Arctera Enterprise Vault™ eDiscovery Installation Guide

15.2

arctera™

Arctera Enterprise Vault™ eDiscovery: Installation Guide

Last updated: 2025-09-11.

Legal Notice

Arctera US LLC | www.arctera.io

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.

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

Contents

Chapter 1

Introducing eDiscovery

This chapter includes the following topics:

Key features of eDiscovery

eDiscovery is an electronic discovery and review system that integrates with Enterprise Vault services and archives. eDiscovery lets authorized users search for, retrieve and preserve, analyze, review, mark, and export or produce emails, documents, and other electronic items for lead counsel examination or court-ready production—rapidly and in a cost-effective manner.

Using attorneys and external counsel to review large numbers of items is costly. With eDiscovery, you can create a hierarchy of reviewers for a discovery action or case, with different levels of reviewers able to assign certain review marks. In this way, paralegal staff and non-legal staff can perform an initial review of search and collection results and leave only the privileged, relevant, or questionable items for counsel. Optionally, you can then produce the relevant items with an appropriate *Bates* number or else simply export them from eDiscovery in various formats.

About the eDiscovery components

Table 1-1 lists the primary eDiscovery components.

Table 1-1 The eDiscovery components

Component	Notes
eDiscovery client	The client is used by eDiscovery administrators to set up and manage the system and by reviewers to access the items that they are to mark.
Enterprise Vault Business Accelerator Administration (EVBAA) website	This website lets you set up multiple eDiscovery databases in which to store your data.
Enterprise Vault eDiscovery Manager service	This service handles the requests from the Arctera Surveillance web client and works with the Enterprise Vault components to access archives, perform searches, and so on.
Customer database	The customer database is a SQL database in which eDiscovery stores details of cases, user roles, search results, review marks and tags, and more. You can set up multiple customer databases.
Configuration database	The configuration database is a SQL database that specifies the location of the customer databases and stores details of the SQL Server, database files, and log files to use.
Insight eDiscovery Custodian Manager website (optional)	This website lets you store the details of the *custodians* (individual employees) and custodian groups for which you want to search with eDiscovery. A custodian group is any collection of employees, such as Windows or Domino groups and distribution lists, Active Directory or Domino LDAP searches, and Active Directory containers.
eDiscovery API website (optional)	This website lets you use the eDiscovery API to integrate third-party tools with the software, and thereby retrieve data from or export it to a eDiscovery customer database. For more information on the eDiscovery API, contact Arctera Support.
Conversation UI website	This website lets eDiscovery display Microsoft Teams data in Teams like UI. It also facilitates infinite scrolling for teams chat to get more context of the item being reviewed.

Product documentation

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

Table 1-2 The eDiscovery documentation set

Document	Comments
Installation Guide	Outlines how to perform a first-time installation of the eDiscovery server and client software.
Upgrade Instructions	Explains how to upgrade an existing installation of eDiscovery.
Administrator's Guide	Provides information for eDiscovery administrators on how to set up and assign roles, search for items to include in the review set, export items for offline review, create reports, and more.
Reviewer's Guide	Describes the features of the eDiscovery client that are available to reviewers.
Online Help	Accompanies all the eDiscovery 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 eDiscovery.
Best Practices Guide	Provides extensive information on how best to plan for and implement eDiscovery. To obtain this guide, go to the following page of the Arctera Support website: https://www.veritas.com/docs/100024378

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 1-3 White papers on the Arctera Support website

White paper	Describes
Accelerator Deduplication	The deduplication features in eDiscovery.
Effective Searching	How to conduct searches with eDiscovery.

Table 1-3 White papers on the Arctera Support website *(continued)*

White paper	Describes
Effective Reviewing	The features and tools that are available to eDiscovery reviewers.
Best Practices for Enhanced Accelerator Reporting	How to create custom eDiscovery reports using the Open Data (OData) protocol.

eDiscovery training modules

Arctera Education Services provides comprehensive training for eDiscovery, from basic administration to advanced topics and troubleshooting. Training is available in a variety of formats, including classroom-based and virtual training.

For more information on eDiscovery training, curriculum paths, and certification options, see https://www.veritas.com/services/education-services.

Chapter 2

Preparing to install eDiscovery

This chapter includes the following topics:

Configuration options for eDiscovery

eDiscovery 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.

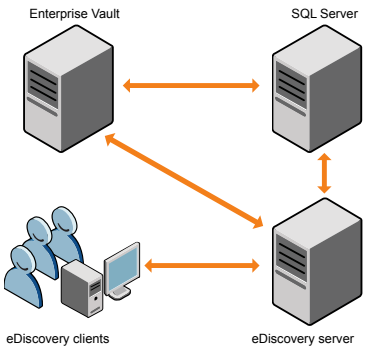
You can choose from several configuration options. If your planned configuration is different and you are unsure of what to configure on the eDiscovery computer, contact Arctera for advice.

eDiscovery configuration for large installations

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

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

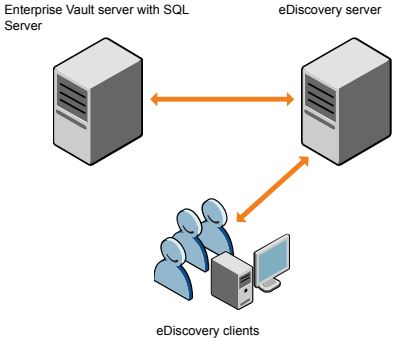
Figure 2-1 Configuration for large installations



eDiscovery 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 eDiscovery, SQL Server, and Enterprise Vault on the same computer.

