IR Server** feature enables a single Surveillance Server to be dedicated to processing all customers for Intelligent Review, irrespective of which Surveillance Server they are configured on. This option is provided so that the end user can move a load of IR processing to a less-loaded Surveillance Server if required.

To configure a Surveillance server as a dedicated IR server

1. On **Enterprise Vault eDiscovery Manager**, select **EVBAADMIN**, and open the **Server Properties** dialog box
2. Select the **Dedicated IR Server** check box adjacent to the Surveillance server you want to dedicate for Intelligent Review processing.

---

Note: There can only be a single Dedicated IR Server in the environment and is supported in a scenario where Configuration Database is shared. Refer to the following example.

---

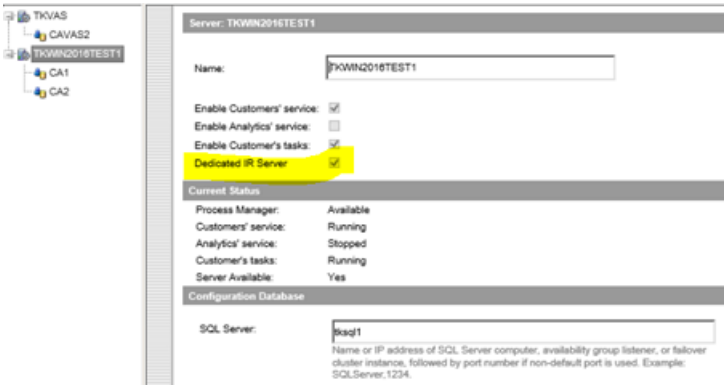
Refer to the scenario below.

Server TKVAS has only one customer (CAVAS2).

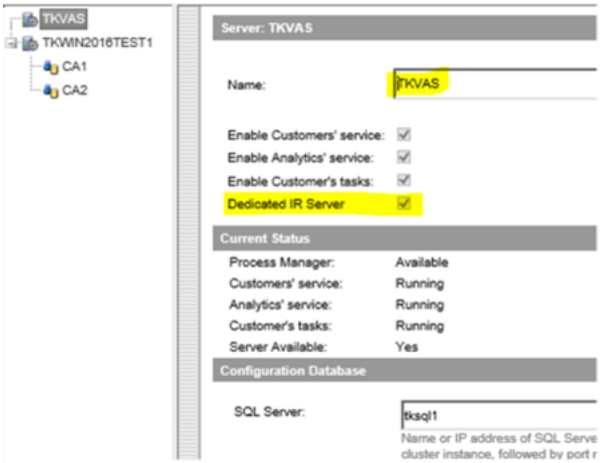
Server TKWIN2016TEST1 has two customers (CA1 and CA2).

By default, IR 2.0 services on TKVAS will process the customer CAVAS2 and IR 2.0 services on TKWIN2016TEST1 will process customers CA1 and CA2.

However, if you select the TKWIN2016TEST1 server as a Dedicated IR Server, it will serve as the only IR Server in the environment. It will process all the customers - CAVAS2, CA1, and CA2 for Intelligent Review. The IR components on another server TKVAS will not be used for IR Processing. These servers will only verify if there is any work to do. Else, these servers remain dormant. If you change the Dedicated IR Server to some other Surveillance Server, those services will then start processing Intelligent Review-related work.




Another deployment option is installing an additional Surveillance server only for IR processing. This server may not have any customers associated with it. For example, in the below sample image, there are 2 servers, where TKVAS does not have any customers and is only used for IR processing.




## Configuring Insight Surveillance for use in a SQL Server Always On environment

You may want to implement high availability and disaster recovery for Insight Surveillance by configuring it for use in an SQL Server Always On environment. An Always On solution can take advantage of two major SQL Server features for configuring high availability: *availability groups* and *failover cluster instances*. The SQL Server documentation provides extensive instructions on how to configure applications for use in such environments.

If you move your Insight Surveillance databases from a standalone SQL Server computer to an Always On availability group or failover cluster instance (FCI), you must update your configuration accordingly. The following procedures outline the required steps.

---

Caution: If you are upgrading to the latest version of Insight Surveillance from an earlier version, you must complete the upgrade before you move the databases to an Always On availability group or FCI. You cannot move the databases and then upgrade Insight Surveillance.

---

To configure Insight Surveillance for use in a SQL Server Always On environment

1. Open the eDiscovery Manager website (http://*server_name*/EVBAAdmin).
2. In the left pane of the eDiscovery Manager website, right-click the server name and then click **Properties**.
3. Set the required details for the Insight Surveillance configuration database. You can specify either of the following:
   - The name or IP address of a standalone SQL Server computer.
   - The virtual network name or IP address of an Always On availability group listener or FCI.

