Veritas eDiscovery Platform™

Identification and Collection Guide

9.0.1

VERITAS™

Veritas eDiscovery Platform™: Identification and Collection Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Last updated: 2018-3-5.

Legal Notice

Veritas Technologies LLC
500 East Middlefield Road
Mountain View, CA 94043
http://www.veritas.com

Contents

Identification and Collection Guide

Welcome to the *Veritas eDiscovery Platform Identification and Collection* guide. The *Identification and Collection* guide provides administrators and end users of the Identification and Collection module of Veritas eDiscovery Platform with the tools and information for network and data source setup; as well as data identification, collection, management, and analysis and reporting; in addition to placing holds on data.

The Identification and Collection module provides Collection Administrators with greater visibility and control over the sources required for collecting data used to create a case, and adds more filtering capability which administrators can apply during collection and analysis.

This section contains the following sections:

About This Guide

This guide provides an overview of the Identification and Collection module, a licensed add-on feature to eDiscovery Platform. The sections in this guide describe how to identify and associate data sources, create and run collection tasks, analyze and manage collection, and perform other regular administrative and maintenance tasks.

This guide is intended for System Managers also called as System Administrators, Collection Administrators, Group Administrators, decision makers, and anyone who is interested in understanding how eDiscovery Platform leverages data sources using the Identification and Collection feature.

Related Documents

Refer the following documents for additional information related to the Identification and Collection module:

- *Veritas eDiscovery Platform Collection Reference Card*
- *Veritas eDiscovery Platform OnSite Collection Reference Card*
- *Veritas eDiscovery Platform Navigation Reference Card*

Revision History

The following table lists the information that has been revised or added since the initial release of this document. The table also lists the revision date for these changes.

Revision Date	New Information
March 2018	• Added information related to Enterprise Vault discovery of deleted archives • Added information related to Content only collection sets and managing collection sets
December 2017	• Added information related to Microsoft Outlook 2013 updates • Added troubleshooting information for Office® 365 collections • Minor edits
June 2017	• Added information related to – Exchange 2016 – Enterprise Vault 12.0 – Enhancement in EV Collection defensibility report • Added troubleshooting information for collection from Office 365 sources. • Minor edits throughout the guide
June 2016	• Re-branding changes • Changes related to Access Group feature • Information on securing source account credentials • Troubleshooting the collection task failures • Minor edits throughout the guide
August 2015	• Documented new features: – Support for Enterprise Vault 11.0.1 – Support for collection from SMTP and Internet Mail archives – Support for collection from Office 365 archive mailbox – Access Group permissions for collection sets • Edits related to Locations tab moved from All Collections to All Cases • Removed Rights Management Guide from the Product Documentation section • Added troubleshooting information for collection from SharePoint and Office 365 sources. • Removed the Prompt for reason code field from the Document Access Rights section • Minor edits throughout the guide

Revision Date	New Information
March 2015	• Documented new features: – Support for CMIS compliant Documentum, Livelink, and FileNet data sources – End of support for non-CMIS compliant Documentum, Livelink, and FileNet data sources – Support for Microsoft Office 2013 documents and end of support for Office 2010 documents • Added information on enhanced features such as Browse and Add functionality for CMIS compliant data sources • Added a section on troubleshooting data collections from SharePoint 2013 • Branding and minor edits
October 2014	• Documented new features: – Support for EV.cloud source – Support for direct collection from SharePoint 2013 and FileShare – Support for Enterprise Vault 11 – Support for Lync 2013 data collection – Group permissions for Source, Destination, and Legal Holds – Filter archive – Support for collection of old versions of SharePoint documents • Added information on Enterprise Vault Search enhancements • Added information on end of license for DocuShare, iManage, and CM8 sources • Added information on source account permissions
December 2013	• Data collection from Office® 365 • Support for Enterprise Vault 10.0.4 • Support for Enterprise Vault 10.0.4 sources from Exchange 2013, SharePoint 2013, and File System Archiving from Windows 2012 • Support for direct collections from Exchange 2013 • Support for direct collections from IBM Domino 9.0 64-bit • Enterprise Vault reliability enhancements • Enterprise Vault Retry Release Hold functionality • Bulk Import Format Requirements • Troubleshooting Exchange 2013 collections, SharePoint collections, and Enterprise Vault Retry Failures

Revision Date	New Information
June 2013	• Documented new features: – Custodian management functionality – Preview and Analytics for Enterprise Vault (EV) collections – Ability to delete failed or stopped tasks – Ability to retry failed Enterprise Vault items (introduced in 7.1.2 Fix Pack 1) – New Email Address Column to sort/filter Enterprise Vault archive & Exchange collections (introduced in 7.1.2 Fix Pack 1) • Added "Move Collected Data" section (feature first introduced in 7.1.2) • Added "Using special characters in the directory path" section • Added information on Enterprise Vault DLL, StorageOnlineOpnsps.dll • Clarified Enterprise Vault scaleout property information. (See *"Troubleshooting" on page 201*.)
September 2012	• Added source support for: – Four new collectors (See *"Supported Source Types" on page 21*.) – Enterprise Vault SharePoint, Enterprise Vault File Share Archives • Documented new features: – Licensing: Separated from Processing, Analysis & Review module license – Enhanced Enterprise Vault and Archive source management – Enhanced filtering for Enterprise Vault sources: Email-to-custodian mapping for journal archiving, message type, retention category, policies, custom attributes – Retention and Tag Policy creation and application to Enterprise Vault collections – Hold in Place feature (for Enterprise Vault source users) - introduced in 7.1.1, added to this document for 7.1.2 – Set property to scale Enterprise Vault collection to multiple deployment servers (allowing simultaneous search and retrieval)
March 2012	• Added source collection support for Veritas Enterprise Vault • Documented additional new features: – Archive/restore collections – Collection Reports
February 2012	• Documented procedure for obtaining a license update; formatting changes throughout
November 2011	• Added source collection support for: – Exchange 2010 (discovery, search, mailbox) – SharePoint Web pages • Documented new features: – Bulk import of custodians via CSV or Script – Reusable custodian licensing – Keyword-based collection

Revision Date	New Information
May 2011	• Documented OnSite Collector secure encryption option
February 2011	• Added support for: – SharePoint with proxy – MAC (for OnSite) collection • Documented Folder Exclusion feature
December 2010	• Added (to Data Sources list) support for: – Microsoft® Exchange Cloud Servers (BPOS) – Lotus® Domino Server (Lotus Notes) • Documented new features: – Custodian Merge – Bulk Import of Sources to data maps • Moved OnSite Collection Details to stand-alone reference: Refer to "*OnSite Collections Reference Card*"
September 2010	• Created guide for new Identification and Collection module.

Technical Support

Technical Support maintains support centers globally. All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policies.

For information about our support offerings and how to contact Technical Support, visit our website:

https://www.veritas.com/support

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

https://my.veritas.com

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

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

Documentation

Make sure that you have the current version of the documentation. The latest documentation is available from:

- **Documentation** link at the bottom of any page in the eDiscovery Platform landing page.
- **Veritas Products Web site:** https://www.veritas.com/product/a-to-z

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:

eDiscovery.InfoDev@veritas.com

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

https://vox.veritas.com/

Getting Started

Use this section to help guide you through verifying your setup, and what to do after logging on to Veritas eDiscovery Platform.

In this section:

About Data Identification and Collection

The Identification and Collection module allows you to:

- keep a catalog of multiple data sources (such as File Shares, PCs, Exchange servers, SharePoint and Lotus Domino servers, Veritas Enterprise Vault archives, among others) in your data map
- set up Collection Tasks, which create copies of data from these data sources, grouped into Collections
- search, analyze, and preview data before collection
- place and manage holds on data (from Enterprise Vault sources)
- move the data through Processing and Analysis by creating Collection Sets
- archive and restore collections as needed to optimize data storage and custodian licenses
- report on collection data with summary and error reports, run as jobs and/or available in Microsoft XLS formats

Typically, IT builds the Data Map and supplies the proper account credentials and locations for relevant data sources. However, a Collection Admin and a Group Admin with appropriate permissions can add as many data sources to the Data Map as needed, and perform multiple collections from these sources.

Identification and Collection Module User Interface

There are two views of the Identification and Collection module: All Collections, or a single collection within a selected case.

To view collections across all cases on the appliance, click **All Collections**:

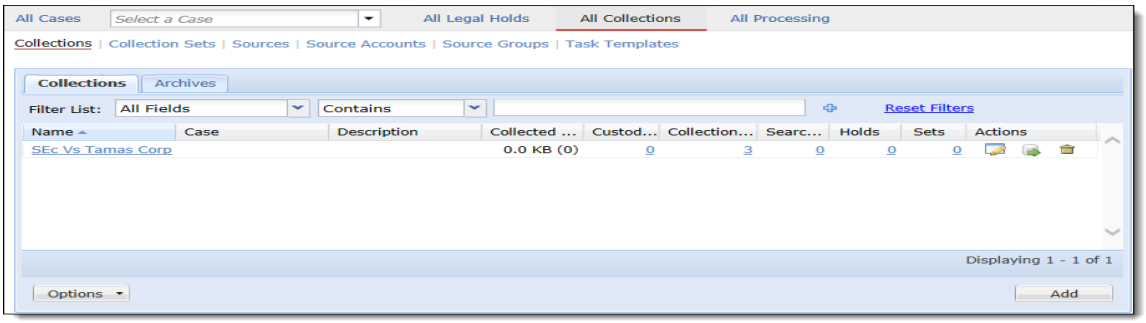


Figure: Identification and Collection Module: All Collections view

From the All Collections view, a user can manage Collections, Collection Sets, Sources, Source Accounts, Source Groups, and Task Templates across all cases in the appliance.

To view collections and related tasks in a specific case, click the drop-down to select a case, or select **Create a new case**.

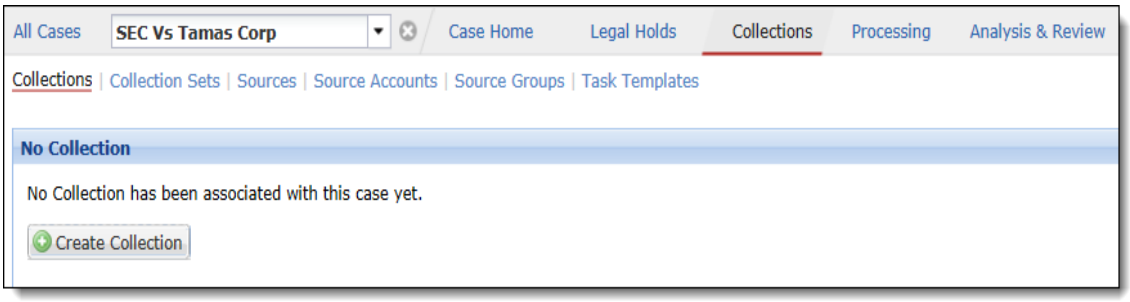


Figure: Identification and Collection Module: Within a Selected Case (No Collections)

When a case is selected within the Identification and Collection module, a Collections Admin can view the same set of sub-tasks before a collection is created. Each case can have only one collection. Once the collection is created, the user can view only the collection associated with the selected case.

Click **Create Collection** to start a new collection. See *"Create/Add a New Collection" on page 103*.

Checklist: Before You Begin...

Use the following checklist to verify your setup before you begin working with the Identification and Collection module:

- Appliance is properly installed.
  Refer to the "Veritas eDiscovery Platform Installation Guide" to verify your installation and configuration.
- Network is set up for data collection.
  See *"Network and Data Map Setup" on page 21* for information about how to set up your IT environment and ensure your network is ready for mapping your source data.
- Data Map and Collections License is installed.
  See *"Managing Your Collections License" on page 194* to check for license information, including the number of custodian licenses currently available for use. (Custodian licenses are reusable.)
- Change/update account, Help, and Support link information.
  See *"Logging On" in the next section*.

Logging On

The first time you log on, be sure to:

1. Change the account password.

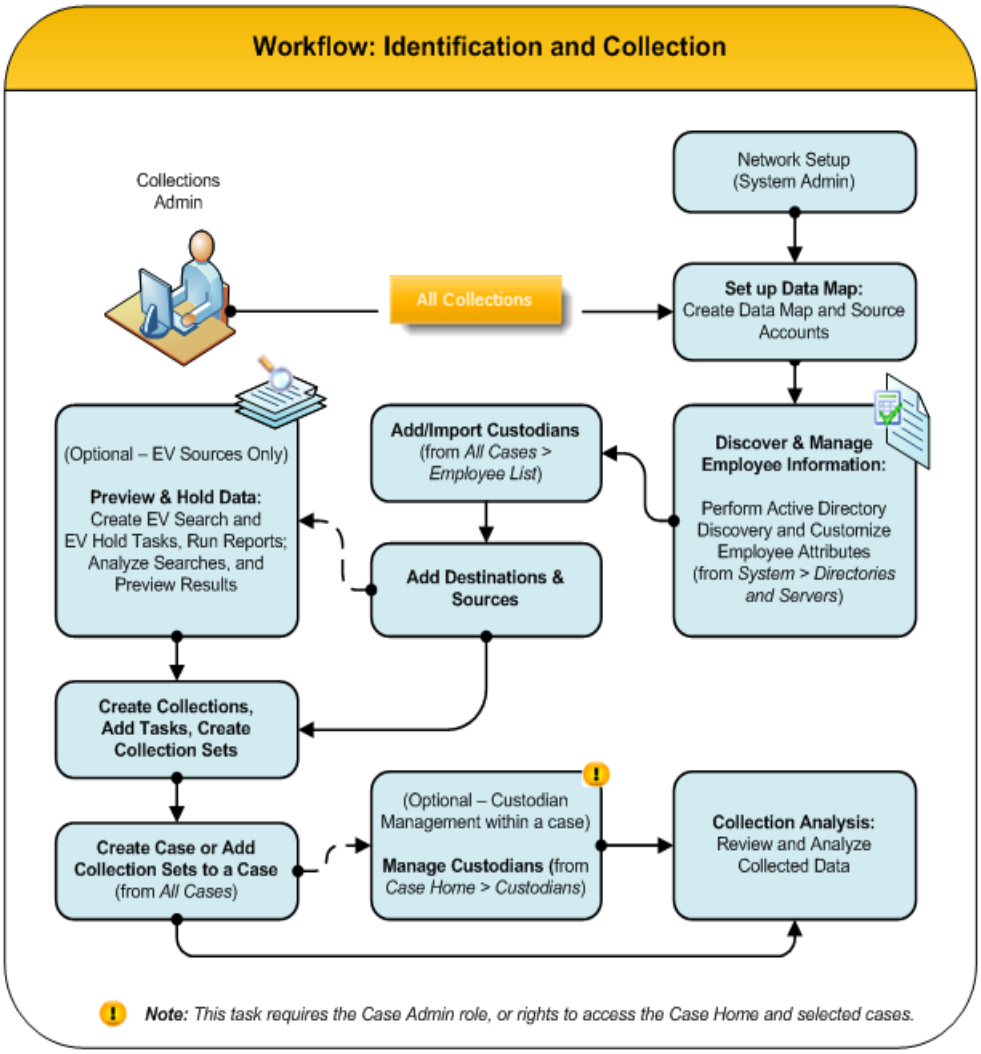
   Note: The password is the same on every appliance. Leaving the default password opens your system up to vulnerabilities.

2. Update the **Need Help?** link on the Login page.

3. Update the Support link.

Collection Workflow

After your System Administrator has set up your network for collections, follow these basic steps to prepare your data sources for case creation and management.



- **Data Map, Account, and Source Setup**. Set up your data map, learn best practices, add and manage source accounts. (See *"Network and Data Map Setup" on page 21*.)
- **Discovery, Employee & Custodian Management, Sources**. Discover and customize employee information, add/import custodians, and add sources. (See *"Mapping Employee Attributes" on page 35*, and *"Importing Custodians to Your Data Map" on page 36*. To manage custodians within a specific case, see *"Managing Custodians (Across a Case)" on page 187*.)
- **Searches, Holds, and Collections**. Create searches and holds on Enterprise Vault sources (optional), and create collections; add collection tasks, run and schedule collections and onsite collections.

(See *"Creating and Managing Search Tasks" on page 141*, and *"Creating and Managing Hold Tasks" on page 151*, or *"Creating and Managing Collections" on page 101*.) Refer also to the *Collection Reference Card*, and *Onsite Collection Reference Card*.

- **Collection Sets and Analysis.** Create a case, or create collection sets and add to a case, then Analyze and process collected data. (See *"Creating, Analyzing and Processing Collections" on page 163*.)

Occasionally, you may also want to set collections user permissions, perform backups, check licensing information, and perform other maintenance tasks. See *"Collection Administration and Maintenance" on page 177*.

Network and Data Map Setup

This section describes how to ensure your network is properly set up before mapping your data sources to Veritas eDiscovery Platform.

About Data Mapping

Through the Identification and Collection module, administrators can set up a data map by associating all available data sources in preparation for collection.

Supported Source Types

Veritas eDiscovery Platform supports the following source types for identification and collection. The following table lists only the tested versions of the source types. For the most up-to-date, detailed information on the supported versions of the source types, see the *Veritas eDiscovery Platform™ Compatibility Charts* guide.

Source Types

Source	Version / Type Supported	Details
Network File Shares		
Distributed File System (DFS)		
Personal Computers	Windows	Network, and OnSite collection
	Mac	Off-network only / OnSite collection
Exchange Servers	2007, 2010, 2013, 2016	
	Office 365	
	Lync 2013 with Exchange 2013	
SharePoint®	2007, 2010, 2013, SharePoint Online (as part of an Office 365 suite)	with proxy
		Web page sources **Note:** SharePoint Online is not supported when deployed in Active Directory Federation Services (AD FS) environment.
Lotus Domino®	Server 8, 8.5, 9	
Veritas Enterprise Vault (Sources and Archives)	Exchange	User Mailbox Archive (Enterprise Vault Exchange, SMTP or Internet Mail) and Journal Archive (Enterprise Vault Exchange, SMTP or Internet Mail)
	Lotus Domino	Mailbox and Journaling Archives
	SharePoint Archive	
	File System Archive	
Veritas Enterprise Vault.cloud	EV.cloud	
OpenText™ ECM Suit Livelink	10.5	CMIS compliant Livelink E-mail collection method is deprecated in 8.1.

Source Types

Source	Version / Type Supported	Details
EMC® Documentum	6.7	CMIS compliant
IBM® FileNet®	5.1.0	CMIS compliant

The DocuShare, CM8, and iManage data sources have reached End of Support Life (EOSL). Starting with the release 8.0, collection from DocuShare, CM8, and iManage data sources is not supported. Therefore, you cannot create a new collection task or rerun an existing collection task for these sources. Also, you cannot add a new source for these non-supported data sources from **All Collections** > **Sources**. The existing sources of these non-supported data sources are not shown at the Sources screen.

Starting with 8.1, non-CMIS compliant data sources including Documentum, Livelink, and FileNet are not supported. Release 8.1 and later only support CMIS compliant versions of these data sources. The existing sources and collections tasks/ templates created for the non-CMIS compliant data sources cannot be used as it is after upgrading to Release 8.1. To use the existing sources and collection tasks/templates, users must reconfigure their existing non-CMIS compliant sources to CMIS compliant sources. Also, if folder filter criteria were defined for the tasks/ templates in previous release, then users must redefine the folder filter criteria for the existing collection tasks/ templates.

Best Practices

This section outlines the best practices which Network Administrators and eDiscovery practitioners should consider before setting up your network environment to use the Identification and Collection module in Veritas eDiscovery Platform.

IMPORTANT! Read this section first, before completing the tasks in the following sections, according to the source type(s) you are setting up for identification and collection.

Network Impact and Performance

The Identification and Collection module is an eDiscovery solution, allowing you to search, filter, and collect data from various data sources. Collection can happen directly (via "OnSite" collection onto an external hard drive) or across the network. Network collections can come from multiple data sources, including Microsoft Exchange Server, Lotus Domino Server, File Shares, Veritas Enterprise Vault, EV.cloud, SharePoint, and various collector sources. (See all *"Supported Source Types" on page 21*).

Collections are performed on-demand, only when the user starts a specific Collection Task. The Identification and Collection module is not maintaining or updating a persistent index of data at these data sources. Network impact is limited to the scope of the specific collection tasks. For most eDiscovery use cases, these tasks should be targeted at individual subsets of data at these sources, rather than the entire source.

For example:

- collecting a single or a small number of specific Exchange mailboxes

- collecting a user's Public File Share folder
- SharePoint collections leveraging Veritas eDiscovery Platform's federated search feature

This submits the search request to SharePoint's own index, and Veritas eDiscovery Platform will collect (and occupy the network for) just the positive results.

Veritas eDiscovery Platform Collection Methodology and Setup

In consideration of network impact and performance, collection filters are applied intelligently - scanning for metadata matches first, and then performing (the more network-intensive) keyword scanning second.

The number of simultaneous collection tasks and threads are limited across all collections. These limits are adjustable, and can be set by a Veritas solutions consultant, services professional, or support.

Recommended Numbers of Collection Tasks & Threads by Source Type

Supported Source Type	Collection Tasks Limit	Notes
Local Exchange Server	• 5 max parallel tasks, 1 thread per task	• Each task must be single-threaded: this is a MAPI limitation • To collect multiple mailboxes truly in parallel simultaneously, the user needs to create separate Exchange Sources, each one attached to a different Source Account • You can do this for up to 5 mailboxes, depending on the appliance specs and whether the Exchange server has set limitations
EV.cloud	• 10 max parallel tasks, 49 max threads per task	
Local SharePoint	• 10 max parallel tasks, 500 max threads per task	• Source Setup (by Source Type) •
Lotus Domino Server	• 1 thread per task	• Multiple tasks can run in parallel as long as they do not have overlapping mailboxes
FileShares	• 10 max parallel tasks, ~128 max threads per task	• # of threads actually is dynamically configured based on # of CPUs
PC on the network	• (same as FileShares)	• (same as FileShares)
PC and Mac (for OnSite Collection)	• No throttle.	• These are direct-to-drive collections, typically not done over the network

Note: If you run more than 10 parallel tasks, then only first 10 tasks run successfully at a given time and the remaining tasks will result in failure.

Tips, Troubleshooting, and Technical Support

For troubleshooting information in this guide, see *"Troubleshooting" on page 201*, and refer to the appropriate section depending upon the source type.

Setting Up Your Data Map

As you prepare to add sources to your data map, check the overview information and network setup references in this section first to ensure you have what you need to get started.

Before You Begin...

- Ensure your network is properly set up before adding sources:
  - Review *"Best Practices" on page 22* for setting up your network.
  - See *"Troubleshooting Exchange collections" on page 203*
- Determine the sources and accounts needed for setup:
  - See *"Source Account Overview" in the next section*
  - See *"Verify Network Setup by Data Source" on page 26*
  - See *"Adding a Source Account" on page 30*
  - See *"Define Source Groups (Optional)" on page 30*
  - See *"Securing source account credentials" on page 31*
  - See *"Data Discovery Overview" on page 34*
- As needed, map, add (or import) custodians, and specify locations and policies:
  - See *"Mapping Employee Attributes" on page 35*
  - See *"Importing Custodians to Your Data Map" on page 36*
  - See *"Adding Locations for Collected Data" on page 45*

Source Account Overview

A source account is the authentication used to control access to:

- the preservation destination where collected data will be stored
- the source data that you want to collect

From the **All Collections** > **Source Accounts** screen, administrators can create multiple accounts if the network setup requires different authentication accounts to access source data.

From your list of sources, you can use the **Filter List** menu to view accounts by *Name*, *Description*, Type, Group, Location, Custodian, Templates, or Accounts currently in use (enabled accounts are listed by default) and apply additional filter parameters. To edit an account, click the source account name, change the account settings, and click **Save**.

While adding a source, you can specify the source account that has the required access permissions to the source data. If a source account is not specified while creating a source, then Veritas eDiscovery Platform runs collections using the *EsaApplicationService* user account credentials.

For information on source account requirements, see *"Verify Network Setup by Data Source" on page 26*.

For information on how to add a source account, see *"Adding a Source Account" on page 30*.

Verify Network Setup by Data Source

The Identification and Collection module allows you to configure multiple data sources, each with an associated authentication account. Use this as a checklist when populating your data map with the sources your organization will use.

Data Source Setup Checklist

Check	Supported Source Type	Source Account Requirements	Notes
☑	**Local Exchange Server**	• **Source Account must**: – have permission to open other mailboxes – belong to a Local Administrator group (on the appliance) – include the following "admin account" permissions according to your setup: For an **individual target mailbox** setup: – Read – Open mail send queue – Execute – Read metabase properties – Read permissions – Read properties – Receive as For **mailbox store access**, add these permissions to those above: – List contents – List objects – Create name properties in the information store – Administer information store – View information store status	• All versions of Microsoft Exchange Server (later than 2000) rely entirely on the Microsoft Active Directory service for directory operations • Similar account permissions are required for retrieving email using BlackBerry® Enterprise Server • See *"Securing source account credentials" on page 31*.
☑	**Exchange BPOS/Office 365**	• The source account user must: – be a Domain User for the enterprise domain – be a member of the Local Administrator's group on the appliance – have full access permissions on the mailboxes in BPOS/Office 365	• See *"Securing source account credentials" on page 31*.

Data Source Setup Checklist

Check	Supported Source Type	Source Account Requirements	Notes
☑	**SharePoint**	• The source account user must be a member of a group having the Design permission level. **Note:** If the source user belongs to a group having a "Full Control" permission level, user profiles will also get collected. Therefore, to imply stricter security compliance, it is recommended that the source user should belong to a group having the "Design" permission level rather than the "Full Control" permission level. **Note:** For SharePoint Online only: The default domain name that the system recognizes is microsoftonline.com. eDiscovery Platform looks at the domain name used in the username while determining the source as SharePoint Online. If you use a domain name other than microsoftonline.com, then you need to set the value of the ***esa.icp.collection.sharepoint.online.userdomain*** propertry as the domain name used in the username. For example, if your username is abc@xyz.com, then the value of this property must be set as xyz.com. You can specify multiple domain names by separating the values by comma.	• Appliance connects to the SharePoint site via HTTP or HTTPS • The SharePoint server must be reachable from the appliance
☑	**Lotus Domino Server**	• An **Administrator Key File** must have permissions to open or read data from collected mailboxes	• If the appliance and Domino server are on different domains, a cross-certificate may be needed. • See *"Securing source account credentials" on page 31*.
☑	**FileShares**	• **Source Account** should have at least *Read* privileges	• Appliance and file shares should be in the same Active Directory domain forest • Veritas eDiscovery Platform collects from folders and subfolders that are visible to the specified account

Data Source Setup Checklist

Check	Supported Source Type	Source Account Requirements	Notes
☑	**PC on the network**	• **Source Account** should have *Read* privileges on the local workstation/ laptop	• Only volumes, folders and files visible to the specified account will be collected • Local drives or volumes on the PC must be configured to allow sharing • Local PC should be configured with **Windows Firewall turned Off**
☑	**PC (for OnSite Collection)**	• **User Logged On to OnSite PC** should have privileges to run the OnSite Collector (.exe) file. • Local Admin privileges are a required to run the OnSite Collector installation (.msi) file.	• Veritas eDiscovery Platform OnSite Collector is an .exe file. (*Some anti-virus configurations prevent .exe files from running from an external drive*.) • USB ports could be blocked due to policy restrictions • After creating and downloading an OnSite Collector file, extract the package and run the installation .msi file. • PC should not be in use while you are collecting from it. In particular, MS Outlook and MS Office programs must be closed.
☑	**Mac (for OnSite Collection)**	• [No additional setup required]	
☑	**Documentum**	• The source account is the account used to access the Documentum Content Server. • The user must have either an administrative privileges or permissions to access the repository.	
☑	**FileNet**	• The source account is the account used to access the FileNet Server. • The user must have either an administrative privileges or permissions to access the Repository.	

Data Source Setup Checklist

Check	Supported Source Type	Source Account Requirements	Notes
☑	**OpenText™ Livelink**	• The source account is the account used to access the LiveLink Content server. • The user must have either an administrative privileges or permissions to access the Repository.	
☑	**Veritas Enterprise Vault**	• **Check Veritas Enterprise Vault API Runtime version**. Upgrading to Veritas eDiscovery Platform 9.0 automatically installs Enterprise Vault 11.0.1 API Runtime client. If you want to use a different certified version instead of Enterprise Vault 11.0.1, you can avoid installing Enterprise Vault 11.0.1 by clearing the check box for Enterprise Vault 11.0.1 on the "Select Features" screen of the InstallShield Wizard while upgrading to Veritas eDiscovery Platform 9.0. If you already have installed Enterprise Vault 11.0.1 and now choose to use a different certified version, you can do the following: Uninstall, then reinstall a certified version of Enterprise Vault: 1.Stop Veritas eDiscovery Platform services. 2.On Windows, go to **Control Panel > Add/Remove Programs** and uninstall **Veritas Enterprise Vault API Runtime**. 3.Restart the server. 4.Install the certified version of Veritas Enterprise Vault API Runtime. • **Add Domain Account** to the Local Administrators group. (Create as many Local Users on the appliance as needed. Source accounts will be needed for each user.) • **Ensure Admin Account has Read permissions** to the Enterprise Vault archives for discovery, then change the *EsaEVCrawlerService* credentials. (By default, Veritas eDiscovery Platform uses *EsaApplicationService* credentials.) These credentials should be used when creating a source account for Enterprise Vault, before adding the source.	• The Enterprise Vault API Runtime client must be compatible with the Enterprise Vault server version. • Veritas eDiscovery Platform certifies Enterprise Vault API Runtime versions: 10.0.4, 11.0, 11.0.1, and 12.x as of 9.0. • After upgrading to 9.0, before logging on to Veritas eDiscovery Platform, clear the Browser's cache (history). • An updated license is required for the Veritas Enterprise Vault server option to appear in Veritas eDiscovery Platform. • Multiple Local Users can be created on the appliance. (to enable concurrent multiple PST creation). For more information, see *"Collection Administration and Maintenance" on page 177*. • Appliance must be in the same domain as the Enterprise Vault Directory server. • The FQDN of the Enterprise Vault Directory server is reachable so that the Enterprise Vault Discovery task runs successfully.

Adding a Source Account

A source account must be added before you add the source.

To add a source account

1. From **All Collections**, click **Source Accounts**.

   A list of source accounts displays.

2. Click **Add**, then specify the following information. An asterisk (*) indicates a required field.

Source Account

Field	Description
Account*	Enter a name for the source (up to 35 characters). The name is not case sensitive, but must be unique. Use only letters, numbers, and underscores. Be sure to use appropriate formatting.
Description	Enter a description for this source account (up to 255 characters).
User*	Enter the user's network ID or email account. (Example: CORP/mike or mike@corpemail.com.)
Password* Confirm Password*	Enter and verify a case-sensitive password for the source account.

   Note: You can test these credentials by accessing the source directly (outside of Veritas eDiscovery Platform) using the same credentials.

3. Click **Save** to add the new account.

Define Source Groups (Optional)

As part of adding sources to your data map, you can (optionally) create customized groups for your sources. Source groups can help organize larger data maps containing multiple sources. You can assign a specific source group to each data source, then filter or search for sources within a specific group.

To add a source group

1. From the **All Collections** module, click **Source Groups**.
2. Click **Add** and choose where the source group belongs.
3. Enter a name for the source group, and a description (optional). An asterisk (*) indicates a required field.
4. Click **OK** to submit the new group, or click **Cancel** to discard your changes.

Securing source account credentials

For collecting data from data sources, users need to create source accounts and provide login credentials to access these data sources. While performing Active Directory sync and data collection, eDiscovery Platform passes these credentials to the data source's executables for authentication.

Release 8.2 and later provides security enhancements for source account credentials for collecting data from data sources such as Exchange and Domino. The eDiscovery Platform system components now pass the source account credentials using an SSL channel. This results in enhanced security of source account credentials.

eDiscovery Platform by default uses the self-signed certificate that is shipped with the appliance. If a user intends to use the default certificate, then users do not need to perform any additional action related to certificates.

If a user wants to use a custom certificate, they need to perform additional steps as described below.

- If users generate and install a self-signed certificate using the appliance's Clearwell Commander, then they must set the property: ***esa.common.security.custom.cert.thumbprint***. The value for this property is the thumbprint of the certificate. If this property is set, the commander-generated certificate is used for securing source account credentials.
- If users plan to use their own certificate, then they must first perform the following steps as described in the Provider-Generated Certificate section in the System Admin Guide.

    A. Generate a CSR file and keypair.

    B. Install the certificate.

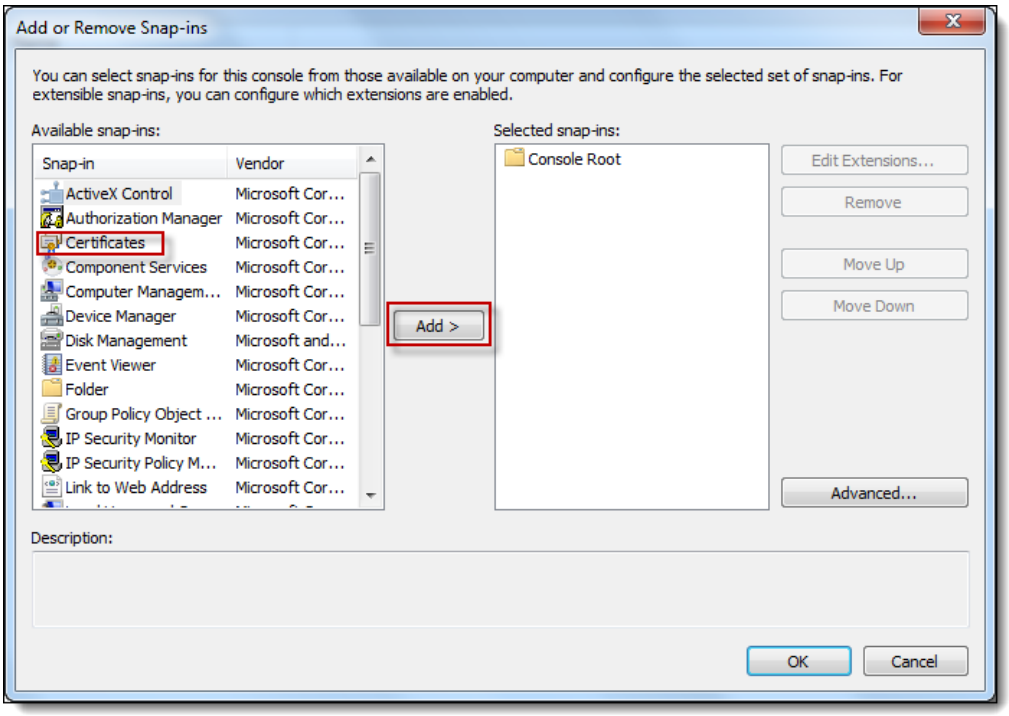
    C. Copy the Valid Certificate Where Needed.

    After performing the above steps, the user must set the property: ***esa.common.security.custom.cert.thumbprint***. The value for this property is the thumbprint of the certificate. If this property is set, the provider-generated certificate is used for securing source account credentials.

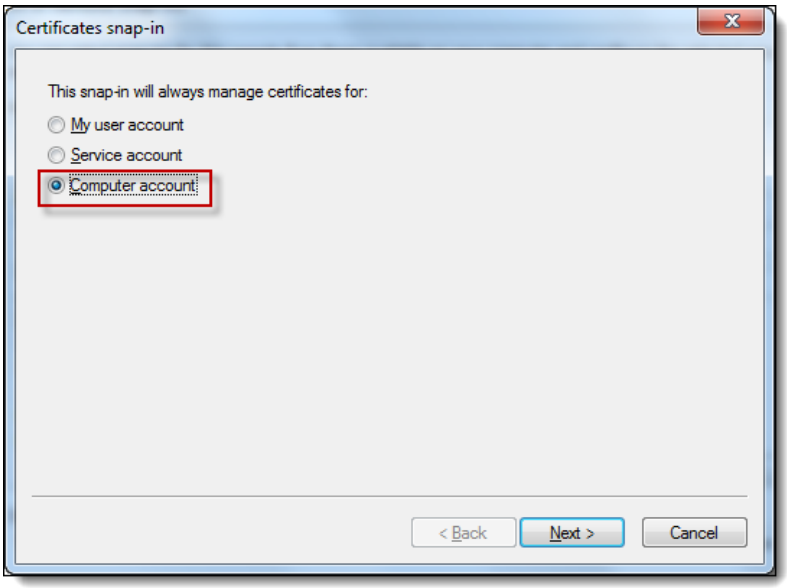
If Active Directory discovery or collection fails or a certificate gets expired or corrupt, users can see details in the server logs.

To locate a certificate's thumbprint:

1. From **Start** > **Run** > type **mmc**, and then click **Enter**.
2. Open the Microsoft Management Console (MMC) snap-in for certificates.
3. Click **File** > **Add/Remove Snap-in**. The Add or Remove Snap-ins window appears.

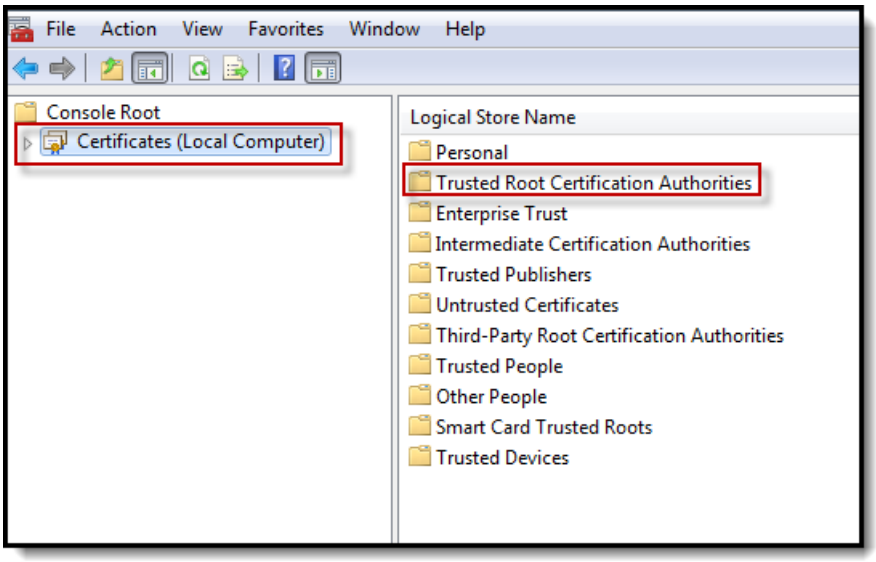


4. Select **Certificates** from the Available snap-ins section, and then click **Add**. The Certificates snap-in window appears.

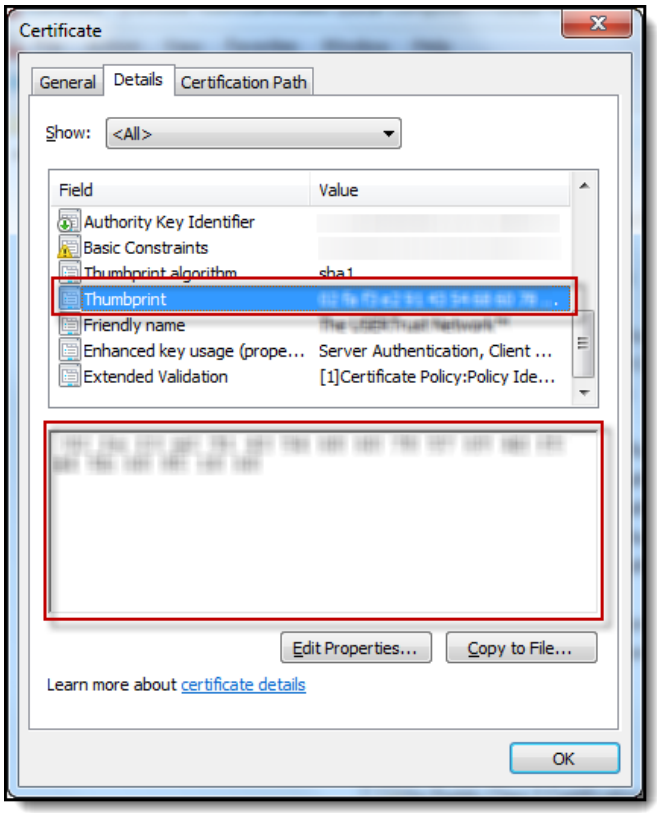


5. Select **Computer account**, and then click **Next**.
6. Click **Finish**, and then click **OK**.

7. In the Console Root window's left pane, click **Certificates (Local Computer)**.



8. Click the **Trusted Root Certification Authorities** folder to expand it.
9. Click the **Certificates** folder to expand it, and then double-click the desired certificate.
10. In the Certificate dialog box, click the **Details** tab.

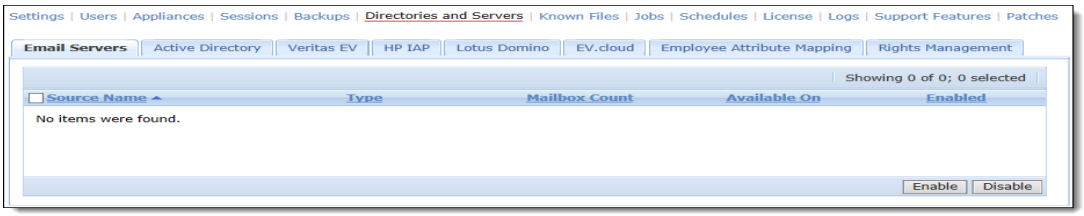


11. Scroll through the list of fields and click **Thumbprint**.
12. Copy the value displayed in the box to set the value of the property as mentioned earlier.

Data Discovery Overview

Data discovery populates your data map with employee data, called "custodians" when it becomes available for collection. Typically, email servers represent a critical source of data from which to collect. To add email servers to your data map, be sure to perform discovery on Active Directory or Lotus Domino (for Lotus Notes sources) first.

From **System** > **Directories and Servers**, select the tab for the source you want to discover.



Note: Check with your System Administrator to verify whether discovery may have already been done on email servers during network setup of your collections environment.

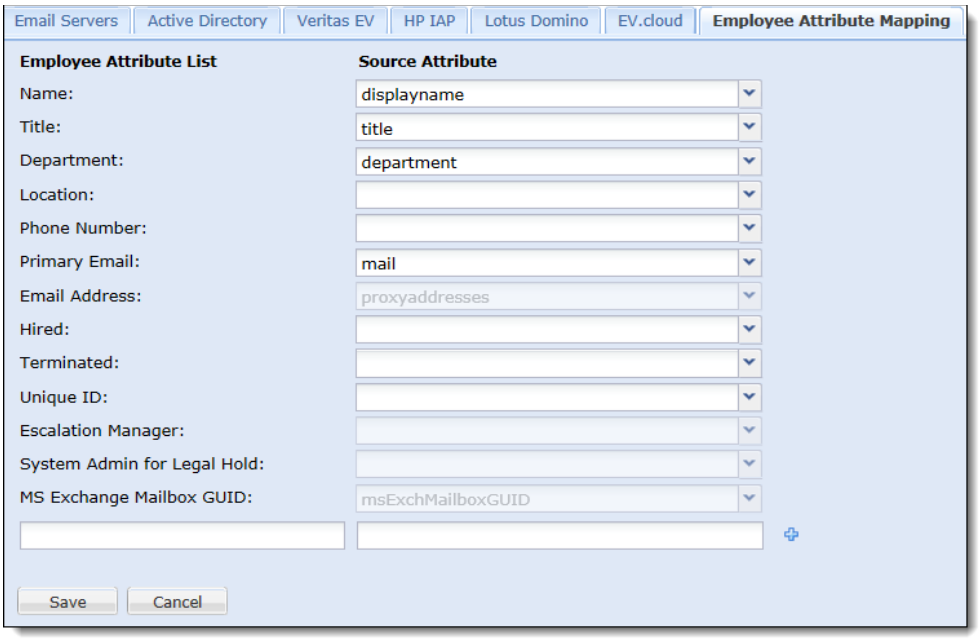
The main server/archive sources include:

- **Email Servers**
  - Shows a repository of all discovered Exchange servers, Domino Servers, Enterprise Vault Vault Stores, and HP IAP servers
- **Active Directory**
  - Shows domain sources available for discovery (or click to add a domain if the domain source exists, but does not appear on the list.) Verify that the sources to be added are part of your Active Directory Forest. See *"Setting up Data Sources" on page 47* for detailed steps to perform discovery depending on Exchange source type.
- **HP IAP**
  - Shows HP IAP archive sources available for discovery. Alternatively, click **Add** if the HP IAP source exists, but does not appear on the list.) When finished, click **Start Discovery**.
- **Veritas Enterprise Vault**
  - Shows results for all Enterprise Vault sources and archives from discovery. To discover a new Enterprise Vault vault directory, you must have the Directory Server Host Name. Under "Policies", rules can be applied to Enterprise Vault sources later, when specifying filter criteria in preparation for collection. See *"Veritas Enterprise Vault" on page 87*.
- **Lotus Domino**
  - Shows Lotus Domino server sources available for discovery (or click to add if the Domino server source exists, but does not appear on the list.) See *"Lotus Domino® Server Setup" on page 82*.
- **EV.cloud**
  - Shows all previously discovered EV.cloud sites and archives. To discover a new EV.cloud site, you must have the Site URL and Admin user credentials.

To perform discovery and/or start adding sources, continue with steps in *"Setting up Data Sources" on page 47* for each specific source type you want to add.

Mapping Employee Attributes

Any time you want to add or change one or more attributes for an employee, use the **Employee Attribute Mapping** tab. The **Employee Attribute Mapping** tab displays (by default) the list of default attributes predefined for an employee.



Veritas eDiscovery Platform attributes can be mapped to other Sources attributes by typing in the name of the Source attribute, or by selecting the attribute from the drop-down list. New Veritas eDiscovery Platform attributes can be added by clicking the "+" icon.

Attribute mapping is used to bring in the corresponding data values from Active Directory (AD) when the AD synchronization takes place, as well as from other sources of employee data through CSV or Script Imports. This is helpful when you need to update custodian information for a single individual directly in Veritas eDiscovery Platform, without re-importing the custodian's data to capture the changes (depending on the source of information you determine for these attributes).

To map employee attributes

1. Select or type a definition for one or more employee attributes that you want to be imported into the Employee List. (Fields that appear unavailable cannot be changed.) For field details, see the table in the steps *"To add a custodian individually (option B)" on page 43*.

2. Optionally, enter a custom attribute in the blank field. (Click the "+" icon to add more custom fields.)

   Note: The maximum number of custom attributes that you can add by default is 10. You can add up to 15 custom attributes if the *"esa.icp.employee.maxCustomAttrAllowed"* property is set.

3. When finished, click **Save** to update changes in the system.

Importing Custodians to Your Data Map

The eDiscovery Platform system imports new custodians automatically, upon discovery. However, you can still import custodians manually. There are several ways to add custodians: synchronize with Active Directory, import from a CSV or Script file, or add individually. To import using CSV or script, refer to the format requirements in this section.

Note: To add or import custodians (plus other custodian management options), after adding them to a case, see *"Managing Custodians (Across a Case)" on page 187*.