Supported versions of Enterprise Vault in eDiscovery environments

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

- Enterprise Vault Services
- Enterprise Vault API Runtime

Note the following important points:

- All Enterprise Vault servers in all Enterprise Vault sites in a eDiscovery environment must run the same version of Enterprise Vault.
  For example, when using eDiscovery 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 eDiscovery and Enterprise Vault, you must first upgrade eDiscovery itself, then Enterprise Vault on all Enterprise Vault servers, and finally Enterprise Vault on all eDiscovery servers.

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

Prerequisites for Arctera eDiscovery

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 eDiscovery 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 eDiscovery 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 eDiscovery server computer

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

Table 2-1 Required software for Arctera eDiscovery server installation

Item	Notes
.NET Core	You require ASP .NET Core Runtime 8.0.x Hosting Bundle. The minimum supported version is 8.0.0. See the `Links To Related Software` folder in the distribution media.
.NET Framework	You require .NET Framework 4.5.2 and .NET Framework 4.7.2 Runtime See the `Links To Related Software` folder in the distribution media.
Enterprise Vault	If Arctera eDiscovery is installed on a separate computer from Enterprise Vault, you must install the Enterprise Vault software on the Arctera eDiscovery computer. You require an 15.2 version of one of the following: ■ Enterprise Vault Services. ■ Enterprise Vault API Runtime. See "Supported versions of Enterprise Vault in eDiscovery environments" on page 13. There is no need to configure Enterprise Vault after you have installed it on your Arctera eDiscovery server computer; do not run the Enterprise Vault configuration wizard. In addition, if the Enterprise Vault Admin service is running on your Arctera eDiscovery server computer, we recommend that you stop it and set its startup type to Disabled. To search on content with Arctera eDiscovery, set indexing on the Enterprise Vault archives to full.

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

Item	Notes
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. 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. Install the client in single-user mode, using the account under which the eDiscovery Manager service runs.
Outlook	You require Outlook 2013 SP1 or later so that client users can export Exchange Server items in PST format and download the original versions of the items. The export-to-PST feature requires a 32-bit version of Outlook 2013 SP1 or later; it does not work with the 64-bit version. Add the AttachmentMax and RecipientMax values to the registry on the Arctera eDiscovery server to avoid problems when processing items that have many attachments or many recipients. See "Configuring Outlook to enable the processing of items with many attachments or many recipients" on page 19.
Visual C++ Redistributable	You require the Microsoft Visual C++ 2015-2019, or later Redistributable (x86). See the `Links To Related Software` folder in the distribution media.

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

Item	Notes
Web browser	You require one of the following: ■ Microsoft Edge. ■ Microsoft Internet Explorer 11. For optimum results, do the following: ■ Configure the privacy settings in the browser to allow cookies. ■ Turn off any pop-up blockers. ■ Ensure that the advanced option **Play animations in webpages** is selected. In Internet Explorer, click **Internet Options** on the **Tools** menu. Then, on the **Advanced** tab, locate the required option in the **Multimedia** category.
Windows	We recommend that you do the following: ■ Before you install the Arctera eDiscovery server software, ensure that the Windows Server service is running. See "Ensuring that the Windows Server service is running on the eDiscovery server" on page 24. ■ Disable the Windows Search Service to stop it from interfering with the progress of Arctera eDiscovery export runs. See "Disabling the Windows Search Service on the eDiscovery server" on page 23.

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

- At least 16 GB of memory.
- Sufficient hard drive space to accommodate the searches and export runs that you expect to undertake.
  All transaction requests from eDiscovery web application to the Enterprise Vault and Arctera eDiscovery 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 eDiscovery searches and export runs. On both the Arctera eDiscovery 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.

The *Best Practices Guide* provides extensive information on the Arctera eDiscovery server's hardware requirements. You can obtain this guide from the Arctera Support website at https://www.veritas.com/docs/100024378.

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 eDiscovery 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 Arctera eDiscovery client computers

Table 2-2 lists the software items that you must install and configure on the computers that are to run the Arctera eDiscovery client software.

Table 2-2 Required software for Arctera eDiscovery client installation

Items	Notes
.NET Framework	You require .NET Framework 4.5.2 and .NET Framework 4.7.2 Runtime. See the `Links To Related Software` folder in the distribution media.
Notes client	You require version 9.0 or later of the Notes client to view Domino items in their original form rather than in an HTML representation of the items. Install the client in single-user mode.

Table 2-2 Required software for Arctera eDiscovery client installation *(continued)*

Items	Notes
Outlook	You require one of the following to view Exchange Server items in their original form rather than in an HTML representation of the items: ■ Outlook 2013 SP1. ■ Outlook 2016. ■ Outlook 2019.
Visual C++ Redistributable	You require the Microsoft Visual C++ 2015-2019 or later Redistributable (x86) to view Domino items in their original form rather than in an HTML representation of the items. See the `Links To Related Software` folder in the distribution media.
Web browser	You require one of the following: ■ Microsoft Edge. ■ Microsoft Internet Explorer 11.
Windows	You require one of the following: ■ Windows 8.1. ■ Windows 10. For optimum performance on a Windows 8.1/10 computer, run the client in Windows 7 or Windows XP compatibility mode. See the Windows documentation for guidelines on how to do this.

The recommended screen resolution for the Arctera eDiscovery client is 1024x768 or higher. For the best results, ensure that your client computers have at least 2 GB of memory.

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

You must install a supported version of Outlook on the eDiscovery 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 eDiscovery server computer" on page 15.