   You must append the port number if you have chosen to use a non-default port. For example, **SQLServer,1234**.
4. For each customer database, do the following:
   - In the left pane of the eDiscovery Manager, right-click the required database and then click **Properties**.
   - In the **SQL Server** field, set the required details for the database.
     As before, you can specify the name or IP address of a standalone SQL Server computer or an Always On availability group listener or FCI; and you must append the port number if you have chosen to use a non-default port.

## Using SQL Server Reporting Services in an Always On environment

Microsoft does not fully support the use of SQL Server Reporting Services in an Always On environment and, consequently, neither does Insight Surveillance. As the following article explains, however, it is possible to configure Reporting Services to work with an Always On availability group:

https://msdn.microsoft.com/hh882437.aspx

In summary, you must do the following to make the Insight Surveillance reports work in an Always On environment:

- Install SQL Server Reporting Services on all the replicas in the availability group.
- On all the secondary replicas, assign the same reporting server credentials to the Vault Service account as you assigned to this account on the primary replica:
  - The System Administrator role
  - The Content Manager role on the Home folder

  Use the Report Manager tool that comes with SQL Server to assign the credentials.
- On the primary replica, use the Encryption Keys page of Reporting Services Configuration Manager to back up the encryption keys for the report server databases to a file.
- Add the report server databases, ReportServer and ReportServerTempDB, to the availability group.
- When you upload the Insight Surveillance report templates through the eDiscovery Manager website, take care to specify the correct URL for the reporting server. Rather than specify the name or address of a standalone SQL reporting server, you must specify the virtual network name of the appropriate availability group listener. For example, you might specify the reporting server URL as follows:
  http://*availability_group_listener*/ReportServer
- After failover occurs, do the following:
  - Use the Reporting Services Configuration Manager to point the report server service on the new primary replica to the failed-over databases, ReportServer and ReportServerTempDB.
    Take care to specify the report server database credentials for the same domain user as you previously specified on the old primary replica.
  - On the Encryption Keys page of Reporting Services Configuration Manager, restore the encryption keys from the backup file that you previously created on the old primary replica.

## Installing Insight Surveillance in a clustered environment

Arctera does not support installing the Insight Surveillance server software on any node in a Windows Server failover cluster or Arctera Cluster Server (ACS) cluster. So, if you have configured Enterprise Vault for use in a cluster, you must

not install the server software on one of the cluster nodes. However, an unclustered Insight Surveillance installation can reference a clustered Enterprise Vault virtual server.

In addition, you can enhance the scalability, performance, and high availability of Insight Surveillance by configuring it for use in a Network Load Balancing cluster.

### Configuring Insight Surveillance for use in a Network Load Balancing cluster

Network Load Balancing (NLB) is a clustering technology that Microsoft offers as part of Windows Server 2012 or later.

NLB balances the network traffic across all the nodes in a cluster, which work together to run a common set of applications and provide the image of a single system to client users. NLB helps to enhance the scalability and performance of Insight Surveillance by distributing client requests across the nodes in the cluster; background Insight Surveillance tasks are unaffected. It also provides high availability by detecting node failures and automatically redistributing traffic to operational nodes.

The process of setting up an NLB cluster requires you to specify a virtual name or IP address for the cluster. When they start the application, your users must specify this virtual name or address as the server to which they want to connect.

To configure Insight Surveillance for use in an NLB cluster

1. Ensure that each node that you want to include in the NLB cluster has a fixed IP address.

   If you do not have these fixed addresses, you can obtain them from your network administrator.

2. Use the Network Load Balancing Manager that comes with Windows to set up and manage the cluster.

   Consult the documentation that accompanies Network Load Balancing Manager for guidelines on how to do this.

3. Install the Insight Surveillance server software on each node in the cluster.

   As a minimum, you must install the Enterprise Vault eDiscovery Manager service on each node.

## Maximizing security in your Insight Surveillance databases

The following actions can be taken to maximize the security in your Insight Surveillance databases.

- **Change database ownership and control access privileges**
  By default, the Vault Service account owns all the Insight Surveillance databases and can access all the objects in them. To maximize security in your SQL Server environment, you may want to change the ownership of each database and revoke many of the Vault Service account's access privileges. The following article on the Arctera Support website describes how to perform these activities:
  https://www.veritas.com/docs/100038151
- **Back up configuration databases**
  Configuration Database contains crucial security information such as encryption keys for every customer. This information is used to encrypt the data stored in Surveillance. To protect this security information, it is recommended to back up the configuration database regularly.

# Uninstalling Insight Surveillance

If you remove a Insight Surveillance server from an Enterprise Vault environment, you must manually remove the entry for the server from the AcceleratorConfigEntry table of the Enterprise Vault directory database. Otherwise, the Enterprise Vault Storage service may experience problems when any item is next sent for archiving.

In outline, the procedure for uninstalling Insight Surveillance is as described below.