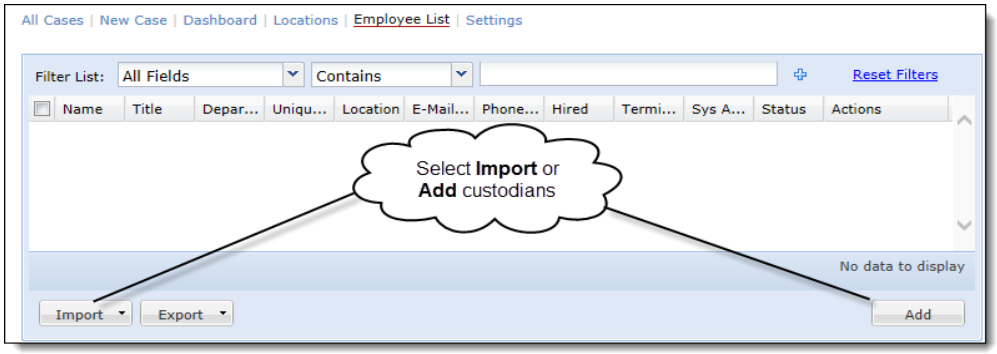
About Merging/Unmerging Custodians

Later, after your selected custodians have been added to a case, you can use the "Custodian Merge" feature to resolve any same-name, or similarly-named custodians (that represent the same source or individual). Alternatively, use the "Unmerge" feature to keep Collection Set custodian names unique if similarly-named (representing other individual) custodians already exist. For more information, refer to *"Merging Custodians" in the Case Administration Guide*.

Note: Custodians in Veritas eDiscovery Platform's Processing, and Analysis & Review (PAR) modules are *not* case-sensitive. As a result, custodians in the Identification & Collections (IC) module may be merged with similar custodian names in PAR. For example, the IC custodians "joe admin", "Joe admin", and "Joe Admin", who are all considered unique in IC, are treated as the same custodian in PAR. Thus, when you add a collection set (created in IC) containing the custodian "joe admin" to a PAR case that contains another custodian "Joe Admin" they are merged as one custodian. However, if that same PAR case contained no similarly-named custodians, and all three IC custodians were added to the case, they will be considered unique. In any case, to ensure your IC custodians remain unique, you can either specify custodian names with a numeric designation, or simply unmerge custodians in PAR.

To add custodians

1. From the **All Cases** view, click **Employee List**.



   (Alternatively, within a case under the **Collections** module, click **Sources**, then from the **Custodian** box, click **Edit Custodians**, then **Add**.)

2. From the Employee List, choose one:

A. **Import** custodians (by synchronizing with Active Directory, or using a script or CSV file). See *"To import custodians (option A)" on page 37*.

B. **Add** custodians individually. See *"To add a custodian individually (option B)" on page 43*.

To import custodians (option A)

1. Click **Import** and select one of the following options:

   – **Synchronize with Active Directory**. This submits an "Employee Synchronization Job" which checks Active Directory for any new or modified custodian data. Click **OK** at the prompt, then check the **Jobs** window for results. (See *"Synchronize with Active Directory" on page 37*.)

   Note: Veritas eDiscovery Platform performs an Active Directory discovery to synchronize Active Directory domains, Exchange servers, Exchange mailboxes, and Active Directory users (i.e. employees). In some environments, information related to employees is stored in a repository other than Active Directory. In such an environment, employee records are imported into Veritas eDiscovery Platform using CSV or Script. In this case, synchronization of Active Directory users through an Active Directory process can be disabled by setting the value for the property **esa.icp.employee.skipEmployeeSync** as **True** by using **System** > **Support Features** > **Property Browser**. By default, this property is set to **False** that causes automatic synchronization with Active Directory.

   – **From CSV** | **Script**. Depending on the file type, from the *Import from* [*CSV* or *Script*] dialog, enter the file name, or click to browse to the location, then click **OK**. (See *"Importing Custodians from CSV or Script" on page 38* for format requirements).

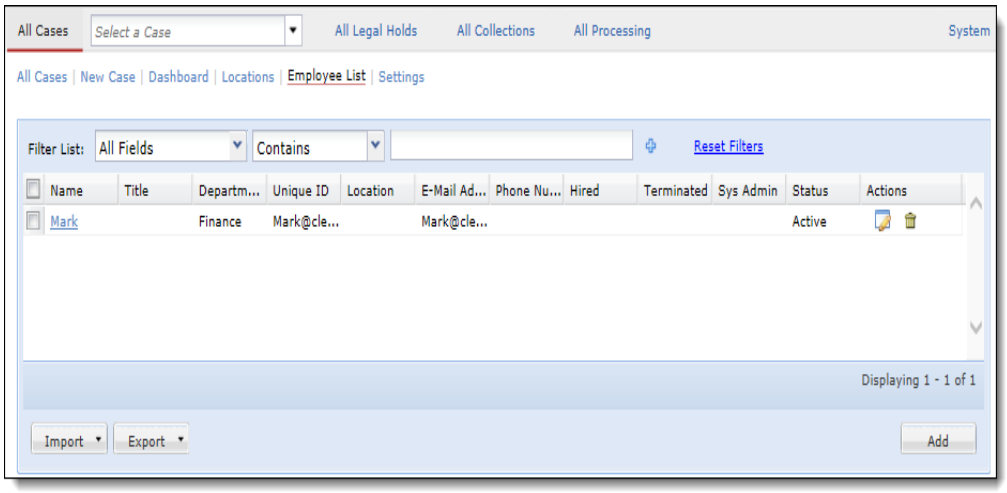
2. If your import/synchronization was successful, all new or updated custodians appear in the employee list.

Synchronize with Active Directory

After synchronizing for employee information updates, the date/time stamp at the top shows your last successful synchronization with Active Directory. Active Directory synchronization can also be scheduled to run at a later time, from the **System > Schedules** screen.

Note: It is recommended that you schedule recurring Active Directory synchronizations so that employee history can be built and made available for use for narrowing employee searches within a given time range.

The updated custodian information can be viewed from the Employee list by attributes such as *Name*, *E-Mail Address* or any other custom-mapped attribute. Use the *Filter List* menu and additional fields to search, sort, and filter on attributes, including customizing columns and sort order.



You can also sort on the history of custom attributes by date range. For example, by selecting "Contains" and entering "Between", you can specify dates within which to narrow your search.

Importing Custodians from CSV or Script

The Collections Admin can automatically populate the Employee List by providing a CSV or script file which meets specific requirements for bulk import into Veritas eDiscovery Platform. Before importing your custodians, ensure your CSV file or script meets the following requirements.

Note: When importing custodians from a file, the names are added in the system similar to a processed job. To view the status of your CSV or Script file import, click the **Jobs** link at the top of the screen. If an error occurs during import, a warning icon appears next to the link. Click the book icon in the Status column to view details in the job status log.

CSV Import Format Requirements

The CSV file should be provided in the following format:

1. **Header row** - First row of the file, consisting of the column names (in any order), separated by commas. The following column names should be specified:

   Note: An asterisk (*) indicates a required field.

CSV Import Format Requirements

Column Name	Format	Max Limit	Example
Name*	UTF-8	256	John Doe
Domain	UTF-8	256	Veritas
File owner name	UTF-8	256	John Doe
File owner SID	UTF-8	255	1122
Title	UTF-8	256	Analyst
Division	UTF-8	256	Sales
Location	UTF-8	512	California
Phone Number	UTF-8	64	555 1234567
Hired Date	MM/DD/YYYY	10	05/02/2010
Terminated Date	MM/DD/YYYY	10	08/10/2011
Email	UTF-8	100	John@Veritas.com johnie@Veritas.com **Note:** Maximum number of email addresses per employee is 20.
Primary Email	(Integer) Index	255	0 **Note:** Email with index 0 in the list of emails will be displayed as primary: John@Veritas.com
Escalation Manager Unique ID	UTF-8	255	5599
System Admin	TRUE/FALSE (FALSE by default)	5	FALSE
Unique ID*	UTF-8	255	1133
[Custom Attribute]		512	

2. **Employee Record** - Each of the following rows will be interpreted as an employee record, with each attribute separated by a comma. The number of fields in each row must match the number of columns in the header row.

   The following rules apply to attributes or columns in a CSV file for Employee List bulk import:

CSV Import Format Requirements

Attribute or Column	Rule(s)
Column names	• Case-Sensitive; (must be typed as shown in Table 1.) • Can be written in any order **Note:** Custom attribute column names must match custom attribute display names.
"Domain" Column	• (Optional) Must be present with "File owner name" column (or both columns must be absent). Cannot be individually selected. • Values must also be consistent in both columns if present (empty or populated).
"File owner name" Column	(Same rules apply as for "Domain" column.)
Fields containing line breaks (CRLF), double quotes, and commas	• Must be enclosed in double quotes. (") • If using double quotes to enclose fields, a double quote appearing inside a field must be preceded with another double quote. **Example**: "employee one","mc""adams".
Adding multiple values	When adding multiple values to a field, the values should be separated by commas (,) **Example**: Name, Phone Number, Unique ID John Doe, "555 8901234, 5550984321", 2

CSV Import Format Requirements

Attribute or Column	Rule(s)
Unique "Domain" and "File owner name" values	Domain and File Owner Name pairs must be unique across all employees. This does not apply to records with empty Domain and File Owner Name values.
Unique IDs	If an employee entry contains the same Unique ID as another employee entry, the following rules will apply: – New employee's "Email", "File owner name", "File owner SID", and "Domain" column fields will be appended to the existing employee's entry. – All other columns will be replaced. **Example**:

	Name	Email	Unique ID
Existing entry in Employee List	John Doe	JohnDoe@JohnDoe.com	1
New entry from CSV	Johnnie Doey	JohnnieDoey@JohnnieDoey.com	1
Resulting entry	Johnnie Doey	JohnDoe@JohnDoe.com, JohnnieDoey@JohnnieDoey.com	1

Script Import Requirements

An asterisk (*) indicates a required field.

Script Import File Format Requirements

Column Name	Format	Max Limit	Example
Name*	UTF-8	256	John Doe
Domain	UTF-8	256	Veritas
File owner name	UTF-8	256	John Doe
File owner SID	UTF-8	255	1122
Title	UTF-8	256	Analyst
Division	UTF-8	256	Sales
Location	UTF-8	512	California
Phone Number	UTF-8	64	555 1234567
Hired Date	MM/DD/YYYY	10	05/02/2010
Terminated Date	MM/DD/YYYY	10	08/10/2011
Email	UTF-8	100	John@Veritas.com johnie@Veritas.com **Note:** Maximum number of email addresses per employee is 20.

Script Import File Format Requirements (Continued)

Column Name	Format	Max Limit	Example
Primary Email	(Integer) Index	255	0 **Note:** Email with index 0 in the list of emails will be displayed as primary: John@Veritas.com
Escalation Manager Unique ID	UTF-8	255	5599
System Admin	TRUE/FALSE (FASLE by default)	5	FALSE
Unique ID*	UTF-8	255	1133
[Custom attribute]		512	

Script File Format and Location

All CSV formatting requirements also apply to those used for bulk import. However, to ensure security while running executable (.exe) files, all scripts must be stored in the folder: "D:\customerScript\bulkImport". Appliance users should ensure that access to this folder is restricted to authorized users, since running executables on the appliance can pose significant security threats to the system.

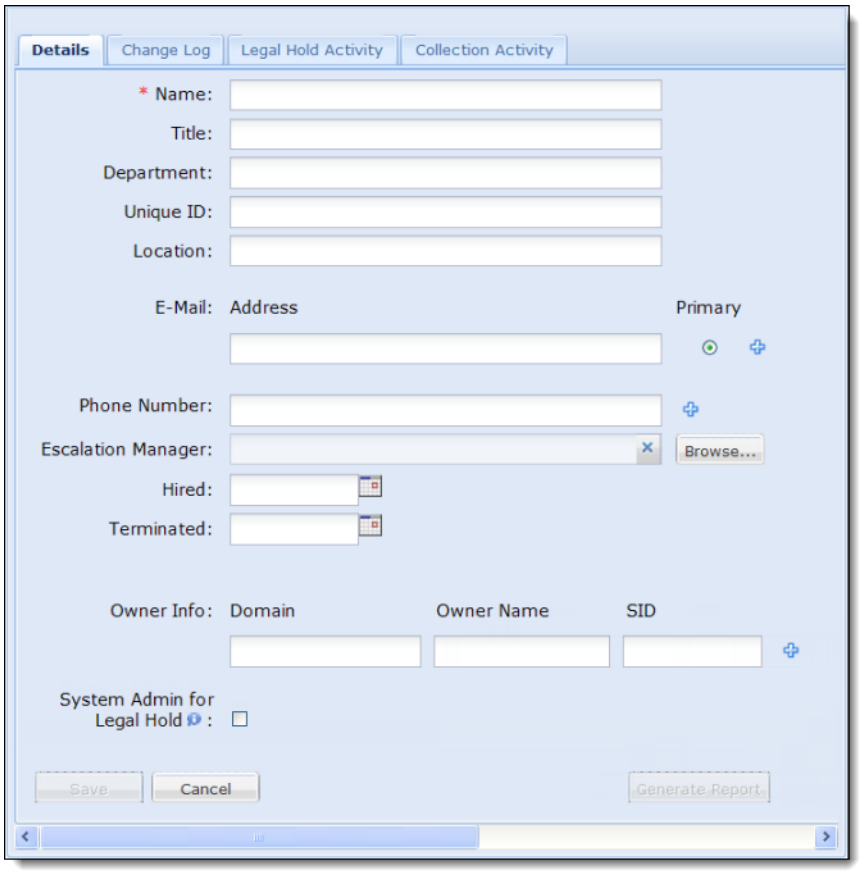
Note: Unless the file is an executable (.exe), then it should contain the location of the executable used to run it (as shown in the first line of the following example).

Example script:

```
#!c:\Perl\bin\perl.exe
print "Name,Email,Unique ID\n";
print "John Doe,JohnDoe\@johnDoe.com,1122\n";
print "Johnnie Doey,JohnnieDoey\@johnnieDoey.com,1122";
```

To add a custodian individually (option B)

1. From the **All Cases > Employee List** screen, click **Add**.



Note: The Legal Hold option will be visible only if your enterprise has a Legal Holds module license installed, and the logged on user has appropriate permissions.

2. On the **Details** tab, specify the following information. An asterisk (*) indicates a required field.

Adding a Custodian to the Employee List

Field	Description
Name*	Enter the name of the custodian (up to 35 characters). The name is not case sensitive.
Title	Enter the custodian's title (if applicable).
Department	Enter the custodian's division or department (if applicable).
Unique ID	Enter an identification number or code unique to this custodian.
Location	Enter a location.

Adding a Custodian to the Employee List

Field	Description
E-Mail: Address	Enter the employee's email address. (Example: jsmith@acmemail.com). By default, the icon is selected to indicate that this is the *Primary* address. Click the icon to add additional addresses for this custodian.
Phone Number	Enter a phone number for the employee. Click the icon to add additional phone numbers for this employee.
Escalation Manager (Legal Hold users only)	Enter or browse for the name of this employee's manager to whom legal hold notifications should be escalated.
Hired / Terminated	Enter the date of hire and termination (if applicable), or click the calendar icon to select a date.
Owner Info: Domain, Owner Name, SID	Enter the Domain name, owner name, and the Security Identifier. **Note:** The owner name will only be collected (when filtering for collection) if the Windows user for the collection is running as the source account (or *EsaApplicationService* user if there is no account on the source), and it is in the domain where the owner name is kept.
System Admin for Legal Hold (Legal Hold users only)	Select this check box if this employee's role is a System Administrator, for use in customizing Legal Hold notifications.
Legal Hold History (Legal Hold users only)	Displays summary of Legal Hold activity associated with this custodian. (Includes names of Legal Holds and Notifications, and date notifications were last sent.) For more information, refer to the section *"Administering User Accounts" in the System Administration Guide*.

Note: Additional fields may appear if custom attributes were created and mapped in the Employee List. (Custom attributes automatically become available at the bottom of the **Details** tab once they have been created.)

3. Click **Save** to associate the new employee to the selected source, or click **Cancel** to discard your changes.
4. Optionally, click **Generate Employee Report** to view an activity report for the newly-added employee.
5. Optionally, click the other tabs to view additional information pertaining to this employee across all cases. (Use the *Filter List* menu and additional fields to search, sort, and filter changes, including customizing columns and sort order.)
   - **Change Log**. Displays a list of historical activities performed (for enabled attributes only) on the selected employee, showing both the previous and new values. Also use the filter list to search change history (by date range - for history-enabled attributes only), for the employee across all cases. Change log is shown for history enabled attributes only. Following employee attributes, is history (enabled by default) for *Name*, *Title*, *Department*, *Location*, *Email* attributes, plus all custom attributes.
   - **Legal Hold Activity**. Displays a summary of holds and notification activities associated with the selected employee. (Includes names of Legal Holds and Notifications, status, and date notifications were last sent.)

– **Collection Activity**. Displays a summary of collection activities associated with the selected employee. (Includes names of Collections, types, task sources, and status.)

Note: If employee information is viewed from the Case Custodian screen, only cases specific to Legal Holds and Collections are shown. If employee information is viewed from the Employee list, Legal Holds and Collections across cases are shown. The same views apply to reports generated using the "Generate Employee Report" task. To manage custodians for a single case, after processing, see *"Managing Custodians (Across a Case)" on page 187*.

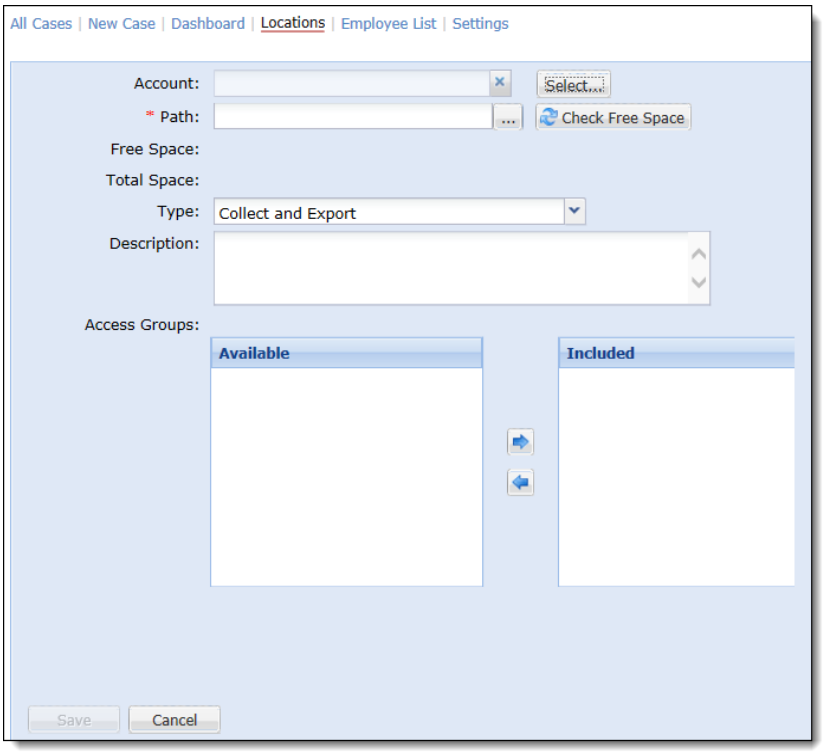
Adding Locations for Collected Data

After setting up an authentication account, add a *Preservation Destination*, the location where you want collected data to be copied. You can add multiple locations to manage storage across geographical locations and by priority.

Note: Be sure to monitor your disk space usage if you are using a single appliance or location as the preservation destination for all your collections. Lack of disk space on the appliance could impact performance in other areas of the product. The eDiscovery Platform system allows you to move data (after collection) from one preservation destination to another location. For more information and steps for how to move data after collection, see *"Move Collected Data to Another Location" on page 133*.

To add a location

1. From the **All Cases** > **Locations** screen, click **Add**.



2. Specify the following information. An asterisk (*) indicates a required field.

Source Data Location

Field	Description
Account	Enter the name of the source account you created, or click **Browse** to select one from the list of accounts.
Path*	Enter the path to the location where the collected data will be stored. Click the ... button to select a File Share or remote directory. Click **Check Free Space** to verify data storage capacity.
Type	Select the type of the location, including Collect and Export, Export Only, and Collect Only.
Description	Enter a description for this source account (up to 255 characters).
Access Groups	By default, all groups to which the user has access are listed in the **Included** column which results in the location being added in all groups. Keep only those groups in the **Included** column in which you want to add the location and move all the remaining groups to the **Available** column. If a location is not added to any group, then that location will be available to all users.

3. Click **Save** to submit the location, or click **Cancel** to discard your changes.

Setting up Data Sources

Follow the steps in this section (by source type) to perform the tasks necessary to set up your organization's IT environment for Identification and Collection using Veritas eDiscovery Platform.

For a general overview about adding (any) sources:

- *"About Adding (or Importing) Sources to Your Data Map" in the next section*
  - *"Required Source Information" on page 49*
  - *"Import Sources from CSV or Script" on page 50*

To start adding sources (by source type) refer to the appropriate section:

- *"Local Domain Exchange Setup" on page 53*
  - *"Lync 2013 Setup" on page 59*
- *"Office® 365 Setup" on page 61*
- *"BPOS Exchange Setup" on page 71*
- *"Lotus Domino® Server Setup" on page 82*
- *"SharePoint Source Setup" on page 84*
- *"File Share and Windows PC Setup" on page 86*
- *"Veritas Enterprise Vault" on page 87*
- *"EV.cloud" on page 95*
- *"Collecting from Documentum, FileNet, and Livelink" on page 98*

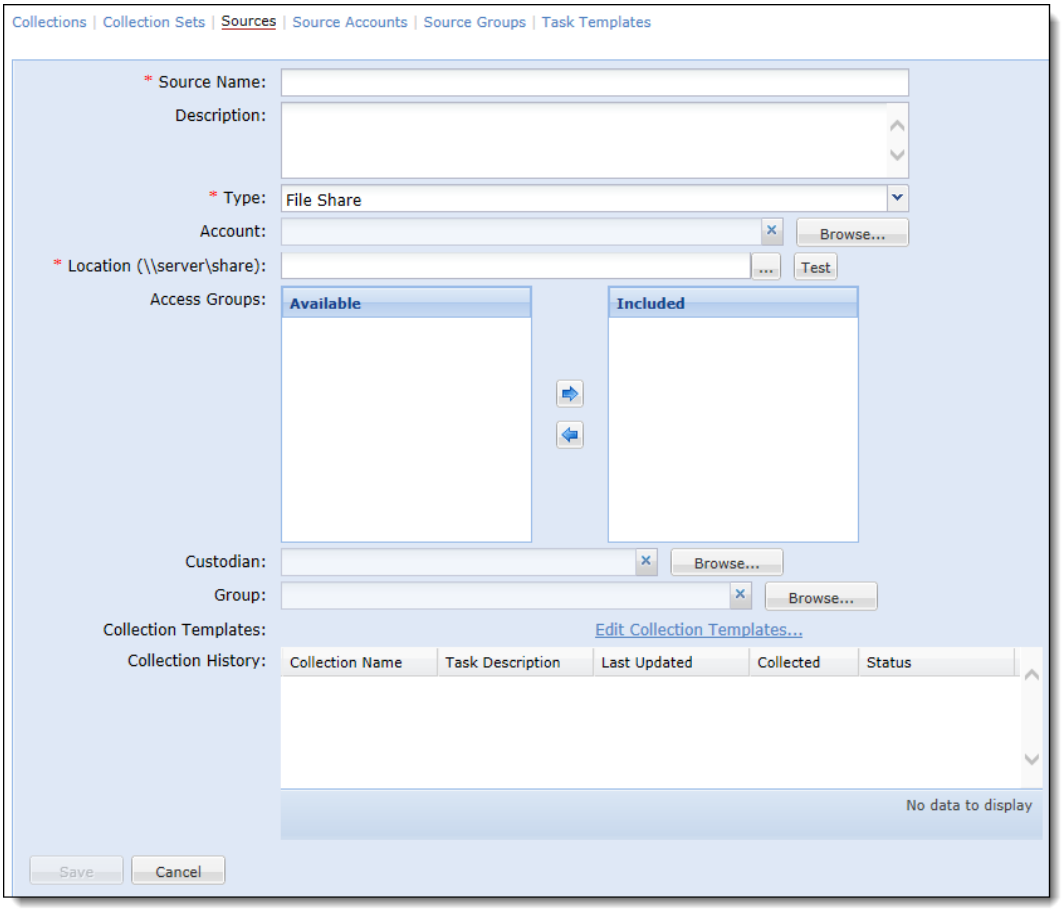
About Adding (or Importing) Sources to Your Data Map

Identify the sources of data (where the data will be collected from), or populate your data map automatically using the bulk import feature. Typical sources may include File Shares, Exchange Servers, SharePoint, Lotus Domino Servers, Enterprise Vault, EV.cloud, or remote locations such as a personal computer.

Starting with 8.0, users can view only those sources that are added in the groups to which the user has access or the sources that are not added to any group. Sources are considered as open to all when they are not associated with any group. By default, when a new source is created, it becomes part of all groups to which the user has access. The Access Groups permissions should be enforced explicitly.

Starting with Release 8.1, only CMIS compliant versions of Documentum, Livelink, and FileNet are supported. The existing sources that were created for the non-CMIS compliant versions of these data sources cannot be used as it is after upgrading to Release 8.1 and later. To use the existing sources, you must reconfigure the existing non-CMIS compliant sources to CMIS compliant sources. A banner and a warning message appears suggesting you to reconfigure the sources. Unless you reconfigure the source, you will not be able to add new collection tasks/templates and perform some actions for the existing collection tasks/templates that are associated with the existing sources. If folder filter criteria were defined for the tasks/templates in the previous release, then users must redefine the folder filter criteria for the existing collection tasks/templates.

From the **Collections** module, click **Sources**, then **Add**. (FileShare is shown in this example.)



You will need to add a source for each type of data source--the storage device and location from which you want to collect data. Later, you will create collection tasks for each of these sources to begin collecting the data.

Note: Additional fields will be shown for Enterprise Vault source types, such as "Site" and "Archive Type", and for Documentum, FileNet, and Livelink sources, such as "Repository".

Also note:

- For Enterprise Vault collection, Veritas eDiscovery Platform can run federated searches across all sites, however, the searches are specific to the Vault Site. If searches must be run across multiple sites, different collection sources must be created for each site, allowing collection tasks to be created and run for each of the sites.
- If you are adding a collector, but the collector does not appear in this list, or if you have a trial license you want to use, go to **System > License** and click **Update License**. Follow the on-screen instructions in the Update License Wizard to upload or copy/paste an available license for the appropriate collector(s).

Required Source Information

Depending on which type of sources you add, you will need to specify the following information. An asterisk (*) indicates a required field.

Source Data

Field	Description
*Source Name	Type the name of your data source (up to 35 characters).
Description	Enter a description of the source (up to 255 characters).
*Type	Enter or select the source type. (Example: PC).
*Site *Archive Type	(Enterprise Vault Source only): Enter the site and select an archive type to be used for this Enterprise Vault source. For example, entering the site: EVVAULTSITE and selecting the Enterprise Vault Domino mailbox archive allows collections from any mailbox archives in Lotus Domino from within EVVAULTSITE. **Note:** For details, refer to the steps in *"Veritas Enterprise Vault" on page 87*.
*Site	(For EV.cloud source): Select the EV.cloud site URL.
Account	Enter the name of the source account you created, or click **Browse** to select one from the list of accounts.
*Content Server CMIS URL	(For Livelink, FileNet, and Documentum sources only) Enter the Content Server CMIS URL, which is also referred as RESTful AtomPub Binding URL. **Note:** For Collectors, the full HTTP address is required. For example: Documentum: http://<host>/emc-cmis-ea/resources/ Livelink: http://<host>/ot-elib/cmis/atom FileNet: http://<host>/fncmis/resources/Service Verify the correct location convention with your System Administrator. Click **Fetch Repositories** to populate the list of repositories.
*Location (\\server\share) *Location (Host name)	(For File Share and PC sources only) Enter the path (for example, File Share or PC), or URL (SharePoint) to the location of the data source.
*Repository	(For Livelink, FileNet, and Documentum sources only): Select the repository to use for collection from the Documentum, Livelink, or FileNet source. (Multiple repositories may exist.)
Collect through a proxy	(For SharePoint source): To collect from a SharePoint source through a proxy, select the **Collect through a proxy** check box. Enter the name of the source account you created, or click **Browse** to select one from the list of accounts. Enter the Server DNS Name and the Port number. **Note:** Authenticated proxy login is not supported. A collection task fails when authenticated proxy login is used.
Max Data Transfer Rate	(For SharePoint source): Enter the maximum data transfer rate in Mbps.

Source Data (Continued)

Field	Description
Custodian Group	Type the name of the custodian or group associated with the data source (Example: John R. Smith), or click **Browse** to select one from the list of custodians/groups.
Access Groups	By default, all groups to which the user has access are listed in the **Included** column which results in the source being added to all groups. Keep only those groups in the **Included** column in which you want to add the source and move all the remaining groups to the **Available** column. If the source is not added to any group, then that source will be available to all users.
Collection Templates and Collection History	Indicates whether a template has been applied to the collection. (Click link to edit collection templates.) View list of collections and task details.

Import Sources from CSV or Script

If you have multiple sources to add to your data map, you can import them all at once from a pre-formatted CSV file located in your Active Directory, or from a script (already discovered in Veritas eDiscovery Platform). For more information about CSV and script formats, see Table "Source Import File Format Requirements". Scripts are useful if you frequently update your source list information and want to schedule the script to run periodically. (See *"Schedule a Script Run" on page 52*.)

Note: When sources are imported from CSV or script, then the Access Groups security settings are not applied to these sources. These free sources are available to all users. The Access Groups permissions should be enforced explicitly.

To start importing sources, see *"To import sources using CSV or Script"* in this section.

Bulk Import Format Requirements

Before importing your sources, ensure that the header fields are exactly as: Name*, Description, Type*, Locator*, Group Path, Account Name, Password, Custodian Names, IP_ADDRESS, HOSTNAME, FQDN, MAC_ADDRESS, and THRESHOLD, where an asterisk (*) indicates a required field. Note that the header fields are case-sensitive and can be in any order. Non-adherence to the header fields requirements results in failure of importing sources.

Source Import File Format Requirements

Format	Requirements	Rules
Script	Write output CSV file in UTF-8 to STDOUT	
CSV	UTF-8	

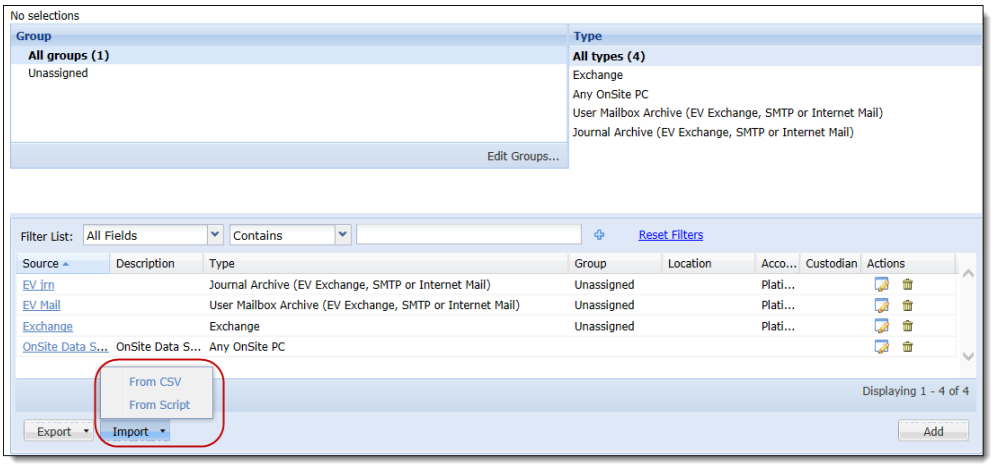
Source Import File Format Requirements (Continued)

Format	Requirements	Rules
CSV and Script	Contain header row with the following fields:	
	• Name*	(up to 100 characters)
	• Description	(up to 255 characters)
	• Type*	Must match a supported type (File Share, PC, Exchange, SharePoint, Domino). **Note:** If no sources are listed or do not match, this field is ignored.
	• Locator*	• Must list full UNC path for File Shares • Complete Host name for PCs • (Not needed for Exchange) • Full URL path for SharePoint **Note:** If this field is not listed or is incorrectly formatted, the field is ignored.
	• Account User Example: DOMAIN\user	• If account does not exist, one will be created. (Account name can match this username) • If an account already exists for this username, than a previously-existing account will be used.
	• Account Password	• If there is a username that does not exist and no password is provided, then no account will be added.
	• Custodian Name	• If custodian (by exact name) does not exist, one will be created. • If a single custodian already exists with this exact name, existing will be used. • If multiple custodians already exist with this exact name, leave the custodian field blank.
	• Group (Group name or group hierarchy)	• If a group with this name and hierarchy branch does not exist, one will be created. • If a group with this name and hierarchy already exists, than a previously-existing group will be used. **Note:** A group hierarchy can be separated by a "\" (back slash), such as: "HQ\Sales\Europe".

To import sources using CSV or Script

1. From the **Collections** module, click **Sources**.
2. Click **Import** and select an option:
   A. **From CSV** (imports sources listed in a comma separated values file)
   B. **From Script** (launches a script which automatically generates a CSV file.

Note: Use this option if you regularly update your sources, but do not maintain a CSV file. If the script is discoverable in the correct path and properly formatted (see Table *Source Import File Format Requirements*.)



3. Whether importing sources from a CSV or Script file, the source names are added to the case similar to a processed job. To view the status of your CSV or Script file import, click the **Jobs** link at the top of the screen. If an error occurs during import, a warning icon appears next to the link. Click the book icon in the Status column to view details in the job status log.

4. If your import was successful, all sources you selected to add or import appear in the list of sources. Click **Save** to associate the new sources to the selected case, or click **Cancel** to discard your changes.

Schedule a Script Run

Import scripts can be scheduled to run once or periodically.

To schedule your script to run automatically

1. Select **All Cases** from the **Cases** drop-down menu.
2. From the **All Cases** view, click **Schedules**.
3. Click **Add**.
4. From the Add Schedule page, select the Task Type **Bulk Source Import**.
5. Enter or select an Initial Run Date and Start Time.
6. To schedule the script to run as a recurring event, select the frequency. (Default is Once.)
7. Click **Save**.

Local Domain Exchange Setup

Setting up data collection from your Local Domain Exchange source requires the following steps:

1. Create an Admin Account* for Exchange Mailbox Discovery and Collection
2. Discover mailboxes using Active Directory Discovery and import custodians
3. Add the Local Domain Exchange source to your data map
4. Test an Exchange mailbox collection

Note: For the purposes of this setup, the domain user account is referred to as "Admin Account".

Continue with the following steps:

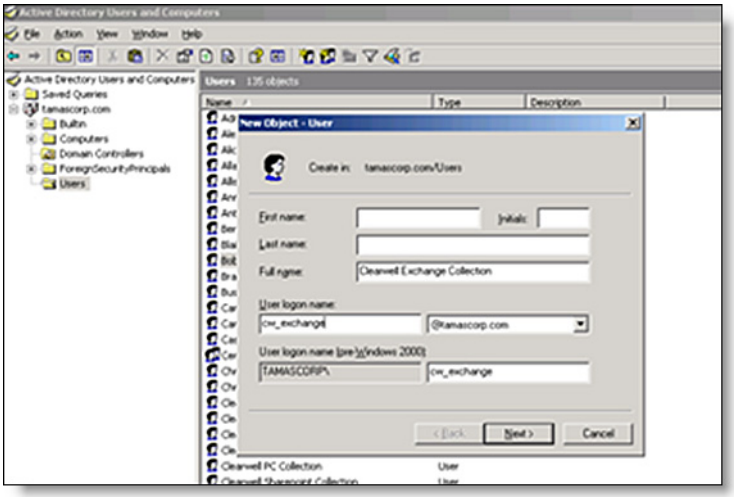
- *"Step 1: Create a New Domain Admin Account" in the next section*
- *"Step 2: Perform Active Directory Discovery and Import Custodians" on page 56*
- *"Step 3: Add Exchange Source to the Data Map" on page 57*
- *"Step 4: Test an Exchange Mailbox Collection" on page 58*

Veritas eDiscovery Platform provides an ability to collect the Lync 2013 conversations that are archived on the Exchange 2013 server. For more details, see *"Lync 2013 Setup" on page 59*.

Step 1: Create a New Domain Admin Account

To create a new domain account

1. In your Windows interface, open **All Programs** [or for newer versions: **Control Panel**] > **Administrative Tools > Active Directory Users and Computers**.
2. Click to expand the domain, then right-click **Users** and select **New > User**.
3. Enter the name and logon information for the Veritas eDiscovery Platform Exchange Collection admin.



4. Click **Next**.

5. Enter a Password and select (only) the option **Password Never Expires**, then click **Next**.
6. Clear the option to create an Exchange mailbox. (An Exchange mailbox is not required), then click **Finish** to create the admin account.

Continue with next steps to set up your admin account permissions, depending on your mailbox setup.

1a: Set up Exchange Local Account Permissions

Collecting from mailboxes in a Local Exchange server requires setting up a domain account with appropriate Exchange security permissions.

The "Admin Account" MUST be:

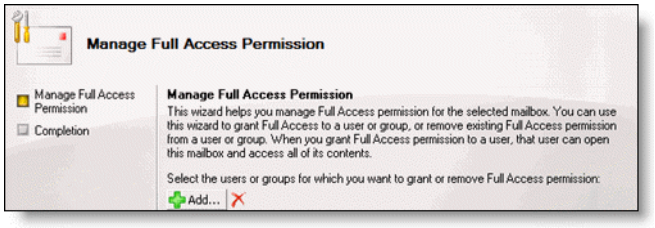
- a Domain User for the enterprise domain
- a member of a Local Administrator group on the appliance
- able to access and collect the target mailboxes (see below for access provisioning)
- able to write to the Preservation Destination

Choose one of three options depending on how you want to set up the Admin Account:

- Option 1: Give "Admin Account" access to individual target mailboxes
- Option 2: Give "Admin Account" access to a store of mailboxes
- Option 3: Run a PowerShell Script to automate running multiple mailboxes

Option 1: Give "Admin Account" access to individual target mailboxes

1. Open the Exchange Management Console on your Exchange Server, then select the target custodian mailbox(es) from the listed mailboxes.
2. Select the option to **Manage Full Access Permission…**
3. The Manage Full Access Permission window opens.



4. Click **Add** to the "Admin Account" and grant access.
5. Click **Manage**. A confirmation screen appears. Ensure that the following permissions are available to the "Admin Account":
   - Read
   - Open mail send queue
   - Execute

- Read metabase properties
- Read permissions
- Read properties
- Receive as

Option 2: Give "Admin Account" access to a store of mailboxes

Exchange allows mailboxes to be grouped under Storage Groups and Stores. You can give the Veritas eDiscovery Platform "Admin Account" access to an entire Store or Storage Group, and Veritas eDiscovery Platform will be able to access all of the contained mailboxes.

In addition to the permissions listed for Managing Full Access, in Option 1, also give the "Admin Account" the following five permissions:

- List contents
- List objects
- Create name properties in the information store
- Administer information store
- View information store status

Note: Ensure that any inherited permissions for this account do not take precedence and inadvertently deny these permissions.

Option 3: Run a PowerShell Script to automate provisioning many mailboxes

Follow the steps for Option 1, then repeat for multiple mailboxes by using a PowerShell script. This script should mirror the syntax shown on the confirmation screen when using the Exchange Management Console to set permissions.

For example:

Exchange Management Shell Command Completed:

```
Add-MailboxPermission -Identity
'CN=CUSTODIANUSER,CN=Users,DC=DOMAIN,DC=local' -User
'DOMAIN\ADMINUSER' -AccessRights 'FullAccess'-InheritanceType all
```

Step 2: Perform Active Directory Discovery and Import Custodians

Given the domain(s), Veritas eDiscovery Platform will perform an Active Directory discovery for mailboxes and groups.

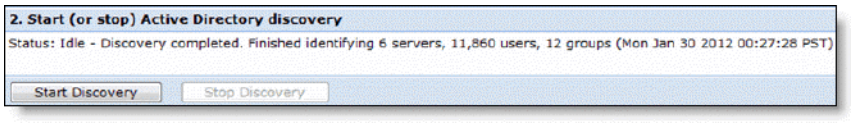
Note: It is recommended to provide credentials for a domain user account which has permissions to read the domain users as well as permissions to read the deleted objects container in Active Directory. This is required to mark correct status such as “Active” and “Inactive” for custodians as displayed in the Employee List. If these credentials are not set, Veritas eDiscovery Platform will default to using its Application Service credentials.

In addition to discovering mailboxes, Veritas eDiscovery Platform looks for specific patterns or attributes to determine on which servers these mailboxes reside.

Once Active Directory completes, you can import custodian data.

To perform Active Directory discovery

1. Log on to the appliance using "Admin Account" (the Domain user).
2. In the Veritas eDiscovery Platform interface, in the **All Cases** view, click **System > Directories and Servers**.
3. Select the **Active Directory** tab.
4. To add a new domain, click **Add Domain** then enter the domain name, and the administrator user name and password, and click **Save**.
5. When ready, click **Start Discovery**. This automatically detects the appropriate domain, and performs Active Directory discovery.



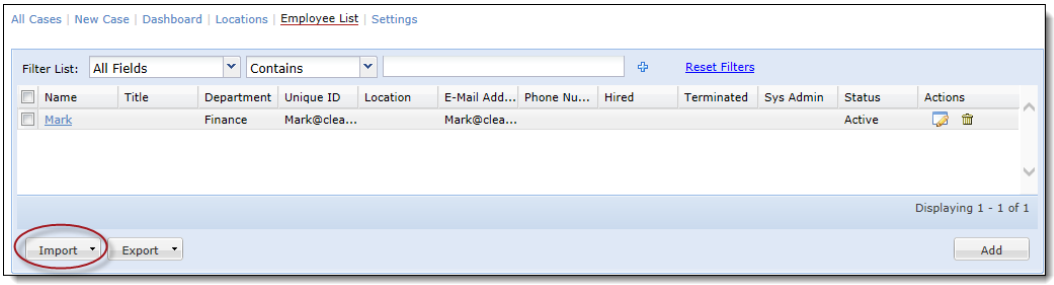
   Technical Note: This function checks for domains which contain the appliance. Once the domain is detected, Veritas eDiscovery Platform used the logged in account ("Admin Account") to discover servers, mailboxes, and groups from Active Directory. Typically, this should automatically discover the same Active Directory domain used by Exchange (if applicable).

   Troubleshooting: In rare cases, the desired domain may not be automatically discovered. For example, if the enterprise has legacy domains that may have been consolidated or deleted. In this case, you can manually enter your enterprise domain and account credentials by clicking **Add Domain** on the **System > Directories and Servers** screen.

6. When the Active Directory discovery is complete, the **System > Directories and Servers > Active Directory** tab displays servers, users, and groups that have been discovered.

To import the Employee List from Active Directory

1. From the **All Cases** view, click **Employee List**.



2. From the Employee List, click **Import** and select **Synchronize with Active Directory** (imports all custodians at once).

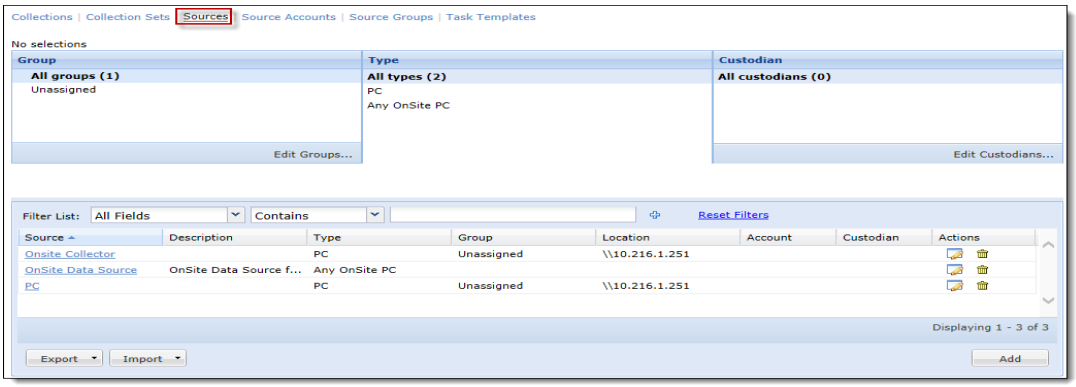
   Note: After import, use the Filter List menu to view by Name, User Name, or E-Mail Address and apply additional filter parameters.

For more details, refer to the section *"Importing Custodians to Your Data Map" on page 36*.

Step 3: Add Exchange Source to the Data Map

To add the Local Exchange source to your data map

1. In the **All Collections** module, click **Sources**.



2. On the Sources screen, click **Add**.

3. Specify the following information. An asterisk (*) indicates a required field.

Source Data

Field	Description
*Source Name	Enter a name for your Exchange source. Use the "Admin Account" you set up in *"1a: Set up Exchange Local Account Permissions" on page 54*.
Description	Enter a description of the source (up to 255 characters).
*Type	Select Exchange as the source type.
Account	Enter the name of the source account you created, or click **Browse** to select one from the list of accounts. **Note:** If you leave the **Account** field blank, Exchange collections will run using the *ESAApplicationService* account permissions.
Custodian Group	Type the name of the custodian or group associated with the data source (Example: John R. Smith), or click **Browse** to select one from the list of custodians/groups.
Access Groups	By default, all groups to which the user has access are listed in the **Included** column which results in the source being added to all groups. Keep only those groups in the **Included** column in which you want to add the source and move all the remaining groups to the **Available** column. If the source is not added to any group, then that source will be available to all users.
Collection Templates and Collection History	Indicates whether a template has been applied to the collection. (Click link to edit collection templates.) View list of collections and task details.

4. When finished, click **Save**.

Step 4: Test an Exchange Mailbox Collection

Note: Veritas eDiscovery Platform performs an Active Directory discovery to synchronize the Exchange servers, mailboxes, and archive mailboxes. If an archive mailbox is created after the Active Directory discovery is performed, Veritas eDiscovery Platform does not execute collections from the archive mailbox. Therefore, it is recommended to schedule an Active Directory discovery job before executing Exchange collections from the archive mailboxes. This helps to successfully execute collections from the archive mailbox.

To test the collection of a mailbox

1. In the **All Collections** module, click **Collections**. (In a selected case, **Collections > Sources**.)
2. Click **Add** to add a new collection.
3. On the Add Collection dialog, enter a name, location, and click **Save**.
4. From the **Collection Tasks** screen, click **Add** to add a task to the selected collection.
5. On the Sources dialog, select the Exchange source type you just created and click **Select**.

6. In the **Mailbox** tab under Filtering, select a target mailbox you want to test, then click **Save and Start**.

   For more information about adding collections and tasks, refer to the section *"Creating and Managing Collections" on page 101*.

Lync 2013 Setup

Starting with 8.0, Veritas eDiscovery Platform supports collection of Lync 2013 conversations that are archived on the Exchange server using the Exchange collector. The supported configuration includes integration of Lync Server 2013 on-premise and Exchange Server 2013 on-premise.

When Lync Archiving integration is enabled for a user, the archived data is stored in the Purges folder in the user's mailbox. The archived data is in the form of email messages with Lync items as its attachments. The Purges folder is hidden in a normal view.