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 eDiscovery server.

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

1. On the eDiscovery 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 eDiscovery 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 eDiscovery 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 eDiscovery server and applications, eDiscovery makes occasional use of various folders for temporary storage. To protect against unauthorized access to these folders, which can contain sensitive data, eDiscovery checks access to them on startup and periodically thereafter. If the security check fails on the eDiscovery 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, eDiscovery 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.
- The folder that you specify as the "Temporary storage area" through the API configuration options in the eDiscovery client. By default, this folder is also the Windows `%TEMP%` folder.

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

In both cases, eDiscovery 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 eDiscovery 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 eDiscovery 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: 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 eDiscovery environment

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

To disable networking facilities that can disrupt a eDiscovery environment

1. Disable the following features on your designated eDiscovery 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 eDiscovery servers.

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

Disabling the Windows Search Service on the eDiscovery server

If the Windows Search Service is running on the eDiscovery server, it can sometimes prevent eDiscovery 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 eDiscovery export folders.

Ensuring that the Windows Server service is running on the eDiscovery server

When you run the installation program for the eDiscovery 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 eDiscovery server.

To ensure that the Windows Server service is running on the eDiscovery server

1. On the eDiscovery 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

eDiscovery 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.

You must also ensure that the SQL Server Agent service is running if you want to use the analytics facilities in eDiscovery to mark or tag items automatically. For more information on these facilities, see the *Administrator's Guide*.

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 eDiscovery. The two required roles are as follows:

- dbcreator (database creator). The facility to create configuration and customer databases with eDiscovery is dependent on the Vault Service account having this role.
- sysadmin (system administrator). eDiscovery 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, eDiscovery assumes that you want to make a user with the sysadmin role the creator and owner of them.

  In addition, you require the sysadmin role to enable eDiscovery cases for analytics.

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 eDiscovery 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

eDiscovery 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 eDiscovery 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

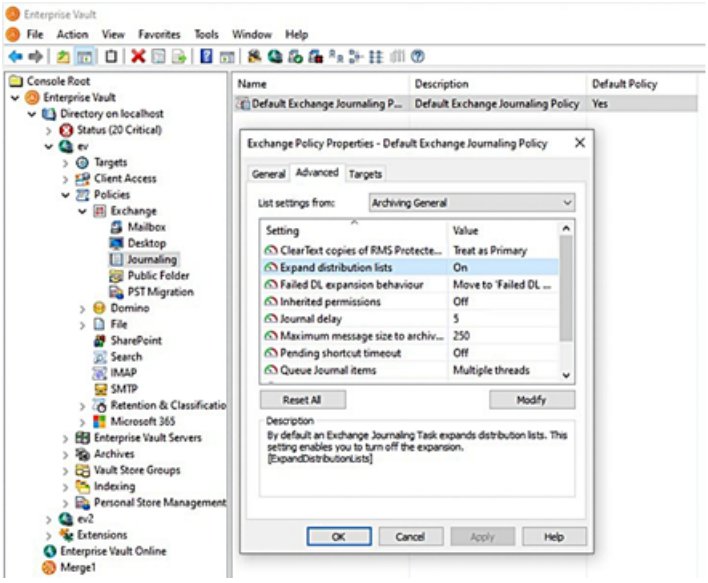
In Microsoft Exchange environments, you must ensure that the Enterprise Vault Exchange Journaling Task expands distribution lists in the To, CC, and BCC fields of items.

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.

Chapter 3

Installing eDiscovery

This chapter includes the following topics:

Installing the eDiscovery server software

Follow the instructions in this section to perform a first-time installation of the eDiscovery server software. If you want to upgrade an existing eDiscovery installation, see the `DAUpgradeInstructions` 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 Surveillance server software is not supported.
- You can configure eDiscovery 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 eDiscovery in a clustered environment" on page 48.

To install the eDiscovery 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 eDiscovery server software.
   - In Windows Explorer, browse to the `Arctera Enterprise Vault eDiscovery\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 eDiscovery installation.

3 On the **Prerequisites** screen, scroll up and down to view the list of hardware and software required for the eDiscovery 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, except eDiscovery client. See "About the eDiscovery components" on page 7. This option is recommended for most users. After you click **Typical**, The default path is displayed. Ensure that the path to the folder where you want to install eDiscovery 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.

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

8 If you have chosen to install the **Auditing Websites** feature, the **Enhanced Auditing Configuration** screen is displayed. Enter the following details:

- **Server Alias**: DNS Alias name or FQDN for the eDiscovery Server
- **Website Port**: Port for the Auditing website
- **Internal Port**: Port for the Auditing API site

9 Click **Next**.

10 On the **Ready to install** screen, click **Install** to start eDiscovery 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 eDiscovery 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 31.

12 To ensure that all the endpoints are encrypted, eDiscovery generates self-signed certificate for the Auditing web application during configuration. It is recommended to replace such self-signed certificates with certificates signed by well-known authorities.

13 If you want to use the Legal Hold facility to stop users from deleting items from their archives, install a eDiscovery license on each storage server in your Enterprise Vault site.

Allowing Enterprise Vault to communicate with eDiscovery through the Windows firewall

You must configure the Windows firewall on the eDiscovery server to permit Enterprise Vault to communicate with eDiscovery through it. Certain interactions between the Enterprise Vault server and the eDiscovery server require unrestricted communication. You can allow Enterprise Vault to communicate with eDiscovery 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 eDiscovery 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 eDiscovery 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 eDiscovery 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 cases, user roles, search results, review marks and tags, 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 eDiscovery. 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 eDiscovery system. Setting up two customers lets both departments use eDiscovery without needing access to the same eDiscovery setup.