To uninstall Insight Surveillance

1. On the Insight Surveillance server, uninstall the Insight Surveillance server software and the Enterprise Vault software.
2. Delete the AcceleratorConfigEntry table from the Enterprise Vault Directory database. You can use the following script to do this:

```
DELETE FROM
[EnterpriseVaultDirectory].[dbo].[AcceleratorConfigEntry]
```

---

Note: Uninstalling Insight Surveillance automatically removes Arctera Insight Surveillance.

---

Appendix A

# Ports that Insight Surveillance uses

This appendix includes the following topics:



## Default ports for Insight Surveillance

Table A-1 lists the default ports that Insight Surveillance uses.

Table A-1 Default ports for Insight Surveillance

| Port | Used for |
|---|---|
| 80 for HTTP, or 443 for HTTPS | Used for hosting Surveillance website in IIS. |
| 389 | Communications between the Insight Surveillance server and the Active Directory Global Catalog server for the purpose of synchronizing employee profile information through LDAP queries. |
| 449 | Communications between Enterprise Vault Storage Server and IRAPIEndPoint web application on CA Server. |
| 1433 | Communications between the Insight Surveillance server and the SQL Server computer. |
| 8085 | Communications between the Insight Surveillance server and the eDiscovery Manager website. |

Table A-1 Default ports for Insight Surveillance *(continued)*

| Port | Used for |
|---|---|
| 8086 | Communications between the Insight Surveillance server and the Insight Surveillance clients. |
| 81 and 82 | Used for hosting Surveillance website in IIS. |

Insight Surveillance uses standard DCOM ports to communicate with the Enterprise Vault server for searching, reviewing, and exporting. For information on the ports that Enterprise Vault uses, see the Enterprise Vault *Administrator's Guide*.

# Changing the ports that Insight Surveillance uses

You can set Insight Surveillance to use different ports if another application requires the default ones.

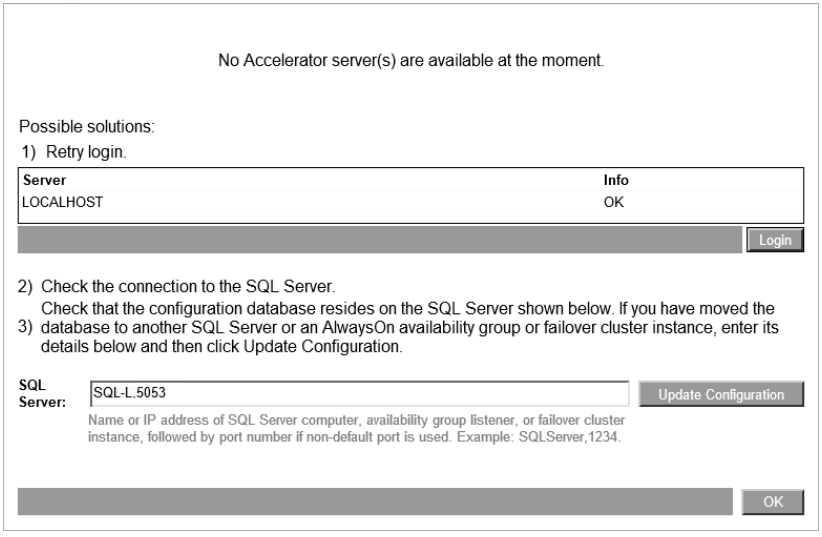
To change the port used for communications with SQL Server, if you do not use SQL Always On

1. On the Insight Surveillance server, open the eDiscovery Manager website.
2. In the left pane, right-click the server name and then click **Properties**.
3. In the **Name** field, specify the required SQL Server computer as *server_name,port_number*.
4. Click **OK** to save the change that you have made.
5. For each customer database, do the following:
   - In the left pane, right-click the name of the database and then click **Properties**.
   - In the **SQL Server** field, specify the required SQL Server computer as *server_name,port_number*.
   - Click **OK** to save the change that you have made.

To change the port used for communications with SQL Server, if you do use SQL Always On

1 If the Enterprise Vault eDiscovery Manager service is running on the Insight Surveillance server, stop it.

2 Open the eDiscovery Manager website and wait for the following page to appear (this may take several minutes):




3 In the **SQL Server** field, enter the required details and then click **Update Configuration**. For example, in the figure above, this field specifies an availability group listener (SQL-L), which is followed by a comma and then the port number 5053.

4 Start the Enterprise Vault eDiscovery Manager service.

To change the port used for communications between the Insight Surveillance server and the Insight Surveillance websites

1 On the Insight Surveillance server, locate the copies of the `Web.config` file in the `AcceleratorAdminWeb` and `ComplianceWebMin` subfolders of the Insight Surveillance installation folder. (The `ComplianceWebMin` subfolder is only present if you have chosen to install the Insight Surveillance website.)