Veritas eDiscovery Platform collects all data that is archived by Lync to the Exchange server, including:

- Peer-to-peer instant messages
- Conferencing messages, including uploaded content (for example, handouts) and event-related content (for example, joining, leaving, uploading sharing, and changes in visibility)
- Whiteboards and Polls shared during a conference

The following types of content are not archived to the Exchange server:

- Peer-to-peer file transfers
- Audio/video calls for peer-to-peer instant messages and conferences
- Desktop and application sharing for peer-to-peer instant messages and conferences
- Persistent chats

Contact your Exchange/Lync administrator for configuring the Lync Server 2013 setup.
For more details on the integration of Lync Server 2013 and Exchange Server 2013, see the Microsoft Lync documentation at *http://technet.microsoft.com/en-us/library/jj688098.aspx*.

- Prerequisites for Integrating Microsoft Lync Server 2013 and Microsoft Exchange Server 2013: *http://technet.microsoft.com/en-us/library/jj721919.aspx*
  - Assign server-to-server authentication certificates
  - Configure autodiscover service on Exchange server
  - Modify the Lync Server OAuth configuration settings
- Configuring Partner Applications in Microsoft Lync Server 2013 and Microsoft Exchange Server 2013: *http://technet.microsoft.com/en-us/library/jj688151.aspx*
  - Configuring a Partner Application for Lync Server and Exchange Server
  - Test the integration of Lync Server 2013 and Exchange 2013

- Configuring Microsoft Lync Server 2013 to Use Microsoft Exchange Server 2013 Archiving: *http://technet.microsoft.com/en-us/library/jj679896.aspx*
  - Enable Exchange archiving
  - Enable the archiving of internal and/or external communications
  - Configure the *ExchangeArchivingPolicy* property

Office® 365 Setup

Setting up your Office® 365 source for collection requires the following steps:

1. Make sure that the KB3114941 update for Microsoft Outlook 2013 32-Bit Edition is installed.
2. Assign full access permissions to a Source Account user for Office® 365 mailbox discovery and collection.
3. Perform Active Directory discovery.
4. Add the Source Account user into the local administrators group of the appliance.
5. System automatically configures the appliance's Outlook Template Profile.
6. Add the Office® 365 source to your data map.
7. Test an Exchange mailbox collection.

Note: For the purposes of this setup, the domain user account is referred to as "Source Account".

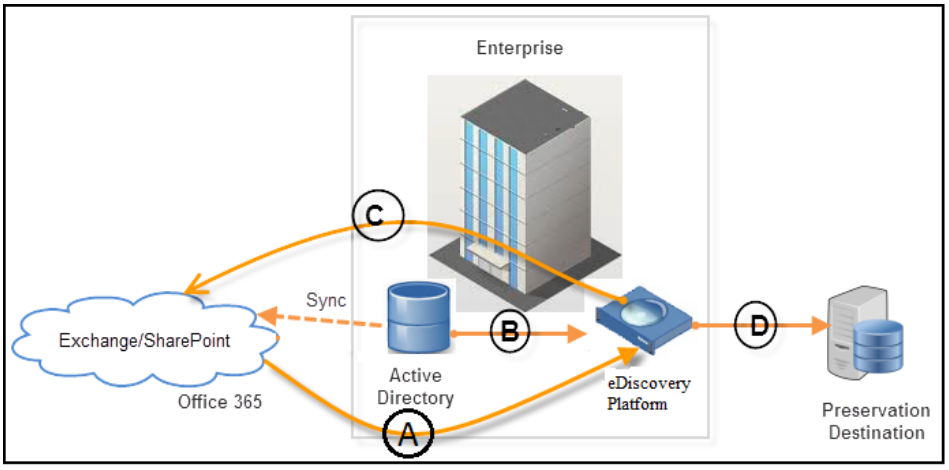
For an introduction, and sample diagram, see the *"Overview" in the next section*, then continue with the following steps:

- *"Step 1: Validate if Outlook is enabled for connection to Office® 365 using MAPI/HTTP" on page 63*
- *"Step 2: Set up Office® 365 Account Permissions" on page 64*
- *"Step 3: Perform Active Directory Discovery" on page 67*
- *"Step 4: Add the Source Account user from the Active Directory into the local administrator groups" on page 68*
- *"Step 5: System automatically configures the appliance's Template Profile" on page 69*
- *"Step 6: Add the Office® 365 Source to your Data Map" on page 69*
- *"Step 7: Test an Exchange Mailbox Collection" on page 70*

Overview

When adding your Exchange source, ensure that Exchange collections will run under the correct account. This is especially important if you are adding an Office® 365 source to your data map for Office® 365 collection within a cloud environment.

The following diagram illustrates the process for collection in an Office® 365 environment using Veritas eDiscovery Platform:



A. Veritas eDiscovery Platform collects data from Office® 365 mailboxes.

B. An on-premise Active Directory is used to get the user accounts and collect data from their mailboxes in Office® 365.

C. To collect from Office® 365 mailboxes, an Outlook profile on the appliance is configured to connect to Office® 365 (via MAPI)

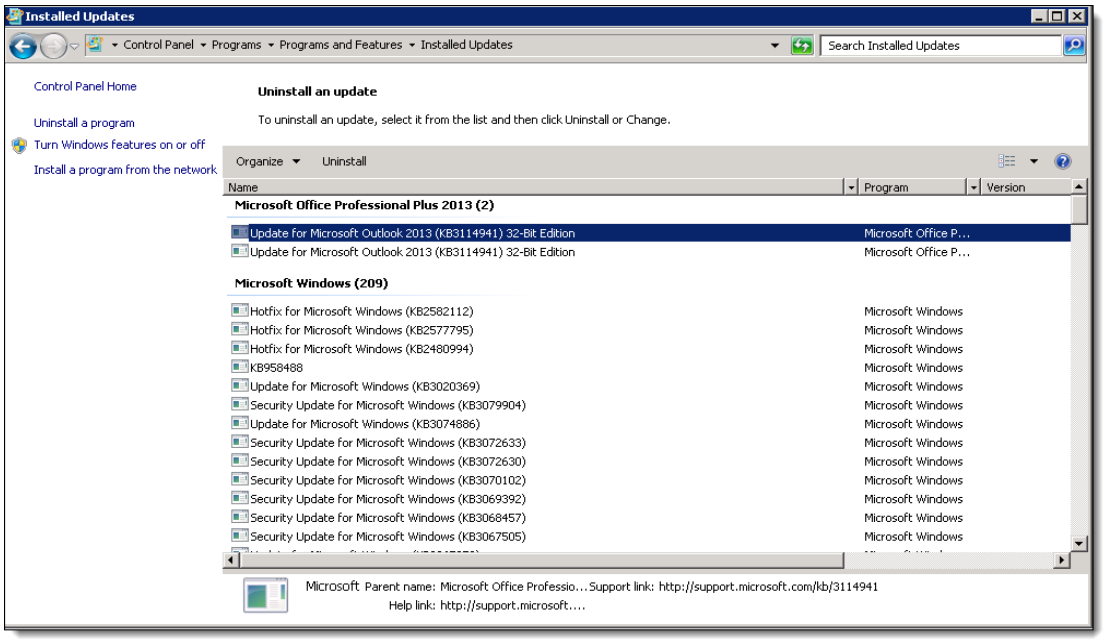
D. During Collections, the appliance connects to Office® 365 as an Outlook client would, copying messages in PSTs at the Preservation Destination

Note: For Office® 365 sources, a collection task can collect data from the main mailbox and its dumpster. Starting with 8.1.1, if the Office 365 mailbox has an archive mailbox, then the data from the archived mailbox and its dumpster will also be collected along with the data from the main mailbox and its dumpster.

Step 1: Validate if Outlook is enabled for connection to Office® 365 using MAPI/HTTP

Microsoft has deprecated support for RPC over HTTP. Accordingly, Veritas eDiscovery Platform requires Microsoft Outlook 2013 to use MAPI/HTTP to connect to Office® 365. When you install or upgrade to 9.0, the eDiscovery Platform installer installs the KB3114941 updates for Outlook 2013 32-Bit Edition that enables Office® 365 connection using MAPI/HTTP.

It is recommended to validate if the update (KB3114941) is installed before you start collection from Office® 365 mailboxes. To see the installed updates, go to **Control Panel** > **Programs and Features** > **View Installed Updates** > Search Installed Updates for KB3114941.



If you do not see the KB3114941 Outlook update installed, download it from https://www.microsoft.com/en-us/download/details.aspx?id=51720 and then manually install it.

Step 2: Set up Office® 365 Account Permissions

Collecting from mailboxes in the Office® 365 requires setting up a domain account with appropriate access permissions.

The "Source Account" should be:

- a Domain User for the enterprise domain
- added to the Local Administrator's group on the appliance
- able to access and collect the target Office® 365 mailboxes, as explained below

These requirements must be met in order to successfully collect mailboxes from Office® 365.

You can set up the Office® 365 permissions in two ways:

- Using the Office 365 Admin Portal

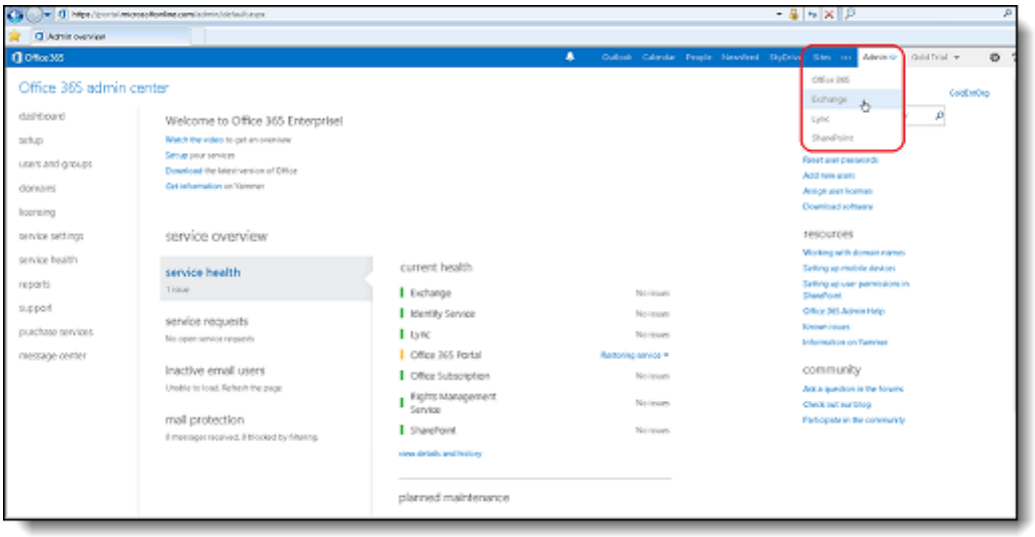
  See *"To assign full access permissions to a user on the mailboxes in Office® 365 to collect data in appliance:"*

- Using a PowerShell script

  See *"To assign full access permissions using PowerShell"*

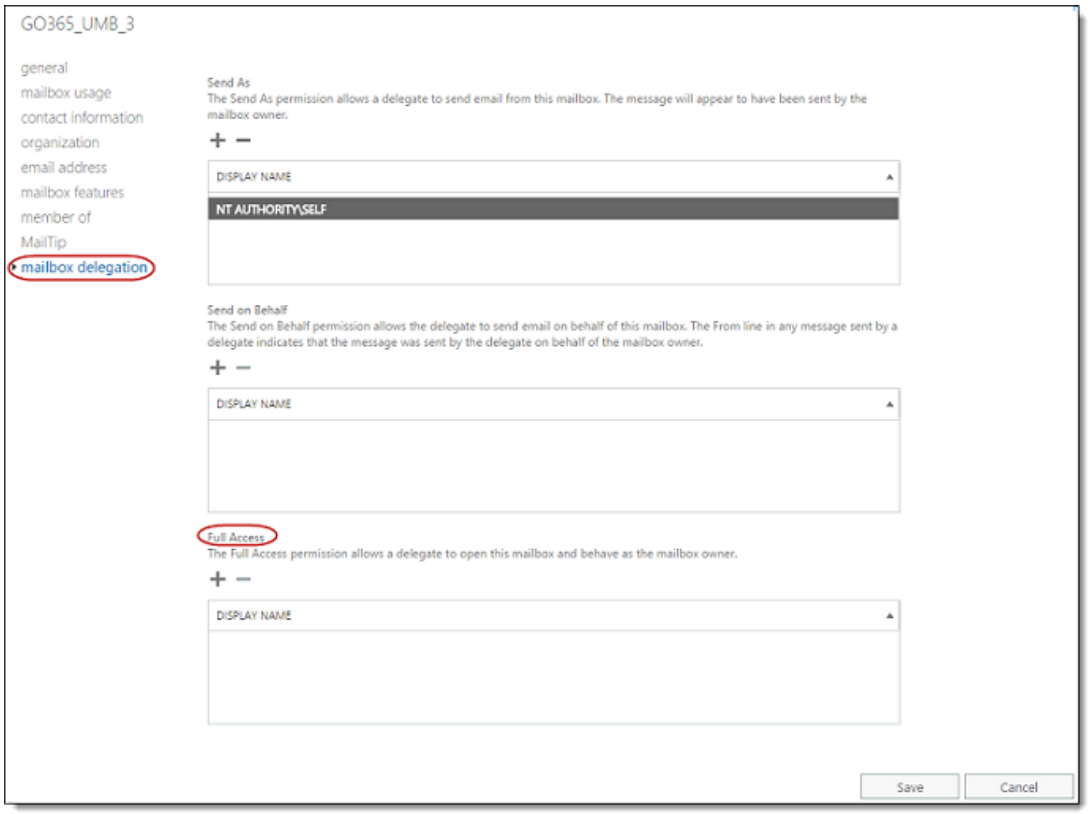
To assign full access permissions to a user on the mailboxes in Office® 365 to collect data in appliance:

1. Login to the Office 365 Admin Portal. The Office 365 admin center screen appears.



2. Select **Admin** > **Exchange**. The Exchange admin center screen appears.
3. Click the **mailboxes** tab. The list of user mailboxes is displayed.
4. Double-click on the name of the User mailbox from which you want to collect the data.

5. Click **general** and then click **mailbox delegation**. Users having full access are listed under the Full Access section.



6. Select the user mailbox to assign full access permissions to a new user, and then click the plus (**+)** sign under **Full Access** to add the source account.
7. Search the user mailbox and then click **add**.
8. Click **OK**.
9. Click **Save**.

To assign full access permissions using PowerShell

Using PowerShell commands, you can assign "Source Account" full mailbox access permissions to the target mailboxes. To be able to use PowerShell commands, you must be able to connect to the Office® 365 services using PowerShell.

To connect to Office® 365 services:

1. Import your Online Services module.
2. Enter Office® 365 credentials.
3. Create a remote session.

4. Import that session's commands into your local Windows PowerShell session.
5. Connect to Office® 365 services.

Those five commands to perform the above procedures look like this:

Import-Module MSOnline

$O365Cred = Get-Credential

$O365Session = New-PSSession –ConfigurationName Microsoft.Exchange -ConnectionUri

https://ps.outlook.com/powershell -Credential $O365Cred -Authentication Basic -AllowRedirection

Import-PSSession $O365Session

Connect-MsolService –Credential $O365Cred

If prompted for credentials, then provide your Office® 365 username and password.

You can assign the Source Account full mailbox access to individual mailboxes or many mailboxes. There are 2 possible avenues for provisioning the right level of access.

1a: Give "Source Account" Access to Individual Target Mailboxes

- Using Microsoft's Customer Mailbox Permission Management Tool (CMPMT), grant the "Source Account" full mailbox access to the target mailboxes.

  Note: This should be equivalent to the "Add-MailboxPermission" PowerShell command for on-premise Exchange servers.

  Example:

  Exchange Management Shell command completed:

  ```
  Add-MailboxPermission -Identity
  'CN=CUSTODIANUSER,CN=Users,DC=DOMAIN,DC=local' -User
  'DOMAIN\ADMINUSER' -AccessRights 'FullAccess'-InheritanceType all
  ```

  Troubleshooting Test: On the appliance, run Outlook (under the Source Account) and try to open the target custodian's mailbox. It should open the mailbox without a popup Logon dialog box.

- Repeat for each user mailbox from which you want to collect.

1b: Run a PowerShell Script to Automate Provisioning Many Mailboxes

- This is basically the same as Option 1 above, but repeats it for many mailboxes with a PowerShell script. Work with your Microsoft Technical Account Manager to implement this script, which should mirror the full mailbox access granted by Microsoft's CMPMT, or something equivalent to the syntax shown above (Exchange Management Shell command).
- Note that in a full deployment, this script should be scheduled periodically or should refresh when new employees are added, or when the "Source Account" requires access to a new batch of mailboxes.

Once you have granted "Source Account" permissions, you are now ready to perform Active Directory discovery and create Collection Tasks.

Step 3: Perform Active Directory Discovery

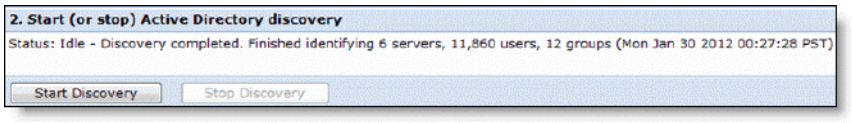
Once you have granted full access permissions to the Source Account, you are now ready to perform Active Directory discovery.

Given the domain(s), Veritas eDiscovery Platform will perform an Active Directory discovery for mailboxes. The credentials can be specified when adding a domain for discovery or editing the listed domain, if already discovered. If credentials are not specified, then it will default to ESA Application service credentials.

In addition to discovering mailboxes, Veritas eDiscovery Platform looks for specific patterns or attributes to determine if mailboxes reside in the Office® 365 environment.

To perform Active Directory discovery

1. In the Veritas eDiscovery Platform interface, on the top navigation bar, click **System > Directories and Servers**, and select the **Active Directory** tab.
2. To add a new domain, click **Add Domain** then enter the domain name, and the administrator user name and password, and click **Save**.
3. When ready, click **Start Discovery**. This automatically detects the appropriate domain, and performs Active Directory discovery.



   Note: This function checks for domains which contain the appliance. Once the domain is detected, Veritas eDiscovery Platform uses the user account specified for the added domain or the ESA service account (if user account is not specified) to discover mailboxes, and groups from Active Directory. Typically, this should automatically discover the same Active Directory domain used by Office® 365.

   Troubleshooting: In rare cases, the desired domain may not be automatically discovered, for example, if the enterprise has legacy domains that may have been consolidated or deleted. In this case, you can manually enter your enterprise domain and account credentials by clicking **Add Domain** on the **System > Directories and Servers** screen. On the Add Domain dialog, you can also enter the fully-qualified domain name (the name given to your enterprise by Office® 365).

4. When the Active Directory discovery is complete, the **System > Directories and Servers** screen displays servers, users, and groups that have been discovered.

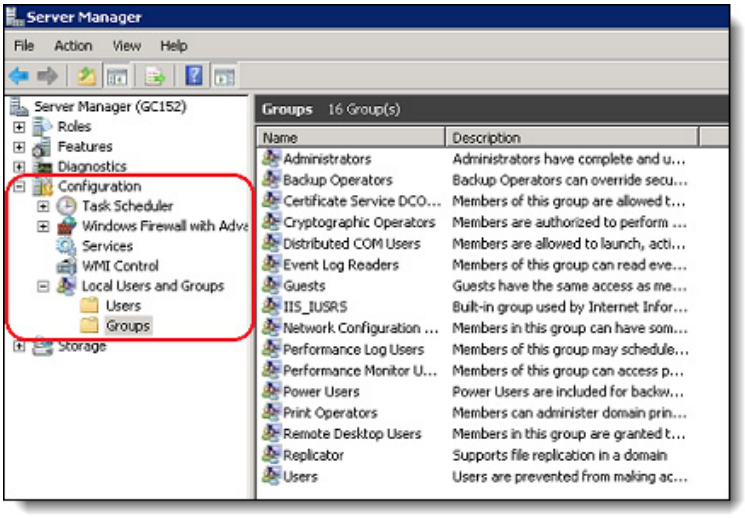
For details on discovery, customizing employee information, synchronizing with the Active Directory, or importing custodians, see *"Data Discovery Overview" on page 34*, *"Mapping Employee Attributes" on page 35*, and *"Importing Custodians to Your Data Map" on page 36*.

Step 4: Add the Source Account user from the Active Directory into the local administrator groups

The source account must have administrative privileges on the Veritas eDiscovery Platform appliance machine.

To add:

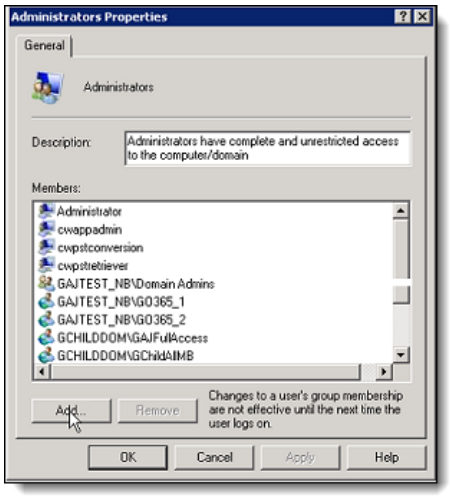
1. Click **Start**, point to **Administrative Tools**, and then click **Server Manager** (Windows Server 2008) or **Computer Management** (Windows Server 2012).



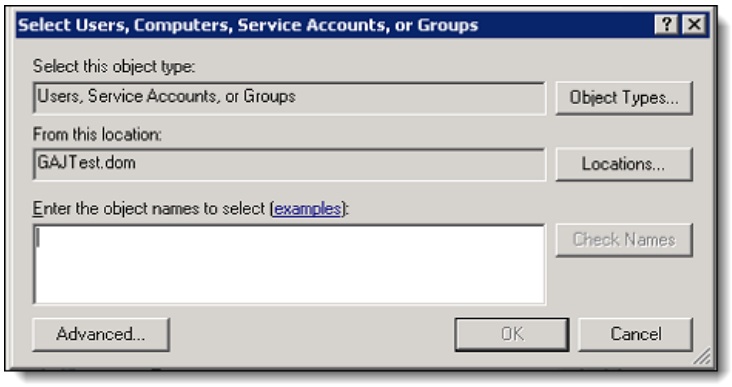
2. (Windows Server 2008) Under **Configuration**, click **Local Users and Groups**. (Windows Server 2012) Under **System Tools**, click **Local Users and Groups**.

3. Click **Users**.

4. Double-click **Administrators**. The **Administrators Properties** dialog appears.



5. Click **Add**. The **Select Users, Computers, Service Accounts, or Groups** dialog appears.



6. Enter the source account name in the **Enter the object names to select** field, and then click **Check Names**. Click **OK**.

7. Click **Apply**, and then click **OK**. The Source Account is added to the local administrators group. Now you are ready to login to the appliance.

Step 5: System automatically configures the appliance's Template Profile

The system needs to have the Microsoft Outlook profile for the Source Account configured on the appliance. An Outlook/MAPI connection to a mailbox requires various configurations in the Outlook profile.

An Outlook template profile is automatically created with a profile name as "**eDP-O365-MapiHttp-TemplateProfile-Do not Delete**". You do not need to manually create the Outlook profile while configuring the O365 setup as it was needed in earlier releases. If your collection task fails, see the troubleshooting section: *"Troubleshooting Office® 365 collections" on page 210*.

Step 6: Add the Office® 365 Source to your Data Map

To add the Office® 365 Source Account to your data map

1. In the All Collections module, click **Source Accounts**.

2. Click **Add**.

3. Enter the name of the Source Account of the Office® 365 mailbox in the **Account** field.

4. Enter the username in the **User** field.

5. Enter the password in the **Password** field and then reenter the same password in the **Confirm Password** field.

6. Click **Save**.

To add Office® 365 source to your data map

1. In the **All Collections** module, click **Sources**.

2. On the Sources screen, click **Add**.

3. Specify the following information. An asterisk (*) indicates a required field.

Source Data

Field	Description
*Source Name	Enter a name for your Office® 365 source.
Description	Enter a description of the source (up to 255 characters).
*Type	Select Exchange as the source type.
Account	Enter the name of the source account you created, or click **Browse** to select one from the list of accounts. Enter the "Source Account" you set up in *"Step 2: Set up Office® 365 Account Permissions" on page 64*. If you leave the **Account** field blank, Exchange collections will run using the *ESAApplicationService* account permissions.
Custodian Group	Type the name of the custodian or group associated with the data source (Example: John R. Smith), or click **Browse** to select one from the list of custodians/groups.
Access Groups	By default, all groups to which the user has access are listed in the **Included** column which results in the source being added to all groups. Keep only those groups in the **Included** column in which you want to add the source and move all the remaining groups to the **Available** column. If the source is not added to any group, then that source will be available to all users.
Collection Templates and Collection History	Indicates whether a template has been applied to the collection. (Click link to edit collection templates.) View list of collections and task details.

4. When finished, click **Save**.

   Note: Before you perform collection tasks for the Office® 365 mailboxes, you should ensure that the mailboxes are discovered within the appliance. To do this, go to **System** > **Directories and Servers** > **Email Servers** > **BPOS** > **Mailboxes**, and then see if the mailbox is present.

Step 7: Test an Exchange Mailbox Collection

To test the collection of a mailbox

1. In the **All Cases** view, under **All Collections**, click **Collections**.
2. Click **Add** to add a new collection.
3. On the Add Collection dialog, enter a name, location, and click **Save**.
4. On the **Collection Tasks** screen for this collection, click **Add** to add a task to the selected collection.
5. On the **Sources s**creen, select the Office® 365 source you just created, and click **Select**.
6. In the **Mailbox** tab under **Filtering**, select a target mailbox you want to test, then click **Save and Start**.

For more information about adding collections and tasks, refer to the section *"Creating and Managing Collections" on page 101*.

BPOS Exchange Setup

Setting up your Microsoft® Business Productivity Online Suite (BPOS) Exchange source for collection requires the following steps:

1. Create an Admin Account* for BPOS Exchange mailbox discovery and collection.
2. Discover mailboxes using Active Directory Discovery and import custodians.
3. Configure the appliance's Outlook Template Profile.
4. Add the BPOS Exchange source to your data map.
5. Test an Exchange mailbox collection.

   Note: For the purposes of this setup, the domain user account is referred to as "Admin Account".

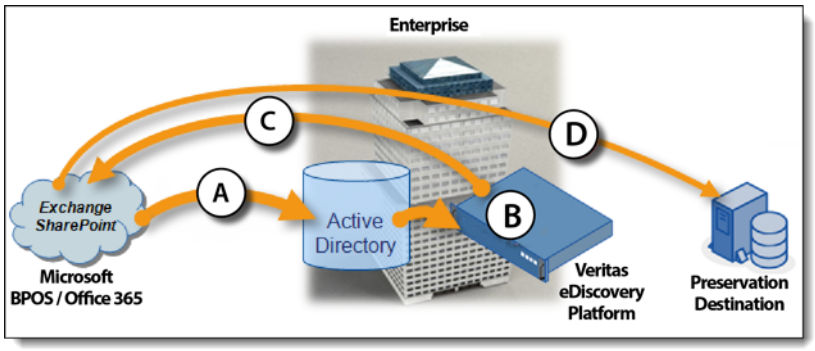
For an introduction, and sample diagram, see the *"Overview" in the next section*, then continue with the following steps:

- *"Step 1: Create a New Admin Account (for BPOS)" on page 73*
- *"Step 2: Perform Active Directory Discovery and Import Custodians (for BPOS)" on page 74*
- *"Step 3: Configure the appliance's Outlook Template Profile" on page 75*
- *"Step 4: Add the Exchange BPOS Source to your Data Map" on page 80*
- *"Step 5: Test an Exchange Mailbox Collection" on page 81*

Overview

When adding your Exchange source, ensure that Exchange collections will run under the correct account. This is especially important if you are adding a BPOS Exchange source (hereafter, "BPOS Exchange", "BPOS", or "Exchange") to your data map for BPOS Exchange collection within a cloud environment.

The following diagram illustrates the process for collection in a BPOS Exchange environment using Veritas eDiscovery Platform:



A. Your Active Directory could be hosted directly by BPOS, or a one-way trust established between BPOS and the Enterprise domain, syncing Active Directory

B. Veritas eDiscovery Platform collection Admin account given account privileges to open custodian mailboxes in BPOS, using Microsoft's Customer Mailbox Permission Management Tool (CMPMT)

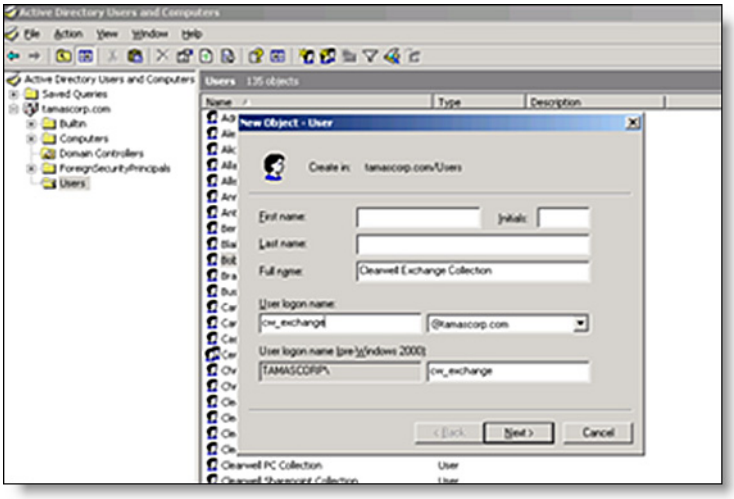
C. To collect from BPOS mailboxes, an Outlook profile on the appliance is configured to connect to BPOS (via MAPI)

D. During Collections, the appliance connects to BPOS as an Outlook client would, copying messages in PSTs at the Preservation Destination

Step 1: Create a New Admin Account (for BPOS)

To create a new domain account

1. In your Windows interface, open **All Programs** [or for newer versions: **Control Panel**] > **Administrative Tools > Active Directory Users and Computers**.
2. Click to expand the domain, then right-click **Users** and select **New > User**.
3. Enter the name and logon information for the Veritas eDiscovery Platform Exchange Collection admin.



4. Click **Next**.
5. Enter a Password and select (only) the option **Password Never Expires**, then click **Next**.
6. Clear the option to create an Exchange mailbox. (An Exchange mailbox is not required), then click **Finish** to create the admin account.

   Continue with next steps to set up your admin account permissions, depending on your mailbox setup.

Set up BPOS Exchange Account Permissions

Collecting from mailboxes in a BPOS Exchange server requires setting up a domain account with appropriate Exchange security permissions.

The "Admin Account" should be:

- a Domain User for the enterprise domain
- a Local Administrator on the appliance
- able to access and collect the target BPOS mailboxes

These requirements must be met in order to successfully collect mailboxes from Exchange BPOS. For the last requirement (This Account must be able to access and collect the target BPOS mailboxes), there are two possible avenues for provisioning the right level of access.

1a: Give "Admin Account" Access to Individual Target Mailboxes

- Using Microsoft's Customer Mailbox Permission Management Tool (CMPMT), grant the "Admin Account" full mailbox access to the target mailboxes.

  Technical Note: This should be equivalent to the "Add-MailboxPermission" PowerShell command for on-premise Exchange servers.

  Example:

  Exchange Management Shell command completed:

```
Add-MailboxPermission -Identity
'CN=CUSTODIANUSER,CN=Users,DC=DOMAIN,DC=local' -User
'DOMAIN\ADMINUSER' -AccessRights 'FullAccess'-InheritanceType all
```

  Troubleshooting Test: On the appliance, run Outlook (under the Admin Account) and try to open the target custodian's mailbox. It should open the mailbox without a popup Logon dialog box.

- Repeat for each user mailbox from which you want to collect.

1b: Run a PowerShell Script to Automate Provisioning Many Mailboxes

- This is basically the same as Option 1 above, but repeats it for many mailboxes with a PowerShell script. Work with your Microsoft Technical Account Manager to implement this script, which should mirror the full mailbox access granted by Microsoft's CMPMT, or something equivalent to the syntax shown above (Exchange Management Shell command).
- Note that in a full deployment, this script should be scheduled periodically or should refresh when new employees are added, or when the "Admin Account" requires access to a new batch of mailboxes.

Once you have granted "Admin Account" permissions, you are now ready to perform Active Directory discovery and create Collection Tasks.

Step 2: Perform Active Directory Discovery and Import Custodians (for BPOS)

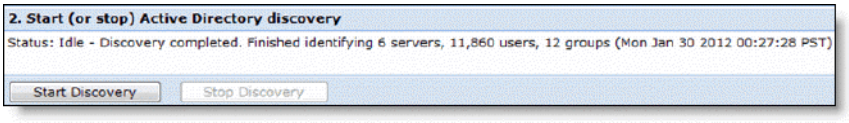
Given the domain(s), Veritas eDiscovery Platform will perform an Active Directory discovery for mailboxes and groups. The admin can provide credentials that this discovery will perform as, or Veritas eDiscovery Platform will default to using its Application Service credentials.

In addition to discovering mailboxes, Veritas eDiscovery Platform looks for specific patterns or attributes to determine if mailboxes reside in the BPOS Exchange environment.

Once Active Directory completes, you can import custodian data.

To perform Active Directory discovery

1. Log on to the appliance using "Admin Account" (the Domain user).
2. In the Veritas eDiscovery Platform interface, on the top navigation bar, click **System > Directories and Servers**, and select the **Active Directory** tab.
3. To add a new domain, click **Add Domain** then enter the domain name, and the administrator user name and password, and click **Save**.
4. When ready, click **Start Discovery**. This automatically detects the appropriate domain, and performs Active Directory discovery.



Note: This function checks for domains which contain the appliance. Once the domain is detected, Veritas eDiscovery Platform used the logged in account ("Admin Account") to discover mailboxes, and groups from Active Directory. Typically, this should automatically discover the same Active Directory domain used by BPOS Exchange.

Troubleshooting: In rare cases, the desired domain may not be automatically discovered, for example, if the enterprise has legacy domains that may have been consolidated or deleted. In this case, you can manually enter your enterprise domain and account credentials by clicking **Add Domain** on the **System > Directories and Servers** screen. On the Add Domain dialog, you can also enter the fully-qualified domain name (the name given to your enterprise by Microsoft BPOS).

5. When the Active Directory discovery is complete, the **System > Directories and Servers** screen displays servers, users, and groups that have been discovered.

For details on discovery, customizing employee information, synchronizing with the Active Directory, or importing custodians, see *"Data Discovery Overview" on page 34*, *"Mapping Employee Attributes" on page 35*, and *"Importing Custodians to Your Data Map" on page 36*.

Step 3: Configure the appliance's Outlook Template Profile

After Active Discovery of mailboxes and importing custodians to your BPOS environment, the appliance's Outlook template profile must be configured. The BPOS environment runs Exchange 2010. An Outlook/MAPI connection to a mailbox requires various configurations in the Outlook profile. System Administrators can collect profile parameter values from an existing Outlook profile connected to a BPOS mailbox. Key parameters include BPOS Exchange CAS Array (Client Access Server), and MAPI over HTTPS proxy server and filter.

Note: The profile name is based on the Outlook version (OL2013). The profile name should be **BPOSExchangeTemplateProfile-OL2013-Do not Delete**.

Note: Release 8.1 and later only support Microsoft Office 2013. In previous release of eDiscovery Platform, the BPOS sources were configured to use the appliance's Outlook Profile name as **BPOSExchangeTemplateProfile-OL2010-Do not Delete**. After you upgrade to 8.1, you must edit the Outlook Profile name to **BPOSExchangeTemplateProfile-OL2013-Do not Delete**.

The following steps use an Outlook 2003 installation scenario, however you can use this as a guideline even if you have Outlook 2013 installed.

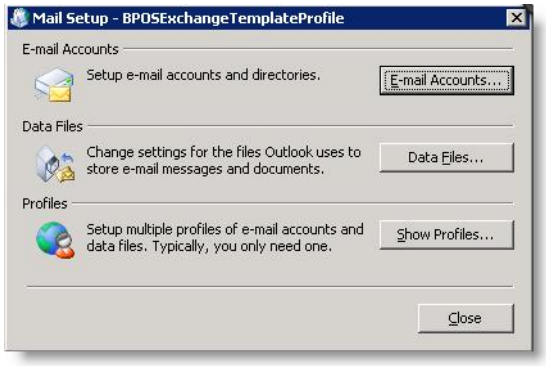
Veritas eDiscovery Platform requires one template profile to be configured, which is used in all Exchange collection jobs to connect to mailboxes in the BPOS environment. In the appliance, a profile called **BPOSExchangeTemplateProfile-OL2013-Do not Delete** is pre-installed. An IT Administrator must configure this profile using the following steps.

To configure the Outlook template profile

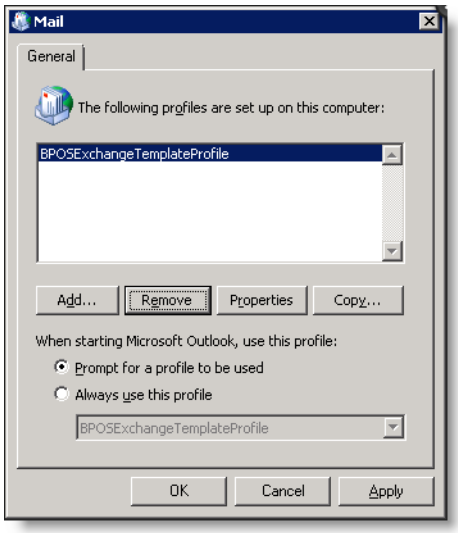
1. Log on to the box as the Exchange source account (Domain\CWAdmin). If any jobs are running, these steps should be done when jobs are completed and all Veritas eDiscovery Platform services that require MAPI are stopped (*PSTCrawler* and *PSTRetriever*). When a MAPI process is running, profile databases are locked and cannot be configured.

2. Launch **D:\CW\<ver>bin\configureBPOSMapiProfile.bat**

   The Mailbox Setup - BPOSExchangeTemplateProfile dialog appears.



3. Select **Show Profiles**. The Mail dialog appears.

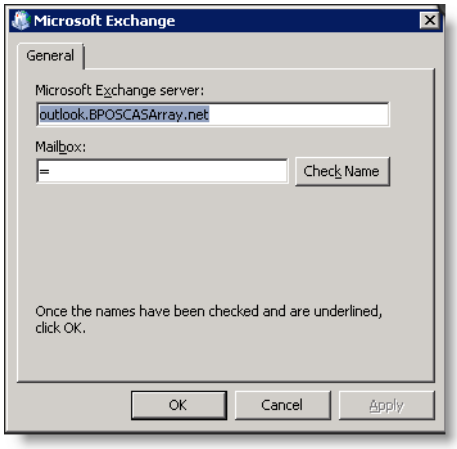


4. Select **BPOSExchangeTemplateProfile-OL2013-Do not Delete**, and select **Properties** and click **Email Accounts**. On the warning dialog, click **OK**.

   Note: If the **BPOSExchangeTemplateProfile-OL2013-Do not Delete** profile is not present, click **Add** and create the profile name.

   On the warning dialog, click **OK**.

5. The Microsoft Exchange dialog (displaying the **General** tab) appears.

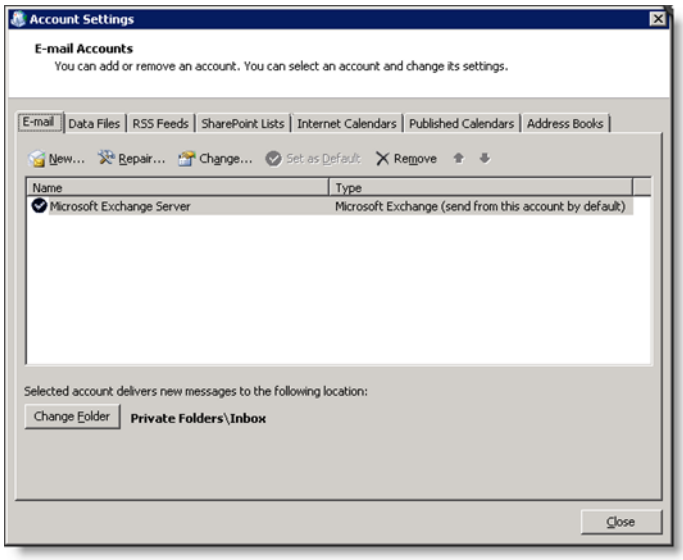


Do not change any fields.

CAUTION: Never select Check Name. If you clicked **Check Name** unintentionally, then be sure to remove the **BPOSExchangeTemplateProfile-OL2013-Do not Delete** profile and add a profile with same name.

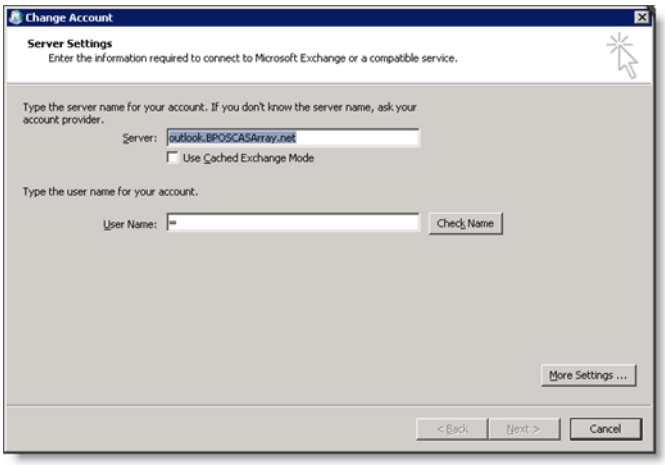
Click **Cancel**.

The Account Settings dialog appears.



6. On the **E-mail** tab, select the **Microsoft Exchange Server** and click **Change**.

   The Change Account dialog appears.



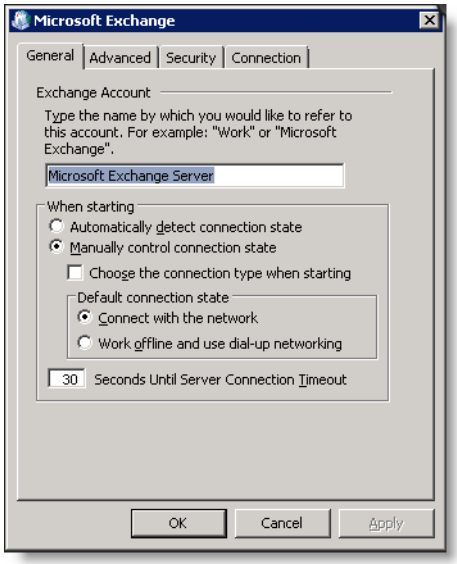
7. In the **Server** field, enter the fully-qualified domain name of the BPOS CAS array.

   CAUTION: Do not select Use Cached Exchange Mode. Also do not change the User Name; leave the User Name as "=".

   Click **More Settings**.

   CAUTION: Never select Check Name. If you clicked **Check Name** unintentionally, then be sure to remove the **BPOSExchangeTemplateProfile-OL2013-Do not Delete** profile and add a profile with the same name.

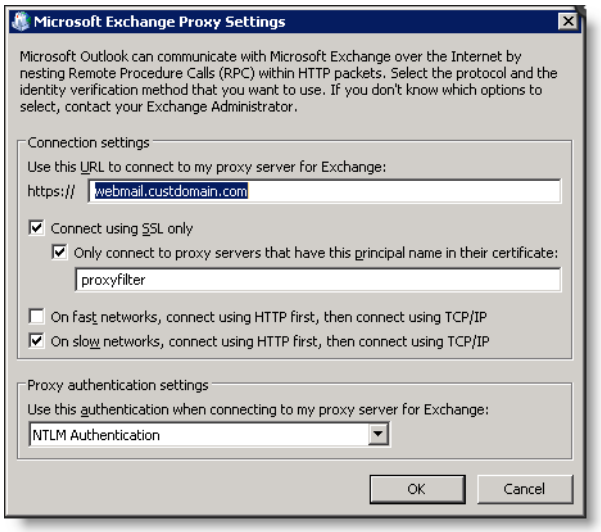
   The Microsoft Exchange dialog appears.



8. Under the **General** tab, select the option to **Manually control connection state when starting**, then click **Apply**.

9. Click the **Security** tab, and select the option to **Encrypt data between Microsoft Outlook and Microsoft Exchange**, then click **Apply**.
10. Click the **Connection** tab, and click **Exchange Proxy Settings...**

    The Microsoft Exchange Proxy Settings dialog appears.



11. Enter your company-specific proxy server and filter settings, then click **OK**.
12. Confirm your changes by clicking **OK** or **Next** to all subsequent dialogs.

    On the "Outlook could not connect" warning dialog, click **OK**.

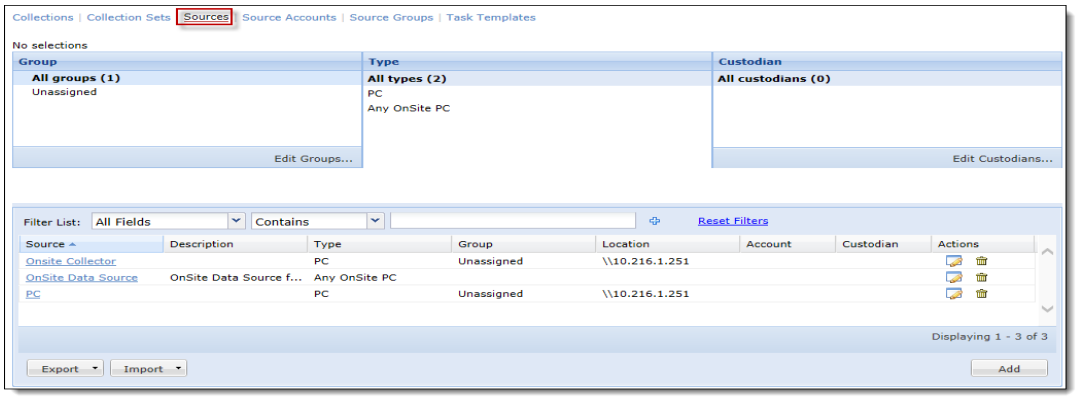
    Click **Cancel** on the Microsoft Exchange dialog (showing the Server Name and Mailbox user. Remember, never click **Check Name**).
13. Click **Finish** on the "Congratulations" dialog and click **Close** to subsequent dialogs and finish configuring the profile.
14. Run the **D:\CW\<ver>\bin\saveBPOSMapiProfile.bat** to save the configured BPOS profile name. This saves the template profile as a registry file in the directory: **D:\cw\<ver>\config\templates\msexchange**

    If you encounter any issues, see *"Troubleshooting Office® 365 collections" on page 210* in the Troubleshooting section.

Step 4: Add the Exchange BPOS Source to your Data Map

To add Exchange BPOS to your data map

1. In the **All Collections** module, click **Sources**.



2. On the Sources screen, click **Add**.

3. Specify the following information. An asterisk (*) indicates a required field.

Source Data

Field	Description
*Source Name	Enter a name for your BPOS Exchange source.
Description	Enter a description of the source (up to 255 characters).
*Type	Select Exchange as the source type.
Account	Enter the "Admin Account" you set up in *"Step 1: Create a New Admin Account (for BPOS)" on page 73*. If you leave the **Account** field blank, Exchange collections will run using the *ESAApplicationService* account permissions.
Custodian	Type the name of the custodian or group associated with the data source (Example: John R. Smith), or click **Browse** to select one from the list of custodians/groups.
Group	
Access Groups	By default, all groups to which the user has access are listed in the **Included** column which results in the source being added to all groups. Keep only those groups in the **Included** column in which you want to add the source and move all the remaining groups to the **Available** column. If the source is not added to any group, then that source will be available to all users.
Collection Templates and Collection History	Indicates whether a template has been applied to the collection. (Click link to edit collection templates.) View list of collections and task details.