Before you proceed, note the following:

- If you have installed eDiscovery 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 eDiscovery server, we recommend that you shut it down temporarily.
  See "Cannot create or upgrade eDiscovery customer databases when Symantec Endpoint Protection is running" on page 59.
- 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 eDiscovery 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. 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: https://msdn.microsoft.com/library/ff878487.aspx 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: **\ / : * ? " < > | '** 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 eDiscovery 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. 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. 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. 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. This password must comply with the Windows Password Policy of the computer that is running the instance of SQL Server. 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. 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 eDiscovery 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 eDiscovery 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 21.

---

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

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	Specifies whether this database is a customer database for eDiscovery or Insight eDiscovery Custodian Manager.
Name	Specifies a unique name for the customer. The name cannot contain any of the following characters: \ / : * ? " < > | '
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. If you want to specify multiple Directory service computers, type the details of each one on a line of its own. All the computers must be running exactly the same version of Enterprise Vault. 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 eDiscovery 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". 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.
Enable Customer's tasks	Enables users to perform activities in the eDiscovery client. 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 for the Discovery API website. This site lets software developers integrate third-party tools with eDiscovery, and thereby retrieve data from or export it to a eDiscovery customer database. No two customers can share the same virtual directory name. The directory name must not include space characters or any of the following characters: *** ? \ / % ' "** Note that you cannot name the virtual directory for any eDiscovery 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 eDiscovery 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 ([]). 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 eDiscovery client. 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. 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. For guidelines on deploying databases in Always On environments, see the following article on the Microsoft website: https://msdn.microsoft.com/library/ff878487.aspx 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: `\ / : * ? " < > | '`
Use Existing Database	Instructs eDiscovery 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. 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. 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.

Database Locations For Analytics section

This area of the page lists existing database locations for analytics data, and lets you add new database locations. You must specify at least one database location for analytics. If you do not intend to use the analytics feature with this customer, use the default database location.

See "Configuring analytics database locations" on page 38.

3 Wait for eDiscovery 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 analytics database locations

When you enable a case for analytics, eDiscovery must fetch all the case items from Enterprise Vault into the customer database, and index them. This requires a large amount of disk space. eDiscovery lets you define locations to host the analytics table file groups and indexes. You can add more locations when you need more disk space.

The Customer page of the eDiscovery Manager website lists existing analytics database locations, and lets you add more. Next to each location, check marks in

the **Table File Group** and **Full Text Indexes** columns show whether the location is used for table files, search indexes, or both.

When you plan and configure analytics database locations, consider the following:

- The volume of data. The collection and indexing of analytics data can generate very large databases and index files. As a rough guide, collecting one million items that are all 20 kilobytes in size can produce a database that is 40 gigabytes or more in size. However, this can vary from one environment to another.

  The *Best Practices Guide* for eDiscovery provides extensive information on how to size your eDiscovery databases appropriately. You can obtain this guide from the Arctera Support website at https://www.veritas.com/docs/100024378.

- Performance. Host each database location on a physically separate disk. If you have more than one analytics database location, eDiscovery uses them in rotation to spread the data and the disk access requirements.

  Each eDiscovery case uses only one location for the search index and one location for the database.

The following examples show two valid configurations for analytics database locations.

Table 3-1 Analytics database locations: example 1

Location	Table File Group	Full Text Indexes
C:\SQL\Data	Selected	Selected
D:\SQL\Data	Selected	Selected
E:\SQL\Data	Selected	Selected
F:\SQL\Data	Selected	Selected

Table 3-2 Analytics database locations: example 2

Location	Table File Group	Full Text Indexes
C:\SQL\Data	Cleared	Selected
D:\SQL\Data	Cleared	Selected
E:\SQL\Data	Selected	Cleared
F:\SQL\Data	Selected	Cleared

To add a database location for analytics

1 Browse to the eDiscovery Manager website.

2 Right-click the appropriate customer, and then click **Properties**.

3 Under **Database Locations For Analytics**, click **New Location**.

4 Enter the path to the new database location. Note the following:

- The database locations must reside on the SQL server, and you must use local paths to refer to them. For example, do not use UNC paths to refer to database locations.
- The eDiscovery Manager website does not verify that the specified locations exist. You must ensure that the paths are valid.

5 Select **Table File Group**, **Full Text Indexes**, or both.

6 Click **OK** next to the new location.

7 Repeat steps 3 through 6 if you want to add more database locations.

Setting up a Insight eDiscovery Custodian Manager website

Insight eDiscovery Custodian Manager is a browser-based application with which you can store the details of the custodians (individual employees) and custodian groups for which you want to search with eDiscovery. A custodian group is any collection of employees, such as Windows or Domino groups and distribution lists, Active Directory or Domino LDAP searches, and Active Directory containers. After you have added the custodians and custodian groups to Insight eDiscovery Custodian Manager, you can pick from them when you define the criteria for a eDiscovery search.

Note: A eDiscovery configuration database can have one Insight eDiscovery Custodian Manager website only. All customers that share the configuration database share Insight eDiscovery Custodian Manager.

To set up a Insight eDiscovery Custodian Manager website

1 Open the eDiscovery Manager website.

If you have installed eDiscovery on a server in which User Account Control (UAC) is enabled, you must open the eDiscovery Manager website with administrator privileges.