2 Open each file in a text editor such as Windows Notepad.

3 Find the following line, and change the port number to a suitable alternative.

```
<add key="RemotePort" value="8085"/>
```

4 Save and close the files.

5 Restart the Enterprise Vault eDiscovery Manager service.

To change the port used for communications with the SQL reporting server

1 On the Insight Surveillance server, open the eDiscovery Manager website.

2 Click **Reporting Server** at the bottom of the page.

The Uploading Reporting Server Templates page appears.

3 In the **Reporting Server URL** field, type the URL with which to access the SQL reporting server in the following form:

http://*server_name*,*port_number*/*virtual_directory*

Appendix B

# Troubleshooting

This appendix includes the following topics:



## Error messages appear in the event log when upgrading to Insight Surveillance 15.2

The following messages may appear in the event log when you upgrade to Insight Surveillance 15.2 from an earlier version of Insight Surveillance:

```
Event Type: Error
Event Source: Accelerator Service Processor
Event Category: None
Event ID: 130
Description:
APP AS - Customer ID: 0 - An error has occurred when initializing
the Customers. System.Data.SqlClient.SqlException: Procedure or
function spConf_Customer_Sel has too many arguments specified.
```

And:

```
Event Type: Error
Event Source: Accelerator Service Processor
Event Category: None
Event ID: 149
Description:
APP AS - Customer ID: 0 - An error has occurred when initializing
the Servers. System.Data.SqlClient.SqlException: Procedure or
function spConf_Server_Sel has too many arguments specified.
```

You can ignore these messages, which are harmless.

# Enterprise Vault eDiscovery Manager service not created

If the installation program is unable to create the Enterprise Vault eDiscovery Manager service on the Insight Surveillance server, you may need to create it manually.

To create the Enterprise Vault eDiscovery Manager service manually

1. In Windows Explorer, search the folders under your .NET Framework installation for the file `InstallUtil.exe`.
2. Open a Command Prompt window.
3. Change to the folder that contains `InstallUtil.exe`.
4. Run the following command:

   `InstallUtil "`*`InstallFolder`*`\AcceleratorManager.exe"`

   Where *InstallFolder* is the path to the folder in which you installed the Insight Surveillance server software.
5. If the command fails, and you have more than one copy of `InstallUtil.exe`, try the same command with each of the other copies.
6. If service creation still fails, reinstall the .NET Framework and then type the command again using the newly installed copy of `InstallUtil.exe`.

# Enterprise Vault eDiscovery Manager service does not start

If you cannot start the Enterprise Vault eDiscovery Manager service, check the status of the Windows Management Instrumentation (WMI) service. If the WMI service has stopped, start it and then start the Enterprise Vault eDiscovery Manager service.

# "Access is denied" message is displayed when you try to create a customer database on a UAC-enabled computer

The following error message may appear in the eDiscovery Manager website when you create a customer database on a computer in which User Account Control (UAC) is enabled:

```
Virtual Directory Error: Access is denied
```

You can work around the issue by opening the eDiscovery Manager website as a user with administrative privileges.

To open the eDiscovery Manager website as an administrator

1. Right-click the shortcut for your web browser on the Windows **Start** menu, and then click **Run as** on the context menu.
2. Type the details of the administrator account that you want to use, and then click **OK**.
3. In the **Address** bar, type the address of the eDiscovery Manager website.

# Cannot create or upgrade Insight Surveillance customer databases when Symantec Endpoint Protection is running

If Symantec Endpoint Protection is running on your Insight Surveillance server, you may be unable to create customer databases or upgrade existing ones. We recommend that you shut down Endpoint Protection while you perform these operations.

When the Insight Surveillance server is running in a centrally managed Endpoint Protection environment, you need only disable the Intrusion Prevention check

that is responsible for the issue. Although this disables the Intrusion Prevention check on all servers that are in the same group as the Insight Surveillance server, it saves you from having to shut down Endpoint Protection completely.

To disable Endpoint Protection's Intrusion Prevention check

1. Log on to the computer where the Endpoint Protection Manager Console is running.
2. Open the Endpoint Protection Manager Console.
3. Click **Policies**.
4. Under **View Policies**, click **Intrusion Prevention**.
5. In the right pane, right-click your Intrusion Prevention policy, and then click **Edit**.
6. Click **Exceptions**.
7. Click **Add**.
8. Select the signature **ID 20079** in the list, and then click **Next**.
9. Set **Action** to **Allow** and **Log** to either option, and then click **OK**.
10. Click **OK**.
11. Wait a few moments for Endpoint Protection to roll out the policy to the servers in the group.