4. When finished, click **Save**.

Step 5: Test an Exchange Mailbox Collection

To test the collection of a mailbox

1. In the **All Cases** view, under **All Collections**, click **Sources**.
2. On the **Sources** screen, click **Add** to add a new collection.
3. On the Add Collection dialog, enter a name, location, and click **Save**.
4. On the **Collection Tasks** screen for this collection, click **Add** to add a task to the selected collection.
5. On the Sources screen, select the Exchange BPOS you just created, and click **Select**.
6. In the **Mailbox** tab under Filtering, select a target mailbox you want to test, then click **Save and Start**.

For more information about adding collections and tasks, refer to the section *"Creating and Managing Collections" on page 101*.

Lotus Domino® Server Setup

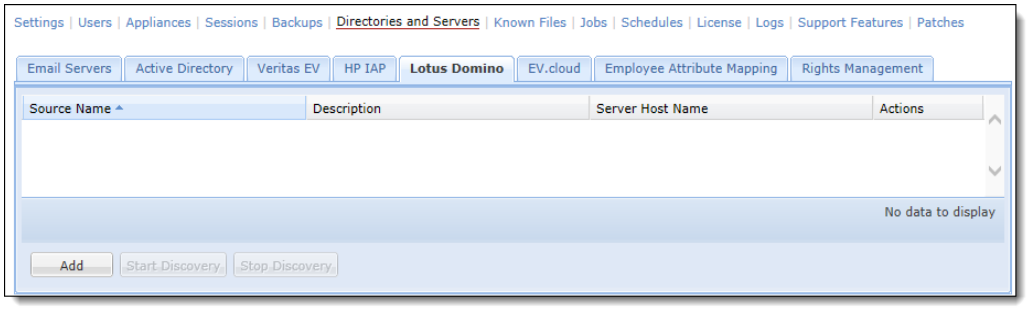
Follow the steps below to set up your Lotus Domino Server as a source for collection:

- *"Step 1: Perform Domino Server Discovery" in the next section*
- *"Step 2: Add the Domino Source" on page 83*

Step 1: Perform Domino Server Discovery

To perform discovery on the Domino server

1. Log on to the appliance using "Admin Account" (the Domain user).
2. In the **All Cases** view, click **System > Directories and Servers**.
3. Click the **Lotus Domino** tab.



4. To add a Lotus Domino server, click **Add** then enter names for the Source and Server Host, ID File, and Password, and click **Save**.
5. When ready, click **Start Discovery**. This automatically detects the appropriate domain, and performs discovery on the Domino server.

   Note: This function checks for domains which contain the appliance. Once the domain is detected, the system uses the logged in account ("Admin Account") to discover servers, mailboxes, and groups from the Domino server.

   Troubleshooting: In rare cases, the desired domain may not be automatically discovered. For example, if the enterprise has legacy domains that may have been consolidated or deleted. In this case, you can manually enter your enterprise domain and account credentials by clicking **Add Domain** on the **System > Directories and Servers** screen.
6. When discovery is complete, the **System > Directories and Servers** screen displays servers, users, and groups that have been discovered.
7. Continue with next steps to add the Domino source to your data map.

Step 2: Add the Domino Source

To add the Domino server as a source

1. In the **All Collections** module, click **Sources**.
2. On the Sources screen, click **Add**.

   Note: A warning message appears at the top of the screen if discovery on the Lotus Domino source was not performed first.

3. Specify the following information. An asterisk (*) indicates a required field.

Source Data

Field	Description
*Source Name	Enter a name for your Domino source.
Description	Enter a description of the source (up to 255 characters).
*Type	Select Domino as the source type.
Account	Enter the "Admin Account" (the Domain user).
Custodian	Type the name of the custodian or group associated with the data source (Example: John R. Smith), or click **Browse** to select one from the list of custodians/groups.
Group	
Access Groups	By default, all groups to which the user has access are listed in the **Included** column which results in the source being added to all groups. Keep only those groups in the **Included** column in which you want to add the source and move all the remaining groups to the **Available** column. If the source is not added to any group, then that source will be available to all users.
Collection Templates and Collection History	Indicates whether a template has been applied to the collection. (Click link to edit collection templates.) View list of collections and task details.

4. When finished, click **Save**.

SharePoint Source Setup

Veritas eDiscovery Platform supports collection from a SharePoint source through a proxy. Whether you are using a conventional SharePoint source, or SharePoint via Proxy, follow the steps in this section to add SharePoint and set up your connection accordingly.

Add the SharePoint Source

To add SharePoint as a source

1. In the **All Collections** module, click **Sources**.
2. On the Sources screen, click **Add**.
3. Specify the following information. An asterisk (*) indicates a required field.

Source Data

Field	Description
*Source Name	Type the name of your data source (up to 35 characters).
Description	Enter a description of the source (up to 255 characters).
*Type	Select SharePoint as the source type.
Account	For the Account, enter a source user that is member of a group having the Design permission level. **Note:** If the source user belongs to a group having a “Full Control” permission level, user profiles will also get collected. Therefore, to imply stricter security compliance, it is recommended that the source user should belong to a group having the "Design" permission level rather than the "Full Control" permission level.
*Location	Enter the location (URL) to the SharePoint site. **Note:** The SharePoint URL must be in a domain name format. The URL must not be in a numeric IP address format. Be sure to enter the full location path, and that the SharePoint source is visible to the appliance. After entering the Location and Account, you can click Test to check the connection. Verify the correct location convention with your System Administrator. Click **Test** to validate the source location as entered.
Collect through a proxy	(For SharePoint source): To collect from a SharePoint source through a proxy, select the **Collect through a proxy** check box. Enter the name of the source account you created, or click **Browse** to select one from the list of accounts. Enter the Server DNS Name and the Port number. **Note:** Authenticated proxy login is not supported. A collection task fails when authenticated proxy login is used.
Max Data Transfer Rate	(For SharePoint source): Enter the maximum data transfer rate in Mbps.
Access Groups	By default, all groups to which the user has access are listed in the **Included** column which results in the source being added to all groups. Keep only those groups in the **Included** column in which you want to add the source and move all the remaining groups to the **Available** column. If the source is not added to any group, then that source will be available to all users.

Source Data (Continued)

Field	Description
Custodian Group	Type the name of the custodian or group associated with the data source (Example: John R. Smith), or click **Browse** to select one from the list of custodians/groups.
Collection Templates and Collection History	Indicates whether a template has been applied to the collection. (Click link to edit collection templates.) View list of collections and task details.

4. Click **Save**.

Username and Password Conventions

When you enter in proxy information and a username/password, standard characters and symbols are allowed, including the "@" character within the password-either at the beginning or at the end of the password.

File Share and Windows PC Setup

Follow the steps below to add Fileshare or PC source to your data map in preparation for collections. If you encounter any issues, see *"Troubleshooting File Server or PC collections" on page 207*.

Add File Share (or PC) Source

To add File Share as a source

1. In the **All Collections** module, click **Sources**.
2. On the Sources screen, select the **File Share** (or **PC**) source type, then click **Add**.
3. Specify the following information. An asterisk (*) indicates a required field.

Source Data

Field	Description
*Source Name	Enter a name for your File Share or PC source.
Description	Enter a description of the source (up to 255 characters).
*Type	Select File Share as the source type.
Account	Enter a source user that has at least read permissions to this location. Alternatively, click **Browse** to select this user.
Location (\\server\share)	Enter the location of the data source. **Note:** For File Share source, be sure to enter the full location path, and that the File Share source is visible and accessible to the appliance. After entering the Location and Account, you can click Test to check the connection.
Access Groups	By default, all groups to which the user has access are listed in the **Included** column which results in the source being added to all groups. Keep only those groups in the **Included** column in which you want to add the source and move all the remaining groups to the **Available** column. If the source is not added to any group, then that source will be available to all users.
Custodian	Type the name of the custodian or group associated with the data source (Example: John R. Smith), or click **Browse** to select one from the list of custodians/groups.
Group	
Collection Templates and Collection History	Indicates whether a template has been applied to the collection. (Click link to edit collection templates.) View list of collections and task details.

4. When finished, click **Save**.

Veritas Enterprise Vault

Veritas eDiscovery Platform integrates with Veritas Enterprise Vault as a data collection source. Veritas eDiscovery Platform certifies Enterprise Vault API Runtime versions 10.0.4, 11.0, 11.0.1, and 12.x. From an Enterprise Vault source, you can collect data from Exchange Mailbox and Journal archives, SharePoint archives, Lotus Domino Journal and Mailbox archives, and File System archives. When Enterprise Vault 11.0.1 or later is used, you can also collect data from Exchange SMTP and Internet Mail archives.

Enterprise Vault 11.0.1 and later supports both IMAP and SMTP archiving. Exchange journal and User mailbox archives might contain messages in both MSG and EML formats. Veritas eDiscovery Platform 8.1.1 and later supports collection of both MSG and EML files from Enterprise Vault 11.0.1 and later for SMTP and IMAP archives.

IMPORTANT: The Enterprise Vault API Runtime client must be compatible with the Enterprise Vault server version. Also, ensure that your appliance is in the same domain as the Enterprise Vault Directory server.

Review these topics prior to setup, then follow the steps:

- *"Enterprise Vault Source Considerations Before Setup" in the next section*
- *"About Enterprise Vault Discovery" on page 89*
- *"Step 1: Perform Enterprise Vault Discovery/Vault Administration" on page 89*
- *"Step 2: Add Enterprise Vault Sources" on page 93*
- *"Step 3: Update your License" on page 94*

Enterprise Vault Source Considerations Before Setup

Before setting up an Enterprise Vault source, System Administrators should consider the following:

1. *If your organization is using Lotus Domino, will journaling be enabled?*

   What Is Domino Server Journaling?

   Domino Server journaling lets you record copies of email communications in your organization and store, or journal, them in a Mail Journaling database. The process of journaling is different from archiving. Journaling is simply a means of retaining copies of your user's messages.

2. *If your environment is using Microsoft Exchange, will Envelope Journaling be enabled? If not, is there another mechanism in place for capturing undisclosed recipients (BCC information) from journalized email messages?*

   What Is Exchange Journaling?

   Exchange Journaling is the ability to record all communications in an organization. Email communications are one of many different communication mechanisms that you may be required to journal. Therefore, journaling in Exchange has been developed to enable the Messaging Administrator to feed messaging data into a larger journaling solution, while using minimum overhead.

Envelope journaling provides a much more useful service because it records data about all recipients that a message is delivered to. One way to understand how envelope journaling works is in the context of distribution groups. Most distribution lists change, and query-based distribution lists are specifically created based on the fact that lists change. This is important to understand prior as this will affect whether or not the information in the BCC field is available for searching via the "To" searching option. Depending on how Exchange is configured, Enterprise Vault may not process the undisclosed recipients resulting in incomplete or inaccurate search results.

Veritas eDiscovery Platform provides the ability to collect fully-expanded "Bcc" and distribution list information in an "envelope" format that also contains the original Enterprise Vault Journal message.

This feature only applies to new collection tasks, and only applies to Exchange Journal email messages. Domino Journal Envelope email messages are not processed by this feature.

For details on processing Journal envelope information, refer to the Case Administration Guide.

3. *Is your organization archiving data other than email such as File Servers, SharePoint Servers, Structured Databases, or Instant Messages?*

   If the Enterprise Vault environment includes archives with non-email content and you plan to search based on content-type, then you will need to have an understanding of what information is available in your vault. If you have legacy data that was archived in version 4.1 or earlier, then this option will not be available (added in version 5.0).

   Note: You can add sources and collect from File share Archives, SharePoint Archives and Shared Archives. If you are upgrading to Veritas eDiscovery Platform, you must re-discover your Enterprise Vault server for collection from these source types.

4. *What level of indexing has the Enterprise Vault system been configured to use?*

   The level of indexing configured will determine what search capability will be available in Veritas Enterprise Vault Collector.

Enterprise Vault Index Levels

Index Level	Description
Brief	Allows searching of the metadata associated with the Author, Recipients, Subject, Date Range.
Medium	Allows searching of the metadata associated with the Author, Recipients, Subject, Date Range, as well as key word searching of the content contained in the message body and the attachments.
Full	Allows searching of the metadata associated with the Author, Recipients, Subject, Date Range as well as key word and phrase searching of the content contained in the message body and the attachments.

5. *Are there multiple Vault Sites in the Enterprise Vault environment?*

   Veritas Enterprise Vault Collector has the capability to run federated searches across all sites, however, the searches are specific to the Vault Site. If searches must be run across multiple sites, different Collection Sources must be created for each site, allowing collection tasks to be created and run for each of the sites.

About Enterprise Vault Discovery

Veritas eDiscovery Platform must first discover all Enterprise Vault related sources to be used for collection, including Enterprise Vault servers, sites, vaults, and archive directories. By selecting Veritas Enterprise Vault as the archive source to be discovered, administrators can perform a new discovery, or add to an existing list of previously discovered Enterprise Vault archive sources.

Note: The *EsaEVCrawlerService* is used to perform the discovery.

Step 1: Perform Enterprise Vault Discovery/Vault Administration

From **System > Directories and Servers**, for Veritas Enterprise Vault servers, you can discover new Enterprise Vault vault directories, and perform other administrative tasks such as check site/vault store and archive statistics, and create policies which you can later use to your collection filters (under the "**Retention and Policy Tags**" tab).

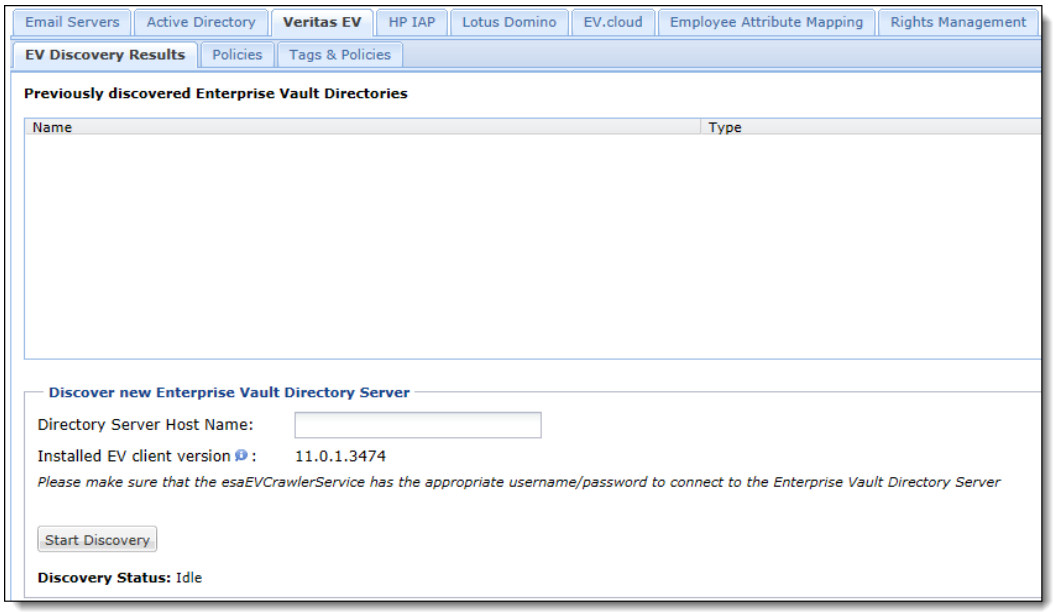
About Enterprise Vault Policies

You can filter your collections and holds in Enterprise Vault by creating policies using policy tags. Policies are updated automatically every time a collection occurs. If documents are encountered with a new policy, the new policy is automatically added to the list of existing policies, by its name, and type.

CAUTION: Before performing Enterprise Vault discovery, check that the correct version of Enterprise Vault API Runtime is installed. For both new installations and upgrades from older versions, 9.0 automatically installs Enterprise Vault 11.0.1 API Runtime on the appliance. To connect to other certified versions of Enterprise Vault, follow the steps to uninstall 11.0.1, then re-install a certified version first. See the entry for "Enterprise Vault (EV)" in the table under *"Verify Network Setup by Data Source" on page 26*.

To perform discovery on the Enterprise Vault server

1. Log on to the appliance using "Admin Account".
2. In the Veritas eDiscovery Platform interface, in the **All Cases** view, click **System > Directories and Servers**.
3. Click the **Veritas EV** tab.



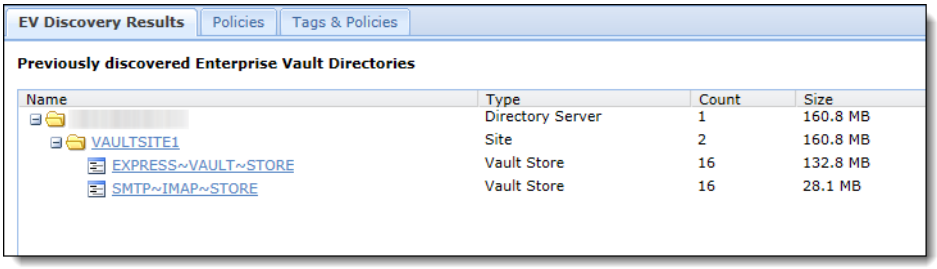
Under the "**EV Discovery Results**" tab appears either a blank field, or list of any previously discovered Enterprise Vault directories.

4. To discover a new Enterprise Vault Directory server, enter the Directory Server Host name.

   Note: The version of the installed Enterprise Vault client is shown. This must exactly match the Enterprise Vault server (API Runtime) version. The *EsaEVCrawlerService* must also be running with the credentials that grant you Read permissions to the archives you intend to collect or hold.
   Make sure that the FQDN of the Enterprise Vault Directory server is reachable so that the Enterprise Vault Discovery task runs successfully.

5. When ready, click **Start Discovery**. This automatically detects the appropriate directories, and performs discovery on the Enterprise Vault Directory server.

When discovery is complete, your discovery results display all Enterprise Vault vault directories that have been discovered.



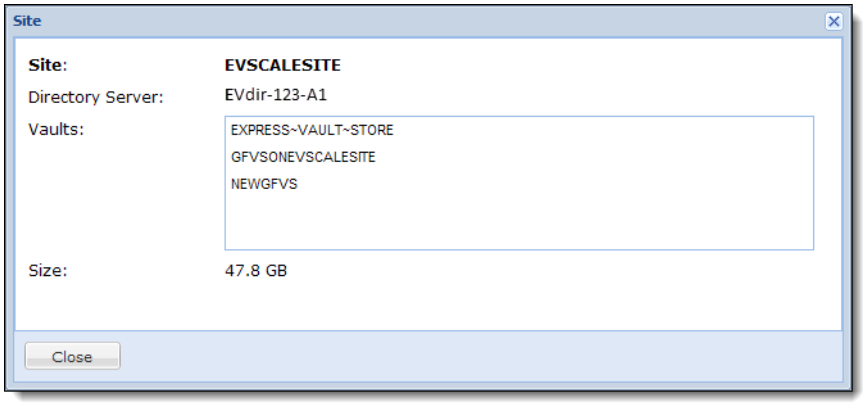
Troubleshooting: If you encounter issues during discovery, check the server logs, including output from the *EsaEVCrawlerService*. Any archives that were dropped for any reason are not reported through the Veritas eDiscovery Platform user interface. Be sure to check these logs first to determine what was dropped.

6. Continue with *"Step 2: Add Enterprise Vault Sources" on page 93*. Alternatively, continue to the next set of steps to view statistics on your discovered directories.

To view vault directory statistics

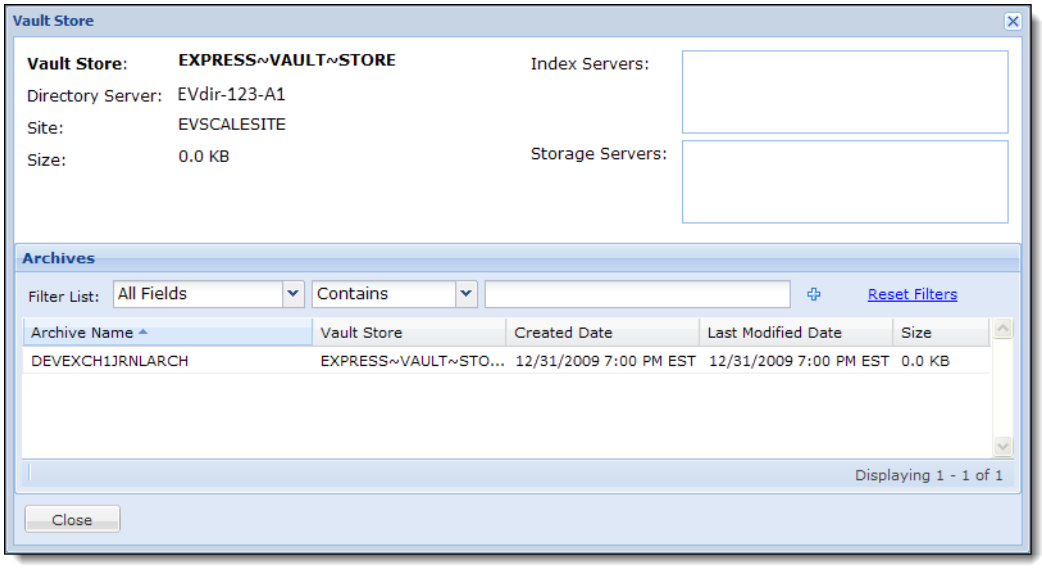
1. Click any link displayed in your discovery results to view statistics about that site and/or its vault stores and associated archives.

   Clicking a parent vault directory displays the Site window:



   This view shows the directory server, associated vaults and total size for the selected site.

Clicking on a vault from the Site window displays the Vault Store's statistics and the associated Archives.

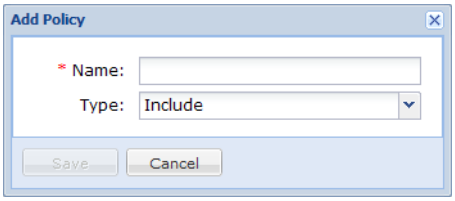


The Archives section displays all associated archives, including its *Vault Store*, *Created Date*, *Last Modified Date*, and *Size*. Click on an archive to view these same statistics, plus view its *Index* status in a new window.

2. Continue with *"Step 2: Add Enterprise Vault Sources" on page 93*. Alternatively, continue to the next set of steps to create a new policy.

To create a policy

1. From **System > Directories and Servers**, with **Veritas EV** selected, click the **Policies** tab.
2. Click **Create New**.
3. In the Add Policy window, enter a name (required) and choose the type of policy (*Include*, *Exclude* or create a *Category*).



4. Click **Save**. The policy can be applied when you create a collection or hold task. The **Retention and Policy** Tags tab appears allowing you to select this (or add a new) policy.
5. To delete one or more policies, click the "trash can" (delete) icon in the Action column, and confirm deletion.

Step 2: Add Enterprise Vault Sources

An Enterprise Vault source is defined by the combination of a Site and Archive Type. Once selected, the system will collect or hold from all specified archive types of the selected site.

To add an Enterprise Vault source

1. In the **All Collections** module, click **Sources**.
2. On the Sources screen, click **Add**.

   Note: If the Enterprise Vault selection does not appear, your license may not have been updated. See *"Managing Your Collections License" on page 194*.

   Note: A warning message appears at the top of the screen if discovery on the Enterprise Vault source was not performed first.
3. Specify the following information. An asterisk (*) indicates a required field.

Source Data

Field	Description
*Source Name	Type the name of your data source (up to 35 characters).
Description	Enter a description of the source (up to 255 characters).
*Type	Enter or select the source type.
*Site *Archive Type	Enter the site and select an archive type to be used for this Enterprise Vault source. For example, entering the site: EVVAULTSITE and selecting the Enterprise Vault Domino mailbox archive allows collections from any mailbox archives in Lotus Domino from within EVVAULTSITE. **Note:** For details, refer to the steps in *"Veritas Enterprise Vault" on page 87*.
Account	Enter the name of the source account you created, or click **Browse** to select one from the list of accounts.
Access Groups	By default, all groups to which the user has access are listed in the **Included** column which results in the source being added to all groups. Keep only those groups in the **Included** column in which you want to add the source and move all the remaining groups to the **Available** column. If the source is not added to any group, then that source will be available to all users.
Custodian Group	Type the name of the custodian or group associated with the data source (Example: John R. Smith), or click **Browse** to select one from the list of custodians/groups.
Collection Templates and Collection History	Indicates whether a template has been applied to the collection. (Click link to edit collection templates.) View list of collections and task details.

4. Click **Save**.

   Note: If there will be multiple users for the Veritas Enterprise Vault source, you must add an account for each added local user.

Step 3: Update your License

Collection from an Enterprise Vault source requires a Veritas eDiscovery Platform 9.0 version license. If you are upgrading your appliance to 9.0, be sure to update your license. In the Veritas eDiscovery Platform user interface, go to **System > License**. For details, see *"Collection Administration and Maintenance" on page 177*.

Continue to *"Creating and Managing Collections" on page 101* to start adding collections and tasks for your Enterprise Vault source.

EV.cloud

Starting with 8.0, Veritas eDiscovery Platform integrates with Veritas Enterprise Vault.cloud (EV.cloud) as a data collection source.

For an EV.Cloud source, you can perform the following:

- Discover EV.Cloud site/accounts
- Search archived mailboxes using filters and custodian assignments
- Collect/recollect data, view and analyze results using Analytics, generate reports
- Export data for processing

About EV.cloud Discovery

You must first perform a discovery for an EV.cloud site to be able to collect data from that site. A site for an organization has a unique URL, and it consist of accounts. Items belong to one or more accounts. When you perform a discovery for an EV.cloud site, you discover EV.cloud accounts. Veritas eDiscovery Platform stores information about the discovered EV.cloud accounts in the Veritas eDiscovery Platform's database.

Step 1: Perform EV.cloud Discovery

Prerequisites:

To be able to discover an EV.cloud site and perform collections, you must:

- Obtain a valid EV.cloud site URL for your organization
- Obtain valid logon credentials to access the EV.cloud site

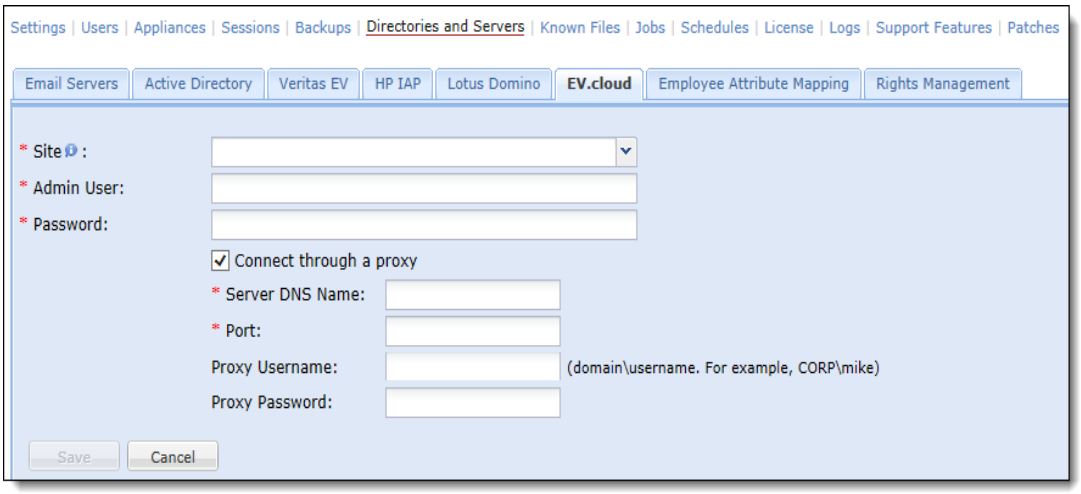
Please contact your EV.cloud administrator if you do not have this information.

To perform discovery on the EV.cloud site

1. Log on to the appliance using "Admin Account".
2. In the Veritas eDiscovery Platform interface, in the **All Cases** view, click **System > Directories and Servers**.
3. Click the **EV.cloud** tab.

   The EV.cloud screen appears either blank or displays a list of any previously discovered EV.cloud sites.

4. To discover a new EV.cloud site, click **Add**.



5. Select your EV.cloud URL if it is listed in the **Site** list. Else, type or paste the URL.
6. Enter the username in the **Admin User** field. The source account must have administrative privileges on the EV.cloud site.
7. Enter the password in the **Password** field.
8. If you are using your company-specific proxy server and filter settings, then to connect through the proxy, you must select the **Connect through a proxy** check box, and then enter the Server DNS Name and Port. If required, enter the Proxy Username and Proxy Password. The Proxy Username must be in the *domain\username* format. For example, *CORP\mike*.
9. Click **Save**. The site URL will appear in the EV.cloud dialog.
10. When ready, click **Start Discovery**. The system starts discovery for the newly added site as well as the previously discovered sites in a sequence. Only one site is discovered at a time.

    Note: The system automatically discovers all accounts on the EV.cloud site. The system also discovers the deleted and hidden accounts from the EV.cloud site. So the actual number of accounts on the EV.cloud site and the number of discovered accounts on the system may not match.

    Discovery of EV.cloud sites can also be scheduled from the **System** > **Schedules** screen.

Step 2: Add EV.cloud Sources

To add an EV.cloud source

1. In the **All Collections** module, click **Sources**.
2. On the Sources screen, click **Add**.

   Note: If the EV.cloud selection does not appear, your license may not have been updated. See *"Managing Your Collections License" on page 194*.

Note: A warning message appears at the top of the screen if discovery on the EV.cloud source was not performed first.

3. Specify the following information. An asterisk (*) indicates a required field.

Source Data

Field	Description
*Source Name	Type the name of your data source (up to 35 characters).
Description	Enter a description of the source (up to 255 characters).
*Type	Enter or select the source type. (Example: PC).
*Site	Select a site from which you want to collect the data. The Site list shows all EV.cloud sites that are discovered.
Access Groups	By default, all groups to which the user has access are listed in the **Included** column which results in the source being added to all groups. Keep only those groups in the **Included** column in which you want to add the source and move all the remaining groups to the **Available** column. If the source is not added to any group, then that source will be available to all users.
Custodian Group	Type the name of the custodian or group associated with the data source (Example: John R. Smith), or click **Browse** to select one from the list of custodians/groups.
Collection Templates and Collection History	Indicates whether a template has been applied to the collection. (Click link to edit collection templates.) View list of collections and task details.

4. Click **Save**.

   Note: Veritas eDiscovery Platform uses the same admin user logon credentials that were used for adding the EV.cloud site, and the same credentials will be used for future EV.cloud sources for that particular site.

If a discovered EV.cloud site is deleted after creating a source for that site, you can still perform collections from the deleted site.

Step 3: Update your License

Collection from an EV.cloud source requires a Veritas eDiscovery Platform 9.0 version license. If you are upgrading your appliance to 9.0, be sure to update your license. Go to **System > License** to see the available licenses. For details, see *"Collection Administration and Maintenance" on page 177*.

Continue to *Creating and Managing Collections* to start adding collections and tasks for your EV.cloud source.

Collecting from Documentum, FileNet, and Livelink

Veritas eDiscovery Platform supports collection from Enterprise Content Management sources such as Documentum, FileNet and Livelink. These are licensed separately. Collection from these sources leverages the Content Management Interoperability Services (CMIS), an OASIS standard. Veritas eDiscovery Platform can collect from CMIS compliant versions of Documentum, Livelink, and FileNet.

Topics in this section:

About Content Management Interoperability Services (CMIS)

CMIS (Content Management Interoperability Services) is a standard approved by Organization for the Advancement of Structured Information Standards (OASIS). The CMIS framework and APIs enables different content management systems to exchange/share information. It provides interoperability across different content management systems. For more information, visit http://www.oasis-open.org.

Veritas eDiscovery Platform 8.1 only supports CMIS-compliant versions of Documentum, Livelink, and FileNet. While there are other data sources that are CMIS compliant, Veritas eDiscovery Platform only supports Documentum, Livelink, and FileNet.

When upgrading to 8.1, sources and collections tasks/ templates created in previous releases for Documentum, FileNet and Livelink need special attention as documented in *"Supported Source Types" on page 21*.

Please note that Livelink E-mail collection method is deprecated in 8.1. A new collection task or a template cannot be created with the Livelink E-mail collection method. The existing collection tasks that were created in the previous releases using the Livelink E-mail collection method cannot be re-run for collection of new or modified data. You can only re-run the existing task for custodian assignment. You can only view the task details, edit its description, create and view the defensibility report, view analytics, and create a collection set.

For a list of supported data sources source types, versions supported, and specifications, see *"Supported Source Types" on page 21*. For information on source account requirements, see *"Verify Network Setup by Data Source" on page 26*.

Step 1: Verify Collector License

In Veritas eDiscovery Platform, go to **System > License** to check for available licenses. The "Data Source Types" should show all licensed data sources that were added to your Collections license.

Once licensed, these data sources appear in your list of available types when adding a new data source in the Identification and Collection module. If the data source you want to use does not appear in the source types list, or if you have a trial license you want to use, click **Update License**. Follow the on-screen instructions in the Update License Wizard to upload or copy/paste an available license for the appropriate collector(s).

For more information, refer to *"Managing Your Collections License" on page 194*.

Step 2: Add the Source Account

A source account must be added before you add the source. If one already exists, skip to step 3.

For details on adding a source account, see *"Adding a Source Account" on page 30*.

Step 3: Add the Data Source

Next, add the data source to your data map in the Identifications and Collection module in Veritas eDiscovery Platform.

To add the data source

1. From the **All Collections** module, click **Sources**.
2. Click **Add**.
3. To add a data source, specify the following information. An asterisk (*) indicates a required field.

Collector Source Data

Field	Description
*Source Name	Type the name of your data source (up to 35 characters). For example "Documentum Source"
Description	Enter a description of the source (up to 255 characters).
*Type	Enter or select the source type. All licensed collectors will appear in the list.
Account	Enter the name of the source account you created, or click **Browse** to select one from the list of accounts. The source account is the account used to access the data source server. The user must have either an administrative privileges or permissions to access the repository. If Account is left blank, Veritas eDiscovery Platform will use the same Clearwell services user account as it is currently running.

Collector Source Data (Continued)

Field	Description
*Content Server CMIS URL	Enter the content server CMIS URL, which is also referred as RESTful AtomPub Binding URL. The full HTTP address is required. For example: Documentum: http://<host>/emc-cmis-ea/resources/ Livelink: http://<host>/ot-elib/cmis/atom FileNet: http://<host>/fncmis/resources/Service Verify the correct location convention with your System Administrator. Click **Fetch Repositories** to populate the list of repositories.
*Repository	Select the repository to use for collection from the Documentum, Livelink, or FileNet source. (Multiple repositories may exist.)
Access Groups	By default, all groups to which the user has access are listed in the **Included** column which results in the source being added to all groups. Keep only those groups in the **Included** column in which you want to add the source and move all the remaining groups to the **Available** column. If the source is not added to any group, then that source will be available to all users.
Custodian	Click **Browse** to select a custodian from (or add a new one to) the list of custodians.
Group	Click **Browse** to select a group from (or add a new one to) the list of groups.
Collection Templates and Collection History	Indicates whether a template has been applied to the collection. (Click link to edit collection templates.) View list of collections and task details.

4. Click **Save** to add the new data source.

   View the new data source type in **All Collections > Sources**.

Step 4: Create a Collection Task

With your new data source added to your source types, you can create a collection task using the newly-added data source. Data collected from the new data sources can be filtered by Author, Date Created, Date Modified, File Type, File Extension, Keyword (except Livelink email), and folder.

For details on how to create a collection task and apply filters, see *"Creating and Managing Collections" on page 101*.

Creating and Managing Collections

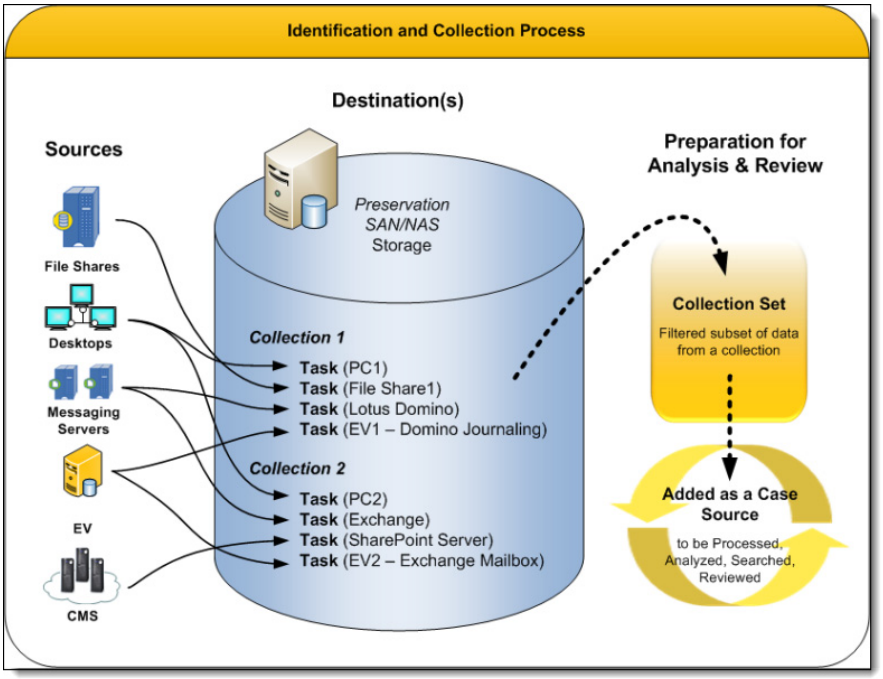
This section describes collections, and related tasks on the Veritas eDiscovery Platform.

About Collection Activities

When creating and managing collections, you can:

- Collect data directly from multiple data sources
- Copy and store this data in a destination preservation store
- Choose and filter a set or subset of collected data to be made into a collection set, which can be added as a Processing case source.

The following diagram shows how data is collected and organized from the source through case processing and analytics. (For more information about Collection Sets, and analyzing your collected and processed data in a case, see *"Creating, Analyzing and Processing Collections" on page 163*.)



A single collection, typically named for a particular legal matter or case, can have any number of *Tasks*. Each task collects data from a single Data Source. Once tasks have finished collecting data, the data or subset of the data can be assembled into a *collection set*. Any number of collection sets can be created from one collection. The collection set can then be added as a case source to any Veritas eDiscovery Platform case before being processed. The same collection set can also be added to multiple Veritas eDiscovery Platform cases. To start creating new collections, see *"Creating a Collection and Running Tasks" on page 103*.

Note: Veritas eDiscovery Platform supports collection of data in UTF-8 encoding format only.

About OnSite Collections

Similar to Network collection tasks, *Onsite Collection Tasks* collect data, however, they also allow you to collect the data using a Flash drive or other external portable data storage device, without requiring data collection over a network.

To collect data from remote sources, locked files, or from sources that are not reliably connected to your network, you can create an OnSite Collector (installer package) to be installed on an external portable drive, or directly onto a custodian's PC or Macintosh.

Note: To launch the Onsite Collector from the MSI installation folder, ensure that the folder name does not contain spaces.

To specify directories you want to include or exclude from PC or Mac OnSite Collection, see *"Include/Exclude Directories" on page 120*. To securely encrypt collected data when using OnSite Collector, see *"Secure Encryption for OnSite Collection Tasks" on page 125*.

For an overview of the OnSite Collection feature, refer to the *OnSite Collections Reference Card*.

Creating a Collection and Running Tasks

Each collection you create can contain one or more collection tasks, in which you specify the data source, set filter parameters, and assign data to custodians (and later, analyze and "package" the results as a collection set) to be added to a new case.

Veritas eDiscovery Platform provides email address visibility when selecting and filtering Enterprise Vault archives and mailboxes associated with a collection task. For more information, see *"Filtering Best Practices (for Enterprise Vault Sources)" on page 113*.

You can set the system so that once tasks are deleted from the user interface (UI), regardless of their status, will also have the associated data in the preservation store deleted automatically. This feature helps reclaim vast amounts of disk space, which weren't previously possible without manually deleting the data from the preservation store. To enable this functionality, you need to set the property **esa.icp.task.deleteOnDiskTaskData** to **True** using **System** > **Support Features** > **Property Browser**.

Process Overview

This list describes the process of adding collections to begin collected data from your sources through creating and running tasks.

1. Add a collection.
   See *"Create/Add a New Collection" on page 103*
2. Add Tasks to the collection.
   See *"Add Tasks to a Collection" on page 104*.
3. Run or Schedule a Task in the collection.
   See *"Run or Schedule a Collection Task" on page 126*.

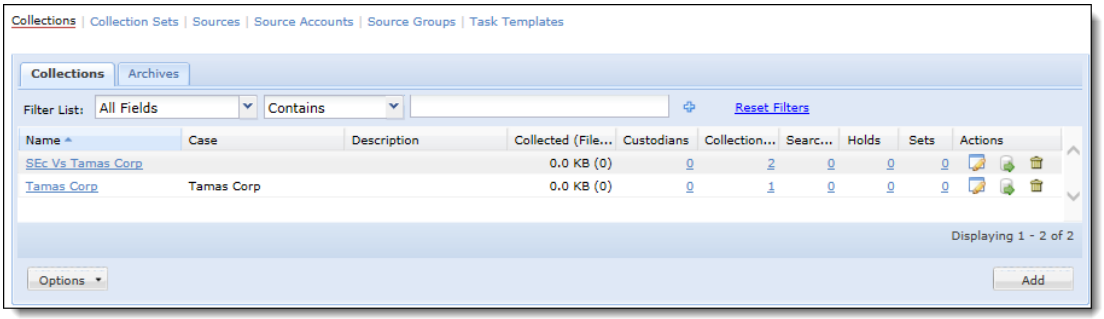
Create/Add a New Collection

Collections provide a simple, efficient way to collect and organize data in preparation for a particular case.

To add a collection

1. Select the **All Collections** module. If no collections yet exist for this case, click **Create Collection**. To add a new collection (when one or more collections exist), click **Add**.

   Note: If a collection is associated with a case, and if the user does not have access to that case, then the information related to that case is filtered out on the All Collections page.



2. The Add Collection window opens.

   A. Specify the following information. An asterisk (*) indicates a required field.

Add a Collection

Field	Description
Name*	Enter a name for the collection (up to 35 characters). The name is not case sensitive, but must be unique. Use only letters, numbers, and underscores.
Description	Enter a description for this collection (up to 255 characters).
Default Location*	Enter the location where data for this collection will be stored, or click **Select** to select one from the list of locations (created during data source setup), or from the Locations window, click **Create New** to locate and add a new location. See *"Adding Locations for Collected Data" on page 45* for procedures to add a location. **Note:** Only those data locations appear on the Locations window whose type is either "Collect Only" or "Collect and Export" and that are added in the groups to which the user has access.
Case	The case you previously selected is shown.) Click the drop-down menu to change the case to which you want to add this collection.

   B. Click **Save** to submit the new collection, or click **Cancel** to discard your changes.

   Tip: You can create a template based on this collection when you start adding tasks. Follow the steps in the next section to continue with adding a task, or see *"Create a Collection Template" on page 125*.

Add Tasks to a Collection

If you have just created a new collection, after clicking **Save**, the *Collection Tasks* screen opens, prompting you to add a task to the same collection. You can also add tasks to any existing collection by selecting the case, choosing the collection, then clicking **Add**.

To add a task (to a newly-created collection)

1. Select the collection you just created to view the *Collection Tasks* screen.

   Note: If you want to add a task to collect data from a PC or laptop onsite (rather than over the network), you can upload the data collected from performing an On-Site collection. See *"Performing OnSite Collection Tasks" on page 137*.

2. Determine if you want to:

   A. Add a new task (whether or not a collection exists). Continue to step 2 in the next procedure: "*"To add a task (to an existing collection)" in the next section*".

   B. Copy the attributes of another task in the same collection. Follow the same steps (as it applies to collection tasks) as described for copying a hold in *"Copy a Hold Task" on page 160*.

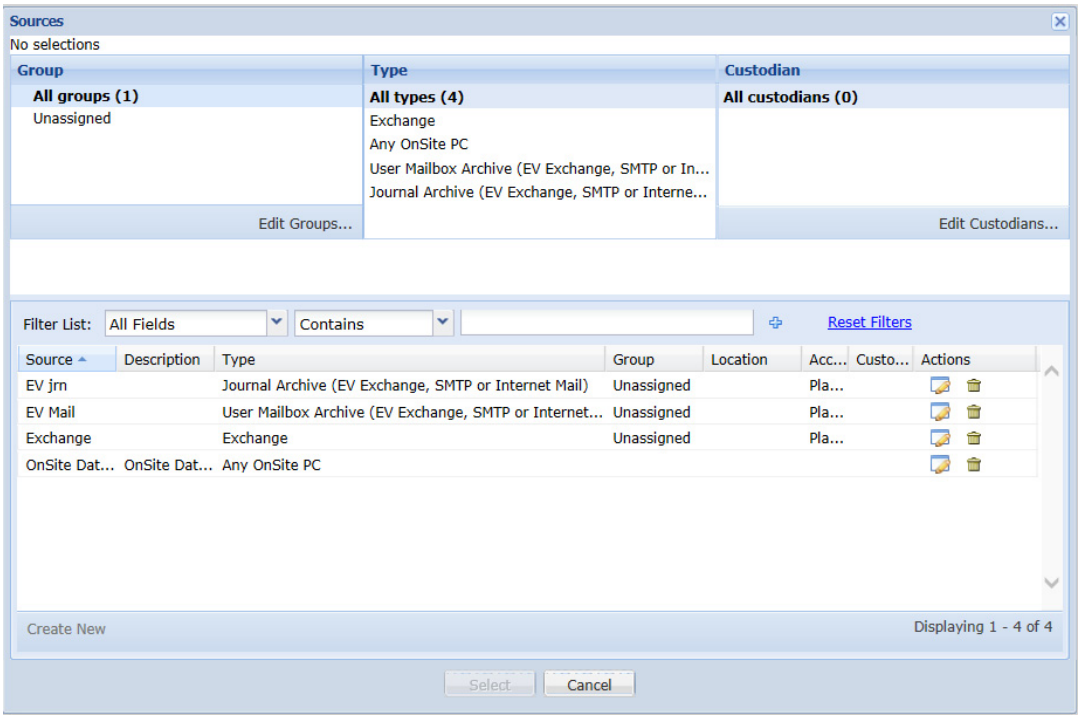
To add a task (to an existing collection)

1. From the **Collections** module (within a case), select a collection from the list.

2. To add a task:

   – From the Collection Tasks screen, click **Add**.

   The Sources window opens enabling you to select a source from which you want to collect data (defined in Data Mapping).



   – For a lengthy list of sources, use the Group, Type, and Custodian boxes to filter the list that appears in the Sources (bottom section).

   The selections you make in each of these boxes appear in the source list, showing the Source, Description, Type, Group, Custodian, and the available actions that can be performed on the task.

   Note: Release 8.1 and later only support CMIS compliant versions of Documentum, Livelink, and FileNet. If you have created sources for non-CMIS compliant Documentum, Livelink, and FileNet data sources in previous releases, you cannot use the existing sources as it is after upgrading to Release 8.1. To use the existing sources, you must reconfigure the existing non-CMIS compliant sources to CMIS compliant sources. Only the new sources and the existing sources that are reconfigured will appear on the Source Picker window. If a required source doesn't appear, you should reconfigure the source from **All Collections** > **Source** screen.
   Also, collection tasks targeted for Filenet sources cannot collect a file which has a "%" character in its filename.