2 Right-click the server node in the left pane, and then click **New Customer**.

3 In the Create Customer page, set the customer type to **Insight eDiscovery Custodian Manager**.

4 Enter your preferred IIS and SQL database details, and then click **OK**.

5 Browse to the Insight eDiscovery Custodian Manager website that you have just created. The address of this website takes the following form:

   http://*server_name*/*virtual_directory*

   For example:

   http://server2/EVBACustodianManager

6 Use the facilities in Insight eDiscovery Custodian Manager to create and manage the custodians and custodian groups. For instructions on how to do this, see the *Administrator's Guide* and the online Help for Insight eDiscovery Custodian Manager.

Assigning the required Active Directory permissions to the Insight eDiscovery Custodian Manager synchronization account

By default, Insight eDiscovery Custodian Manager uses the account under which the eDiscovery Manager service is running when it synchronizes custodians and custodian groups with the corresponding Active Directory accounts. However, if you prefer, you can nominate a different account on a per-domain basis.

For instructions on how to specify a different user account for synchronization purposes, see the *Administrator's Guide*.

The nominated synchronization account must have certain delegated permissions to query the Active Directory domain.

To assign the required delegated permissions to the Insight eDiscovery Custodian Manager synchronization account

1 Open Active Directory Users and Computers.

2 Right-click the domain object, and then select **Delegate Control**.

3 In the Delegation of Control Wizard, click **Next**, and then click **Add**.

4 In the Select Users, Computers, or Groups dialog box, enter the required account name, and then click **OK**, and then click **Next**.

5 In the Tasks to Delegate page, in **Delegate the following common tasks**, select the following tasks, and then click **Next**:

   - Read all user information
   - Read all inetOrgPerson information

6 Click **Finish**.

Enabling the Insight eDiscovery Custodian Manager synchronization account to access the Deleted Objects container

The Insight eDiscovery Custodian Manager synchronization account must also have List Content and Read Property permissions on the Deleted Objects container in Active Directory. Without these permissions, it is not possible to deactivate any custodians and custodian groups whose Active Directory details have been moved to the Deleted Objects container.

The following article on the Microsoft website provides detailed instructions on how to view and set permissions on the Deleted Objects container:

https://technet.microsoft.com/library/cc816824.aspx

Note: You require a recent version of the `dsacls` command-line utility to complete the instructions in this article. Some older versions of the utility do not support all the required commands.

In brief, the procedure is as described below.

To enable the Insight eDiscovery Custodian Manager synchronization account to access the Deleted Objects container

1 Open a Command Prompt window with administrator privileges.

2 Take ownership of the Deleted Objects container by running the `dsacls` command-line utility, as follows:

```
dsacls deleted_objects_dn /takeownership
```

Where the parameters are as follows:

deleted_objects_dn	The distinguished name of the Deleted Objects container.
/takeownership	Take ownership of the Deleted Objects container.

For example:

```
dsacls "CN=Deleted Objects,DC=Contoso,DC=com" /takeownership
```

3 Grant the List Content and Read Property permissions to the user account under which Insight eDiscovery Custodian Manager synchronizes custodians and custodian groups, as follows:

```
dsacls deleted_objects_dn /G user_or_group:permissions
```

Where the parameters are as follows:

deleted_objects_dn	The distinguished name of the Deleted Objects container.
user_or_group	The user or group to whom the permissions apply.
permissions	The permissions to grant. For List Content and Read Property, specify the permissions as LCRP.

For example:

```
dsacls "CN=Deleted Objects,DC=Contoso,DC=com" /G
CONTOSO\VaultAdmin:LCRP
```

Uploading the eDiscovery report templates

Using Microsoft SQL Server Reporting Services as the reporting mechanism, eDiscovery provides extensive facilities for monitoring the details of a case and validating compliance with discovery requests. For information on the available reports and guidelines on how to use them, see the *Administrator's Guide*.

To make the reports available to users of the eDiscovery client, you must upload the supplied template (`.rdl`) files to your SQL reporting server. The template files contain data retrieval and layout information for their respective reports in XML format.

Note: If you want to deploy eDiscovery in a SQL Server Always On environment, take care to configure the Reporting Services appropriately.

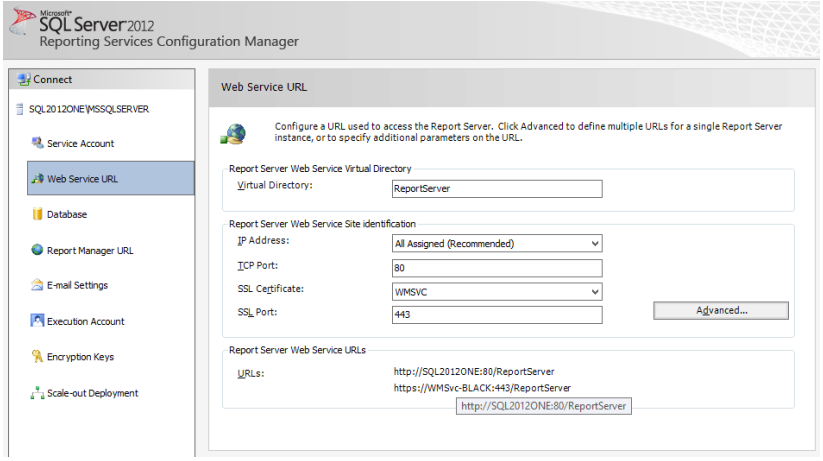
See "Using SQL Server Reporting Services in an Always On environment" on page 47.