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

## Error: Login failed for user NT AUTHORITY\ANONYMOUS LOGON

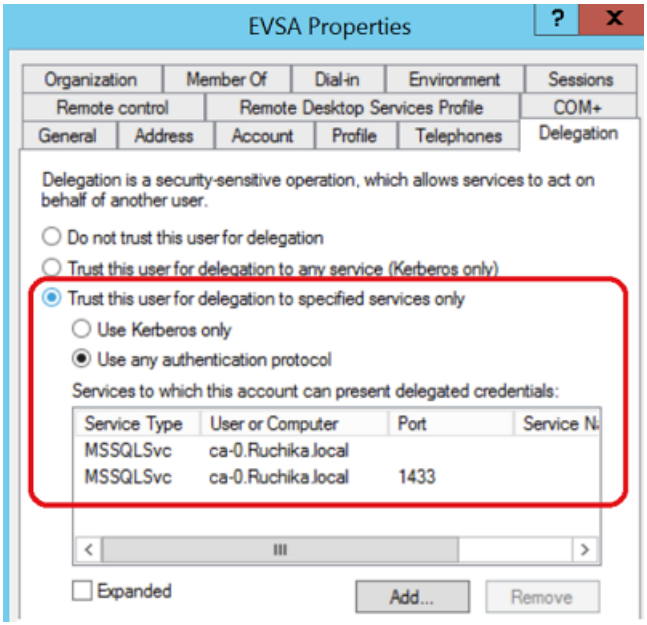
This is a Kerberos double hop error. This error appears if the Kerberos constrained trusted delegation is not set correctly between the Surveillance Server and the Surveillance Database Server.

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.

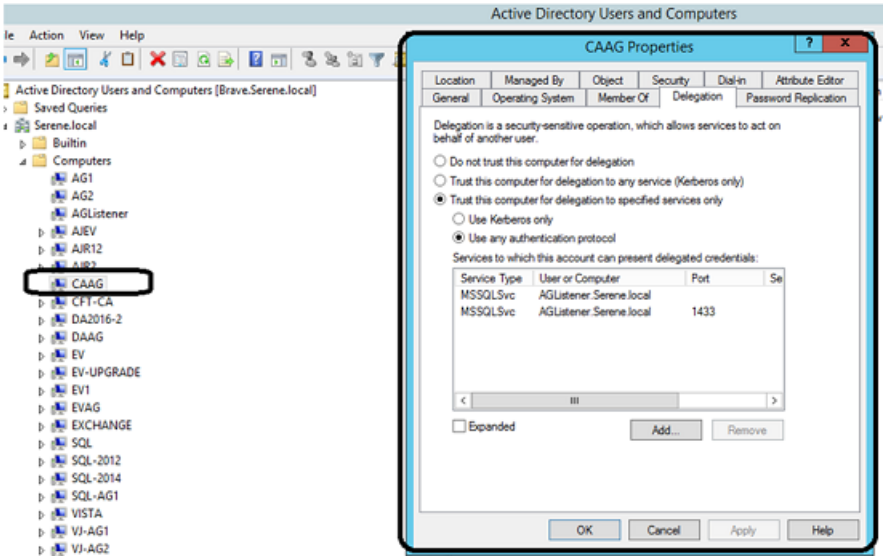



## SQL Always On Setup > Kerberos delegation issues

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.

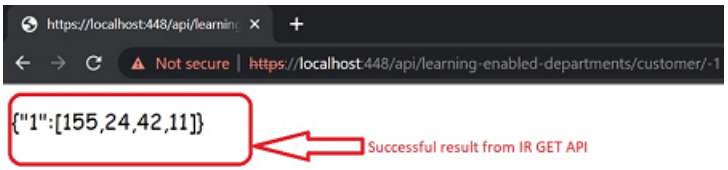



Note: Choose **Add...** while trusting for delegation and choose the SQL Service account (VSA) on which the SPNs are configured.

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.



Appendix C

# Installing and configuring the Enhanced Auditing feature

This appendix includes the following topics:



## Overview

After configuring and enabling the Enhanced Auditing feature for customers, the audit records for that customer are sent to the audit server whenever certain operations and modifications are made to modules as selected in the Audit Settings tab in Arctera Insight Surveillance. Changes to these modules made in Arctera Insight Surveillance, Enterprise Vault Insight Surveillance, or both are logged. The Audit viewer tab in Arctera Insight Surveillance lets you search and export

audit records for various modules and operations at the application, department, and folder levels.

To use the Enhanced Auditing feature, you need to follow the following workflow:

1 Meet the requirements and prerequisites.

See "Prerequisites for the Enhanced Auditing feature" on page 68.

2 Install the Enhanced Auditing feature.

See "Installing the Enhanced Auditing feature" on page 69.

3 Set the **Auditing** configuration options in the **Configuration** tab in the Insight Surveillance client.

4 Use the **Audit Settings** tab in Arctera Insight Surveillance to edit the required settings for auditing.

5 Use the **Audit viewer** tab in Arctera Insight Surveillance to search and export the audit records.

# Prerequisites for the Enhanced Auditing feature

You must meet the following requirements for the Enhanced Auditing feature.

## Hardware requirements

The Enhanced Auditing feature must be installed on a server other than Arctera Insight Surveillance and Surveillance server. This audit server will host both Auditing API endpoint and optionally Elasticsearch.