3. Select the source you want to use to run your task, and click the **Select** button.

4. Next, specify the following information. An asterisk (*) indicates a required field.

Note: Tabbed options, and their order of appearance vary depending on the source type.

Add Task Filter Options

Field	Description
Description	Type a description for this collection task.
Source*	Previously selected source is shown (by default), or click **Browse** to use another source. For Enterprise Vault sources, see *"Filtering Best Practices (for Enterprise Vault Sources)" on page 113*. **Note:** If you have added a source for an EV.cloud site and then deleted the site, you can still use the existing EV.cloud sources created for the deleted site to add a new collection task.
Archives	(For EV.cloud source only) You can choose to collect data from either all discovered accounts or specific accounts. By default, the **Selected** option is enabled. Click the **Add Archives** button to see the discovered accounts. Only the first 500 accounts are displayed on the **Accounts** screen. You can also filter the discovered accounts by name or email address using **Filter List**. You can select an account by clicking the **Add** button or select all accounts by clicking **Add All**. The selected accounts appear under **Selected Accounts**. On clicking **OK**, the selected accounts appear in the **Archives** box. You must add at least one archive. If you want to search and collect data from all discovered accounts, click the **All** button. The **Archives** field also displays the count of the selected archives. If there are large number of archives for EV.cloud source, it is recommended to create multiple collection tasks with fewer archives.
Collection Method*	(Default is "Network"), or click **Cancel** to collect data from a non-network source. For PC collections, choose a network collection, or an OnSite Windows or OnSite Mac collection. See *"Performing OnSite Collection Tasks" on page 137*. Starting with 8.1, Livelink E-mail collection method is deprecated. Therefore, a new collection task or a template cannot be created with the Livelink E-mail collection method. The existing collection tasks that were created in the previous releases using the Livelink E-mail collection method cannot be re-run for collection of new or modified data. You can only re-run the existing task for custodian assignment. You can only view the task details, edit its description, create and view the defensibility report, view analytics, and create a collection set. For EV.cloud, the default collection method is EV.cloud transfer.
The task filter options appears depending on the type of sources. When you create a search query by adding different filter options, the filter options get ANDed together. For example, different filter options like Date, Keywords, File Type are ANDed together.	
[Top Row Tabbed Options:]	
Mailboxes	(For Exchange and Domino Mailbox sources only): Select the mailboxes in the Exchange or Domino source from which you are preparing to collect. **Note:** Veritas strongly recommends not to select the **Include all mailboxes** or **Include only the following servers** options to avoid over-collection from the Exchange and Domino Mailbox sources, and to avoid overload on your email messaging system.

Add Task Filter Options (Continued)

Field	Description
Archives	(For Enterprise Vault sources only): This tab appears only if you are collecting from a Veritas Enterprise Vault source. Select archives to include in your collection task, then click **Add Archives**. Select an available archive by name, vault store, created date, last modified date, or size. For Enterprise Vault User Mailbox Archive (Enterprise Vault Exchange, SMTP or Internet Mail), the **Archives** filter shows all columns that exist in the Employee List including the custom attributes for only those employees which are synchronized through Active Directory. These columns can also be added/removed to show specific columns in the archives list. When Enterprise Vault 11.0.1 or later is used, the Archive picker also displays the SMTP and Internet Mail archives. **Note:** The Archive picker only displays archives that match the source's Site and Archive Type. See *"Archive Selection" on page 113* for information about these Enterprise Vault Source fields. Select vault stores to include in your collection task, then click **Add Vault Stores**. Select an available vault store by name, archive, or size. Starting with 9.0.1, when archives are deleted on Enterprise Vault after you perform the Enterprise Vault discovery on eDiscovery Platform, these deleted archives do not appear in the Archive Picker. When vault store is selected instead of individual archives, the deleted archives are correctly filtered from the vault store. Thus, the task is prevented from resulting into Partial Success.
Filtering	Click to filter by: **Sender/Recipient**, **Traits**, **Retention Policy Tags** (Enterprise Vault Archives only), or **Keywords**, **Date**, **File Type**, **Container Files**, and **Owner or SID** (see "Bottom Row Tabbed Options").
Directories (or Folders)	Select the Server Volumes and Directories (for Folders, for certain source types): Default is shown, or click **Add** to add a new directory, or **Browse and Add** to search. For SharePoint sources, the **Browse & Add** function is used to fetch the complete folder hierarchy of the SharePoint URL. Starting with 8.0, the search time of the **Browse and Add** function is optimized by fetching only two levels of the folder hierarchy initially. If required, you can see further levels of folder hierarchy by clicking the folder expansion (+) sign. The number of folder hierarchy to display can be configured by setting the value for the property **esa.icp.collection.sharepoint.folderhierarchy.numLevels** as greater than two by using **System** > **Support Features** > **Property Browser**. Also, the filter criteria are applied first while searching the SharePoint folder hierarchy. A folder is downloaded only when it satisfies the filter criteria. **Note:** For PC collection tasks, you can choose which directories you want to exclude, as well as include in your collection. See *"Include/Exclude Directories" on page 120*. Starting with 8.1, the **Browse and Add** function for Documentum, FileNet, and Livelink fetch only the first level of folder hierarchy. If required, you can see further levels of folder hierarchy by clicking the folder expansion (+) sign. Folders are listed in an alphabetical order. Only first 50 characters of the folder name are displayed. You can hover on the folder name to see its complete name.
Known Files	Select whether or not to filter out files on a known file list (such as NSRL, a "NIST" list). (Ignore is selected by default.) **Note:** Data collection will take longer if you choose to clear this option; however, you will typically collect a much smaller volume of data.

Add Task Filter Options (Continued)

Field	Description
Data Location	Select the data location to save the collected data. Previously selected location (defined while adding the collection) is shown (by default), or click **Browse** to change the location. **Note:** Only those data locations appear on the Locations window whose type is either "Collect Only" or "Collect and Export" and that are added in the groups to which the user has access. **Compression**: Select this option to save the collected data as a compressed file in the target location.
Custodian Assignment	Choose options to automatically assign a custodian by various source identifiers. See *"Running Custodian Assignments" on page 135*. (For (Journal Archive (Enterprise Vault Exchange, SMTP or Internet Mail), User Mailbox Archive (Enterprise Vault Exchange, SMTP or Internet Mail), or Enterprise Vault Domino Archive sources only): Choose whether to assign to custodian based on associated email addresses, or create a new custodian using the archive's email addresses.
[Bottom Row Tabbed Options:]	
Sender/ Recipient	(For Enterprise Vault sources only): This tab appears only if you are collecting from a Veritas Enterprise Vault (Enterprise Vault) source. Choose a filter for searching email by **Sender or Recipient (To, From, Cc, Bcc)**, **Sender (From)**, or **Recipient (To, Cc, Bcc)**. Enter all email addresses or display names to be searched.
Date	Select any of Creation, Modification, and Last Accessed dates (according to time zone shown). You can reset the Date filters by selecting **All Dates** in the Creation, Modification, and Last Accessed dates. **Note:** Loose MSG and EML files are excluded according to the file's Modification date, not the Sent date. Exclusion based on Sent time still applies to PST and NSF files. (For Enterprise Vault SharePoint Archive source only): Select from Created Date, Archived Date, or Modified Date. **Note:** Indexes of an archive are usually spread across multiple index volume sets. In earlier releases of Veritas eDiscovery Platform, when a date range filter is used for any Enterprise Vault task, all the index volume sets were searched before applying the date filter on an Enterprise Vault task. Starting with 8.0, the search time is optimized. The system now skips the index volume sets which do not fall into the specified date range filter. If you do not want to use this enhancement and want to get all index volume sets to be searched for the specified date range, you should contact Veritas Customer Support. To change the time zone, go to **System > Settings**.

Add Task Filter Options (Continued)

Field	Description
Traits	(Journal Archive (Enterprise Vault Exchange, SMTP or Internet Mail), User Mailbox Archive (Enterprise Vault Exchange, SMTP or Internet Mail), and Enterprise Vault Domino Archive Sources): You can filter by: message type, attachments extensions, custom attributes, and to include or exclude non-indexed items. For message type, indicate whether to include or exclude specified types (or select all), such as: Exchange Email, Instant Messaging, Bloomberg, Fax, or DXL. You can filter by both keyword and attachment extension types. However, the parent message and its attachments are indexed together. So when both filtering traits are applied together, keywords will be filtered based on the whole message, not only to the matching attachments. The parent message will always be collected. **Note:** When you filter by attachments extensions for .eml and .msg, the emails with these extensions are not searched which results in non-collection of these emails. The collection count does not match with the original count. This is a known issue on Enterprise Vault side. For custom attributes, specify the values to restrict collection, and indicate whether to include or exclude documents based on specified custom attribute criteria, such as String, Number, or Date, with corresponding values. Add more lines to enter additional criteria. (Values will be treated as an 'OR' expression.) Non-indexed items are excluded (by default). Click to filter by items that have not been indexed in Enterprise Vault.
Retention and Policy Tag	(Journal Archive (Enterprise Vault Exchange, SMTP or Internet Mail), User Mailbox Archive (Enterprise Vault Exchange, SMTP or Internet Mail), and Enterprise Vault Domino Archive Sources only): For retention tags, indicate whether to include or exclude selected categories by name: Default Retention Tag, Domino Journaling, Exchange Mailbox, and Exchange Journaling. All existing policies appear in the Known Policies box. These are policies that may have been discovered, or created after initial Enterprise Vault source discovery. (Check also **System > Directories and Servers > Veritas EV** tab and click the **Policies** tab.) Click **Add Policy** to create a new policy.
Attachments Extensions	(Enterprise Vault File System Archive and Enterprise Vault SharePoint Sources only): Specify the attachments extensions to filter. (Turned off by default.) Indicate whether to include or exclude specified attachments extensions. Enter each additional extension on a new line.
Author	Choose whether or not to filter by author. If filtering by author, specify those to include by Custodian or Domain\Author. Click **Add Custodians** or **Add Author** if the name does not appear in the list.
Keywords	Filter documents that contain only certain keywords. Enter one or more keywords. (Click the icon to add additional lines for each keyword.) See *"Using special characters in the directory path" on page 118*. For Enterprise Vault sources, Keyword filtering provides the option of listing any, all, or none of the phrases entered. All three categories can be grouped together by an AND expression.

Add Task Filter Options (Continued)

Field	Description
File Type	Filter files by type or extensions to include or exclude. (File type filtering is turned off by default.) (For Enterprise Vault sources, see also File Extensions.) Veritas eDiscovery Platform can also collect PST files, and enables collection of locked files, even if they are still open or locked during collection. **Note:** You can enable error reporting on these files to identify potential issues and view a list of locked items. Veritas eDiscovery Platform attempts to re-open, or remediate locked files. (For SharePoint sources only) Only non-document files such as Discussions or announcements can be collected by selecting the **SharePoint Components** check box under the **Content Type** list in the **File Type** tab. With **Include** filter, the SharePoint documents are collected in the following way: When **SharePoint Components** is selected and other document file types (content types) are not selected, then only non-documents are collected and the documents are not collected. When **SharePoint Components** is not selected and other document file types (content types) are selected, then only documents are collected based on the file type filtering applied and the non-documents are not collected. When both **SharePoint Components** and other document file types (content types) are selected, then both documents (based on the file type filtering applied) and non-documents are collected. When the File Type filter criteria are not specified, both documents and non-documents are collected by default. **Note:** Entering file extensions only searches based on extension name, not actual native file type. To collect prior versions of SharePoint documents, click the **Collect previous versions of documents (default is All versions)** check box. By default, this check box remains deselected. To collect specific number of prior versions of the documents, click the **Only Collect previous versions** check box and then specify the number of prior versions that you want to collect. By default, 3 prior versions are selected. All collected older versions of documents are saved in the "*Previous Versions_timestampofcollctiontask*" folder which resides inside every folder for a SharePoint document container (Library or Folder). When a collection task is rerun, only newer versions of the document are collected along with the original version of the document. The system does not collect older versions of SharePoint non-documents. Author-based filtering for older versions does not work for SharePoint 2007 collections. **Note:** Collection of older versions of SharePoint documents does not work with federated search. You can use either the **Collect previous versions of documents (default is All versions)** option or the **Enable SharePoint federated search** option in the Keywords filter. When collecting from a Fileshare, a password protected Microsoft Word file will not be collected even if the "**Include Microsoft Word**" option is selected under the **File Type** filter. To collect the password protected Word files, you can either use the "**Other Type**" option under the **File Type** filter or specify doc or docs file extension in **File Extension** filter under **File Type** filter.
Container Files	Filter by container files that will always be included in the collection task. If selected, these container files will always be collected, regardless of other filters such as keyword, date range, and owner. **Note:** Any other filter options specified do not apply to container files.
Owner or SID	Filter by specified owner/SID by adding custodians or names and SIDs.

Add Task Filter Options (Continued)

Field	Description
E-Mail to Custodian Mapping	(For Journal Archive (Enterprise Vault Exchange, SMTP or Internet Mail) Sources Only): Specify whether or not to filter by email addresses. Indicate custodian assignment rules to automatically populate their corresponding email addresses to filter. Click to add a new row for each additional custodian to email mapping. To remove or clear a custodian, click the delete icon to delete the row. Click Add Custodian to select a custodian that does not appear in the list. (Email addresses can include wildcard characters.) **Note:** When not filtering by email addresses, all Journaling archives will be attributed to the Source default custodian (or None, if no custodian for the source was specified.) For email address filtering, select one of three options: Sender or Recipient (default), Sender, or Recipient. All email addresses specified in the search will be subject to the same search type.
EV.cloud Filter Options **Note:** A search query can have a maximum of 249 terms, with each term having a maximum of 255 characters. The limit of 249 terms does not consider archive counts and operators like AND/OR. EV.cloud determines the maximum export size based on the number of emails and an average email size. The export task might fail if the size exceeds the estimated export size. In such a case, it is recommended to redefine the search criteria. For further details, refer to the EV.cloud documentation.	
by Keyword or Phrase containing	Filter documents that contain only certain keywords. Enter one or more keywords. Multiple keywords should be separated by comma. (Click the icon to add additional lines for each keyword.) Specify whether to filter by Any, All, Not Any, or Proximity within keywords or phrases. You can filter these keywords in Entire Message, Subject, Message Body, or Attachment Name. **Note:** For Keyword filtering, searches are supported only in English. The Proximity filter is not supported with the Attachment Name filter, and vice versa.
by Sent date	Filter documents by sent date. You can filter by All Dates, Dates On or After, Dates On or Before, or Dates Between options. You can reset the Sent date filters by selecting **All Dates** option.
by Name or Email Address containing	Specify name or email address that contains Any, All, Not Any names within Recipient, To, From, CC, and BCC fields. You can also add names or email address by clicking **Add archives** to see the discovered accounts. From the **Accounts** screen, you can add a name or email address by clicking on the name/ email address or select all accounts by clicking **Add All**. The selected names and email addresses appear under **Selected Accounts**. You can also filter the discovered accounts by name or email address using **Filter List**. Click **OK** to add the selected names and email addresses in the **by Name or Email Address containing** filter.
by Attachment Type containing	Specify the attachment types that you want to include or exclude from the task. Multiple attachments types should be separated by comma. You should use each attachment type only once.

Note: Filtering occurs in the following order to maximize performance: Date, Traits, Retention Policy and Tags, then Keywords.

A. To include/exclude certain directories in your collection, click the **Directories** or **Folders** tab (depending on source type). Continue with steps in *"Include/Exclude Directories" on page 120*.

B. To create a template based on this collection and selected task options, click **Actions** > **Save Collection Template**. Continue with steps in *"Create a Collection Template" on page 125*. (The next time you want to apply this template to a task, select **Actions** > **Load Collection Template**, and select it from the Templates window.)

5. For EV.cloud source:

A. By default, the collection is stored at the location that you specified while creating the collection. To store the collection at other location, click **Select** to browse and specify the location in the **Save to Location** field.

Note: Only those data locations are displayed whose type is either "Collect Only" or "Collect and Export" and that are added in the groups to which the user has access.

B. Choose whether to assign to custodian based on associated email addresses, or create a new custodian using the archive's email addresses. To assign custodians, specify the following information.

Custodian Assignment Details

Option	Sub-Options	Description
Assign items to the Source default custodian (None)		(Default). Selecting this option assigns the same custodian that is associated with the source. Name of the custodian added while creating source is displayed, otherwise "None" is displayed by default.
Assign items to a custodian in priority order as follows	Assign to custodian based on associated email address	Select to assign custodian only if the email address is matched with the email addresses in the Employee List.
If no match is found:		
	Create a new custodian using the archive's email address	If no match (or in cases where a mismatch has occurred), create the custodian using the archive's email address.
	Assign the custodian	Type a specific custodian you want to assign, or click **Browse** to select one from your source list.
	Don't assign a custodian	Specify *not* to assign the source's default custodian to items not found for that custodian.

C. Click **Start Collection** to immediately start running the new task or click **Save Progress** to save the task. On the Start Confirmation dialog, specify the number of retries for the collection task and then click **Yes**. By default, the number of retries is set to 3.

6. For other sources, click **Save** to save the task, or click **Save and Start** to add, and immediately start running the new task.

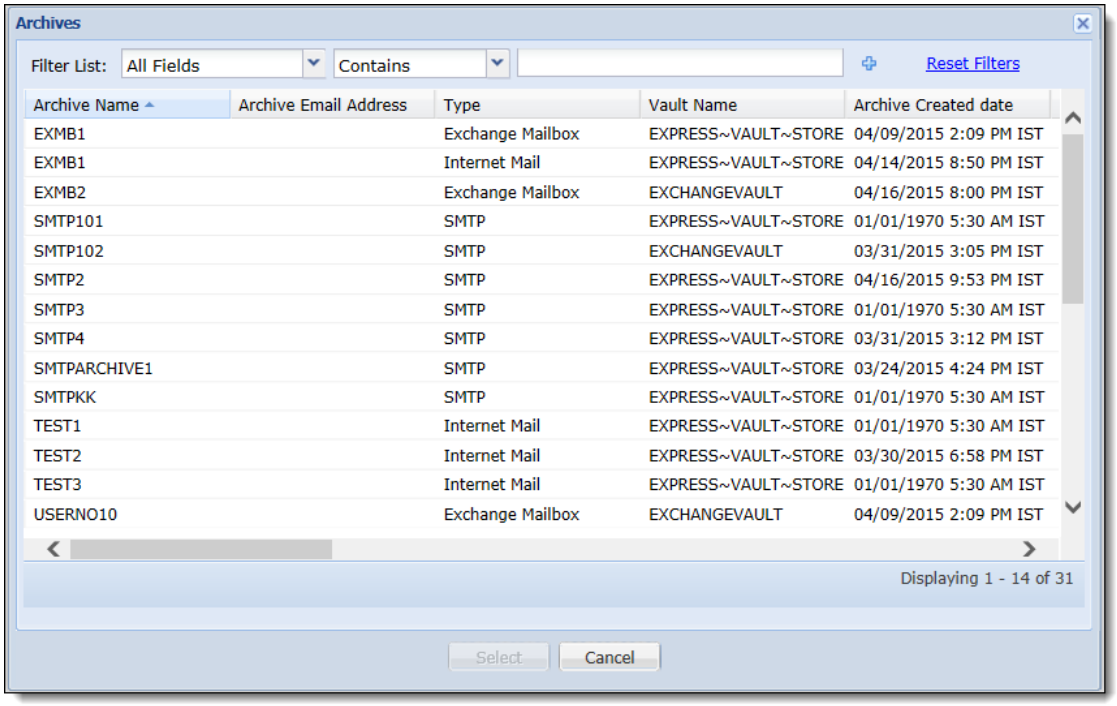
Once the task is saved, click the (Action) icon and select **Copy** to make a copy of this task. This is useful when, for example, you are using the same set of filter criteria to collect from multiple file shares (or PCs). If you have used the **Save Progress** option, you can start the task at any time or you can also schedule the collection task. See *"Run or Schedule a Collection Task" on page 126*.

Filtering Best Practices (for Enterprise Vault Sources)

Refer to this section for tips and guidance during your Enterprise Vault archive selection and helpful search techniques when filtering criteria on Enterprise Vault source data.

Archive Selection

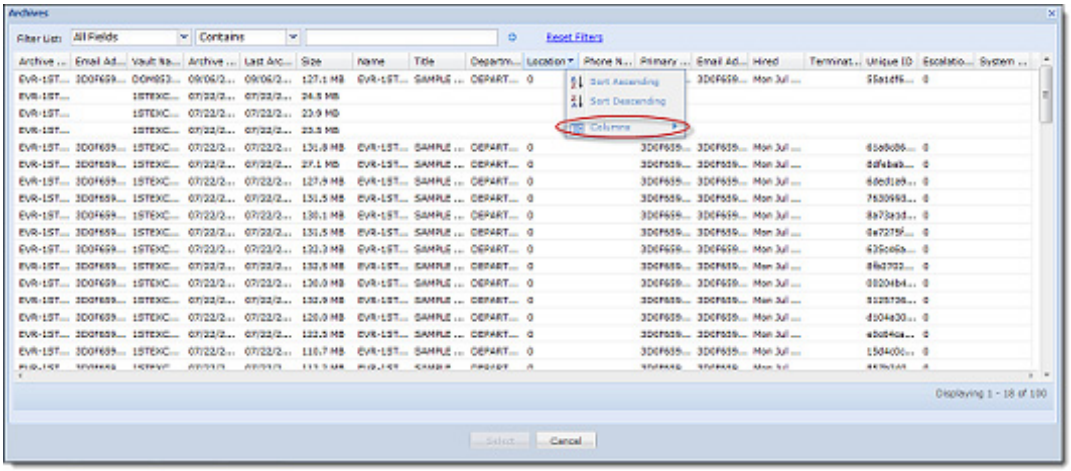
When you add an archive from your collection task "**Archives**" tab filter, the Archives window opens allowing you to select from all discovered archives for the selected source.



From here, you can filter the list for specific archives to add, by *Archive Name*, *Vault Store*, *Created Date*, and *Last Modified Date*. Use the Boolean search operators, and type in keyword criteria to filter the list as needed. Click the "+" icon to add more filtering rows. Click any column heading to sort by that data type.

Archives with blank name are also discovered during archive discovery and then displayed as "_Unnamed_Archive" in the "Archive Name" column.

For the Enterprise Vault User Mailbox Archives (Enterprise Vault Exchange, SMTP or Internet Mail), the **Archives** filter shows all columns that exist in the Employee List including the custom attributes for only those employees which are synchronized through Active Directory. These columns can also be added or removed to show specific columns in the archives list.



Note: A maximum of 1000 archives can be selected. If you select more than 1000, a warning appears that performance may be affected as the large number of archives are added to the collection task. You are prompted to confirm whether or not the system should proceed.

> **Tip:** Alternatively, from the same "**Archives**" tab, click to **Add Vaults**. This allows you to include/exclude entire vaults, rather than individually selecting their archives without affecting performance. For example, adding an entire vault that contains 100,000 archives would occur almost instantly.

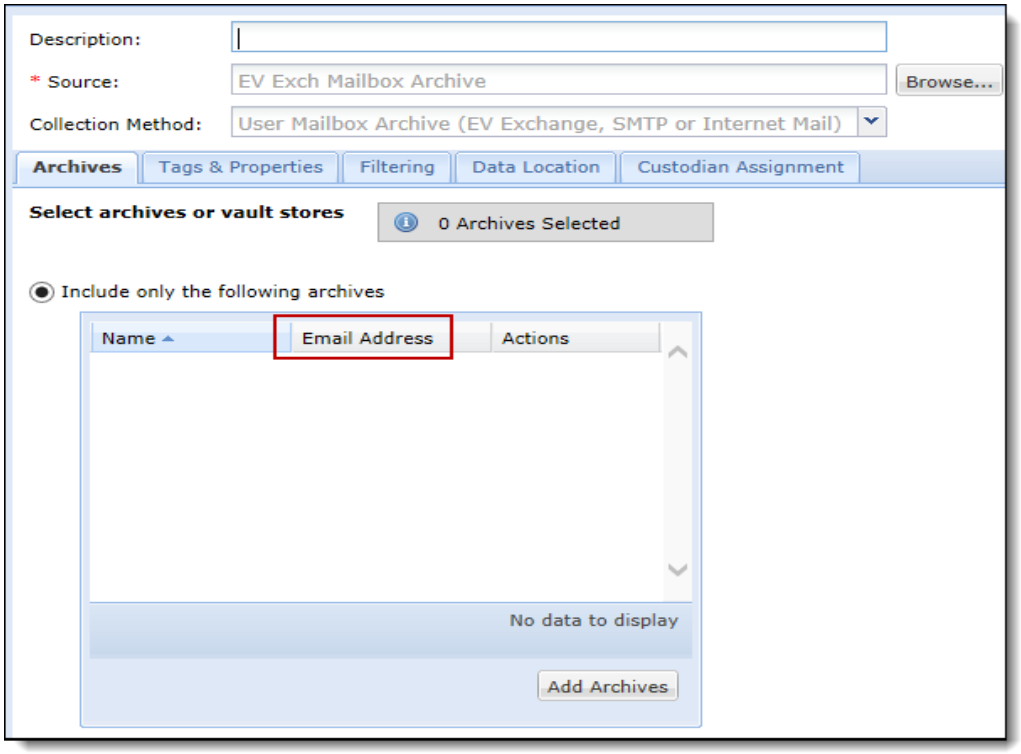
Email Address Selection

You can filter archives by their corresponding user email address. This function applies to Journal Archive (Enterprise Vault Exchange, SMTP or Internet Mail), User Mailbox Archive (Enterprise Vault Exchange, SMTP or Internet Mail), Enterprise Vault Domino Archives, Exchange Mailboxes and Domino Mailboxes.

Note: You must have already run Active Directory, Domino, and Enterprise Vault discovery on your sources to ensure this feature is available. After upgrading, you must re-run Active Directory, Domino, and Enterprise Vault discovery on the Veritas eDiscovery Platform server to enable this functionality.

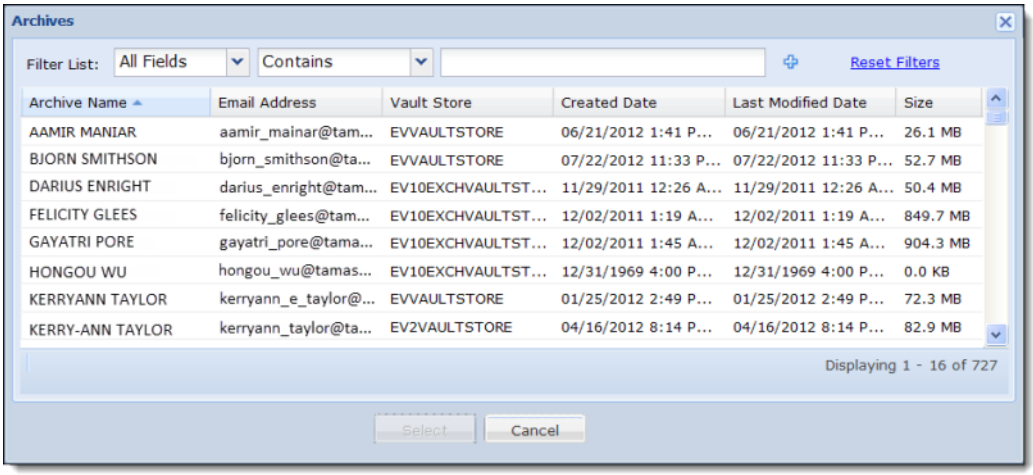
From **All Collections**, when creating (or editing) a collection task (for an Enterprise Vault Archive, Domino, or Exchange mailbox source), the **Archives** tab automatically shows the Email Address column.

A new column added to the Archives window (and shown in the **Archives** tab when setting collection task attributes), gives users more selection and filtering criteria to further refine their collections.

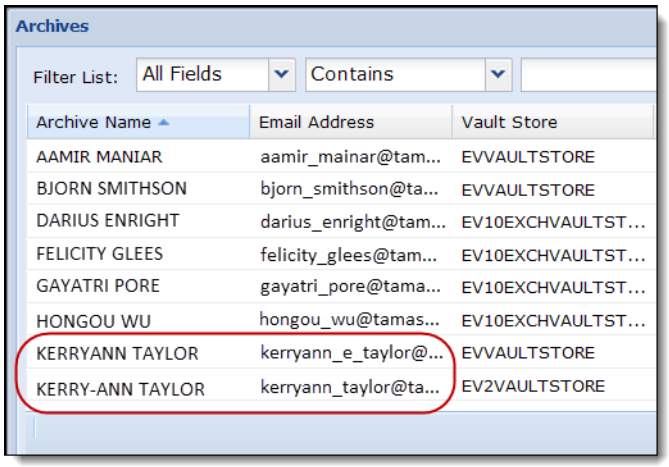


Click **Add Archives** to select from archive names that have an Email Address.

From the Archives window, use the Email Address column to help you determine which specific, especially those very similar archives to add to your collection task.



Archives window (with upgrade to 7.1.2 Fix Pack 1 or later)



Example: If there are two names that appear to be duplicate archives and dates, size, or Vault store doesn't provide enough distinctive information, the Email Address column will show that they are two individual archive names each with a different address.

Note: To show email addresses, the system uses the Primary Email Address configured for a custodian.

You can also view email address filter criteria (if available) in Collection Task defensibility reports. See *"Collection Reports" on page 137*.

Search Techniques

The following search techniques serve as effective filtering methods when preparing to collect from a Veritas Enterprise Vault source. This section provides a brief overview of the search types to use in the **Sender/Recipient** and **Keywords** tabs for Enterprise Vault collection.

Note: Enterprise Vault keyword search works only with the subject and the message body. For searching in any other metadata fields, use the **Traits** filter.

For details on these and all other search types, particularly for reviewers using the Analysis & Review module, refer to *"Advanced Search" in the Veritas eDiscovery PlatformUser Guide*.

Using Wildcards in Enterprise Vault Searches

A wildcard is a character that may be used in a search term to represent one or more other characters. Enterprise Vault sources support the use of the wildcards: Question Mark (?) and the Asterisk (*). You can broaden or narrow your search by truncating search terms using these wildcards to represent single (?) or multiple (*) characters.

Single Character

Use the question mark (?) o represent a single alphanumeric character in a search expression, at the end of a word. When searching, you must have at least three leading characters of the keyword.

Example using (?)

Entering	Returns
Trader?	Trader, Traders
Risk?	Risk, Risks, Risky

This is particularly useful when searching for single character variations to one or more keywords.

Multiple Characters

To specify zero or more alphanumeric characters, use an asterisk (*). Similar to the single character wildcard, you must have at least three leading characters before the asterisk. (A search term with only one asterisk, no preceding characters, could retrieve every record from the Enterprise Vault.)

Example using (*)

Entering	Returns
Market*	Market, Markets, Marketing
Invest*	Invest, Invests, Investment, Investments, Investing

This is especially helpful when searching for multiple variations to one or more keywords.

Diacritics

The Enterprise Vault index is in Unicode; therefore, searching may be language specific. For example, a search for “éléphant” would only yield the French variant of the word (more specifically, the accented “e” in the word, regardless of the language in which it was written). If you know that you have non-English or international email which may contain special characters or accented letters, Veritas recommends analyzing your search criteria and either generating multiple specific variations or using the single character wildcard (?) to ensure that you return meaningful results.

Unicode is defined as a series of character encoding standards intended to support the characters used by a large number of the world's languages.

Searching Email Domains

To search for all email to, or from a specific domain, you do not need to use the “@” symbol or any wildcards. When in the to/from search field, enter just the domain name, such as *Veritas.com*

Searching custodians

Custodian email addresses, display names and SMTP CN addresses can be searched using the **Filtering > Sender/Recipient** tab. The collected items will only include those which satisfy the search rule (Sender or Recipient/Sender/Recipient) and the email, display names, or SMTP CN addresses specified in the text field.

Searching Non-Indexed Items

In some organizations, there are occasions where an encrypted, corrupted, or protected document or a very large document is archived and not indexed. When Enterprise Vault archives an item without indexing, it adds a "Not Indexed" attribute to allow searching.

Note: These items, by default, will not be collected. Take precautions knowing that these documents will appear in all result sets, regardless of the search query, when the "search non-indexed" option is selected.

Punctuation

When Enterprise Vault indexes an item, any punctuation is treated as a "Space". When setting up a collection from Enterprise Vault, and searching against a phrase or name with punctuation such as a middle initial followed by a period, the "Period" will be ignored.

Enterprise Vault Index Level

The level of indexing configured determines what search capability is available in Veritas eDiscovery Platform for Enterprise Vault collection.

Index Level	Description
Brief	Allows searching of the metadata associated with the Author, Recipients, Subject, Date Range.
Medium	Allows searching of the metadata associated with the Author, Recipients, Subject, Date Range, as well as key word searching of the content contained in the message body and the attachments.
Full	Allows searching of the metadata associated with the Author, Recipients, Subject, Date Range as well as key word and phrase searching of the content contained in the message body and the attachments.

Using special characters in the directory path

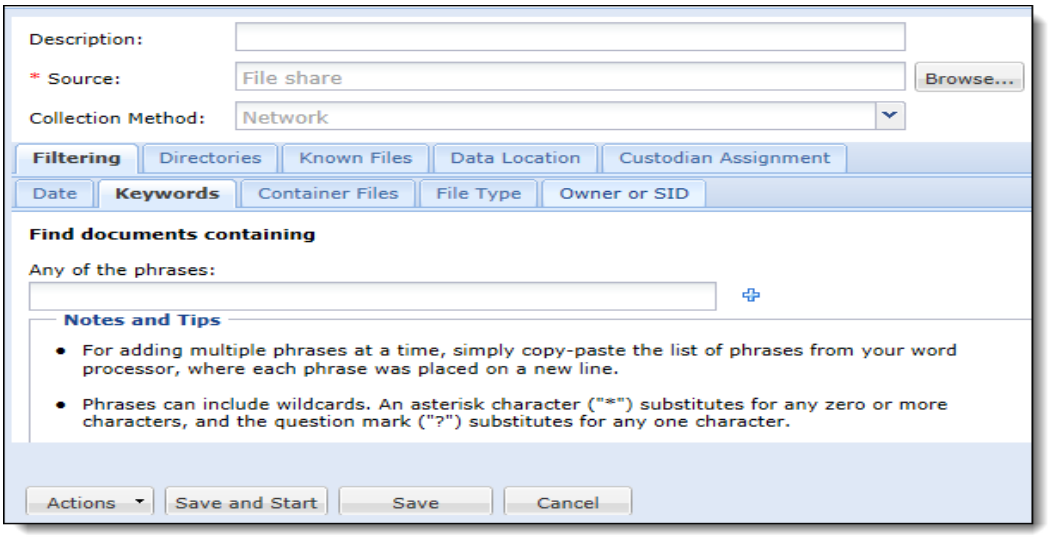
While specifying the directories you want to include or exclude, ensure that you do not use special characters such as "$", "_", and so on in the folder or directory path. These special characters are ignored in collection and search tasks done with Enterprise Vault sources. Presence of special characters in the directory path that you want to include may result in over-collection. Presence of special characters in the directory path that you want to exclude may result in under-collection. However, this over- or under-collection will not happen if the position of the special characters in the name is different.

For example, if the source has two folders "folder_1" and "folder$1," then when you search for "folder_1," Enterprise Vault will search for "folder$1" as well. This is because the folder names are identical except the position and number of the special characters. In this case, Enterprise Vault ignores the special characters and subsequently hits results for both folders.

However, this over- or under-collection will not happen if the folder names are "fol_der1" and "folder$1" as the position of the special characters in the name is different.

Keyword-Based Collection (Non-Enterprise Vault Sources)

Veritas eDiscovery Platform's **Keywords** filtering feature applies to all Identification and Collection source types including File Share, PC, Exchange (and BPOS), SharePoint, Livelink, Domino, EV.cloud, On-site PC and On-site Macintosh.



When you select Keyword-based filtering, only documents that include any of the specified keywords will be collected. However, keyword filtering does not apply to any container (such as .zip, .rar, .gz, .tar) files, program files, images, audio files, video files, attachments, or SharePoint non-documents.

When a Keyword filter entry is composed of multiple words, Veritas eDiscovery Platform interprets it as an exact phrase. For example, if you enter the keyword: **"John Doe"** only documents (excluding non-applicable file types) that contain the exact phrase "John Doe" will be collected, including documents containing variations such as: "John Doey", or "AJohn Doey".

In addition to the exact phrasing, Keyword filtering allows wildcard searches. An asterisk (*) substitutes for multiple characters (within a 128 KB data range), and a question mark (?) substitutes for any single character. More advanced search types, such as Boolean, Stemmed, Proximity, and Concept searches can be performed in the Analysis & Review module, after collection data has been processed.

With collection tasks targeted for Exchange mailboxes, keyword-based filtering does not work for the Cc and Bcc fields. It works only for To, From, Subject fields. Also, keyword-based filtering for Exchange and Office 365 does not work for mails formatted as Rich Text (RTF). Keyword search works only for mails formatted as Text or HTML.

For SharePoint Sources, it is recommended to use the SharePoint federated search option. This option allows Veritas eDiscovery Platform to use the SharePoint built-in index for optimized performance when using Keyword filtering. Check with your federated search provider for specific rules on wildcard usage. The SharePoint federated search option is supported only with SharePoint On Premises, and it is not supported with SharePoint Online.

Note: For Documentum, Livelink, FileNet, and SharePoint (for non federated search) sources, if the filename is 251 characters long, the collection task collects the file even if the specified keyword is not present in the file.

Keyword Tips and Guidelines:

- The maximum number of keywords supported for a specific Collection Task is 100.
- Double quotes (") and single quotes (') are not allowed in Keyword Filters.
- For adding multiple keywords:
  - to the filter, press **+** at the end of the input text field.
  - at one time, copy and paste the list of keywords from a source document, where each keyword was placed on a new line.

Include/Exclude Directories

When collecting from a network or OnSite PC or laptop, you can target your source folders by selecting which directories to include and/or exclude. For example, rather than collecting all data from the "C$" drive, you can choose to collect only from "C$\My Documents" for the selected custodian(s). Similarly, use the Exclude section if you know which specific folders or directories from which you do not want to collect data.

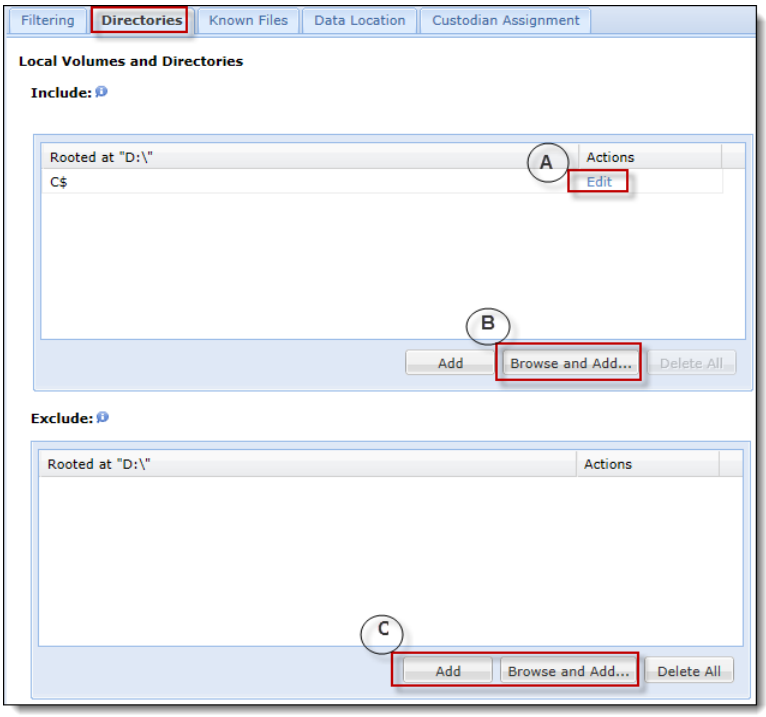
CAUTION! You must have sufficient permissions for browsing/selecting directories. (The logged on user account is shown at the bottom of the Source Directories window.) Ensure that you are logged on with the correct account user and role. Veritas strongly recommends logging on with the correct account first, before attempting to browse and add PC folders or directories.

Specifying Directories for OnSite Collections

You can select directories and folders for any OnSite collection, PC or Mac. For OnSite PC collection, follow the steps in this section "To include/exclude directories for an OnSite PC". For an OnSite Mac collection, see the steps "To include/exclude directories for an OnSite Macintosh" in this section.

To include/exclude directories for a network PC or File Share

1. On the Add Task page (for Network PC collection task), click the **Directories** tab.



2. On the **Directories** tab, do one or more of the following:

   A. To change the default "C$" directory to include specific subdirectories or subfolders, click **Edit** then enter the folder or directory path to include, and click **Update**. (Click **Add** for each additional folder or directory to include.)

   B. Click **Browse and Add** to search folders on the Source Directories window.

   C. To exclude any directories or folders, click **Add**, then enter the folder or directory path to exclude, and click **Update**. Repeat for each additional folder or directory to exclude. You can use wildcards (only for Exclude) such as * or ? when specifying shares or folders. For example: C$\win* or C$\win???? collects from the folder: C$\windows

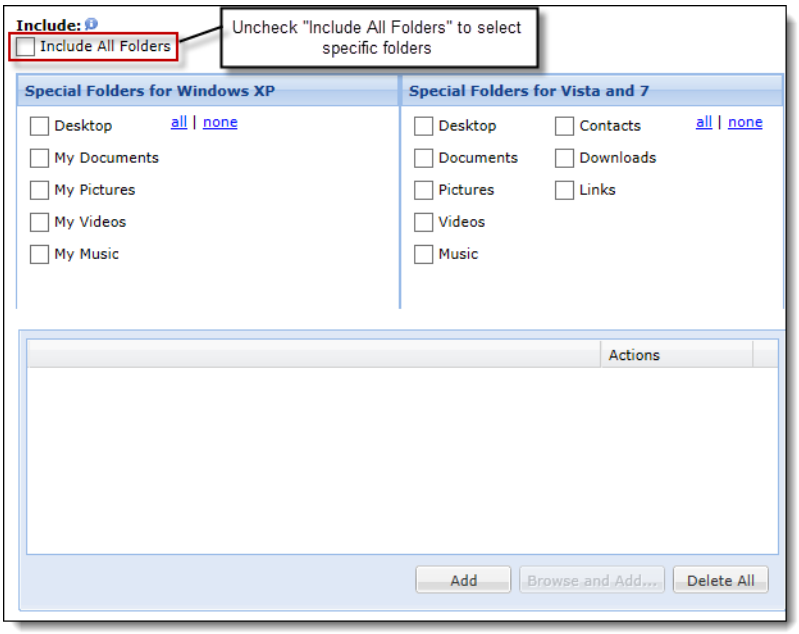
   Note: Excluded folders must be in one of the specified directories in your "Include" list above. If a selected folder is not in one of the "Include" folders, the collection task will ignore the entry.

   Alternatively, click **Browse and Add** to search folders on the Source Directories window. (You must be logged on with the correct account user and role. Veritas strongly recommends logging on with the correct account first, before attempting to browse and add PC folders or directories.)

3. Continue selecting other filters for your task, as described in *"Add Tasks to a Collection" on page 104*.

To include/exclude directories for an OnSite PC

1. On the Add Task page (while creating a task for an OnSite Windows PC collection), click the **Directories** tab. (For an OnSite Macintosh collection, skip to the next section.)



   Note that unlike for a network PC source, Veritas eDiscovery Platform automatically includes all directories for OnSite PCs. (The **Include All Folders** option is selected by default.)

2. Clear the **Include All Folders** option to specify which folders (by version) to include for this OnSite PC. (Alternatively, click **all** or **none** at the top of the box for the version.)

3. To add any directories or folders to include, click **Add**, then enter the folder or directory path, and click **Update**. Repeat for each additional folder or directory to include.

4. If you want to exclude any directories or folders, click **Add**, then enter the folder or directory path to exclude, and click **Update**. Repeat for each additional folder or directory to exclude. You can use wildcards (only in the Exclude section) such as * or ? when specifying shares or folders. For example, entering: C:\win* or C:\win???? will collect from the folder: C:\windows

   Note: Excluded folders must be in one of the specified directories in your "Include" list above. If a folder selected to be excluded is not in one of the "Include" folders, the collection task will ignore the entry.

5. Continue selecting other filters for your task, as described in *"Add Tasks to a Collection" on page 104*.

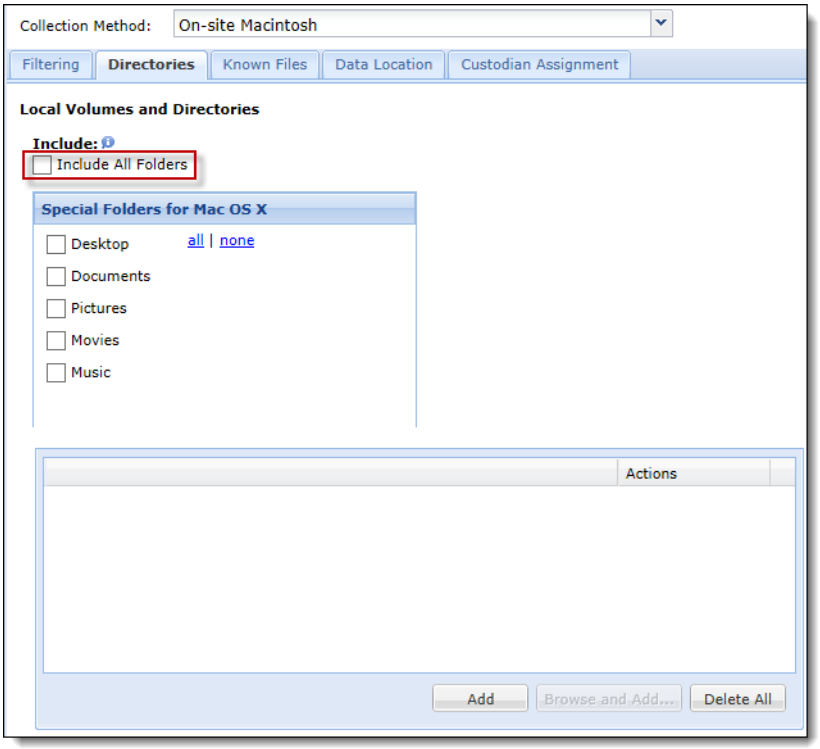
To include/exclude directories for an OnSite Macintosh

1. On the Add Task page (while creating a task for an OnSite PC collection), click the drop-down menu to select the **On-site Macintosh** collection method.

2. Click the **Directories** tab.

   Similar to the OnSite Windows PC source, Veritas eDiscovery Platform automatically includes all directories for OnSite PCs. (The **All** option is selected by default.)

3. Clear the **Include All Folders** option to specify which folders (by version) to include for this OnSite PC. (Alternatively, click **all** or **none** at the top of the box.)



   Note: Veritas eDiscovery Platform supports OnSite collection from Mac OS X.

4. To add any specific directories or folders to include, click **Add**, then enter the folder or directory path, and click **Update**. Repeat for each additional folder or directory to include.