To upload the eDiscovery report templates

1 If you have not already done so, install and configure SQL Server Reporting Services on the selected reporting server.

You can check the configuration of SQL Server Reporting Services by using the Reporting Services Configuration Manager on the reporting server. Make a note of the virtual directory name on the Web Service URL page, as you need to specify this name later. The default name of the virtual directory is **ReportServer**.

The following figure shows the typical settings in a Web Service URL page.



2 On the SQL reporting server, assign the following roles to the Vault Service account:

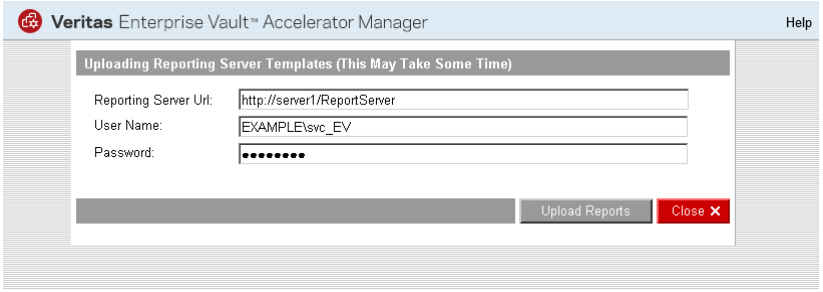
- The System Administrator role on the SQL reporting server.
  You can assign this role by using the browser-based Report Manager tool that comes with SQL Server. First click **Site Settings** on the global toolbar in Report Manager and then click **Security**. Then click **New Role Assignment** and assign the System Administrator role to the Vault Service account.
- The Content Manager role on the Home folder of the SQL reporting server.
  To assign this role in Report Manager, click **Security** on the **Properties** tab for the Home folder. Then click **New Role Assignment** and assign the Content Manager role to the Vault Service account.

See the Microsoft Reporting Services documentation for more information.

3 On the eDiscovery server, open the eDiscovery Manager website.

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

The Uploading Reporting Server Templates page appears.



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

http://*server_name*/*virtual_directory*

Where *server_name* is the host name, fully qualified domain name, or IPv4 or IPv6 address of the SQL reporting server, and *virtual_directory* is the name of the required virtual directory. For example:

http://EVSQL/ReportServer

Note the following:

- If you have multiple SQL Server instances, type the URL in the following form:
  http://*server_name*/*virtual_directory*$*instance_name*
- If you have configured the SQL reporting server to listen for HTTP requests on a port other than the default, 80, type the URL in the following form:
  http://*server_name*:*port_number*/*virtual_directory*

6 In the **User Name** field and **Password** field, type the credentials for the Vault Services account. By doing so, you identify the Vault Services account as the owner of all exchanges between the eDiscovery server and SQL reporting server.

7 Click **Upload Reports**.

Note that it can take several minutes to upload the report templates to the server. A confirmation message appears when the process has completed.

Configuring eDiscovery for use in a SQL Server Always On environment

You may want to implement high availability and disaster recovery for eDiscovery 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 eDiscovery 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 eDiscovery 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 eDiscovery.

To configure eDiscovery 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 eDiscovery 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, and the Insight eDiscovery Custodian Manager 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 eDiscovery. 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 eDiscovery 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.
  See "Uploading the eDiscovery report templates" on page 43.
- 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 eDiscovery 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 eDiscovery in a clustered environment

Arctera does not support installing the eDiscovery 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 eDiscovery installation can reference a clustered Enterprise Vault virtual server.

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

Configuring eDiscovery 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 eDiscovery by distributing client requests across the nodes in the cluster; background eDiscovery 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.

For more information on load balancing, see the *Best Practices Guide*. This is available from the following page of the Arctera Support website:

https://www.veritas.com/docs/100024378

To configure eDiscovery 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 eDiscovery 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 eDiscovery databases

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

- **Change database ownership and control access privileges**
  By default, the Vault Service account owns all the eDiscovery 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 eDiscovery. To protect this security information, it is recommended to back up the configuration database regularly.

Installing the eDiscovery client

Caution: The version of the client that you install on your users' computers must exactly match that of the eDiscovery server software on the eDiscovery server.

Modifying the configuration file for the eDiscovery client

Before you proceed, it is a good idea to modify the configuration file that accompanies the installation package. One of the settings in this file is the name or address of the computer on which you have installed the eDiscovery server software. By providing this information in the configuration file, you can save your users from having to supply the computer name or address when they first start the eDiscovery client.

To modify the configuration file for the eDiscovery client

1 Locate the configuration file `AcceleratorClient.Exe.Config` in the installation media for the eDiscovery client.

2 Open the configuration file in a plain text editor such as Windows Notepad.

3 Find the following configuration setting:

```
<add key="AcceleratorServer" value="localhost" />
```

4 Replace the value with the name, fully qualified domain name, or IPv4 or IPv6 address of the computer on which you installed the eDiscovery server software. For example:

```
<add key="AcceleratorServer" value="server2" />
```

If you have configured eDiscovery for use in a Network Load Balancing cluster, you must specify the virtual name or IP address of the cluster.

5 Save and close the file.

Using the MSI installer package to install the eDiscovery client

Typically, you distribute the eDiscovery client software by directing users to a central location from which they can run the MSI installer package. By default, the installer package for the eDiscovery client software performs a per-user installation of the software. This type of installation does not permit other users of the computer to run the application. However, if you have administration privileges on the computer and want to permit all users to run the application, you can perform a per-machine installation.

To install the eDiscovery client software

1 Ensure that the configuration file `AcceleratorClient.Exe.Config` file is in the installation folder for the eDiscovery client software.