The audit server must have a minimum configuration of 8 GB RAM, 2 CPUs, and 100 GB HDD.

## Software requirements

- Windows Server 2016, Windows Server 2019, Windows Server 2022 or Windows Server 2025
- Microsoft .NET 4.7.2
- Internet Information Services 8.5 or later version
- IIS Security feature - IP and Domain Restrictions feature must be installed using the Roles, Role Services, and Features wizard of the Server Manager console.
- ASP .NET Core Runtime 8.0.x Hosting Bundle. The minimum supported version is 8.0.16.
- PowerShell 4.0 or later version

Note: The Enhanced Auditing feature installer installs the other required applications, including Elasticsearch 7.17.4 (only if the existing Elasticsearch is not being used). In case the installer fails to install Elasticsearch, you must manually install it. If you already have installed Elasticsearch, you can use the existing Elasticsearch URL and server details.

Even if the Enhanced Auditing feature is uninstalled, Elasticsearch does not get uninstalled.

Enhanced Auditing is not supported with Elasticsearch version 6. Update to the latest supported version of Elasticsearch for Enhanced Auditing, which is 7.x. (Elasticsearch 8.x is not supported).

# Installing the Enhanced Auditing feature

Follow the instructions in this section to perform a first-time installation of the Enhanced Auditing feature.

Before you proceed, note the following:

- You must belong to the local Administrators group.
- You must be a domain user.
- You meet the minimum hardware and software requirements.

To install the Enhanced Auditing feature

1. Copy the MSI file of the Enhanced Auditing feature on the server you want to use as an audit server.
2. In Windows Explorer, browse to the MSI file, and then run *setup.exe*. The *setup.exe* program launches the Windows Installer (.msi) package.
3. Click **Next** on the **Welcome** screen.
4. On the **Prerequisites** screen, see if you meet the listed prerequisites. If yes, select the **I have read and met the above prerequisites** check box and then click **Next**.
5. On the **Prerequisite Status** screen, the installer performs a check for all required software. When the prerequisite check is completed, click **Next**.
6. On the **End-User License Agreement** screen, read the Arctera Software License Agreement. If you agree the terms, select the **I accept the terms in the License Agreement** check box and then click **Next**.
7. On the **Installation location** screen, the default installation location is displayed. If you want to use a different installation location, click **Browse** to select the installation location.

8 On the **Auditing Service Account Login** screen, provide the following account details for the Auditing Service.

- **Domain**
- **Username**
- **Password**

9 On the **Arctera Enhanced Auditing Configuration Welcome** screen, provide the following required details for creating the Audit Server URL and enabling it for secure access.

- **Server Name**: DNS Alias name or FQDN for the audit server.
- **Port**: Port for the audit server site. Enter a port that is available to use. You must not use the default IIS port 80.
- **Comma-separated list of IP addresses from where the audit server can be accessed**: Enter a comma-separated list of IPv4 addresses of the Insight Surveillance server.

  ---

  Note: Although installing the audit server on the Insight Surveillance server is possible, its configuration may fail due to lack of IPv6 support. To avoid potential issues while configuring the audit server:

  - Configure the audit server on a server separate from the Insight Surveillance server, or

  - Disable IPv6 configuration on the Insight Surveillance server.

  There is no need to disable IPv6 when configuring *SupervisionAPI*, *SupervisionWeb*, and other Insight Surveillance services.

  ---

- **Holding folder Path**: A directory where the audit data will be stored temporarily.

  ---

  Note: Ensure that the Access Control List (ACL) of the Holding Folder is not changed.

  ---

Based on these details, the audit server URL format becomes: `https://<auditservername>:<portnumber>`.

Click **Next** after entering all required details.

10 On the **Arctera Enhanced Auditing Configuration Settings** screen, enter details of either an existing Elasticsearch server or a new Elasticsearch server.

For an existing Elasticsearch server, select the **Use an existing Elasticsearch server** details, and then provide the following details:

- **Elasticsearch URL**: URL of the Elasticsearch server.

  ---

  Note: Ensure that security is enabled with native realm.

  If Elasticsearch has TLS enabled, then ensure that the required configurations also exist on the audit server. For more information on security in Elasticsearch, refer to the Elasticsearch documentation.

  ---

- **Elasticsearch Username**: Username of the Elasticsearch superuser. This superuser is displayed at the time of upgrading and modifying the Enhanced Auditing feature. The Enhanced Auditing feature uses this superuser to perform the user and role management operations on Elasticsearch.
- **Elasticsearch Password**: Password of the Elasticsearch superuser.

To install a new Elasticsearch server, enter the password in the **Set password for Elasticsearch built-in users** field. When prompted, specify the **Elasticsearch installation location** where you want to install Elasticsearch.

Click **Next** after entering all required details.

11 Click **Install** to proceed with the installation.

12 On the final screen of the setup, the **Audit Server URL** is displayed. You need this URL while configuring the **Auditing** settings in the **Configuration** tab in the Insight Surveillance client.