5. If you want to exclude any directories or folders, click **Add**, then enter the folder or directory path to exclude, and click **Update**. Repeat for each additional folder or directory to exclude.

   Alternatively, click **Browse and Add** to search folders on the Source Directories window. (Ensure that you are logged on with the correct account user and role. Veritas strongly recommends logging on with the correct account first, before attempting to browse and add PC folders or directories.)

   Note: Excluded folders must be in one of the specified directories in your "Include" list above. If a folder selected to be excluded is not in one of the "Include" folders, the collection task will ignore the entry.

6. Continue selecting other filters for your task, as described in *"Add Tasks to a Collection" on page 104*.

OnSite Mac Collection Considerations

In Macintosh OnSite collections, Veritas eDiscovery Platform collects data with the following considerations:

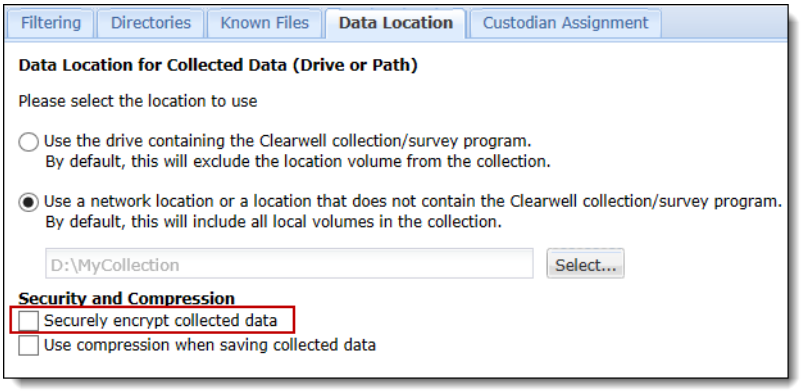
- **Invalid Character handling—**Backslashes, colons, forward slashes: Unlike for PC collection, in which all files with invalid characters for Windows except for the backslash (\) are collected when compression is off, for OnSite Mac collection, users can create files and folders with forward slashes (/), but are listed instead with a colon (:) in Macintosh file listings. Thus, Veritas eDiscovery Platform collects files with forward slashes, but the slashes appear as colons. Veritas marks these files as containing "invalid characters in filename" during package upload so that they are not processed further. However, Veritas eDiscovery Platform cannot validate characters such as the backslash, colon, and forward slash as they may actually appear in Windows paths. Files containing these three characters in their names are not marked as having invalid characters, but instead will appear as "item was not found" in validation logs.
- **Unusual Filenaming**
  - Folders whose names end with dots or spaces are collected, but marked as "item does not exist" in validation logs.
  - Folders whose names start with dots are collected and validated.
  - Files which are targets of symbolic links are collected and validated.
- **File paths**—Long paths up to 900 characters are collected. (Macintosh limit is 1024 characters, however Veritas OnSite Mac collection will not exceed 900 characters, as both the destination path and content path can otherwise exceed 1024 characters.)
- **Mounted volumes**—Any mounted volume, including network volumes, USB drives, CD drives, external harddisks are collected, if required.

Veritas eDiscovery Platform does not collect data in an OnSite Macintosh collection with the following conditions:

- **Invalid Filenames and/or Characters**
  - Filenames that are considered invalid in Windows are not collected. File types including AUX, CON, PRN, NUL, COM0..9, LPT0..9 are logged, but not collected.
  - Files with a star (*), question mark (?), or double quotes (") are logged, but not collected if compression is turned On.
- **Other Folders and Directory Types**
  - Symbolically-linked directories—Directories which are targets of symbolic links are not collected (though configurable using a property in Support Features).
  - **/dev** and **/proc** folders on Macintosh machines are not collected.

Secure Encryption for OnSite Collection Tasks

To ensure that the data you collect remains locked and protected until uploaded into Veritas eDiscovery Platform, when creating an OnSite collection task, on the **Data Location** tab for "Security and Compression" select the option to **Securely encrypt collected data**.



For more information about how to create an OnSite Collection task, refer to the *OnSite Collections Reference Card*.

Create a Collection Template

If you have many collections and tasks to create, templates are a quick way to apply source information you want to reuse in future collections and tasks. There are three ways to create Collection templates. You can either save a template when adding a new task, editing a task, or from the **Collection Templates** menu. Follow the set of steps that best suit your needs.

Note: Collection tasks and templates created for non-CMIS compliant versions of Documentum, Livelink, and FileNet data sources in previous releases cannot be used until these sources are reconfigured to CMIS compliant versions of these data sources. To use the existing collection templates, you must reconfigure the existing non-CMIS compliant sources to CMIS compliant sources and redefine the folder filter criteria. A banner and a warning message appears suggesting you to reconfigure the source and update the folder filter. Unless you reconfigure the source, you will not be able to add new collection tasks and templates and perform some actions for the existing collection tasks/templates that are associated with the existing sources.

To create a collection template (from the menu)

1. In the **Collections** module, click **Task Templates**.
2. Click **Add** to open the Add Templates page.
3. To add a template:
   A. Specify the following information. An asterisk (*) indicates a required field.

Add a Collection Template

Field	Description
Collection Template*	Enter a name for the template (up to 35 characters). The name is not case sensitive, but must be unique. Use only letters, numbers, and underscores.
Description	Enter a description for this template (up to 255 characters).
Source	Previously selected source is shown (by default), or click to select another source. See the Note above for Documentum, Livelink, and FileNet data sources.
Collection Method	(Default is "Network"), or click **Cancel** to collect data from a non-network source. See *"Performing OnSite Collection Tasks" on page 137*. Starting with 8.1, Livelink E-mail collection method is deprecated. Therefore, a new collection task or a template cannot be created with the Livelink E-mail collection method. The existing collection tasks that were created in the previous releases using the Livelink E-mail collection method cannot be re-run for collection of new or modified data. You can only re-run the existing task for custodian assignment. You can only view the task details, edit its description, create and view the defensibility report, view analytics, and create a collection set.

B. For all other tabbed option information, see Table 1-3 *"Add Task Filter Options" on page 106*.

C. Click **Save** to submit the new collection template, or click **Cancel** to discard your changes.

Run or Schedule a Collection Task

Clicking **Save** upon creating a collection, the Collection Tasks screen appears. Each collection contains one or more collection tasks, in which you specify the data source, set filter parameters, assign data to custodians, and later, allow you to analyze and report results.

To run a collection task

1. From the **Collections** module, select a collection containing the task you want to run.

   To run the task now, or schedule for later, skip to step 3. To verify selections or make changes first, continue to step 2.

2. To verify or edit the task first, then run:

   A. On the **Collection Tasks** screen, click the  (Edit) icon under Actions, or click the task name to open the Edit Task page.

   B. Check your selections, then click **Save and Start** to start running the task. For EV.cloud, click **Start Collection**.

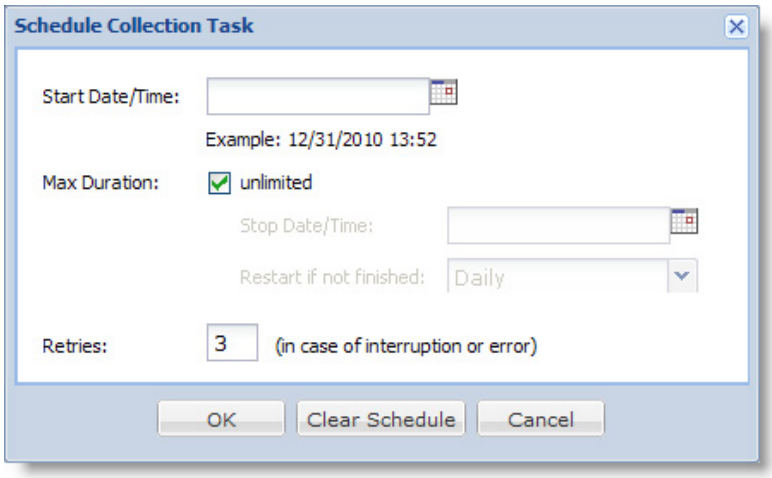
3. To run or schedule a task (from the collection):

   – To run a task, from the **Collection Tasks** screen, click the  icon to start running the task.

– To stop a task, click the icon. The system asks for a confirmation to stop the task. When you stop the task, the task status changes to stopped. You can check the status of the stopped task by clicking **Stopped** in the status column. Stopping a collection task on the **Collection Tasks** screen only pauses the collection task on Veritas eDiscovery Platform.

  To restart the task, click the icon. The system will collect the remaining data. Restarting a task does not recollect the already collected data. If the data on EV.cloud changes for the search criteria specified in the collection task, then the restarted task will not consider those changes and data collection will happen with the already received search results.

– To schedule a task to run later, click the icon to schedule a run time.
  › In the Schedule Collection Task window, enter the Start Date/Time, Max Duration (default is Unlimited), and number of retries the system will attempt to run the task.



  › Enter a Stop Date/Time if you want to ensure the collection will not run passed a specified time, then indicate when you want the task to restart if collection is incomplete. You can also schedule the task to recur after the collection is finished. See *"Schedule a Recurring Collection Task" on page 128*.

  › Click **OK** to schedule, or **Clear Schedule** to discard changes and reschedule.

4. To perform other actions on a task:

   A. To copy the task, click the (Action) icon, and select **Copy**.

   B. To set up a recurring collection on the task (due to new or modified data), click the icon. (See *"Schedule a Recurring Collection Task" in the next section*.)

   C. To delete the task, click the icon.

Schedule a Recurring Collection Task

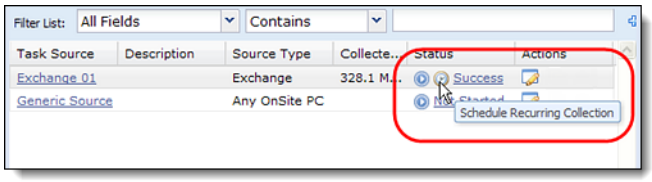
Recurring collection tasks are tasks within a collection which need to be run again when data has been added or changed in the source for the selected tasks. After a task has completed running, you can schedule a recurring collection to ensure all new and modified data will be collected.

To run a recurring collection task

1. Follow the steps in *"Run or Schedule a Collection Task" on page 126*, to select a collection task that has already run for the first time.

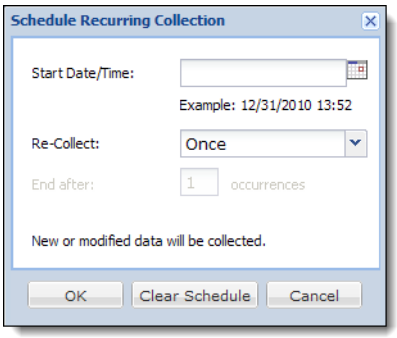
2. To schedule the same task to run again:

   A. Click the  icon to set up a recurring collection time.



   › In the Schedule Recurring Collection window, enter the Start Date/Time, and how often you want to re-collect data (Once, Weekly, or Monthly), then enter the number of occurrences after which to end the collection for all new or modified data.

   › Click **OK** to schedule, or **Clear Schedule** to discard changes and reschedule.



   When the task re-collection has completed, a new task is created with "Recollect #[#]:" in the description and a numbered designation. For example, when a recurring collection on task "Exch01" with a description "CEO laptop" completes, the new task (containing recollected data) appears as: "Exch02" with the description "Recollect #1: CEO laptop".

Note: Each re-collection from an existing task creates a new task. The new task contains the change in data collected from the original task and the re-collection. Each subsequent re-collection on the original task collects all changes (new or modified data) in the original, plus each of the previous re-collections.

Rerunning a Collection Task

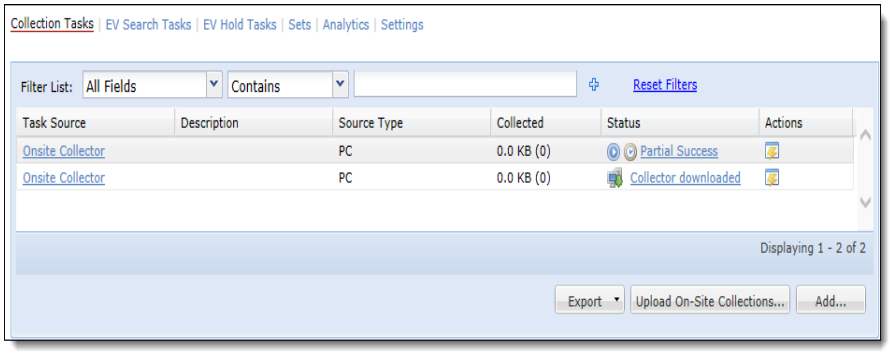
Collection tasks which result in a "Partial Success" or "Partial Failure" status can be retried, so that new or modified items are recollected.

Some considerations:

- If the data was collected completely when the task was run last time and there is no new or modified data available, then rerunning a collection task does not collect any new items.
- Rerunning a collection task does not collect the old data that was not collected previously. To get this data, a new collection task must be created. However, new or modified items will be collected.
- For File Shares, the system collects all files from the directory at the folder level containing the new and modified data, detected by the date modified, the number of files in the directory, or a change in the size of the directory. For all other sources in your data map, Veritas eDiscovery Platform collects all new or modified data detected.
- If you have reconfigured your Documentum, Livelink, and FileNet sources to support CMIS compliant data sources and redefined the folder filter after upgrading to 8.1 or later, then rerunning an existing collection task for the first time collects all original, new, and modified data.
- For EV.cloud source, when an existing collection task is rerun, a new collection task is created with same filters as the existing task. Apart from the existing filters, an additional “SentAt” filter is passed to EV.cloud with its value set to the last execution date. This ensures that the data generated after the last execution date is collected. For a collection of data from all archives, rerunning a collection task for new or modified data will also collect data for the newly discovered archives only from the last execution date of the collection task.
- When Enterprise Vault 11.0.1 or later is used, items from SMTP and Internet Mail archives can also be collected. When upgraded to 8.1.1 or later, rerunning a collection task for archives with EML files will not collect the existing EML files. It can only collect new EML files that were added after the collection task was run for the last time.

To rerun a collection task

1. After first running a collection task that resulted in a "Success" or "Partial Success" state, click the (play) icon.

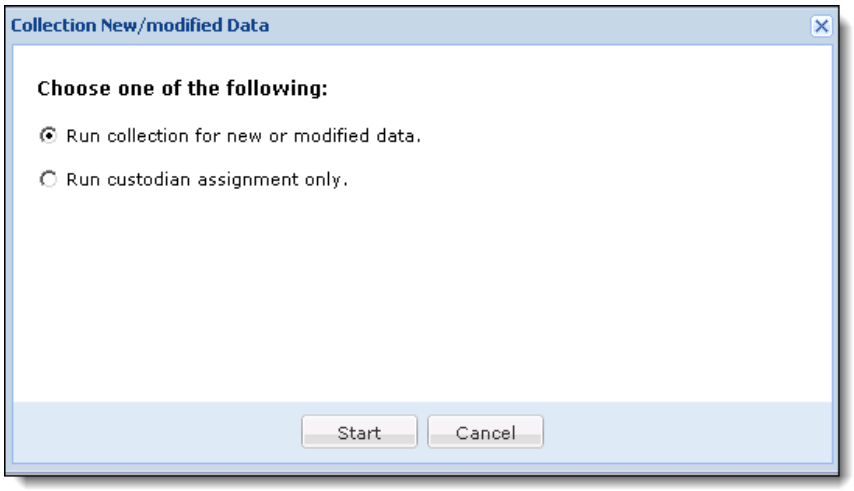


2. From the Collection New/modified Data window, select one of the following option, and then click **Start.**

   – Run collection for new or modified data: collects any new or modified data that was added after the task was run for last time.

   – Run custodian assignment only: assigns custodians to the already collected data in the previous runs according to the set custodian assignment rules. See *"Running Custodian Assignments" on page 135* for more details.

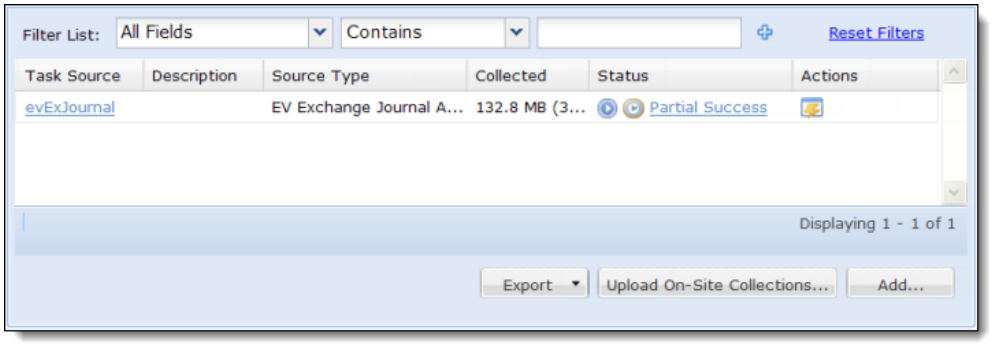
   Note: If the collection task is resulted in partial success, then a third option appears for collecting the errored data. For more details, see *Retrying a Failed Collection Task (for Enterprise Vault and EV.cloud Sources)*.



3. From the Jobs window, you can open the job's status log file to check whether the new or modified items were collected.

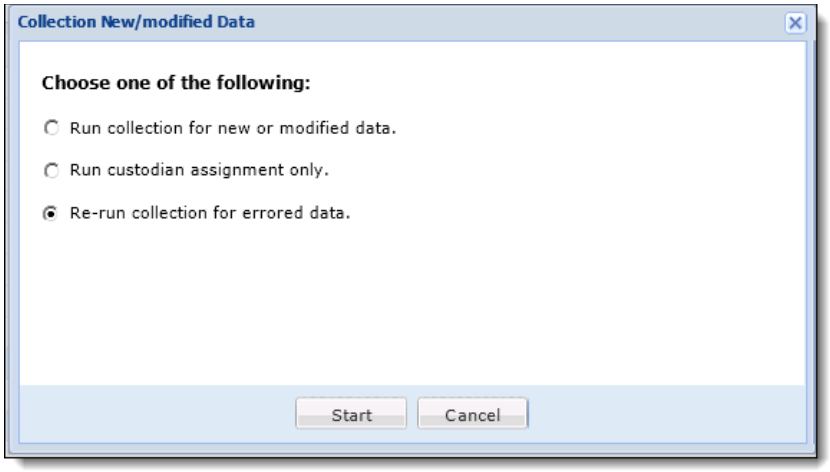
Retrying a Failed Collection Task (for Enterprise Vault and EV.cloud Sources)

Collection tasks against Enterprise Vault and EV.cloud sources which result in a "Partial Success" or "Partial Failure" status can be retried, so that only the failed items are recollected. If you re-run a collection task in a “Partial Success” status, you cannot collect errored data for the previous collection task. Also, if you re-run a collection task in a “Partial Success” status with same filter criteria within 7 days of the first run, the system does not collect a new data.



To retry a failed task

1. After first running a collection task that resulted in a “Partial Success,” click the (play) icon.
2. From the Collection New/modified Data window, select the option **Re-run collection for errored data**, and click **Start**.

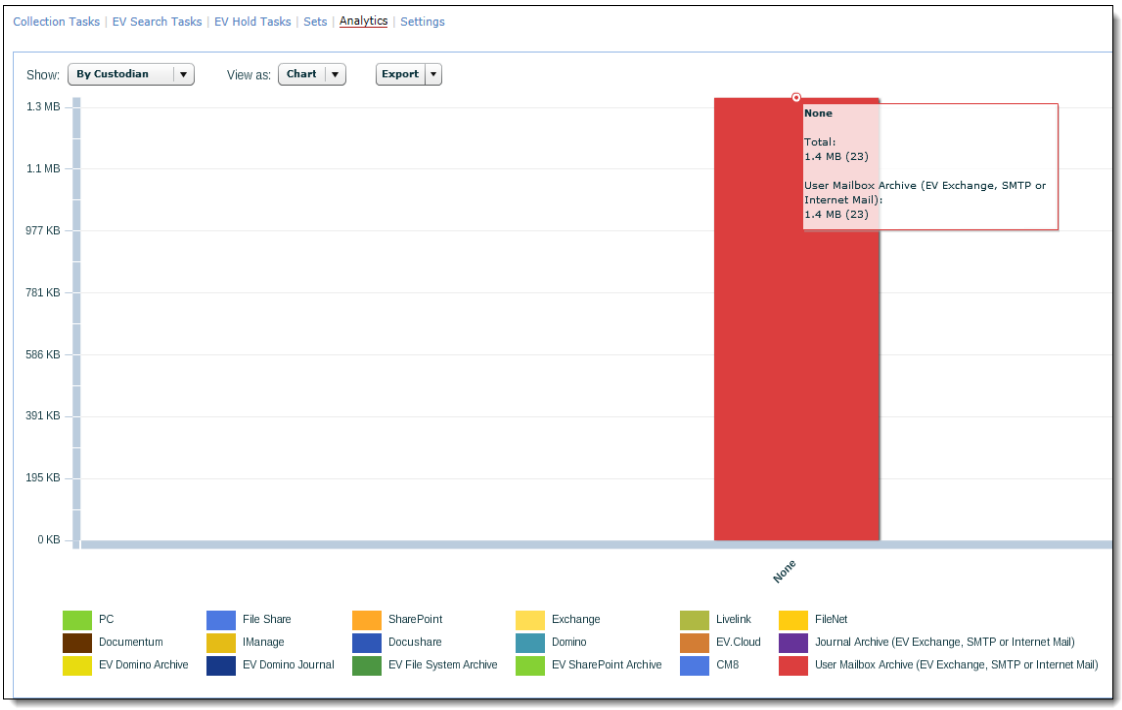


When retrying the collection for errored items only, the system attempts to collect more subsequent failed items each time the task is re-run. The system appends each new collected item to the original task.

3. From the Jobs window, you can open the job’s status log file to check whether the failed items were collected.

Analytics

From the **Analytics** screen, the bar graph or chart (or table) is updated to reflect the new item counts (from the source, and total collected). The following example shows the total number of items and items collected from the Exchange Journal Archive after successfully collecting the failed items on subsequent retries.



Note: If a collection job fails completely during data collection from an Enterprise Vault source, then you will not be able to re-run the task. A collection job may fail completely if a network outage occurs while the task is running. The ability to retry a task requires that it contain at least one item successfully collected, and at least one item that failed to be collected.

For details on how the retry feature works with Enterprise Vault Hold Tasks, see *"Creating and Managing Hold Tasks" on page 152*.

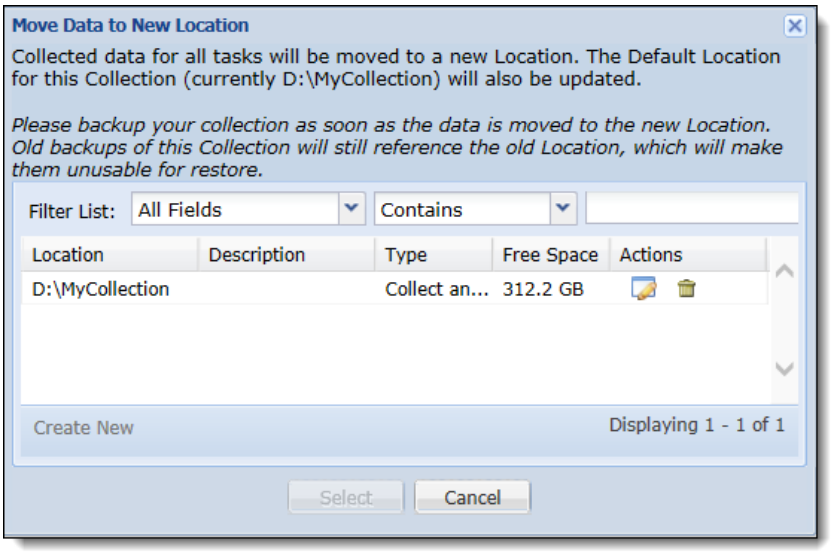
Move Collected Data to Another Location

After collection, you may want to relocate where the data is stored, either to save disk space on an appliance hard drive or server, or if all data for a particular case is required to be in a single location.

Note: You may also want to protect the data for disaster recovery purposes, and need to move the collected data from one location to another for preservation.

To move collected data

1. From **All Collections**, for each collection shown, the (move) icon appears under *Actions* column. Clicking the move icon opens the *Move Data to New Location* dialog, with a description for the selected collection.



Note: It is recommended to back up your collection once the data is moved to its new location. Backups for this collection done prior to this move will still reference the current location, and therefore cannot be restored (from previous backups).

Collected data for all tasks associated with the collection will be moved to a new location. The default location for the selected collection will also be updated.

Tip: You can sort/filter and reset your view of the *Location*, *Description*, *Free Space*, and *Actions* columns by clicking the drop-down arrow when you hover over the column header.

2. The default location is always shown. If there are locations other than the default, a list of locations displays. Only those data locations are displayed whose type is either "Collect Only" or "Collect and Export" and that are added in the groups to which the user has access. If the new location where you want to move the data to is not listed, click **Create New**. (The new location must always be different from the current location.)

3. When finished, highlight a new location, and click **Select**. Clicking **Select** initiates a "Move" job. Click **Jobs** to view the move task in the Jobs window.

   Note: While the move job is running the collection being moved is locked. It cannot be edited, archived or deleted.

More About Collection Move Jobs

Can I stop or cancel a collection move job?

Yes, collection move jobs can be stopped/cancelled, but cannot be paused and resumed. In this case, the original location will still be intact and any data that has been copied to the new location will be deleted.

What should I see if the collection move job was successful?

You should be able to see all the collection data in the new location. The location for the collection should be updated in the system, and reflected in the defensibility report.

What if the collection move job fails?

The collection move job will fail if:

- The collection contains at least one failed task
- The new location runs out of disk space due to another operation running which is using up disk space
- A network outage occurs while the collection move job is running

Can collection sets be moved?

No, collection sets cannot be moved. Metadata-only collection sets that are generated prior to moving a collection will be rendered unusable. However, collection sets containing both content and metadata that are generated prior to moving the collection can be successfully processed.

Can I back up the collection, move it, then restore from that backup?

No. Backing up a collection, performing a collection move job, then attempting to restore it after moving will render the collection useless and inaccessible. To have a backup that can be used in the new location, move the collection to its new location first and then back it up from the new location.

Running Custodian Assignments

During data collection, by default, the Veritas eDiscovery Platform Identification and Collection module assigns items to the default custodian if it identifies them with the same custodian you associated with the source during setup. When adding or editing tasks in a collection before collecting the data, you have the option of changing the default, to further narrow data collected from the source by assigning custodians based on a number of specific filter options.

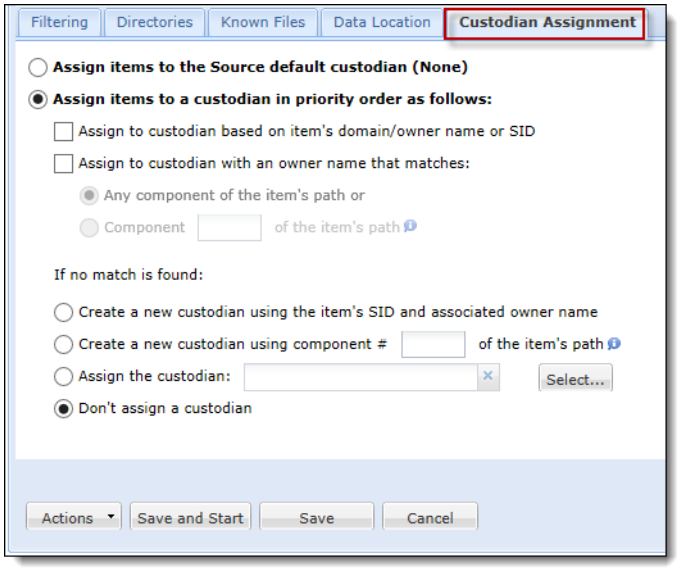
Note: If your task contains uploaded data from an OnSite collection, Veritas eDiscovery Platform will only retain custodian assignment options if the parent task is also part of the same collection. For more information, see *"Performing OnSite Collection Tasks" on page 137*.

Enterprise Vault Considerations

Before you begin: If you are assigning custodians to an Enterprise Vault Mailbox archive source, verify that discovery has been performed first, prior to custodian assignment. Since Enterprise Vault mailbox archives are email-based collections, email addresses are required for custodian assignment. Since archives themselves do not have email addresses associated with them, Active Directory for Exchange, and/or Domino discovery (depending on your source) is necessary to match archives with appropriate email addresses.

To assign custodians (before running a task)

1. From the collection within your case, select a task to edit. If you are adding a new task, see *"Add Tasks to a Collection" on page 104*. (If you are editing an existing task, you can also click the click the (Action) icon, and select **View/Edit**.
2. On the Edit Task window, click the **Custodian Assignment** tab.



3. To assign (change) custodian filtering options:

   A. To change the default selection, specify the following information.

Custodian Assignment Filter Details

Option	Description	Sub-Options
Assign items to the source's default (None)	(Default). Leaving this option selected does not assign custodians by any additional filters.	
If items are found:		
Assign items to a custodian in priority order as follows:	Assign to custodian based on item's domain/owner name or SID	Select to assign custodian only if items found match custodian's domain, owner name or SID.
	Assign to custodian with an owner name that matches:	Select to assign custodian only if items' owner name matches either: • Any component of the path, or • Specified component in the path
If no items are found:		
	Create a new custodian using the item's SID and associated owner name	If no match (or in cases where a mismatch has occurred), create the custodian based on the identified owner and SID.
	Create a new custodian using component # of the item's path	Specify the component path number for the item.
	Assign the custodian:	Type a specific custodian you want to assign, or click **Browse** to select one from your source list.
	Don't assign a custodian	Specify *not* to assign the source's default custodian to items not found for that custodian

   B. To create a template based on this collection and selected task options, click **Actions** > **Save Collection Template**. See *"Create a Collection Template" on page 125*.

   C. Click **Save** to save your custodian assignments, or click **Save and Start** to save, and immediately start running the new task.

Performing OnSite Collection Tasks

To collect data from remote sources, or from sources that are not reliably connected to your network, you can create an OnSite Collector (installer package) to be installed on an external portable drive, or directly onto a custodian's PC or Macintosh.

You can stop/restart an OnSite collection task to collect all new or modified data. However, when you stop the OnSite collection task, exit the OnSite Collector and unplug the USB drive, and later plug it back in to the same PC and start the collection task, then a new OnSite collection task is created.

When you want the collection in compressed format, make sure that the C: drive have sufficient TEMP space to temporarily store the collected data before depositing it on the USB drive. The maximum size of a file that can be stored on the USB drive depends on whether the USB drive is FAT32 or NTFS formatted volume.

For information on how to create an OnSite Collector, refer to the Identification and Collection *OnSite Collections Reference Card*.

To specify directories you want to include or exclude from PC or Mac OnSite Collection, see *"Include/Exclude Directories" on page 120*.

Running Collection Reports

Veritas eDiscovery Platform provides details about collections in two report types: Collection defensibility report and Error File List Report. These allows Collections users and legal representatives to increase the defensibility and tracking of collections.

Collection Reports

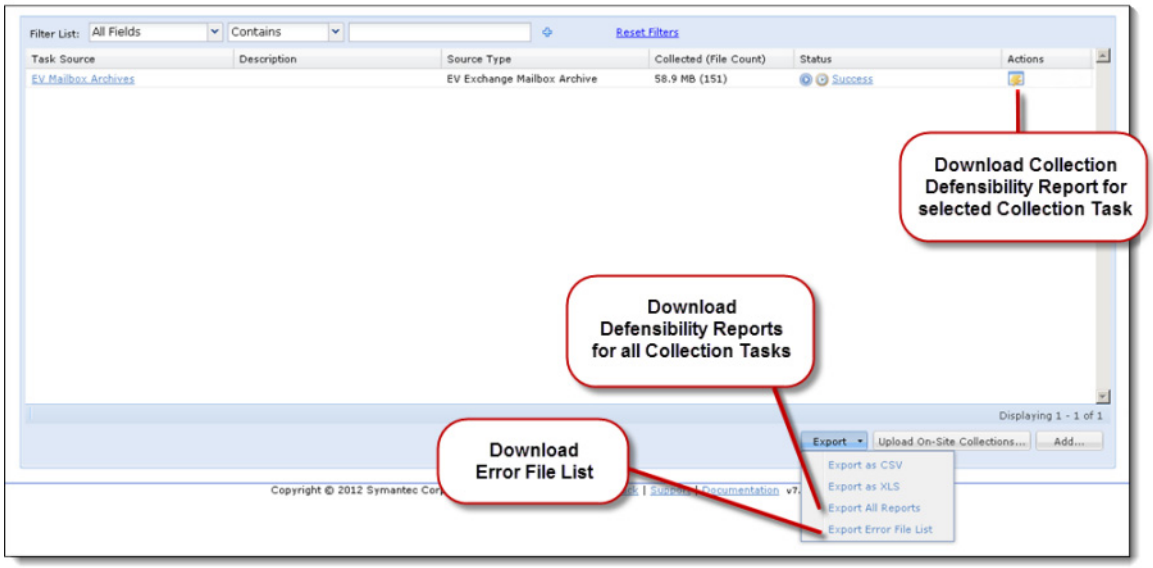
The Collection defensibility report provides evidence of all collection activity (also referred to as "Collection Task Summary Report"). Report data includes when collection tasks were run, how much data was collected, filters and custodian assignment rules used to configure the collection task, as well as recent activity and status of the collection.

Starting with 8.2 Cumulative Hotfix 4, the Enterprise Vault Collection defensibility report is improved to show detailed information about the custodian assignment, message types, custom attributes, retention categories, and policies. The defensibility report now lists the custodians which were selected in the **Email to Custodian Mapping** tab, the message types that were selected or deselected, the custom attributes that were included or excluded, and the retention categories and policies that were selected or deselected while creating the collection task.

Viewing errors in the Error File List Report is especially helpful if your collection task job finished with a "Partial Success" or "Errored" state. You can quickly access a list of files which failed or were uncollected, then check to see if they are still acceptable. Typically, for a PC collection task for example, errors may occur from open/locked files that could not be collected at the time the collection was run. Knowing the details can help you plan when to run, or schedule the task to start again.

For Documentum sources, after the Documentum file is collected, the filename is appended with the Documentum ID and the version of the file.

From the **Collections** module, on the Collection Tasks screen, you can download reports in .xlsx (Microsoft® Excel) format for either individual collection tasks, or for all collection tasks.



To download or view a report

1. From the **All Cases** view, click **All Collections**. Alternatively, select a specific case and click **Collections**.
2. On the Collection Tasks screen, do one or more of the following:
   A. For Defensibility (task summary) Report:
      - Click the (Action) icon, and select **Report** to download the report for the selected collection task.
      - On the Download window, choose to **Open** or **Save** the report. Note that the filename "CollectionTaskActivityReport" is appended with the collection task name, and task ID.

   B. For Error File List Report:
      - Click **Export**, then select **Export Error File List**.

        Note: If there were no errors contained in the collection job, no report is shown.
      - On the Download window, choose to **Open** or **Save** the report. Note that the filename "CollectionTaskActivityReport" is appended with the collection task name, and task ID.

C. For All Reports

› Click **Export**, then select **Export All Reports**. This generates the report as a job which can be viewed from the **Jobs** window.

› Click the icon under the status column to view defensibility reports for all collection tasks in that collection.

Creating and Managing Search Tasks

Veritas eDiscovery Platform 7.1.3 introduces the Enterprise Vault Search Tasks feature, allowing Identification and Collection module users with one or more Enterprise Vault sources, the ability to create, view, and edit Enterprise Vault searches, analyze results, and preview a sample of Enterprise Vault collections before the data is added to a case.

Main topics in this section:

About Enterprise Vault Search Task Activities

As part of the Identification and Collection module in Veritas eDiscovery Platform, Enterprise Vault Search Tasks provide collection users (with Enterprise Vault sources) with the ability to:

- search Enterprise Vault sources for information in their current Enterprise Vault location without collecting data
- view/edit searches and analyze results
- copy search tasks from which to create a hold or collection task
- generate search task reports for defensibility
- test filter parameters and preview selected source sample prior to collection
- delete unwanted search tasks

Collections Administrators can use Enterprise Vault search tasks to survey the size of their collection task before actual collection. Using this search feature, administrators can also "test" their search and filter parameters on a selected Enterprise Vault source before having to collect the data. Similar to Enterprise Vault Hold Tasks, this feature is useful to administrators who want greater visibility and transparency into their source data prior to collection.

This feature applies to any collection task, and all Enterprise Vault data source types (including Enterprise Vault Mailbox, Journal, File Stores, SharePoint, and other (custom) archives). This feature is particularly helpful for Enterprise Vault Collection Tasks, if administrators also use the Discovery Accelerator function of Enterprise Vault. At least one Enterprise Vault source must be discovered to be able to view and access the *Enterprise Vault Search Tasks* option.

Prerequisites

Before getting started, verify the following:

- Ensure you are running a certified version (10.0.4, 11.0, 11.0.1, or 12.x) of Enterprise Vault.
- Ensure you specify the correct credentials for the Enterprise Vault server prior to discovery.
- Change the *EsaCrawlerService* service account to an account that has access to the Enterprise Vault server.

  Note: This account must be a part of the Local Admin group on the same appliance.

- Add the service account that can access Enterprise Vault as a source account in the Veritas eDiscovery Platform utility.
- Ensure that the administrators with rights to collect from Enterprise Vault data sources also have rights to create search tasks (as well as search task users with rights to collect from Enterprise Vault data sources).

Creating and Managing Search Tasks

Similar to collection tasks for any source, you can create search tasks on Enterprise Vault sources. Follow the steps in this section for the search activities you want to perform:

- *"Create a Search" in the next section*
- *"Schedule a Search (or Run On-Demand)" on page 146*
- *"View/Edit Search Tasks" on page 147*
- *"Copy a Search Task" on page 148*
- *"Analyze Results" on page 148*
- *"Sample Preview" on page 149*
- *"Run a Report" on page 150*
- *"Delete a Search Task" on page 150*

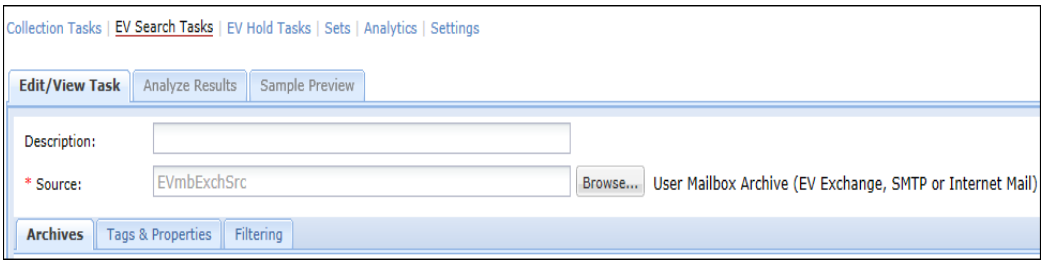
Create a Search

Create a search task when you want to search, analyze, and preview your Enterprise Vault source data before you decide to refine the search criteria, hold the data in place, or collect it. (To collect and hold the data, see *"Create a Hold and Collection Task" on page 157*.

To create a search task

1. From **All Collections**, select the collection for which you want to create a search task. (If none exists, create a new collection task. See also *"Create/Add a New Collection" on page 103*.)
2. With the collection selected, click **EV Search Tasks**.
3. On the *EV Search Tasks* screen, click **Add** (to add a search task for this collection).
4. From the Sources window, select the source containing the data you want to search, then click **Select**.

5. Enter a description for this search. (The source type and archives you selected appear in the search task. Click **Browse** to change source information.)



6. Next, specify the following information. An asterisk (*) indicates a required field.

Note: Tabbed options vary depending on Enterprise Vault Source type.

Add Task Filter Options

Field	Description	
[Top Row Tabbed Options:]	Archives	Click **Add Archives** to select which archives/vault stores to include in your hold task. **Note:** The Archive picker only displays archives that match the source's Site and Archive Type. See *"Archive Selection" on page 113* for information about these Enterprise Vault Source fields. When Enterprise Vault 11.0.1 or later is used, the Archive picker also displays the SMTP and Internet Mail archives. Select vault stores to include in your collection task, then click **Add Vault Stores**. Select an available vault store by name, archive, or size. Starting with 9.0.1, when archives are deleted on Enterprise Vault after you perform the Enterprise Vault discovery on eDiscovery Platform, these deleted archives do not appear in the Archive Picker. When vault store is selected instead of individual archives, the deleted archives are correctly filtered from the vault store. Thus, the task is prevented from resulting into Partial Success.
	Filtering	Click to filter by: **Sender/Recipient**, **Date**, **Keywords**. (See "Bottom Row Tabbed Options"). **Note:** The filter criteria specified in different filter tabs in Veritas eDiscovery Platform are ANDed together while making a search query into Enterprise Vault. Items containing all filter criteria will be returned in the results.
	Tags & Properties	Specify the Enterprise Vault tags, Enterprise Vault properties, and social media properties that you want to include in the search task.
	Directories	(For Enterprise Vault FileShare Archive only) Specify the directories you want to include or exclude. Ensure that you do not use special characters such as "$", "_", and so on in the folder or directory path. Click Add to add the directories. See *"Using special characters in the directory path" on page 118*.
	Folders	(For Enterprise Vault SharePoint Archive source only) Specify the folders you want to include or exclude. Ensure that you do not use special characters such as "$", "_", and so on in the folder or directory path. Click Add to add the directories. See *"Using special characters in the directory path" on page 118*.

Add Task Filter Options (Continued)

Field	Description	
[Bottom Row Tabbed Options:]	Sender/ Recipient	Select email filter(s) you want to apply: • **Sender or Recipient (To, From, Cc, Bcc)**, • **Sender (From)**, or • **Recipient (To, Cc, Bcc)** Enter all email addresses or display names to be searched.
	Traits	(Journal Archive (Enterprise Vault Exchange, SMTP or Internet Mail), User Mailbox Archive (Enterprise Vault Exchange, SMTP or Internet Mail), and Enterprise Vault Domino Archive Sources only): Allows you to filter by: message type, attachments extensions, custom attributes, and to include or exclude non-indexed items. For message type, indicate whether to include or exclude specified types (or select all), such as: Exchange Email, Instant Messaging, Bloomberg, Fax, or DXL. You can filter by both keyword and attachment extension types. However, the parent message and its attachments are indexed together. So when both filtering traits are applied together, keywords will be filtered based on the whole message, not only to the matching attachments. The parent message will always be collected. **Note:** When you filter by attachments extensions for .eml and .msg, the emails with these extensions are not searched which results in non-collection of these emails. The collection count does not match with the original count. This is a known issue on Enterprise Vault side. For custom attributes, specify the values to restrict collection, and indicate whether to include or exclude documents based on specified custom attribute criteria, such as String, Number, or Date, with corresponding values. Add more lines to enter additional criteria. (Values will be treated as an 'OR' expression.) Non-indexed items are excluded (by default). Click to filter by items that have not been indexed in Enterprise Vault.
	Retention and Policy Tag	(Journal Archive (Enterprise Vault Exchange, SMTP or Internet Mail), User Mailbox Archive (Enterprise Vault Exchange, SMTP or Internet Mail), and Enterprise Vault Domino Archive Sources only): For retention tags, indicate whether to include or exclude selected categories by name: Default Retention Tag, Domino Journaling, Exchange Mailbox, and Exchange Journaling. All existing policies appear in the Known Policies box. These are policies that may have been discovered, or created after initial Enterprise Vault source discovery. (Check also **System > Directories and Servers > Veritas EV** and click the **Policies** tab.) Click **Add Policy** to create a new policy.
	Keywords	Filter documents that contain only certain keywords. Enter one or more keywords. (Click the icon to add additional lines for each keyword.) For Enterprise Vault sources, Keyword filtering provides the option of listing any, all, or none of the phrases entered. All three categories can be grouped together by an AND expression.

Add Task Filter Options (Continued)

Field	Description	
	Date	Filter by Date. Click the drop-down menu to select a filter type, and if applicable, enter or select a date. **Note:** Indexes of an archive are usually spread across multiple index volume sets. In earlier releases of Veritas eDiscovery Platform, when a date range filter is used for any Enterprise Vault task, all the index volume sets were searched before applying the date filter on an Enterprise Vault task. Starting with 8.0, the search time is optimized. The system now skips the index volume sets which do not fall into the specified date range filter. If you do not want to use this enhancement and want to get all index volume sets to be searched for the specified date range, you should contact Veritas Customer Support. The default time zone is shown. To change time zone, go to **System**, and click **Settings**.
	E-Mail to Custodian Mapping	(For Journal Archive (Enterprise Vault Exchange, SMTP or Internet Mail) and Domino Journal Archives sources only) Filter emails by Sender or Recipient (To, From, Cc, Bcc), Sender (From), Recipient (To, Cc, Bcc). By default, source's default custodian is used for custodian mapping.
	File Extensions	(For Enterprise Vault FileShare and SharePoint sources only) Filter data by file extensions. Specify the file extensions that you want to include in the search task. By default, filtering by file extensions is disabled.
	Author	(For Enterprise Vault SharePoint sources only) Filter data by authors. Specify the custodians or authors that you want to include in the search task. By default, filtering by author is disabled.

7. (Optional) To create a template based on this search task, click **Actions** > **Save Collection Template**. Continue to step 8. (The next time you want to apply this template to a task, select **Actions** > **Load Collection Template**, and select it from the Templates window.)

8. Click **Save**, or **Save and Start** depending on when you want to run the search. (No new sources can be added to the current search after starting.) *"Schedule a Search (or Run On-Demand)" in the next section*.

   View progress and status of your search task from the *Jobs* window. After the search has completed, the task appears on the main *EV Search Tasks* screen. The *Size* column displays the total size (and file count) of the items targeted by the search. To view and analyze your search results, see *"Analyze Results" on page 148*.

Schedule a Search (or Run On-Demand)

Similar to Hold tasks, you can schedule a search to run on a specific date and time (or simply start the search task by running it on demand.) Scheduling recurring runs allows you to continually search and refine your source data in preparation for collection.

To schedule a search task

1. From the Status column, click the (schedule) icon for the search you want to schedule. (Alternatively, click (run) to start the search immediately).

   The *Schedule Search* window opens. (If the search task has already been run successfully, the window displays *Schedule Recurring Search*.)

2. Enter the Start Date/Time.

   If you are scheduling an incremental search task:

   – Select the frequency of the incremental search task: *Once*, *Daily* or *Weekly*. If more than once, then indicate the number of occurrences after which to end the run. (There is no maximum limit of occurrences for search tasks.) You can also schedule the task to recur after the search job is finished, similar to collection tasks. Refer to *"Schedule a Recurring Collection Task" on page 128*.

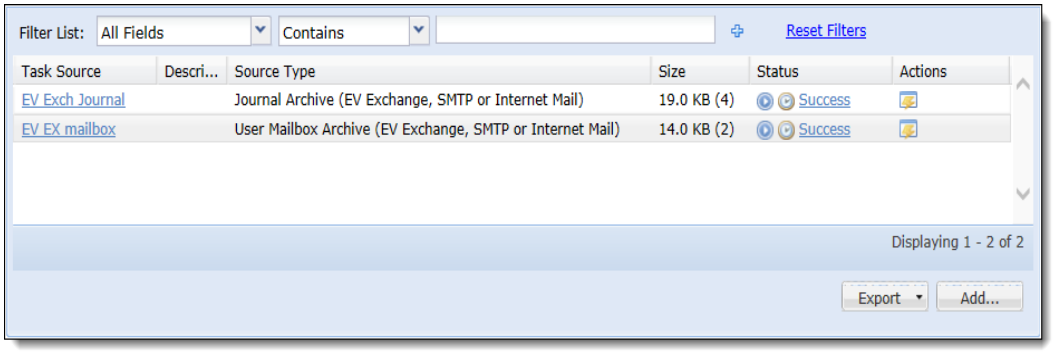
3. Click **OK** to schedule, or **Clear Schedule** to discard changes and reschedule. The date and time when the search is scheduled to run appears in the Status column.