2 Do one of the following:

- To perform a per-user installation, start the eDiscovery installer package (`Arctera Enterprise Vault eDiscovery Client.msi`).
- To perform a per-machine installation, open a Command Prompt window and then type the following:

  `msiexec /I "`*`path_to`*`/Arctera Enterprise Vault eDiscovery Client.msi" TARGETDIR="`*`install_path`*`" ALLUSERS=1`

  Where:

path_to	Specifies the path to the `.msi` file.
install_path	Specifies the path to the folder in which to install the client software.

For example, you might type the following:

```
msiexec /I "D:\Arctera Enterprise Vault eDiscovery Client.msi"
TARGETDIR="C:\Program Files (x86)\" ALLUSERS=1
```

Caution: If User Account Control (UAC) is enabled on your computer, you must open the Command Prompt window with administrator privileges.

---

3 Follow the on-screen instructions.

4 After you have installed the client software, set the access permissions on the installation folder to prevent unauthorized users from tampering with it—for example, by placing malicious files in the folder. Only authorized users should have Modify and Write permissions on this folder.

Appendix A

Ports that eDiscovery uses

This appendix includes the following topics:

- Default ports for eDiscovery
- Changing the ports that eDiscovery uses

Default ports for eDiscovery

Table A-1 lists the default ports that eDiscovery uses.

Table A-1 Default ports for eDiscovery

Port	Used for
80 for HTTP, or 443 for HTTPS	Communications between the SQL reporting server and the eDiscovery clients and server.
81	Communications between the eDiscovery server and eDiscovery client.
82	Communications between the Auditing website and the Auditing API website.
389	Communications between the eDiscovery server and the Active Directory Domain Controller for the purpose of synchronizing custodian information through LDAP queries.
1433	Communications between the eDiscovery server and the SQL Server computer.
8085	Communications between the eDiscovery server and the eDiscovery websites (eDiscovery Manager, Insight eDiscovery Custodian Manager, and eDiscovery API).

Table A-1 Default ports for eDiscovery *(continued)*

Port	Used for
8086	Communications between the eDiscovery server and the eDiscovery clients.

eDiscovery 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 eDiscovery uses

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

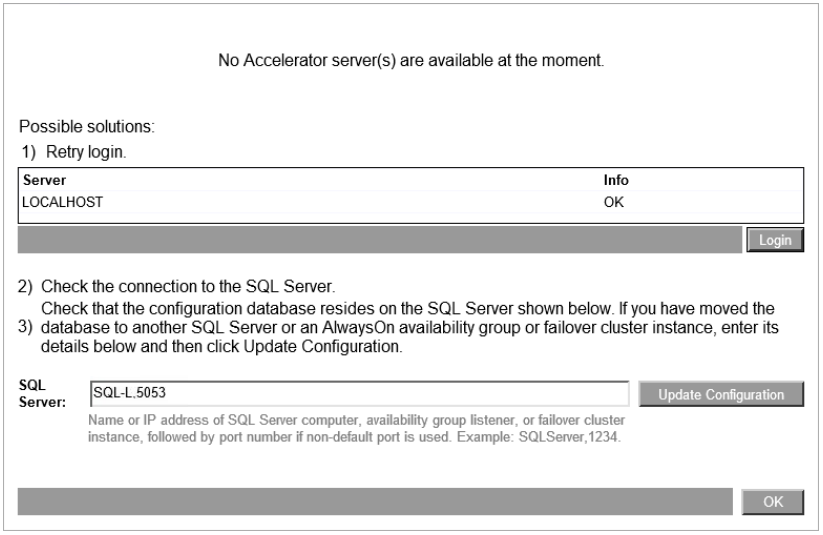
To change the port used for communications with SQL Server, if you do not use SQL Always On

1. On the eDiscovery 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 eDiscovery 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 eDiscovery server and the eDiscovery websites

1 On the eDiscovery server, locate the copies of the `Web.config` file in the `AcceleratorAdminWeb` and `CustodianManagerWeb` subfolders of the eDiscovery installation folder.

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 between the eDiscovery server and the eDiscovery clients

1 On each eDiscovery client computer, locate the `AcceleratorClient.Exe.Config` file in the installation folder.

This folder is typically `%HOMEPATH%\Local Settings\Application Data\Enterprise Vault eDiscovery\Client`.

2 Open the 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="AcceleratorServerPort" value="8086" />
```

4 Save and close the file.

5 If you need to change port 8086 to another port and you want to use Open Data (OData) web service to create reports, make sure that you update the OData configuration to use the same port. To update the port number, do the following:

- On each eDiscovery server computer, locate the `AcceleratorService.Exe.Config` and `AcceleratorManager.Exe.Config` files in the installation folder.
- Open each file in a text editor such as Windows Notepad.
- Find the following lines, and change the port number to match the setting in the AcceleratorClient.Exe.Config file.

```
<add key="Windows Client Remoting Channel Configuration" value="8086" />
<add key="Windows Client Remoting Channel Configuration IPv6" value="8086" />
```

- Save and close the file.

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

1 On the eDiscovery 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*

To change the ports used for communications with Auditing websites

1 Launch the eDiscovery Server MSI using setup.exe.

See "Installing the eDiscovery server software" on page 28.

2 On the **Modify, repair, or remove installation screen**, select **Modify**.

3 On the **Prerequisites** screen, review the list of hardware and software required for the eDiscovery installation.

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

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

5 On the **Custom Setup** screen, click **Next** without making any changes.

6 On the **Accelerator Service Account Login** screen, provide the accelerator service account password. Click **Next**.

7 On the **Enhanced Auditing Configuration** screen, change the required port number to a suitable alternative.

8 On the **Ready to Install** screen, click **Install**.

9 Click **Finish** to close the installer wizard.

Appendix B

Troubleshooting

This appendix includes the following topics:

Error messages appear in the event log when upgrading to eDiscovery 15.2

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

```
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 eDiscovery 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 eDiscovery 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 eDiscovery customer databases when Symantec Endpoint Protection is running

If Symantec Endpoint Protection is running on your eDiscovery 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 eDiscovery 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 eDiscovery 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.