13 To view the installation-specific logs, navigate to the folder where you have installed the Arctera Enhanced Auditing setup and access the **Temp** folder.

---

Note: Even after the Enhanced Auditing feature is uninstalled, Elasticsearch does not get uninstalled.

---

# Post installation steps

## Install certificates

After successful installation of the audit server, the installer creates a self-signed certificate named *AuditAppCert*. It is recommended that the self-signed certificate on the audit server should be replaced with a valid certificate from a well-known authority.

You must export the certificate from the audit server and manually install it on the Arctera Insight Surveillance server's trusted certificate store.

### Configurations in Insight Surveillance client

After you complete the installation of Enhanced Auditing, complete the required steps for configuring the **Auditing** settings in the **Configuration** tab in the Insight Surveillance client. For details, refer to the Insight Surveillance client Help.

### Configurations in Arctera Insight Surveillance

Later, you also need to perform additional Auditing settings in Arctera Insight Surveillance. For details, refer to the Arctera Insight Surveillance Help.

## Upgrading the Enhanced Auditing setup

To upgrade the Enhanced Auditing setup

1. Navigate to the Arctera Enhanced Auditing windows installer setup on your local computer.
2. Extract the zipped content to access the Windows installer package file (MSI file).
3. Launch the Arctera Enhanced Auditing installer. To launch the installer, do any of the following steps:
   - Run the MSI file from the **Command Prompt**.
   - Right-click on the available MSI file and click **Run as administrator**.

   The installer opens the **Welcome** wizard.

   ---

   Note: Click **Cancel** if you want to cancel the installation at any stage. After you click **Cancel**, the application prompts you to confirm the operation. If you interrupt the installation process, the installer prompts you to run the installation again whenever required. Click **Yes** to complete the operation and click **Finish** to abort the installation. Click **No** to continue the installation.

   ---

4. Click **Next** to proceed to the **Settings** wizard.

   The application displays the **Prerequisites** page.
5. Verify the prerequisites, and select the **I have read and met the above prerequisites** check box to confirm you have all the prerequisites.

6 Click **Next** to view the **Prerequisite Status** page.

If the required prerequisites are not installed on your computer, it shows **Error** instead of **OK** for the corresponding prerequisite. The **Next** button remains disabled. You need to install the corresponding perquisites to enable the **Next** button.

7 Click **Next** to view the **Auditing Service Account Login** page, and provide the correct credentials.

---

Note: This user must be a domain user that belongs to the local administrator's group.

---

8 Click **Next** to view the **Arctera Enhanced Auditing Configuration** page, and provide Elasticsearch superuser credentials.

The installer displays the Elasticsearch URL and the Username that a user is using currently.

9 Click **Next** to navigate to the next page, and click **Install**.

To review or change the configuration, click **Back**. To cancel the installation at this stage, click **Cancel**.

10 After the upgrade is complete, click **Finish** and restart the server to apply the changes.

11 To view the upgrade log file, navigate to the folder where you have installed the Arctera Enhanced Auditing setup and access the **Logs** folder.

# Modifying the Enhanced Auditing setup

To modify the Enhanced Auditing setup

1 Launch the Arctera Enhanced Auditing installer. To launch the installer, do any of the following steps:

- Run the MSI file from the command prompt.
- Right-click on the available MSI file and click **Run as administrator**.
- Navigate to the **Control Panel** and double-click the **Add or Remove Programs** applet. Find and click Arctera Enhanced Auditing in the list of installed programs.

The installer opens the **Welcome** wizard.

Note: Click **Cancel** if you want to cancel the installation at any stage. After you click **Cancel**, the application prompts you to confirm the operation. If you interrupt the installation process, the installer prompts you to run the installation again whenever required. Click **Yes** to complete the operation and click **Finish** to abort the installation. Click **No** to continue the installation.

2 Click **Next** to proceed to the **Settings** wizard. On the **Modify, repair, or remove installation** page, click **Modify**.

3 On the **Arctera Enhanced Auditing Configuration** page, provide the following details to create an Audit Server website and enable it for secured access. Then, click **Next**.

- **Server Name**: Change the DNS Alias name or FQDN for the audit server, if required.
- **Port**: Change the Port for the audit server site, if required. Enter a new port that is available to use. You must not use the default IIS port 80.
- **Comma-separated list of IP addresses from where the audit server can be accessed**: Enter a comma-separated list of IP addresses of the servers from which the audit server needs to be accessed. These are the IP addresses for the Arctera Insight Surveillance server. If you want to keep the previous IP addresses, do not delete them. If you delete the previous IP addresses, the new IP addresses overwrite the previous ones. You can add the new IP addresses by separating every IP address by a comma. You can also provide ranges of IP addresses, for example - 10.219.5.227,10.219.5.226-229.
- **Holding folder Path**: Browse to another directory where the audit data is stored temporarily, if required.
  Even though the previously selected holding folder may not be in use, it does not get deleted after the modification.