   For recurring scheduled task (for searches already run successfully), the *Next Schedule Run* and *Final Schedule Run* fields also appear, to display what you have scheduled. After completing successfully, statistics reflect the size, and file count of items found, plus the date/time stamp of the run.

View/Edit Search Tasks

After you have created several searches, a quick way to manage them is to view a summary of search task information. Check statistics such as the file count, and size in your search results before collecting data.

The search screen displays all searches by *Task Source*, *Description*, *Source Type*, *Searched Item* Size *(File Count)*, and *Status*.



The run and schedule icons appear for tasks not yet started, then reappear after the search task has completed successfully.

Copy a Search Task

Using the copy function of the Search task feature allows you to save the same task data for later use in a collection, Enterprise Vault hold, or another search task.

To copy a search task

1. From the Actions column, click the (Action) icon and select **Copy**.
2. Select to either **Copy as Collection Task**, **Copy as EV Search Task**, or **Copy as EV Hold Task**.

   The new task opens in their respective locations (*Collection Tasks*, *EV Search Tasks*, or *EV Hold Tasks* screen) within Identification and Collection module. allowing you to add/change the archive/vault sources, or filters. Alternatively, you can specify additional collection criteria if you are copying the search as a collection task. For example, you can choose to specify the location and Custodian Assignments.
3. Save, or start/apply the task:
   A. For collection or search tasks, click **Save** (to run later) or **Save and Start** to save the task and immediately run the collection or search. For more information on collection tasks, see *"Creating a Collection and Running Tasks" on page 103*.
   B. For hold tasks, click **Save** (to run later) or **Apply Data Hold** to save the task and immediately apply a hold on the data. For more information about EV Hold tasks, see *"Creating and Managing Hold Tasks" on page 152*.

Analyze Results

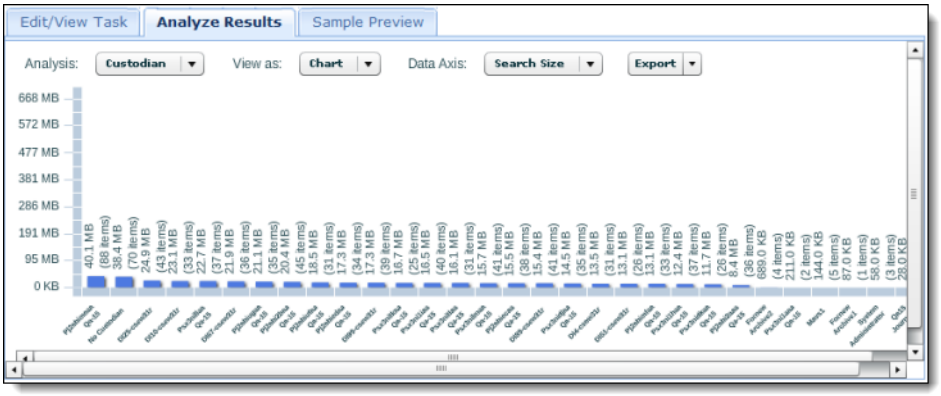
After running a search task, you can view and analyze the results. (The **Analyze Results** tab becomes available only after a search completes successfully.)

Results analysis allows you to check for any adjustments you may need to make in your filter parameters for your next search, hold, or collection task. For example, you may want to reduce the document set based on which time ranges contribute heavily to the search results, or you may discover unusual gaps or spikes in data over time.

To analyze search task results

1. From the Actions column, click the (Action) icon and select **Analytics**.

   The **Analyze Results** tab opens, displaying your search results. (Chart view opens by default).



In this example, the bar graph chart illustrates the amount of data targeted for each day/ month/year (depending on the range), providing insight into which ranges to exclude from the collection.

2. Click any of the drop-down options to change your preferences: Analysis (*Custodian* or *Timeline*), View as (*Chart* or *Table*), and Data Axis (*Search Size* or *Relative*). The system displays data in two views:

Analyze Results View

By	Displays
Date	Size of the data against time, similar to preprocessing displays. (For Enterprise Vault SharePoint and File store archive sources, the X-axis label changes to *Date created.) You can also sort the data for month, quarter, or year using the Show by drop-down options.*
Sender/ Author	Size of the data (Y axis) against the custodians (authors) of the files (X axis). Also note: • Chart only displays the top 1000 custodians (by file size); all other custodians are aggregated in an "Other" category. • Columns are mutually exclusive, since there is only one sender per item. • For non-email messages, the sender is identified as the owner of the file.

Sample Preview

On searches that have completed successfully, you can view the individual documents from your search results. This is especially helpful in evaluating your search criteria either for a new search, prior to a hold in place, or prior to collection. Similar to reviewing documents (in Analysis & Review), each document appears in simple detail mode, allowing you to navigate through each document, and download attachments.

For the container files such as zip files or archive files, Sample Preview first shows the list of files and then shows the content of all files. Sample Preview also shows the content of the MSG and EML files.

Caveats of Sample Preview

- Sample Preview does not support hit-highlighting or further culling down of the search results.
- Sample Preview fails if the search task fails.
- Item preview might fail because of item retrieval failures.

To sample a preview of your search

- From the Actions column, click the (Action) icon and select **Preview**. This opens the **Sample Preview** tab, allowing you to view the data as individual documents/items from your search results set for the selected Enterprise Vault source. The sample size is 20 items per page, and the items will appear in random order.

  Note: If a failure occurs when attempting to retrieve an HTML preview for a set of documents, the system displays a message explaining the reason for the failure.

Run a Report

To download or view a report

1. From the Actions column, click the (Action) icon and select **Report** to download the Search Task defensibility report for the search task you want to view.
2. On the Download window, choose to **Open** or **Save** the report. Note that the filename "**SearchTaskDefensibilityReport**" is appended with the case name, and task ID.

   The report (Microsoft Excel file) displays creation date/time, and time zone information, as well as Task Details, Filters, and Task Activity and Status associated with the hold.

To export all search task information

1. For All EV Search Task Reports, click **Export**, then select **Export All Reports**.
2. At the prompt, click **OK**. This generates a summary "Defensibility Report" job for all search tasks.
3. View report results in the Jobs window. In the Status column, click the link to download the report. (Choose to **Open** or **Save** the report. Note that the filename is appended with the case name, and task ID.)

Delete a Search Task

To delete a search task

1. From the Actions column, click the (Action) icon and select **Delete** for the search task you want to delete.
2. If the search had been run and completed successfully, the Delete Confirmation window opens.
3. Click **Yes** to delete the task.

Creating and Managing Hold Tasks

For users with one or more Enterprise Vault sources, Veritas eDiscovery Platform adds the Enterprise Vault Hold feature, allowing Identification and Collection module users to hold in place documents identified in their Enterprise Vault archives that may be needed, with or without collection.

Main topics in this section:

About Enterprise Vault Hold Activities

As part of the Identification and Collection module in Veritas eDiscovery Platform, Enterprise Vault Hold Tasks provide collection users (with Enterprise Vault sources) with the ability to:

- place a "hold" on information in its current Enterprise Vault location without collecting or copying the data
- (for some data which is already on hold) automatically hold newly-added data in its current location
- both hold and collect Enterprise Vault data
- view/report statistics on Enterprise Vault hold tasks

Placing Enterprise Vault data on hold suspends the data from any automatic disposition or deletion. EV Hold Tasks are useful for Collections Administrators who want greater control over, and visibility into their Enterprise Vault data prior to, or in conjunction with collections. When the data is no longer needed, administrators can release their holds on data with, or without deleting the hold task.

Note: This feature applies only to users with Enterprise Vault archive sources.

Prerequisites

Before getting started, verify the following:

- Ensure you are running a supported version of Enterprise Vault.
- Ensure you specify the correct credentials for the Enterprise Vault server prior to discovery.
- Change the *EsaCrawlerService* service account to an account that has access to the Enterprise Vault server.

  Note: This account must be a part of the Local Admin group on the same appliance.
- Add the service account that can access Enterprise Vault as a source account in the Veritas eDiscovery Platform utility.

- Ensure that the administrators with rights to collect from Enterprise Vault data sources also have rights to create hold tasks (as well as hold task users with rights to collect from Enterprise Vault data sources).

Creating and Managing Hold Tasks

Similar to search tasks for Enterprise Vault sources, you can also create hold tasks on Enterprise Vault sources. Follow the steps in this section for the type of hold activities you want to perform:

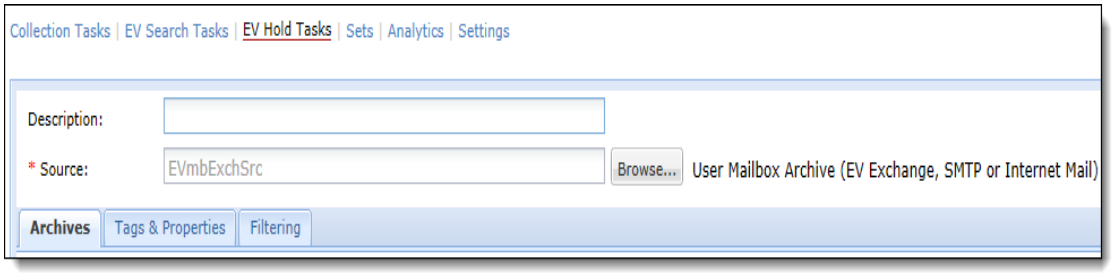
- *"Create a Hold" in the next section*
- *"Schedule a Hold" on page 155*
- *"Create a Hold and Collection Task" on page 157*
- *"View/Report Hold Statistics" on page 158*
- *"Edit/Re-Apply a Hold Task" on page 159*
- *"Copy a Hold Task" on page 160*
- *"Release a Hold" on page 161*

Create a Hold

To place Enterprise Vault data on hold, you create hold tasks. To collect and hold the data at the same time, see *"Create a Hold and Collection Task" on page 157*.

To create a hold

1. From **All Collections**, select the collection for which you want to create a hold. (If none exists, create a new collection task. See also *"Create a Hold and Collection Task" on page 157*.)
2. With the collection selected, click **EV Hold Tasks**.
3. On the *EV Hold Tasks* screen, click **Add** (to add a hold task for this collection).
4. From the Sources window, select the Enterprise Vault source containing the data you want to hold, then click **Select**.
5. Enter a description for this hold. (The source type and archives you selected appear in the hold. Click **Browse** to change source information.)



6. Next, specify the following information. An asterisk (*) indicates a required field.

Add Task Filter Options

Field	Description	
[Top Row Tabbed Options:]	Archives	Click **Add Archives** to select which archives/vault stores to include in your hold task. **Note:** The Archive picker only displays archives that match the source's Site and Archive Type. See *"Archive Selection" on page 113* for information about these Enterprise Vault Source fields. Select vault stores to include in your collection task, then click **Add Vault Stores**. Select an available vault store by name, archive, or size. Starting with 9.0.1, when archives are deleted on Enterprise Vault after you perform the Enterprise Vault discovery on eDiscovery Platform, these deleted archives do not appear in the Archive Picker. When vault store is selected instead of individual archives, the deleted archives are correctly filtered from the vault store. Thus, the task is prevented from resulting into Partial Success.
	Tags & Properties	Specify the Enterprise Vault tags, Enterprise Vault properties, and social media properties that you want to include in the search task.
	Filtering	Click to filter by: **Sender/Recipient**, **Date**, **Keywords**. (See "Bottom Row Tabbed Options").
	Directories	(For Enterprise Vault FileShare Archive only) Specify the directories you want to include or exclude. Ensure that you do not use special characters such as "$", "_", and so on in the folder or directory path. Click **Add** to add the directories. See *"Using special characters in the directory path" on page 118*.
	Folders	(For Enterprise Vault SharePoint Archive source only) Specify the folders you want to include or exclude. Ensure that you do not use special characters such as "$", "_", and so on in the folder or directory path. Click Add to add the directories. See *"Using special characters in the directory path" on page 118*.

Add Task Filter Options (Continued)

Field	Description	
[Bottom Row Tabbed Options:]	Sender/ Recipient	Select email filter(s) you want to apply: • **Sender or Recipient (To, From, Cc, Bcc)**, • **Sender (From)**, or • **Recipient (To, Cc, Bcc)** Enter all email addresses or display names to be searched.
	Traits	(Journal Archive (Enterprise Vault Exchange, SMTP or Internet Mail), User Mailbox Archive (Enterprise Vault Exchange, SMTP or Internet Mail), and Enterprise Vault Domino Archive Sources only): Allows you to filter by: message type, attachments extensions, custom attributes, and to include or exclude non-indexed items. For message type, indicate whether to include or exclude specified types (or select all), such as: Exchange Email, Instant Messaging, Bloomberg, Fax, or DXL. You can filter by both keyword and attachment extension types. However, the parent message and its attachments are indexed together. So when both filtering traits are applied together, keywords will be filtered based on the whole message, not only to the matching attachments. The parent message will always be collected. **Note:** When you filter by attachments extensions for .eml and .msg, the emails with these extensions are not searched which results in non-collection of these emails. The collection count does not match with the original count. This is a known issue on Enterprise Vault side. For custom attributes, specify the values to restrict collection, and indicate whether to include or exclude documents based on specified custom attribute criteria, such as String, Number, or Date, with corresponding values. Add more lines to enter additional criteria. (Values will be treated as an 'OR' expression.) Non-indexed items are excluded (by default). Click to filter by items that have not been indexed in Enterprise Vault.
	Retention and Policy Tag	(Journal Archive (Enterprise Vault Exchange, SMTP or Internet Mail), User Mailbox Archive (Enterprise Vault Exchange, SMTP or Internet Mail) and Enterprise Vault Domino Archive Sources only): For retention tags, indicate whether to include or exclude selected categories by name: Default Retention Tag, Domino Journaling, Exchange Mailbox, and Exchange Journaling. All existing policies appear in the Known Policies box. These are policies that may have been discovered, or created after initial Enterprise Vault source discovery. (Check also **System > Directories and Servers > Veritas EV** and click the **Policies** tab.) Click **Add Policy** to create a new policy.
	Keywords	Filter documents that contain only certain keywords. Enter one or more keywords. (Click the icon to add additional lines for each keyword.) For Enterprise Vault sources, Keyword filtering provides the option of listing any, all, or none of the phrases entered. All three categories can be grouped together by an AND expression.

Add Task Filter Options (Continued)

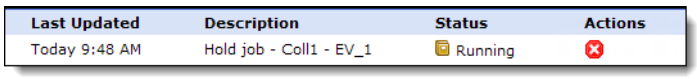
Field	Description	
	Date	Filter by Date. Click the drop-down menu to select a filter type, and if applicable, enter or select a date. **Note:** Indexes of an archive are usually spread across multiple index volume sets. In earlier releases of Veritas eDiscovery Platform, when a date range filter is used for any Enterprise Vault task, all the index volume sets were searched before applying the date filter on an Enterprise Vault task. The system skips the index volume sets which do not fall into the specified date range filter. If you do not want to use this enhancement and want to get all index volume sets to be searched for the specified date range, you should contact Veritas Customer Support. The default time zone is shown. To change time zone, go to **System**, and click **Settings**.
	E-Mail to Custodian Mapping	(For Journal Archive (Enterprise Vault Exchange, SMTP or Internet Mail) & Domino Journal Archives sources only) Filter emails by Sender or Recipient (To, From, Cc, Bcc), Sender (From), Recipient (To, Cc, Bcc). By default, source's default custodian is used for custodian mapping.
	File Extensions	(For Enterprise Vault FileShare and SharePoint sources only) Filter data by file extensions. Specify the file extensions that you want to include in the hold task. By default, filtering by file extensions is disabled.
	Author	(For Enterprise Vault SharePoint Archive only) Filter data by authors. Specify the custodians or authors that you want to include in the hold task. By default, filtering by author is disabled.

7. (Optional) To create a new collection task based on the same filtering criteria, select the option to: **Also create a Collection task with the same attributes**. (See *"Create a Hold and Collection Task" on page 157*.)

   Note: The collection task will not automatically run; collection tasks must be started manually.

8. (Optional) To create a template based on this hold task, click **Actions** > **Save Collection Template**. Continue to step 7. (The next time you want to apply this template to a task, select **Actions** > **Load Collection Template**, and select it from the Templates window.)

9. Click **Apply Data Hold** to hold the data and immediately start running the new task. Once started, the job can be viewed from the *Jobs* window.



   For hold tasks that complete successfully, you will not be able to add any new archives, and the data cannot be deleted until the hold is released. See *"Release a Hold" on page 161*.

   Alternatively, click **Save** to save the task (without running). Once the task is saved, you can make a copy of this task. See *"Copy a Hold Task" on page 160*.

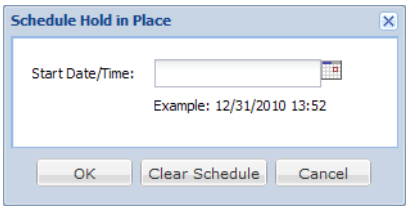
Schedule a Hold

You can schedule the hold to run on a specific date and time (or simply re-apply the hold task by running it on demand. See *"Edit/Re-Apply a Hold Task" on page 159*.) Scheduling recurring runs allows you to place new items on hold in tasks that have already completed successfully.

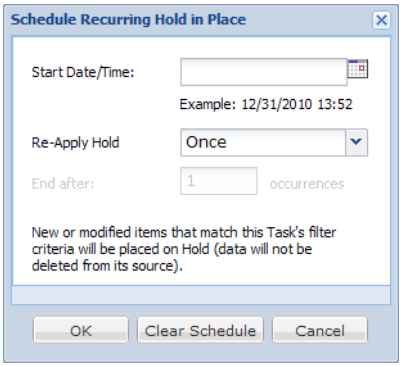
To schedule a hold task

1. From the Status column, click the (schedule) icon for the hold you want to schedule.

   The Schedule Hold Task window opens.



   (If the hold task has already been run successfully, the window displays "Schedule Recurring Hold Task".)



2. Enter the Start Date/Time.

   If you are scheduling an incremental hold task:

   – Select the frequency of the incremental hold task: *Once*, *Daily* or *Weekly*. If more than once, then indicate the number of occurrences after which to end the run. (There is no maximum limit of occurrences for Data Hold Tasks.) You can also schedule the task to recur after the hold is finished, similar to collection tasks. Refer to *"Schedule a Recurring Collection Task" on page 128*.

   Note: Note that new or modified items that match the task's filter criteria will be placed on hold (data will not be deleted from the source).

3. Click **OK** to schedule, or **Clear Schedule** to discard changes and reschedule. The date and time when the hold is scheduled to run appears in the Status column.

   For recurring scheduled task (for holds already run successfully), the description "Hold Re-applied" displays, with the status "Data Hold Task will run again at [date/time]". The *Next Schedule Run* and *Final Schedule Run* fields also appear, to display what you have scheduled. After completing successfully, statistics reflect the size, and file count of items held, plus the date/time stamp of the run.

Create a Hold and Collection Task

When you want to hold Enterprise Vault source data that you also need to collect, you can create both a hold and collection tasks at the same time. You can either create a hold task based on a collection task, or a collection task based on a hold. (Creating a collection task can also be done by editing or copying a hold task. See also *"Edit/Re-Apply a Hold Task" on page 159* and *"Copy a Hold Task" on page 160*.)

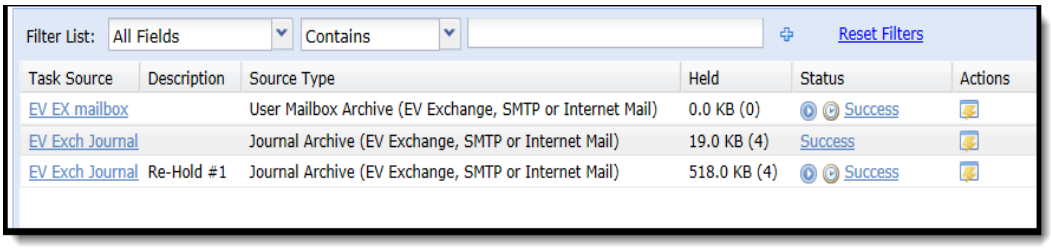
To create a hold and collection task

1. Choose a method:
   A. Create a new hold from a collection task:
      › From **All Collections**, select the Enterprise Vault collection you want to hold, then click **Hold**. Continue to step 2.
   B. Create a new collection from a hold task:
      › From **All Collections**, click **Hold**.
      › Select the hold for the Enterprise Vault data you want to collect. Continue to step 2.
2. Click **Add**.
3. Enter a description for this hold or collection, and the Source. Click **Browse** to select the source from its directory location.
4. Depending on whether this is a hold or collection task, select the option to:
   A. **Also create a Collection task with the same attributes**
   B. **Also create a Data Hold task with the same attributes**
   The new task will not automatically run; these "also" created tasks must be started manually. From the *EV Hold Tasks* or *Collection Tasks* screen, select the task, then click the (run) icon to run the hold or collection.
5. (Optional) If you are creating a collection task, and want to use this as a template, click **Actions** > **Save Collection Template**. Continue to step 6. (The next time you want to apply this template to a task, select **Actions** > **Load Collection Template**, and select it from the Templates window.)
6. Click **Save** to save the hold task (without running). Alternatively, to run the hold task, click **Apply Data Hold** (or for a collection, **Save and Start**).

View/Report Hold Statistics

After you have created several holds, a quick way to manage them is to view a summary of hold task information. Check statistics such as the file count, and size in your search results before collecting data or releasing the hold.

The *EV Hold Tasks* screen displays all holds by *Task Source*, *Description*, *Source Type*, *Held (File Count)*, and *Status*.



The run and schedule icons appear for tasks not yet started, then reappear after the hold task has completed successfully.

The following are all possible hold task Status values from corresponding actions:

User Action, Status, and Result

Action	Status	Result
Save	**Not Started**	Hold saved, but not applied
Apply Data Hold	**Submitted**	Job was started
	Running	System is preparing to aggregate the data
	Aggregating	System is aggregating the data
	Success	Hold ran, and completed successfully
	Failure	Hold failed. (View log details from Jobs window)
(Delete) icon: *Keep Task but Release Hold*	**Released Hold**	Hold has been released, but task was not deleted

To download or view a report

1. From the Actions column, click the (report) icon to download the Hold Task defensibility report for the hold task you want to view.
2. On the Download window, choose to **Open** or **Save** the report. Note that the filename "**HoldTaskDefensibilityReport**" is appended with the hold task name, and task ID.

   The report (Microsoft Excel file) displays creation date/time, and time zone information, as well as Task Details, Filters, and Task Activity and Status associated with the hold.

To export all hold task information

1. For All Hold Reports, click **Export**, then select **Export as CSV** or **Export as XLS**. This generates a summary report for all hold tasks.

2. On the Download window, choose to **Open** or **Save** the report. Note that the filename "tasks" is appended with the date, and task ID.

Edit/Re-Apply a Hold Task

Hold tasks that have not been started yet can be edited before starting. However, once a hold task has been started, it can no longer be edited.

Re-applying a hold task places only new items on hold. You can re-apply the same hold multiple times either by using the Edit action, or by clicking the (run) icon after a hold task has already finished running. To schedule re-applying the hold task for a later date/time, see *"Schedule a Hold" on page 155*.

To edit a hold task

1. From the Actions column, click the (Edit) icon to open the hold task you want to view/change or create new collection tasks.

   Alternatively, if the hold has already finished running, from the Status column, click the (run) icon. This will automatically re-apply and run the hold using the same attributes.

2. Choose one or more of the following:

   A. If the task has not been started, you can:

   - Add archives, vaults, change filters.
   - Create a duplicate hold and save or run: Click **Apply Data Hold**.
   - The existing hold task is run with the same filters and parameters, without creating a new task for each run.
   - Create a new collection or data hold task using the same attributes. Follow steps 4-5 in *"Create a Hold and Collection Task" on page 157*.

   B. If the task has already run, the message "This hold has already been run" appears. You can:

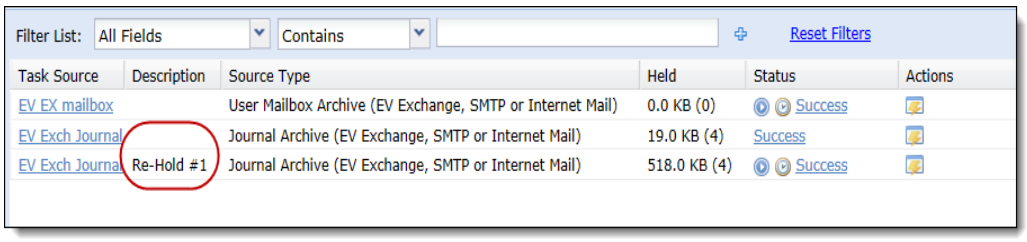
   - Create a new collection or data hold task using the same attributes. Follow steps 4-5 in *"Create a Hold and Collection Task" on page 157*.

     Note: The collection task is not automatically run at the time you create the collection from a hold. You must run it manually from **All Collections > Collect**.)

› Re-apply the hold: Click **Apply Data Hold**.

› The existing hold task is run again with the same filters and parameters, without creating a new task for each run.

For holds re-applied, when completed successfully, the description "Re-Hold" appears with numbered tasks for quick identification.



Alternatively, click **Save** to save the hold task without running (or re-applying) the hold.

Copy a Hold Task

Hold tasks can be copied at any time into either a hold or a collection task.

To copy a hold task

1. From the Actions column, click the (Action) icon and select **Copy**. This copies the hold task to create a new task.
2. Select to either **Copy As Data Hold Task** or **Copy As Collection Task**.

   The hold task opens allowing you to add/change the hold's archive/vault sources, or filters. Alternatively, you can specify additional collection criteria if you are copying the hold to as a collection task. For example, you can choose to specify the location and Custodian Assignments.
3. Save, or start/apply the task:

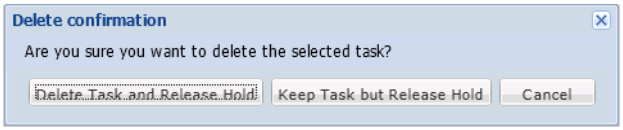
   A. For collection tasks, click **Save** (to run later) or **Save and Start** to save the task and immediately run the collection.

   B. For hold tasks, click **Save** (to run later) or **Apply Data Hold** to save the task and immediately apply a hold on the data.

Release a Hold

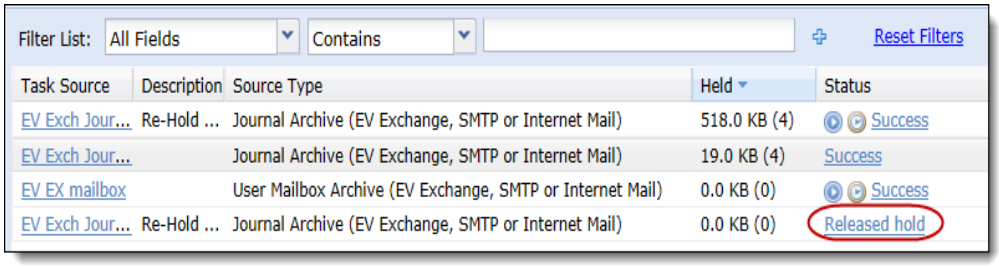
To release a hold

1. From the Actions column, click the (delete) icon for the hold you want to release and keep or delete.
2. If the hold had been run and completed successfully, the Delete Confirmation window opens.



3. Choose whether to delete or keep the task record. In either case, the hold will be released. Select **Delete Task and Release Hold** or **Keep Task but Release Hold**.

   For tasks released, but not deleted, the Status column for the task shows "Released Hold".



Retry Release Hold

The default time out for which Veritas eDiscovery Platform waits for Enterprise Vault to release holds is set as 24 hours. Veritas eDiscovery Platform does not release holds in batches. In case the query takes longer time and Veritas eDiscovery Platform Release Hold tasks fails, then you can configure the following properties to set the default time out duration, number of retry attempts, and the interval between two retry attempts. You can configure these properties from **System** > **Support Features** > **Property Browser**.

- **esa.icp.ev.hold.timeout=86400**
- **esa.icp.collection.ev.releaseHolds.RetryCount=3**
- **esa.icp.collection.ev.releaseHolds.RetryWaitMilliSec=300000**

Enterprise Vault Hold Tasks and Release Guidelines

Review the following guidelines for effectively holding, releasing, and if needed, re-applying Enterprise Vault Holds.

In the Identification & Collection module, holds are applied by running a Hold task, then released by deleting the task that applied the hold. (See *"Release a Hold" on page 161*.) However, once you have applied an Enterprise Vault hold, it cannot be released by restoring (through a backup) a version of the Identification and Collection module that does not contain the Enterprise Vault hold.

Similarly, once Enterprise Vault holds have been released, it is not possible to reapply them by restoring a version of the Identification and Collection module in which the Enterprise Vault holds are set. If you need to re-apply a released hold, it is recommended to copy and rerun the task. (See *"Copy a Hold Task" on page 160*.)

Creating, Analyzing and Processing Collections

This sections describes how to organize your collected data into sets and how to analyze and filter that data in preparation for case management:

About Collection Sets and Analytics

A collection set is a subset of your collected data. Collection sets help you organize your collected data in a defensible and meaningful way that supports the case you create for the Case Administrator to manage and produce. Initially, you may collect more data than will actually process and use for a given case. Creating a collection set is a logical way to segment and further filter the data you eventually process/index and prepare for Search, Analysis, Review, and Production.

Collection Administrators can also preview collected data with the ability to analyze results of items from collections of Enterprise Vault sources. For steps on how to preview collection results, see *"Creating and Managing Search Tasks" on page 141*.

Managing Collection Sets

Creating a new collection set

After you collect data from all sources (in your Active Directory network or other archive source, and from any OnSite Collection) you can organize and filter your collections into sets. Sets can be created from one collection, containing one or more tasks. When you create a collection set, you will be able to further narrow the data, including file types and date range.

A user can create a new collection set for only those collection tasks whose:

- sources and locations are part of the same access group to which the user is added, or
- sources and locations are global

The system administrator must add the existing sources and locations which are either part of an access group or are global to the same access group to which the user is added so that the user gets privileges to create a collection set that consists of these sources and locations.

Editing a collection set

You can edit only the name of an existing collection set and the group access permissions. While editing the collection set, the same group access privileges appear which were added while creating that collection set.
A user can only edit the collection sets which are either global or are part of the same access group to which the user is added.

If you have upgraded to 9.0, the existing collection sets are considered as global, i.e. open to all users. Users who have collection rights to manage collection sets can enforce group access security permissions by editing the existing collection sets.

If a restricted collection set needs to be made global, the sources and locations that are associated with that collection set must be made global first. If the user does not have permissions to make the sources and locations global, then he must contact the System Administrator.

Moving a collection set

You can also move a global collection sets or a collection which is part of an access group across appliances. Such a collection set will be available as a global collection set on the target appliance, and can only be used as a processing source on the Processing, and Analysis & Review (PAR) module.

Creating a collection set

Follow the steps in this section to create a collection set from your collected data.

To create a collection set

1. In the **Collections** module, within a selected case, click **Collections**.
2. Select the collection containing the data you want to filter into a set, then click **Sets**.
3. From the Sets screen, click **Add**.

A preprocessed view of your data appears.

4. To view the collection data before filtering into a set:

   A. Choose from the following filter options:

Adding Collection Sets: Collection Data View

Filter	Description
(Analysis) Summary, Document Type, Custodian, Error Type	View data as a high-level summary, by the type of documents collected, by custodian, or by error type. Select Error Type to view any errors that may have occurred during data collection, such as files that were locked, or encrypted. These errors types include: • could not read file • could not determine file ID • could not calculate MD5 • could not de-NIST • could not access directory • container type not supported • could not handle unicode errors in path • error evaluating the filter expression • compression error • validation error (typically a checksum failure) **Note:** When filtering by custodian for collection, the owner name will only be collected if the Windows user for the collection is running as the source account (or *EsaApplicationService* user if there is no account on the source), and it is in the domain where the owner name is kept. **Note:** The Error Type filtering is not supported for EV.cloud collections.
(View As:) Chart, or Table	Change the output view of the data formatted as a graphic chart or in table form.

Adding Collection Sets: Collection Data View

Filter	Description
(Data Axis:) Collection Size, or Relative	View data by the size of the collected data, or relative to other data points in the collection.
Export	Choose whether to export this data view as a CSV (comma separated values), or XSL (Microsoft Excel) file for reporting purposes. You can also export the "Error File List" file. **Note:** The "Error File List" file is not available for EV.cloud collections.

5. Select options to include in, or exclude from your collection set:

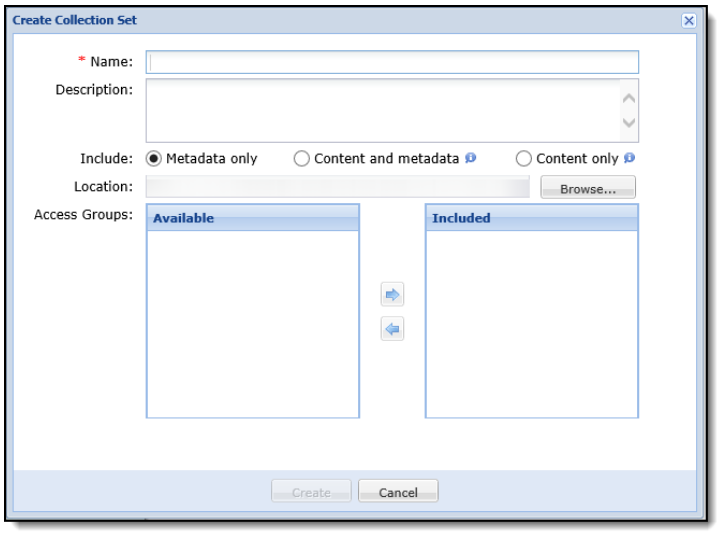
   A. Choose data types to include in your collection set by using the following filter options.

Analysis: Collected Data View

Filter	Description
Tasks / Custodians	Choose to include all or none (no tasks).
• Tasks	Choose to include all or none (no custodians).
Custodians	If you filter your collection set containing one or more custodians, only tasks that actually have data for those custodians will be included in the collection set. However, if you include the "None" custodian (a catch-all for data that has not been assigned to an individual or existing custodian), all the tasks in your set are included. Starting with 9.0.1, you can hover on the task name to see its identifying information that helps to distinguish the task from the other tasks in the list. You can see "*Task description: Task source: Size*" if description was added while creating the collection task. If description for the collection task is not available, then "*Task ID: Task source: Size*" is displayed.
File Type / Date Options	Choose to select all dates, dates on or before, dates on or after, or dates between, then click the calendar icon to select the date.
• [Select Date Options]	Select (or clear) the options to include (or exclude) documents by file type.
Document Type	**Note:** If excluding loose MSG and EML document types, note that exclusion is based on the Modification date, not the Sent date. However, for PST and NSF files, exclusion is still based on Sent time.

   B. Click **Preview** to see a preliminary view of the collection set data based on the filter options you selected.

6. Click **Create…** at the bottom of the window to create your collection set, and specify the following information, and then click **Create**. Else, click **Cancel** to discard your selections.



Creating a Collection Set

Field	Description
Name	Enter a name for the collection set (up to 35 characters). The name is not case sensitive, but must be unique. Use only letters, numbers, and underscores.
Description	Enter a description for this collection (up to 255 characters).
Metadata only	Including metadata only makes a metadata-only collection set. It does not make a full copy of the collection set content. However, PST and NSF files are also copied while creating metadata-only collection set.
Content and metadata	Including content and metadata makes a full copy of the collection set content. This option creates a portable collection set, which can be imported into other Appliance or clusters.
Content only	Including content only makes a content-only collection set. Data for this collection set can only be exported in native format. The data is arranged in an appropriate hierarchy with respect to task, custodian, and source. This collection set does not appear on the collection set list while adding collection sets for processing. It is recommended to define a specific location to store data for the content-only collection sets.
Location	Enter the location where data for this collection set will be stored. **Note:** Users can view/edit the locations whose type is either "Collect Only" or "Collect and Export" and that are added in the groups to which the user has access.

Creating a Collection Set

Field	Description
Access Group	The access groups listed are the ones the user is part of. By default, all groups that consist of the user and associated sources and locations are listed in the **Included** column which results in the collection set being added to all of these access groups. A warning is displayed for the access groups in the **Available** column when the user has access to these access groups but the sources and locations are not part of these access groups. The user cannot move these access groups to the **Included** column. Contact your System Administrator to add these sources and locations to these access groups if you want to use these access groups. You should accept the default access groups listed in the **Included** column as the collection set's sources and destinations are part of those access groups. However, based on your requirements, you can keep only those groups in the **Included** column in which you want to add the collection set and move all the remaining groups to the **Available** column. While adding collection sets to an access group, the user will also need to add its sources and destinations to the access group. When the last access group is removed from the **Included** column which makes this collection set global if it is not part of any other access group, then a warning popup appears for making the associated sources and locations global. In this case, you will need to manually remove the sources and locations from the access groups. From this warning popup window, you can also export the list of these associated sources and locations as a reference. For more information on planning of access group deployments, see *"Planning for access group deployments" on page 182*. **Note:** While creating or editing a collection set, if no access group appears in the **Included** or **Available** column, there might be an error while loading the access groups data. You can still save the collection set, but it will become visible to all users. It is recommended to cancel the operation and then contact your system administrator.

Managing default type of collection sets

By default, only the "Metadata only" collection sets are created. You can manually select the type of collection set by selecting either "Metadata only", "Content and metadata", or "Content only" option.

Starting with 9.0.1, you can change the default type of collection set by setting the following property using **System** > **Support Features** > **Property Browser**.

Property: ***esa.icp.collection.set.create.default_type***

Value:

METADATA_ONLY: To create "Metadata only" collection set by default.

METADATA_AND_CONTENT: To create "Content and metadata" collection set by default.

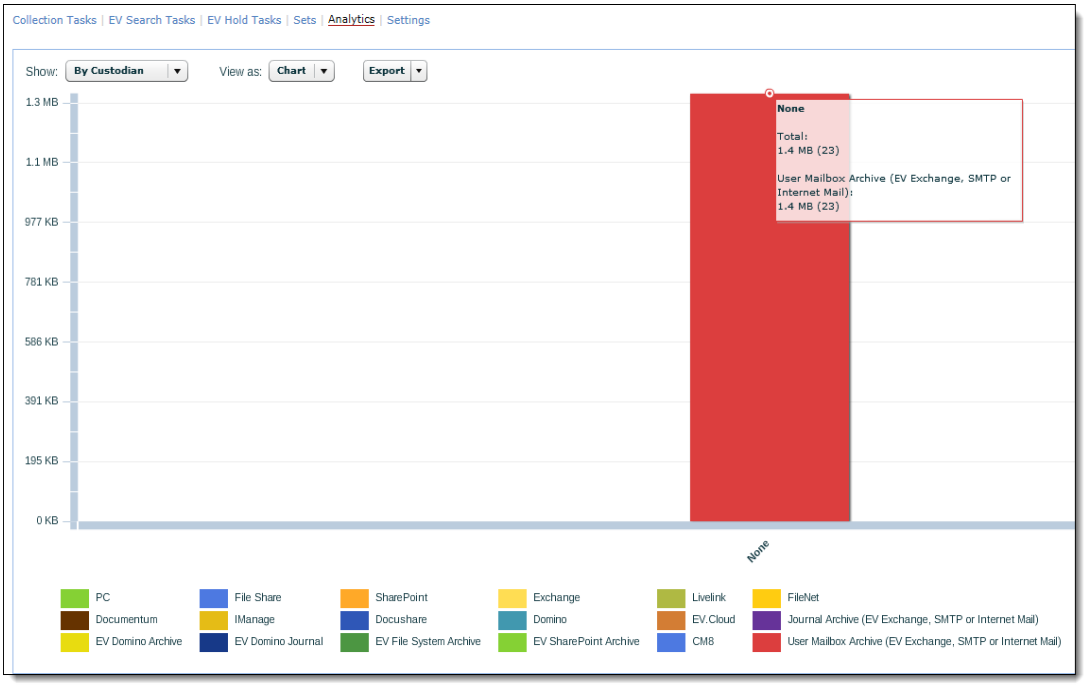
CONTENT_ONLY: To create "Content only" collection set by default.

Analyzing Collection Task Data

Once your data is collected, use the **Analytics** screen to view all data collected. Click **Settings** to change basic information about the collection set.

Viewing Collection Analytics

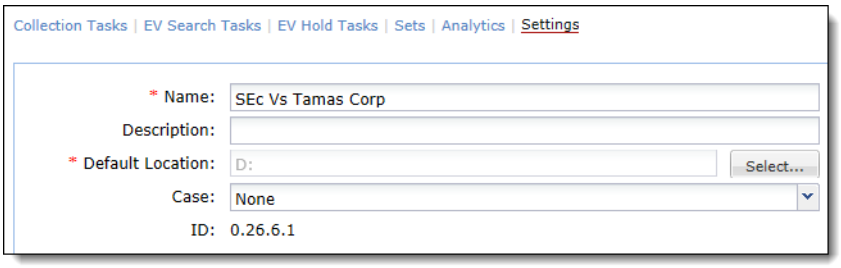
On the top navigation bar, for a selected case, click **Collections > Analytics** to view collection data for the case.



Click the drop-down selectors to show collection data by Custodian, or Source Type, and view data as a chart or table. In Custodian view, a color represents a source type. To report this data in a printable file, you can export as either a CSV or XSL file.

Changing Collection Settings

On the top navigation bar, for a selected case, click **Collections > Settings** to change information about the collection.



Enter a new name, provide a description, or click **Select** to change the default location. To associate this collection set to another case, enter the case name. (For tracking purposes, the ID for the set is also shown.) When finished, click **Save**.

Processing Collection Sets

After creating your collection set, you can now process the data for early case assessment, search, analysis and review.

Note: Use the steps in this section as a basic guideline. For detailed information and options to enter when creating a case, refer to *"Preparing Your Case" in the Case Administration Guide*.

To process a collection set in a case

1. From the **All Cases** view, select the case you want to add the collection set to (or, to add a new case, click the drop-down menu and select **Create New Case**, or under the navigation bar click **New Case** to set up your case. Follow the steps in *"Preparing Your Case" in the Case Administration Guide*.)

   Upon clicking **Save**, the **Case Home** screen appears.

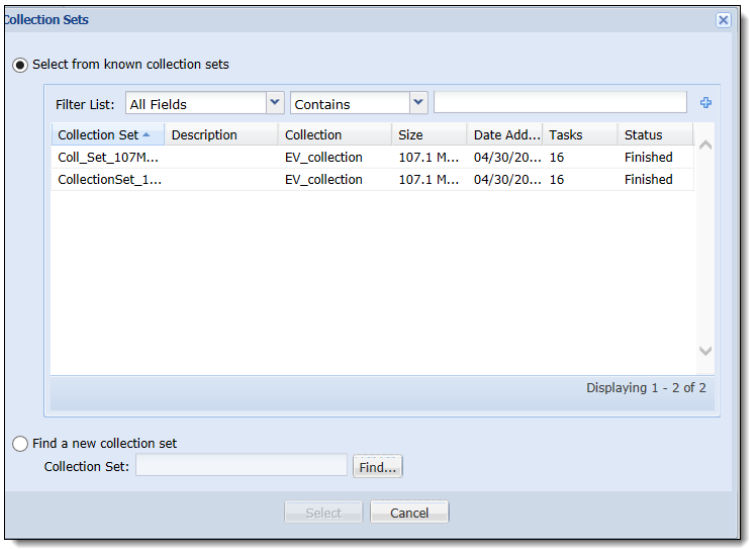
2. To add a collection set to your case:

   A. On the top navigation bar, click the **Processing** module, and select **Sources & Pre-Processing**. The Processing module opens to the **Manage Sources** tab.

3. From the Processing module, click the drop-down menu and select **Add Collection Set**, then click **Go**.

   The Collection Sets window appears. Under **Select from known collection sets**, only those collection sets are displayed that are either global or to which the user has access. You can also use the **Find a new collection set** option to browse the required collection sets. You can use the **Directory Browser** from the **Find Collection Sets** screen to browse to the collection sets. All collection sets that are either global, or belong to the same access group to which the user has access are displayed. The collection sets that are moved from a different appliance across cluster are also displayed as these sets are considered as global.

   Collection sets of type "Metadata only" and "Content and metadata" are available for processing. The "Content only" collection sets are not displayed so they cannot be selected for processing. If you need to process the "Content only" collection sets, then you can add the data of these collection sets for processing under **Processing** > **Sources and Pre-Processing** > **Manage Sources** > **Add Case Folder Source** screen.



Note: If you need to browse collection sets after folder hierarchy level of 5, then you should change the value of "***esa.icp.packageDiscoverDepth***" property using **System** > **Support Features** > **Property Browser**. By default, the value of this property is set to 5 which results collection sets only up to folder hierarchy level 5 being displayed.

4. Select the collection set you want to process with this case, and click **Select**.

5. (Optional) To view your collection set data before processing, select the **Processing Options** tab. A summary of your collection set data appears. (You can also analyze this data by Document Type, Custodian, or Timeline.)

   To continue to process this case with this source data, refer to the *"Processing Source Data" in the Case Administration Guide*.

Analyzing Data (Across Your Case)

After your case (containing the collection set source you added) has completed post-processing, *Data Analytics* are now available on the **Case Home** view. Analytics are the statistical views of your collected and processed data, which not only shows the volume of data collected and processed, but helps you to visually understand the information contained in your case by viewing it in a variety of different ways.

Viewing Processed Data

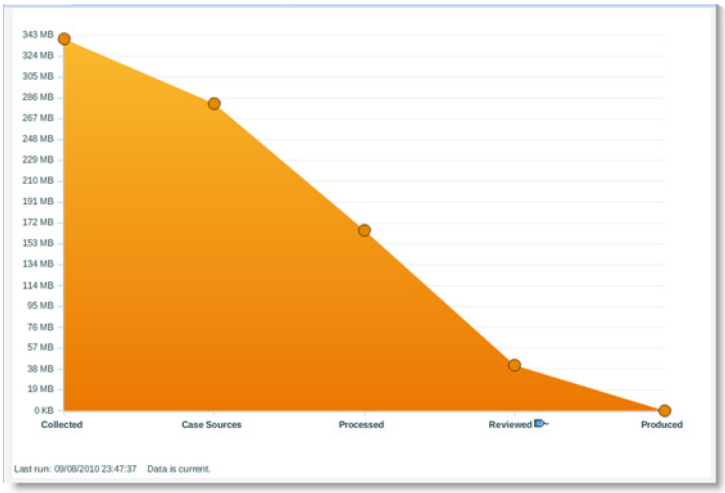
To view your processed data

Note: Your case source data must be processed/indexed before analysis. The "Data Analytics" option becomes available only after your data has completed post-processing.