Permissions error when uninstalling the eDiscovery client from a UAC-enabled computer

When both the following conditions apply, the message "You must be an Administrator to remove this application" appears when you try to uninstall the eDiscovery client from a computer in which User Account Control (UAC) is enabled:

- You performed a per-machine installation of the client by using the MSI installer package, `Arctera Enterprise Vault eDiscovery Client.msi`.
  The issue does not arise when you choose to uninstall a per-user MSI installation.
- You tried to uninstall the client by right-clicking the MSI installer package and then clicking **Uninstall** on the context menu. The issue does not arise when you uninstall the client through the Add or Remove Programs applet in Control Panel.

To uninstall the eDiscovery client in these circumstances

1. Open a Command Prompt window with administrator privileges.
2. Type the following command:

   ```
   msiexec /x "path_to/Arctera Enterprise Vault eDiscovery
   Client.msi" /qb!
   ```

   Where the `/x` parameter specifies that you want to uninstall the client, and the `/qb!` parameter displays a basic user interface during the uninstallation process.

Uninstalling the eDiscovery client from a shared location may prevent other users from starting the client

If a user uninstalls the eDiscovery client from the same shared location to which other users have installed the client, these users may no longer be able to start the client. However, they can easily fix the problem by performing a repair installation of their eDiscovery clients.

To perform a repair installation of the eDiscovery client

1. On each computer where you want to perform the repair installation, start Control Panel.
2. Double-click the **Add or Remove Programs** applet.
3. Find and click **Arctera Enterprise Vault eDiscovery Client** in the list of installed programs.
4. Click the **Click here for support information** hyperlink.
5. Click **Repair**, and then follow the on-screen instructions.

Appendix C

Installing and configuring the Enhanced Auditing feature

This appendix includes the following topics:

Overview

Starting with release 14.4, a new feature named Enhanced Auditing has been introduced. When the Enhanced Auditing feature is configured and enabled for a customer, the audit records for that customer are sent to the audit server whenever certain operations and modifications are made to modules as selected in the Audit Settings tab in eDiscovery client. Changes to these modules made in eDiscovery are logged. The Audit viewer tab in eDiscovery client lets you search

and export audit records for various modules and operations at the application, case, 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 63.

2. Install the Enhanced Auditing feature.

   See "Installing the Enhanced Auditing feature" on page 64.

3. Set the **Auditing** configuration options in the **Configuration** > **Settings** tab in the eDiscovery client.

4. Use the **Audit Settings** tab in the eDiscovery client to edit the required settings for auditing.

5. Use the **Audit viewer** tab in the eDiscovery client to search and export audit records.

Prerequisites for the Enhanced Auditing feature

In addition to the Prerequisites for Arctera eDiscovery, 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 the eDiscovery 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 2012 R2, Windows Server 2016, or Windows Server 2019
- Microsoft .NET 4.7.2
- Microsoft ASP.NET Core Runtime 6.0.20 - Windows Server Hosting
- 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.
- Microsoft Visual C++ 2015-2019, or later Redistributable (x86)
- 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.

Only Elasticsearch version 7.17.4 is 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. Run the MSI file from the **Command Prompt** to launch the Arctera Enhanced Auditing installer. 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.

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 to 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 IP addresses of the servers from which the audit server will be accessed. These are the IP addresses for each protocol (IPv4 and IPv6) that are enabled on the eDiscovery server.
- **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 > Settings** tab in the eDiscovery client.

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

To view and manage the *AuditAppCert* certificate:

1. From **IIS Manager > Connections**, click on the first node (which is your Audit server name).
2. From the **IIS** section of **Features View**, double-click **Server Certificates**.

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 eDiscovery server's trusted certificate store.

Configurations in eDiscovery client

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

Configurations in eDiscovery client

Later, you must enable auditing for individual modules from the **Configuration > Audit Settings** tab in the eDiscovery client. For details, refer to the *eDiscovery User Guide*.

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. Launch the Arctera Enhanced Auditing installer. To launch the installer, run the MSI file from the **Command Prompt**.

   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.

   ---

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

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

5 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.

6 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.

---

7 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.

8 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**.

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

10 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 **Install**.
- 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. Right-click on the installer and click **Change**.

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 will be accessed. These are the IP addresses for each protocol (IPv4 and IPv6) that are enabled on the eDiscovery 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 - 10.1.2.3,10.1.2.11-15.
- **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 **Repair**.

Note: The step performs a silent repair.

- 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. Right-click on the installer and click **Change**.

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.

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 **Logs** 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 **Uninstall**.
- 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. Right-click on the installer and click **Uninstall**.

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.

Note: Uninstalling the Enhanced Auditing feature does not uninstall Elasticsearch.

Managing access from eDiscovery

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 each protocol (IPv4 and IPv6) that are enabled on the eDiscovery server. These IP addresses get listed under allowed sites in IIS Manager. If an IP address of the eDiscovery 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 eDiscovery 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**.