  Note: Ensure that the Access Control List (ACL) of the Holding Folder is not changed. The default users, such as SYSTEM, Built-in administrators, Audit Server Account, and IIS APPPOOL\AuditingServer, must be unchanged.

  Based on these details, the audit server URL format becomes:*https://<auditservername>:<portnumber>*.

4 Click **Next**.

---

Note: If you try to modify the Elasticsearch URL, the application displays a warning message that the existing server data (auditing-specific) will not be automatically migrated to the new server. Therefore, before you change the Elasticsearch URL, ensure that you need to migrate it manually to the Elasticsearch server you want to use. Otherwise, this data will be lost.

---

5 On the **Settings** wizard, on the **Ready to install** page, click **Install**.

6 On the **Arctera Enhanced Auditing Configuration** page, ensure that the Elasticsearch installation location is appropriate. Then, click **Next**.

7 After the modification is complete, click **Finish** and restart the server to apply the changes.

8 To view the modification-specific logs, navigate to the folder where you have installed the Arctera Enhanced Auditing setup and access the **Logs** folder.

# Repairing the Enhanced Auditing setup

To repair the Enhanced Auditing setup

1 Launch the Arctera Enhanced Auditing installer. To launch the installer, do any of the following steps:

- Run the MSI file from the command prompt.
- Right-click on the available MSI file and click **Run as administrator**.
- Navigate to the **Control Panel** and double-click the **Add or Remove Programs** applet. Find and click Arctera Enhanced Auditing in the list of installed programs.

The installer opens the **Welcome** wizard.

Note: Click **Cancel** if you want to cancel the installation at any stage. After you click **Cancel**, the application prompts you to confirm the operation. If you interrupt the installation process, the installer prompts you to run the installation again whenever required. Click **Yes** to complete the operation and click **Finish** to abort the installation. Click **No** to continue the installation.

2 Click **Next** to proceed to the **Settings** wizard. On the **Modify, repair, or remove installation** page, click **Repair**.

The **Auditing Service Account Login** page appears.

3 On the **Auditing Service Account Login** page, ensure that your domain and username are correct. In the **Password** field, provide your correct password, and click **Next**.

4 On the **Arctera Enhanced Auditing Configuration** page, ensure that your Elasticsearch URL and the Elasticsearch Username are correct. In the **Elasticsearch Password** field, provide your correct password, and click **Next**.

5 On the **Repair Arctera Enhanced Auditing** page, click **Repair**.

6 On the **Installation** wizard, on the **Repairing Arctera Enhanced Auditing** page, view the status of the repairing operation. The sample screen is shown below

7 After the repair is complete, click **Finish** and restart the server to apply the changes.

8 To view the repairing-specific logs, navigate to the folder where you have installed the Arctera Enhanced Auditing setup and access the **Log** folder.

# Uninstalling the Enhanced Auditing setup

To uninstall setup from Control Panel

1 On a computer where you want to perform the uninstallation, access **Control Panel**.

2 Double-click the **Add or Remove Programs** applet.

3 Find and click **Arctera Enhanced Auditing** in the list of installed programs.

4 Click **Uninstall**, and then follow the on-screen instructions.

To uninstall setup from Arctera Enhanced Auditing wizard

1 Launch the Arctera Enhanced Auditing installer. To launch the installer, do any of the following steps:

- Run the MSI file from the command prompt.

- Right-click on the available MSI file and click **Run as administrator**.
- Navigate to the **Control Panel** and double-click the **Add or Remove Programs** applet. Find and click Arctera Enhanced Auditing in the list of installed programs.

The installer opens the **Welcome** wizard.

2 Click **Next** to proceed to the **Settings** wizard. On the **Modify, repair, or remove installation** page.

3 Click **Remove**, and then follow the on-screen instructions.

# Managing access from Arctera Insight Surveillance

While installing the Enhanced Auditing feature, you provide a comma-separated list of IP addresses of the servers from which the audit server will be accessed. These are the IP addresses for the Arctera Insight Surveillance server. These IP addresses get listed under allowed sites in IIS Manager. If an IP address of the Arctera Advanced server is changed, you need to update that IP address in IIS Manager on the audit server so that the audit server can be accessed.

To update the allowed IP addresses to access the audit server

1 On the audit server, open the IIS Manager.

2 Expand **Sites**, and then click the Auditing Server site.

3 In the right pane, double-click **IP Address and Domain Restrictions** .

4 On the **IP Address and Domain Restrictions** screen, right-click the entry containing the old address for Arctera Insight Surveillance API server, and then click **Remove**.

5 Under **Actions**, click **Add Allow Entry**.

6 On the **Add Allow Restriction Rule** dialog, add the new IP address in the **Specific IP address** field, and then click **OK**.