1. On the top navigation bar, within a selected case, click **Case Home**, then select **Data Analytics**.

2. The Analytics screen appears with the Overview, showing a chart of the volume of data contained in the case.

   Overview Tab

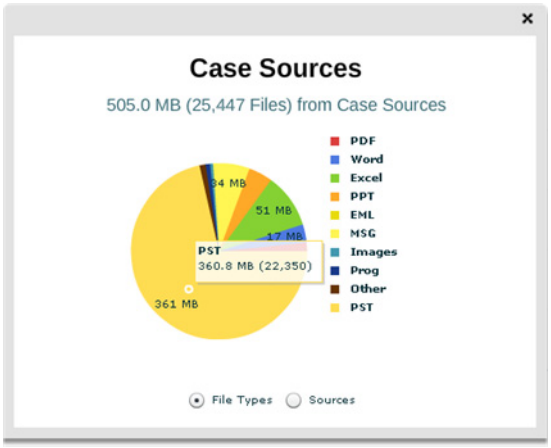


   This overall view of the data is defined by collected data (sources added to be processed), to what was actually processed; to later, what has been reviewed, and produced.

3. As users begin reviewing documents contained in the case, select the "blue tag" icon next to the Reviewed" label in the chart. This allows you to select which Review tags should be included in this Data Analytics chart. If data has been tagged or its status has changed, a "Refresh" link appears at the bottom of the chart. Click **Refresh** to see the most up to date data.

4. To see additional views from the **Overview** tab:

   A. Click any of the circle markers to see a detailed view of the data at any single phase in the process. For example, Case Sources (to view data by file type, or source of collected data).



5. Click the **Collected** tab to view all initial data collected for the case.

   Collected Tab

   The **Collected** tab allows you to view more detailed information about the data collected by selecting filter options providing different views of the same data at the first phase in the process — Collection.

   A. View the collected data information by using the following filter options.

Analysis: Collected Data View

Filter	Description
(Y-Axis) By Files By Volume	View data according to how many different file types were collected. View data by size/volume of data collected. (For example, volume ranges from 0 KB - 248 MB)
Zoom In/Zoom Out	Change the detail level by viewing either a specific area of data, or an expanded view.
(View As:) Chart or Table	Change the output view of the data formatted as a graphic chart or in table form.
Export	Choose whether to export this data view as a CSV (comma separated values) or XSL (Microsoft Excel) file for reporting purposes.
Sort by	Change the sort order by volume, data count, or alphabetic (ascending or descending).

6. Click the **Case Sources** tab to view all source data included in the case, (included, or excluding any initial collected data).

Case Sources Tab

The **Case Sources** tab allows you to view more detailed information about the data ultimately included in the case. This may include additional sources, and/or container files (such as PST, and XSL files) that were added to the case, even after data was collected in the first phase. Alternatively, this view can also reflect sources that may have been removed from the case after initial data collection. Thus, your case source data may appear greater, or smaller than your collected data view.

A. View the case source data information by using the same filter options as described in Table:*"Analysis: Collected Data View" on page 174*.

7. Click the **Processed** tab to view all data that was eventually processed and indexed in the case.

Processed Tab

A. View the case source data information by using the following filter options:

Analysis: Processed Data View

Filter	Description
(Y-Axis) By Documents By Volume	View data according to how many documents were actually processed and indexed. View data by size/volume of data collected. (For example, volume ranges from 0 KB - 248 MB)
Zoom In/Zoom Out	Change the detail level by viewing either a specific area of data, or an expanded view.
(View As:) Chart or Table	Change the output view of the data formatted as a graphic chart or in table form.
Export	Choose whether to export this data view as a CSV (comma separated values) or XSL (Microsoft Excel) file for reporting purposes.
Sort by	Change the sort order by volume, data count, or alphabetic (ascending or descending).

8. Click the **Reviewed** tab to view the postprocessed data that has been reviewed in the case.

   Reviewed Tab

   When analyzing reviewed data, if you notice that it has increased (rather than decreased in volume) it may be due to e-mail attachments and related threads that were selected by the Case Administrator to be reviewer and included in the case.

   To specify which tags you want to view statistics for, click the Tag icon next to *Reviewed* on the graph.

   Note: Any time documents in a case are reviewed, the case analytics view must be updated, indicated by a "Refresh" icon at the bottom left of the Analytics page. Click the icon to ensure you are viewing the latest possible data.

   A. View the processed data information by using the same filter options as described in the Table: *"Analysis: Processed Data View" on page 175*.

9. Click the **Produced** tab to view the production-ready data that has been prepared for case.

   Produced Tab

   A. View the produced data information by using the same filter options as described in the Table: *"Analysis: Processed Data View" on page 175*.

Collection Administration and Maintenance

This section describes how to manage and maintain your collected data in Veritas eDiscovery Platform.

Note: For information about global user accounts, any other user account types, or general account administration on the appliance, refer to *"Managing User Accounts" in the System Administration Guide*.

Managing Collection User Accounts

For information about how to manage user accounts, the roles, and groups that determine each user's access permissions to the Identification and Collection module, see the following topics:

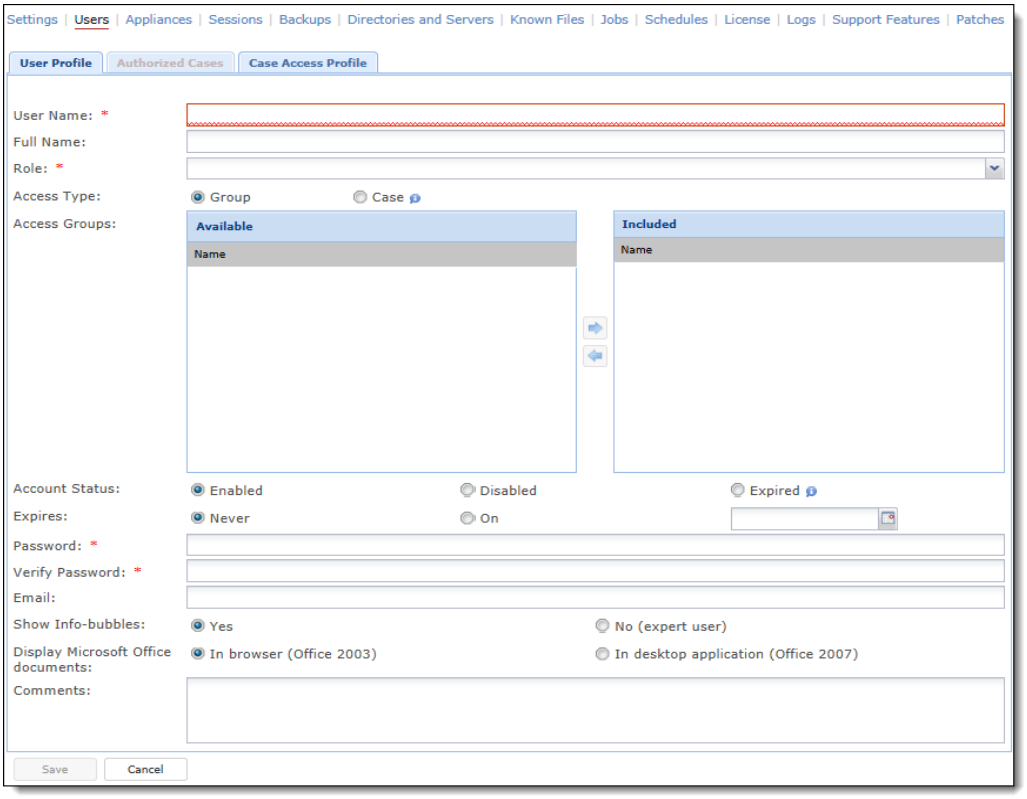
Defining Collections Administration User Accounts

A user's account and its associated user role determine the data source mapping and collection administration tasks that the user can perform.

A Collections Administrator, by default, can manage data maps, collections, and collection sets within in your Veritas network. System Administrator-level users can define Collections Admin options to also allow other general, group access, document access, or case administration rights. Accounts created by the Collections Admin can have collection management privileges, but not system administrative privileges. For more information about System Administrator privileges, refer to *"Managing User Accounts" in the System Administration Guide*.

To add a collections user account

1. From the **System** view, click **Users**.
2. Use the **Show** menu to view all accounts or just the enabled, disabled, or expired accounts (enabled accounts are listed by default).
3. To add a new global user account:
   A. Click **Add** to open the Add User page.



   B. Specify the following information. An asterisk (*) indicates a required field.

Collections Admin Account

Field	Description
User Name*	Enter a login name for the user (up to 35 characters). The name is not case sensitive, but must be unique. Use only letters, numbers, and underscores.
Full Name	Enter the user's full name (up to 255 characters).
Role*	Select the Collections Admin role to specify the user's access to manage Collections. The predefined role (for this module) is: • **Collections Admin**. Allows access to the data map, collections, and collection set management. **Note:** The predefined role cannot be changed. To further define the Collection Admin role, see *"Viewing the Collections Admin Role" on page 180*. For information about defining other general user roles, refer to *"Managing User Accounts" in the System Administration Guide*.
Access Type	Select the access type to allow the user either to access groups or the cases. If "Group" is selected, then the user becomes part of an access group and gets access to all entities that are associated with that access group. If "Case" is selected, the user gets access to limited cases only and Access Group permissions are disabled.
Access Groups	Define an access group the user should have access to. The use will only be able to use the legal holds, sources, locations, and collection sets that are part of the same access group the user is added to. By default, all groups are listed in the **Included** column which results in the user being added to all groups. Keep only those groups in the **Included** column in which you want to add the user and move all the remaining groups to the **Available** column.
Account Status	Select whether the account is enabled or disabled/expired. Disabling an account prevents users from logging in and removes the account from the user lists.
Expires	Select **Never** or select **On** and click  and select a month and day when the account expires (or enter the date as MM/DD/YYYY). The account expires at 12:01 AM on the selected date.
Password* Verify Password*	Enter and verify a case-sensitive password for the account.
Email	Enter the user's email address (up to 255 characters).
Show Info-bubbles	Select whether information icons  are displayed next to some fields. Moving the cursor over the icon opens a "bubble" describing the field.
Display Microsoft Office documents	Select whether a selected Microsoft Office document is opened in the browser (the default) or in a separate application window (requires Microsoft Office 2007 or later).
Comments	Enter additional comments about the user account.

Note: System administrators can create and assign access profiles for any case. For information on how to define new access profiles, refer to the *System Administration Guide*.

C. Click **Save** to submit the new account, or click **Cancel** to discard your changes.

4. To change or enable/disable an account, click the account name, change the account settings, and click **Save**.

Viewing the Collections Admin Role

As with other user accounts, the Collections Admin role specifies a set of access permissions that can be assigned to the specified user's account. Only a System Administrator with the role management privilege can create and assign user roles. To assign a role to a Collections Admin account, refer to *"Defining Collections Administration User Accounts" on page 178*. Among other user roles listed, the **Collection Admin** role allows collection set management, and access to the data map, collection tasks, and collection analytics (by default).

Note: The predefined roles cannot be edited. You can only edit the customized user roles that are not added by default, i.e that are not predefined.

Follow the steps in this section to define the Collection Admin role by editing permissions from the Edit Role page.

To view the Collection Admin role

1. In the **System view**, click **Users**.
2. Click the **Roles** tab to view the list of user roles.
3. To view the Collection Admin user role, click **Collection Admin**. The following information is displayed.

   Note: Only the rights that are predefined for the Collection Admin role are listed here. For details, refer to the *System Administration Guide*.

Collection Admin Role Details

Field	Description
Role Name*	A role name (up to 35 characters).
Description	A description of the role (up to 255 characters).
General Rights	
Allow integrated analytics access	Allows the user to access the Analytics charts found on the Case Home > Data Analytics screen.
Allow mobile access	Enable access to case information using mobile device.
Collection Rights	

Collection Admin Role Details (Continued)

Field	Description
Allow collections access	Allow **read-only** access to Identification and Collection module in Veritas eDiscovery Platform. Includes: Collections, Collection Templates, Collection Sets, Sources, Source Accounts, Source Groups, Custodians, and Locations. • **Data Map Management** - Allows users to add/modify data map objects. Includes: Sources, Locations, Source Accounts, Source Groups, Custodians, and Collection Templates. • **Collections Management** - Allows users to add/modify Collections) • **Clearwell Collection Set Management** - Allows user to add/modify Collection Sets)
System Administration Settings	
Allow Case Home and All Cases Dashboard Access	Enables user to view all activity for a single case from the Case Home view, as well activity across all cases from the All Cases > Dashboard view.

A. Click **Save** to submit the new account, or click **Cancel** to discard your changes.

Managing Access Groups Permissions

In many organizations, there are different business units with their own charter; however, the infrastructure is shared for efficiency. For example, a common Microsoft Exchange or Veritas Enterprise Vault infrastructure is shared between multiple, autonomous business units. These business units would prefer to segregate and safeguard their data. Also, eDiscovery roles and permissions are split between people who collect data versus those who process data. Veritas eDiscovery Platform provides a way to secure data using an optional Access Group security mechanism which helps to control access to data. Use of Access Groups is optional; if not used, system operation remains similar to previous versions of eDiscovery Platform.

The collection rights including **Data map management**, **Collections management**, and **Collection sets management** allow the user to manage sources, locations and collection sets and move them across access groups. A user with the System Manager role has all privileges by default and thus gets access to all secured entities. Starting with release 8.2, a new system-defined Group Admin user role is available. A Group Admin cannot create access groups but can control only those access groups to which they are assigned. By default, only a System Manager can add access groups. However, any customized user with the **Allow user management** and **Allow group management rights** privileges can enforce the group access security permissions to ensure that users can access only those legal holds, sources, locations, collection sets, and cases that should be accessible by them for legitimate use of data. If an administrator prefers to keep an entity accessible to all users, then these entities must not be added to any access group. Source, location, collection set, and cases can be added to multiple access groups.

Users can use only those legal holds, sources, locations, collection sets, and cases:

- that are added in the same access groups to which the user has access
- that are global, i.e. not part of any access group

Planning for access group deployments

Before using access groups for sharing common infrastructure within different business units of your organization, consider planning for access group rollout. System administrators can use the Access Group Report using the **Export Details** button on the **System** > **Users** > **Access Groups** screen. This report includes information on the list of access groups available, and the users, legal holds, collection sources, locations, collection sets, and cases that are part of these access groups.

Also, starting with release 8.2, the option to select all entities such as legal hold, source, location, case, and collection set is removed in order to strengthen access group security. Therefore, users need to associate individual entities to the access group. When upgraded to 9.0 from a prior release, the system modifies the access group mappings and removes the group associations based on all entities option, and then associates individual entities with the access group. The changes in the access group mappings are reported in a new Access Group Change Report which can be accessed from the upgrade\reports folder within the product installation directory.

Create access groups based on the business units that need to use the same infrastructure but need private access to resources and provision users within them. Provision sources and locations based on how you would require collection sets to be accessed. Access groups having these sources and locations would automatically be shown in the Included list on the add/edit collection sets dialog. It is recommended to accept the default access group suggestions as the collection set's sources and destinations are part of those access groups.

Any case, legal hold, collection set, source, location, or user that is not associated with an access group will show up for anyone whose access type is "Group." To use access groups, these entities must be assigned to one access group or another. These entities will not show up for users whose access type is "Case."

Confirm that access groups, users, legal holds, sources, locations, collection sets, and cases have been provisioned correctly by running the Access Groups report again.

An example of access group mapping:

An organization has two business units, Finance and Legal. Both of these units share a common Microsoft Exchange infrastructure that hosts the mailboxes of all users in each unit.

To ensure that right people can access right set of data, the administrator can apply access group security permissions as explained in this section.

Define the users and their eDiscovery roles:

User	Role	BU	Allowed to	Not allowed to	Group assignment
Joe	Exchange Server Admin	IT	Manage Exchange servers	Collect or view contents of mailboxes	NA
Mary	eDiscovery Collections Admin	Finance	Collect from employees of Finance	Process collected data, Collect from employees of other units	Finance
Andy	eDiscovery Collections Admin	Legal	Collect from employees of Legal	Process collected data, Collect from employees of other units	Legal

User	Role	BU	Allowed to	Not allowed to	Group assignment
Adam	eDiscovery Staff, Legal	Finance	Process data into case for Finance, export data from case	Collect data	Finance
Jane	eDiscovery Staff, Legal	Legal	Process data into case for Legal, export data from case	Collect data	Legal
Mark	Group Admin	Finance	Control access group and associated entities for Finance	Control other access groups	Finance
Mat	Group Admin	Legal	Control access group and associated entities for Legal	Control other access groups	Legal

Restrict sources as:

Account ID	Access	eDiscovery Group
Finance_Exchange_eDiscovery	Collect from Exchange mailboxes in the Finance unit	Finance
Legal_Exchange_eDiscovery	Collect from Exchange mailboxes in the Legal unit	Legal

Restrict data locations as:

Locations	Description	Who has access	eDiscovery Group
\\NAS\Finance_Collections	Location for all files collected from the custodians of the Finance unit for eDiscovery purpose	Mary Mark	Finance
\\NAS\Finance_Exports	Location for files exported from cases of the Finance unit	Adam Mark	Finance
\\NAS\Legal_Collections	Location for all files collected from the custodians of the Legal unit for eDiscovery purpose	Andy Mat	Legal
\\NAS\Legal_Exports	Location for files exported from cases of the Legal unit	Jane Mat	Legal

Restrict cases:

Case	Description	eDiscovery Group
Finance_eDiscovery	Case to process collection from Exchange mailboxes in the Finance unit	Finance
Legal_eDiscovery	Case to process collection from Exchange mailboxes in the Legal unit	Legal

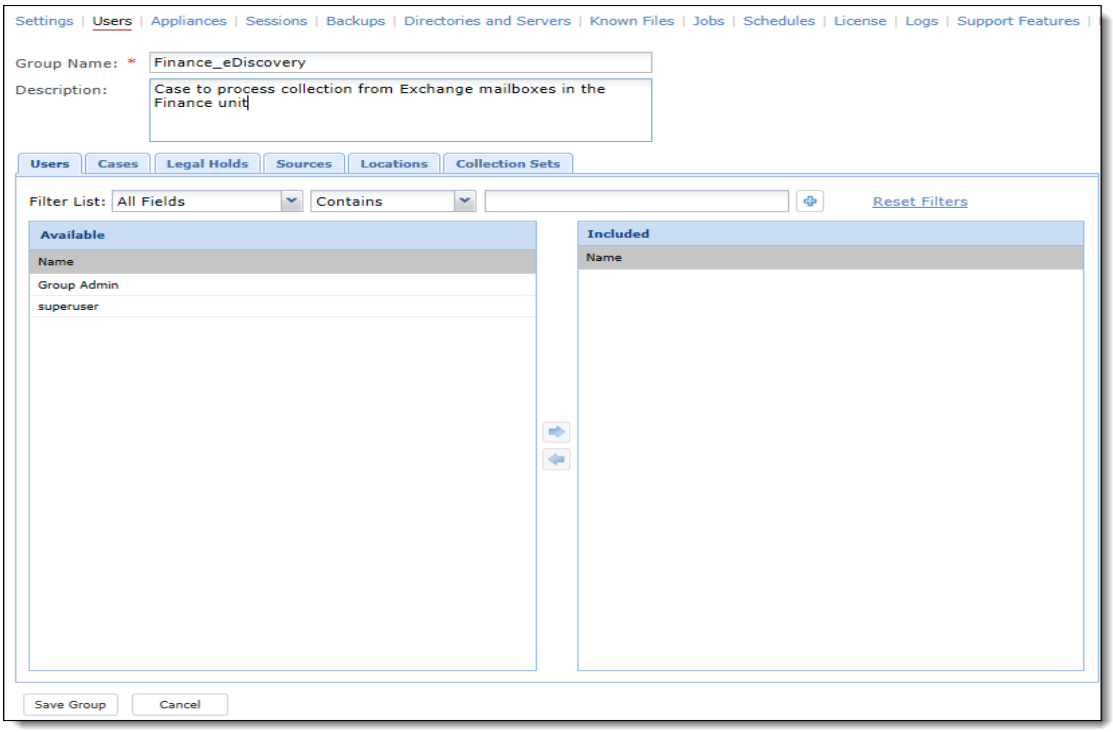
Create access groups and map the users, legal holds, sources, locations, and collection sets as:

Group Name	Users	Source Account	Location	Collection Sets	Case
Finance	Mary, Adam, Mark	Finance_Exchange_eDiscovery	\\NAS\Finance_Collections \\NAS\Finance_Exports	Collection sets containing data of Finance unit custodians	Finance_eDiscovery
Legal	Andy, Jane, Mat	Legal_Exchange_eDiscovery	\\NAS\Legal_Collections \\NAS\Legal_Exports	Collection sets containing data of Legal unit custodians	Legal_eDiscovery

Adding an Access Group

To add a group:

1. In the **System** view, click **Users**.
2. Click the **Access Groups** tab to view the list of groups.
3. Use the **Search** filter to search groups by name and description.
4. To add a new group:
   A. Click **Add** to open the **Add Group** page.



   B. Specify the following information. An asterisk (*) indicates a required field.

Access Groups Permissions

Field	Description
Group Name*	Enter a name for the new group. The group name must be unique. (up to 35 characters)
Description	Enter a description for the group. (up to 255 characters)
Users	All existing users are listed in the **Available** column. To include specific users in this access group, select the appropriate users from the **Available** column and then move them to the **Included** column. Users added in the **Included** column will only be able to use the legal holds, sources, locations, collection sets, and cases that are also added in this group and the legal holds, sources, locations, collection sets, and cases that are global.

Access Groups Permissions (Continued)

Field	Description
Cases	All existing cases are listed in the **Available** column. To include specific cases in this access group, select the appropriate cases from the **Available** column and then move them to the **Included** column. The cases that are listed in the **Included** column will only be accessible to the users who are also member of this access group.
Legal Holds	All existing legal holds are listed in the **Available** column. To include specific legal holds in this access group, select the appropriate legal holds from the **Available** column and then move them to the **Included** column. The legal holds that are listed in the **Included** column will only be accessible to the users who are also member of this access group.
Sources	All existing sources are listed in the **Available** column. To include specific sources in this access group, select the appropriate sources from the **Available** column and then move them to the **Included** column. The sources that are listed in the **Included** column will only be accessible to the users who are also member of this access group.
Locations	By default, all existing locations appear in the **Available** column. To include specific locations in this access group, select the appropriate locations from the **Available** column and then move them to the **Included** column. The locations that are listed in the **Included** column will only be accessible to the users who are also member of this access group.
Collection Sets	By default, all existing collection sets appear in the **Available** column. You need to manually move the collection sets to the Included column so that these collection sets are only used by the users who are also member of this access group. If the user doesn't have permissions on the sources and locations of the collection sets, those sets are disabled from being moved from **Available** to **Included**. When collection sets are moved from **Available** to **Included**, the system displays the list of sources and locations in those sets, which are not already present in the access group. Once the user confirms, those sets and their sources and locations are added to the access group. When a collection set is removed from all groups or if a collection set is removed from the only group it was part of, then it effectively becomes a global collection set. This is prohibited unless the sources and destinations are also global. You will get a warning popup with the sources and destinations that need to be made global. A partial list of such entities is displayed on the warning popup; it is recommended to use the **Export** button to export the list and then manually make all of the sources and destinations global before attempting to move the collection sets. If you do not specify a collection set for this access group, then the users from this access group will not have access to any of these collection set. However, these users will have access to the global collection sets which are not part of any access group.

C. Click **Save Group**.

Deleting an access group

You can delete an access group using the trash icon on the **System** > **Users** > **Access Groups** screen. When an access group is deleted, all the entities including users, legal holds, sources, locations, collection sets, and cases become global if they are not part of any other access group.

Managing Custodians (Across a Case)

After creating a case and processing your custodian data, Case Administrators can continue adding and managing custodians for that case. Similar to how you added and customized attributes on the Employee List for custodians across all cases (*All Cases* > *Employee List*), you can now manage custodians on a case-by-case basis after the case has been processed.

From the *Case Home* view, use the Custodians screen to manage custodians for a specific case, allowing you to:

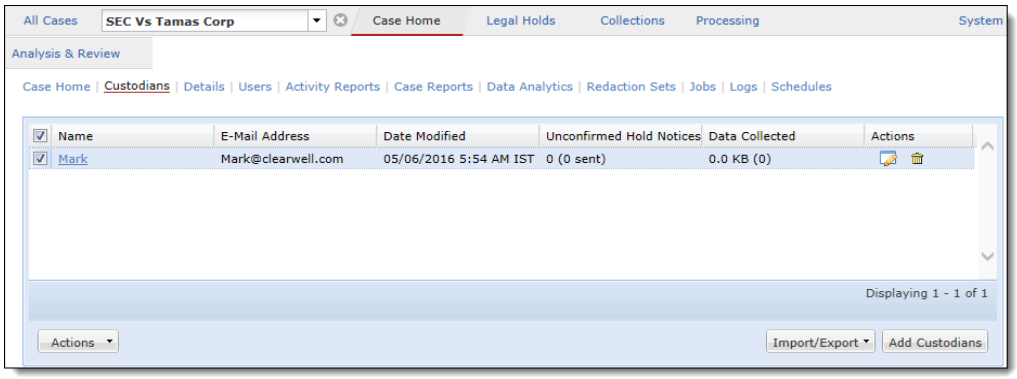
- View/sort consolidated custodian information
- Edit custodian data, with options to view details, changes made, and all Legal Hold and Collection activity for a selected custodian in the case

  Note: To add custodians to a legal hold notification, Legal Hold Administrators have the option of filtering by *Case custodian* or *Employee List*. (You must have a licensed Legal Hold module and appropriate user privileges.)
- Add/associate custodians to a specific case
- Import/export custodian data
- Generate Custodian reports
- Create email digest alerts

To manage custodians in a specific case

1. Select the case you want to add custodians to, then click **Case Home > Custodians**.

   The *Custodians* screen displays all custodians currently associated with the selected case.

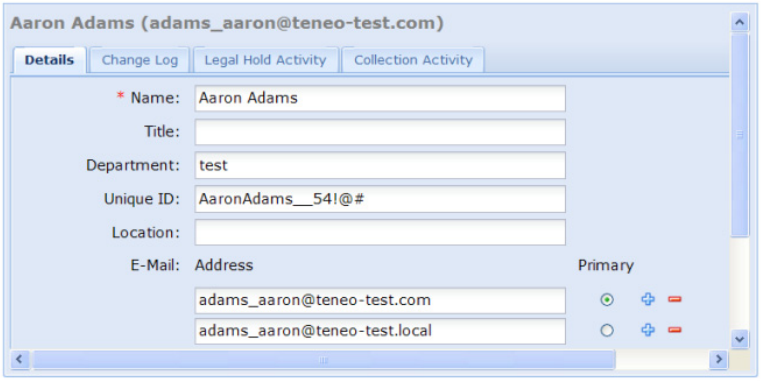


   This view displays a consolidated list of employee information showing all activity for each custodian in a specific case. The columns *Unconfirmed Holds* and *Data Collected* show both Legal Hold and Collection activity in a single dashboard view. From here, you can search and sort by attributes and date range (based on the same criteria used for employee attributes as described in *"Mapping Employee Attributes" on page 35*).

2. Do one or more of the following custodian management tasks:

   A. *Edit Custodians*.

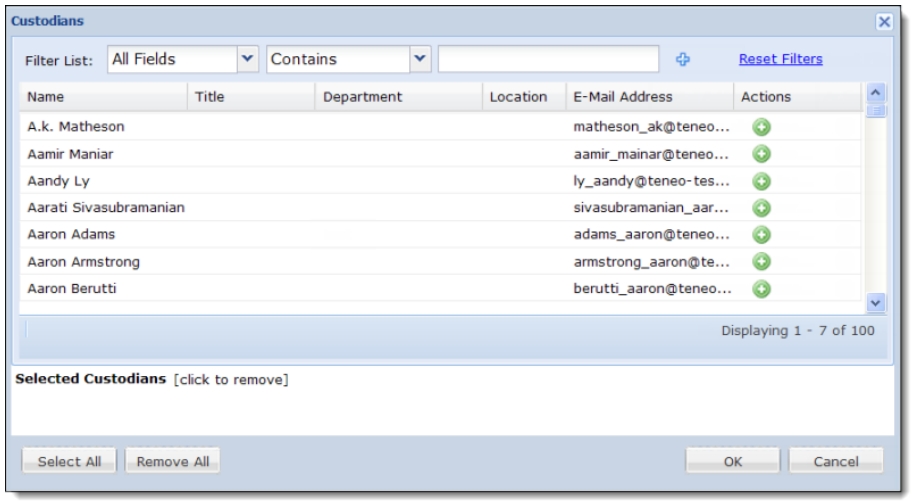
   › Either click the (edit) icon from the Actions column, or click a name in the list to edit the custodian's information.



   From this screen, you can view and edit employee attribute values. (The ***Change Log***, ***Legal Holds Activity***, and ***Collection Activity*** tabs display the historical information which can only be viewed. Remember that the data presented here is specific to the selected case (not across all cases). For details, continue with steps as described in *"Mapping Employee Attributes" on page 35*.

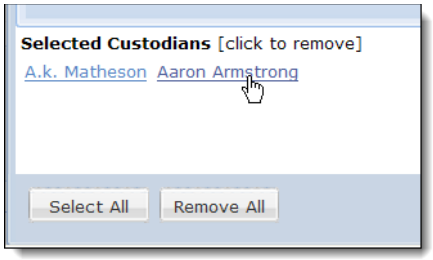
   B. *Add Custodians*.

   › Click **Add Custodians** to add new custodians to the selected case from the *Custodians* dialog.



› From the *Custodians* dialog, Actions column, click the (add) icon to select individual custodians, or click **Select All**.

The custodians are moved to the *Selected Custodians* box. (Click on each name to remove individually, or click **Remove All**.)



The same sort functionality (from the Employee List in the All Cases view) applies to the Custodian dialog. You can view, reset, and filter on attributes, and sort history of custom attributes by date range. For example, use the "Contains" drop-down to display "Information as of" and select "Between" [date] and [date].

C. *Delete Custodians*.

› Either click the (delete) icon from the Actions column, or click the check box next to the custodian(s) you want to delete then click **Actions > Delete Custodians**. At the prompt, click to confirm deletion of the selected items. to delete the selected custodian.

D. *Import (or Export) Custodians*.

When importing custodians into a case, the system attempts to find custodians from the Employee List using *Email* or *Unique ID* column values. Importing custodians can have either one or both the *Email*, *Unique ID* columns. If both columns are present, the system defaults first to the *Unique ID* and matching custodians are added to case. Similarly, custodians matching the *Email* column are added to the cases. If multiple custodians have the same email, all the custodians are added to the case. The custodians for which no match is found, are logged in the job log.

› Click **Import/Export** and select either **Import from CSV**, or **Export as** [**CSV** or **XLS**]. (For details on importing from a CSV, see *"Importing Custodians from CSV or Script" on page 38*.) Clicking an export type opens the Download window. Choose to **Open** or **Save** the file. The filename "custodians" is appended with the date and task ID. (For other export tasks, see *"Collection Reports" on page 137*. In addition to employee data in the Employee List, case-specific custodian export has additional data such as unconfirmed hold notices and data collected.

E. *Generate Custodian Reports*.

› Click **Actions** and select **Generate Custodian Reports**. This generates the report as a job which can be viewed from the **Jobs** window.

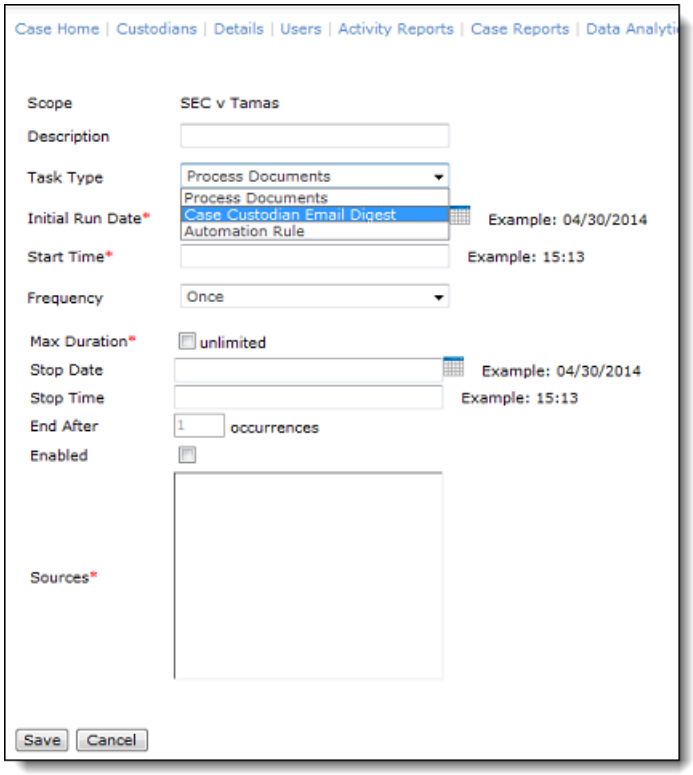
› From there, click the icon under the status column to view custodian reports for all custodians in the selected case.

F. *Create Email Digests*.

Email digests allow administrators to receive email alerts when custodian data changes, such as name, title, or location employee attributes. Email digest messages show a log of the changes that were made to the case custodians since the last digest was sent.

› Click **Import/Export** and select either **Set Email Digest Options**.

› To schedule when you want to receive email alerts on custodian activity, from **Case Home > Schedules**, click **Add** and select **Case Custodian Email Digest**.



› Next, set the *Initial Run Date*, *Start Time*, and *Frequency*. In the *Send To* box, type the email addresses of all recipients (separated by semi-colon, comma, space, or each on a separate line.)

› To enable the email digest to run when scheduled, click the **Enabled** check box. When finished, click **Save**. (You can always enable this task later, from the main Schedules screen, by selecting the task from the list, and clicking **Enable**.)

(For details on other scheduling-related collection tasks, see *"Run or Schedule a Collection Task" on page 126*. For general schedule management tasks, refer also to the *System Administration Guide*.

Archiving, Restoring, and Deleting Collections

Occasionally, you may want to set aside or remove old collections that are no longer necessary, such as when a case containing a collection is no longer active. Alternatively, you may simply want to reduce the custodian license quota by archiving unused collections.

Collection Admins can archive collections in an effort to manage collection data and optimize license capacity. Collection sets cannot be created from archived collections; however, before archiving the collection, you can create a collection set and import it into your case prior to processing for analysis and review. This allows reviewers working in the Analysis & Review module to still perform search tasks on archived collection set data.

Archiving versus Deleting Collections

Both archiving or deleting a collection will remove the collection from active view or use. Additionally, both an archived or deleted collection releases associated custodian licenses. However, only archiving allows you to fully restore the collection at a later date.

When a collection is archived, the custodian licenses are released (if they are unique in the system), allowing you to reuse the custodian licenses for other collections.

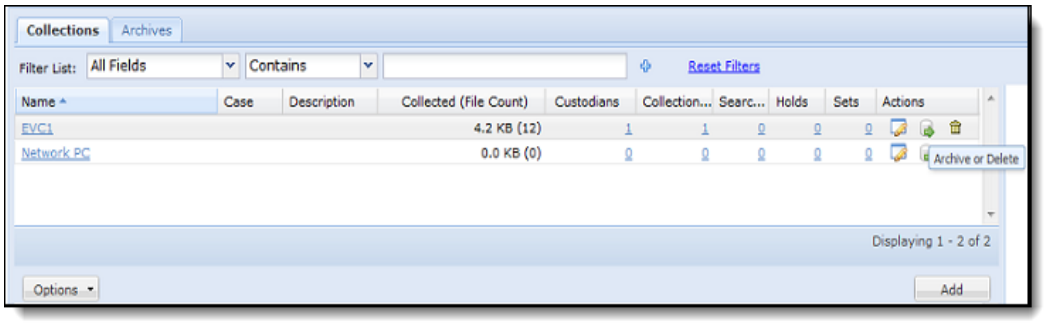
When a collection is deleted, its contents (collections and tasks) are removed from Veritas eDiscovery Platform. The data itself is not actually deleted or moved, but cannot be recovered from its current location. (The default location for the selected legal hold's data is provided. For example: D:\CaseData.)

Note: Veritas does not recommend deleting a collection unless you are certain the data is no longer needed. While the information is not permanently deleted, it cannot be restored in the same way as an archived collection, and may require assistance from Technical Support to recover the data.

To archive or delete a collection

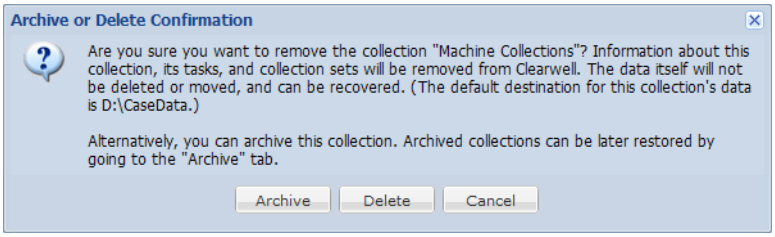
1. From **All Collections** > **Collections** screen, click the **Collections** tab.

   The Collections screen appears showing all collection sets across all cases.



2. Click the (archive or delete) icon under the Actions column for the collection you select.

3. A warning appears with the option of either archiving or deleting the selected collection set.



Confirm your action:

A. To remove the collection by archiving (which can be restored later), and release one or more associated custodian licenses, click **Archive**.

Note: The custodian license is released only if the custodian is unique in the system, and not associated with any other active collections.

B. To remove the collection by deletion (removing all contents, but will not be permanently deleted or moved, and can be recovered), and release custodian licenses, click **Delete**.

CAUTION: Consider your action carefully before deleting a collection. Even though the data is not permanently deleted or moved, and is still in the system, it is not easily or readily recoverable, and may require Technical Support's assistance.

Your archived collection now appears on the **Archives** tab, from where it can later be restored. The associated custodians are no longer counted against your custodian license.

To check, go to **System > License** to view the number of custodian licenses in use. See *"Managing Your Collections License" on page 194*.

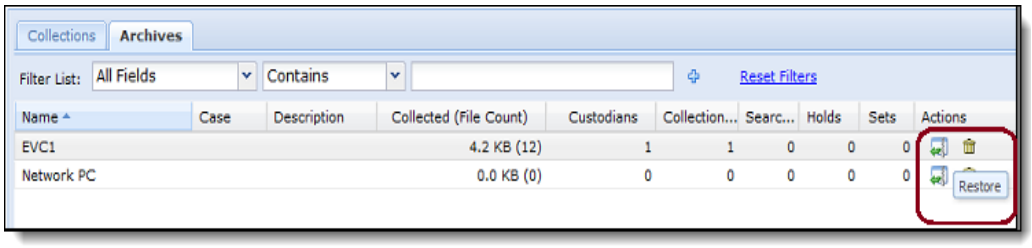
Restoring an Archived Collection

Archived collections can be restored by from the **Archives** tab. The collection you select will be listed among your active Collections.

Note: The custodians associated with the collection(s) you restore will be counted against your license.

To restore an archived collection

1. From **All Collections** > **Collections** scree, click the **Archives** tab.
2. Click the (restore) icon for the selected collection you want to archive.



3. At the prompt, click **Yes, Restore** to continue with restoring the selected collection.

Your collection is now restored, and reappears on the **Collections** tab, where it is available for active use. The associated custodians are once again counted against your custodian license. To check, go to **System > License** to view the reduced number of custodian licenses in use.

You must restart eDiscovery Platform services after restoring a collection backup.

Managing Your Collections License

Your Collections license key is supplied by Veritas Technical Support based on the terms of your license agreement. For new appliances, or for more information about your general Veritas eDiscovery Platform license, refer to the *"Managing Your License" in the -System Administration Guide*.

Note: If you have upgraded Veritas eDiscovery Platform from a prior version, and have a license to collect data from a Veritas Enterprise Vault source, a license update is required. When updated, the Veritas Enterprise Vault source type will appear under the "Collections License" item on the License screen.

About Reusable Licenses

In the Identification and Collection module, your custodian licenses are reusable. When a collection is archived, or a collection task is deleted, or a custodian has been reassigned, the licensed custodian count decreases.

Note: The custodian license becomes reusable in two cases: (1) If the custodian was removed from the collection task, and was not assigned to any other collection tasks, and (2) if the custodian was assigned to a collection which was archived. (In this case, if the collection is ever restored, the custodian will once again count against the custodian license.)

Updating Your License

Use the License screen to view license details and to update (apply a new) license. On the associated Detail page, you can view how much of your licensed capacity each case currently uses. The Collections license is based on a per-custodian use. Updating your license requires license information either to be copied/pasted in, or uploaded from a .zip or SLF file. Have this information handy before you choose to update.

To view or update license information

1. From the **System** view, select **License**.

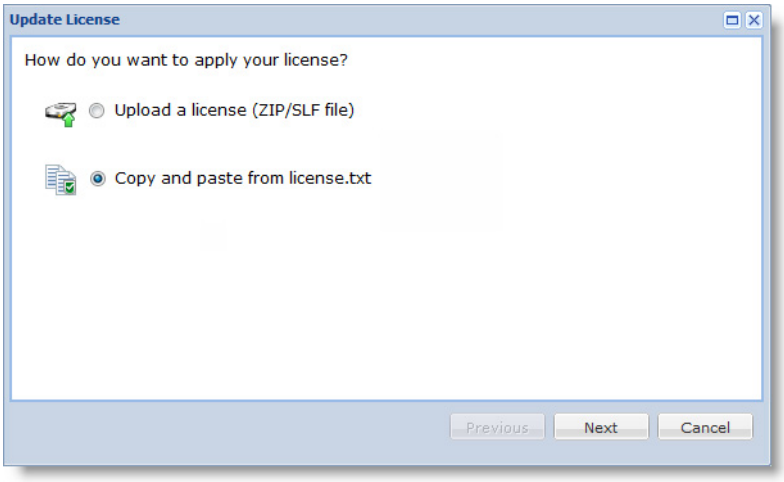
   In this example, the current capacity is for 50 custodians. Periodically note the custodian count, particularly each time you archive a collection or task.

2. To view details for your cases, click **View Details**. The Details page shows each case with the capacity used for each.
   - Click **Done** to return to the License screen.
   - Click an underlined case link to open the Status screen for that case.

3. To update the license, click **Update License**. The Update License Wizard opens.

4. Select the method you want to use to update your license. Copying/pasting a license will *replace* the license information with the new license on the server where it is installed. Uploading a file will add to your existing license.

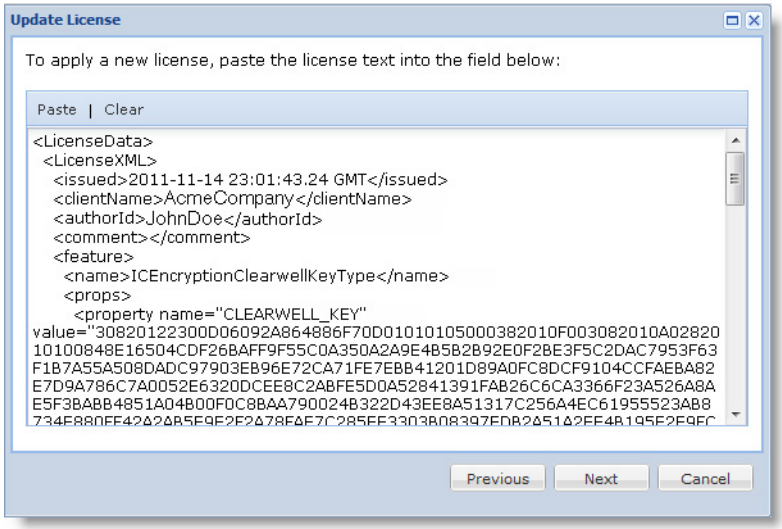
   (As shown in this example, you can choose to copy and paste the license information instead, from "license.txt" file, attached in an email message you received.)



   Click **Next**.

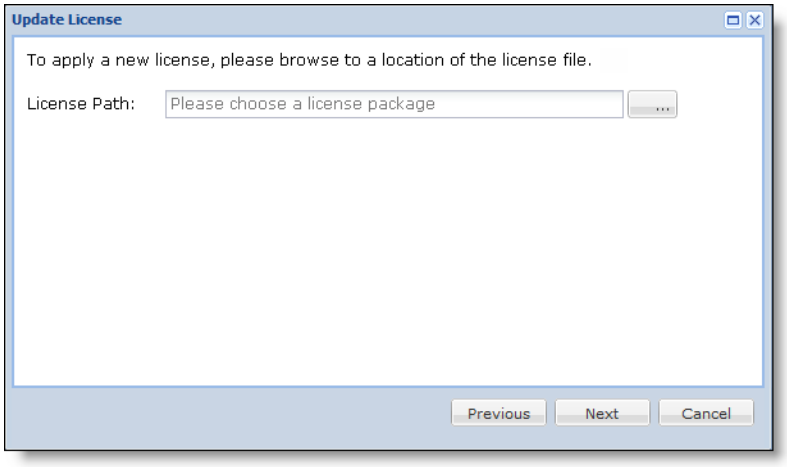
5. Do one of the following:

   A. If copying/pasting the license information, click **Paste** to the place the copied text into the window. (Click **Clear** to delete.)

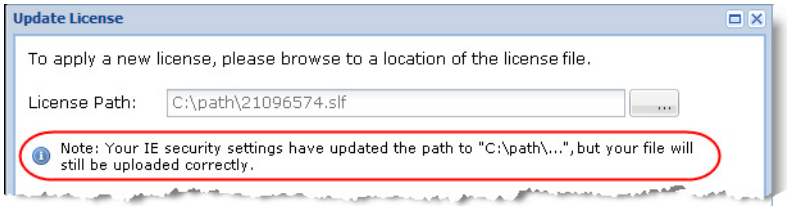


Note: Depending on your Internet Explorer security settings, clicking **Paste** may prompt you to allow access to the System Clipboard. Clicking **Allow access** is safe and will stay in effect until the page is refreshed again.

B. If uploading a license (from a ZIP or SLF file), browse to the location of the license package.



Note that when you select the path, your Internet Explorer security settings are updated to that location, though your license file will still be properly uploaded.

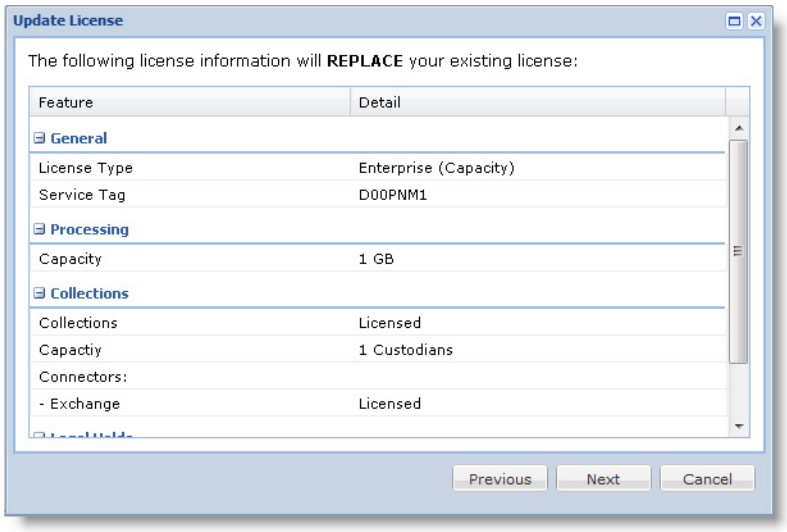


Note: Uploading a file will *add/merge* the license information with the current license on the server where it is installed.

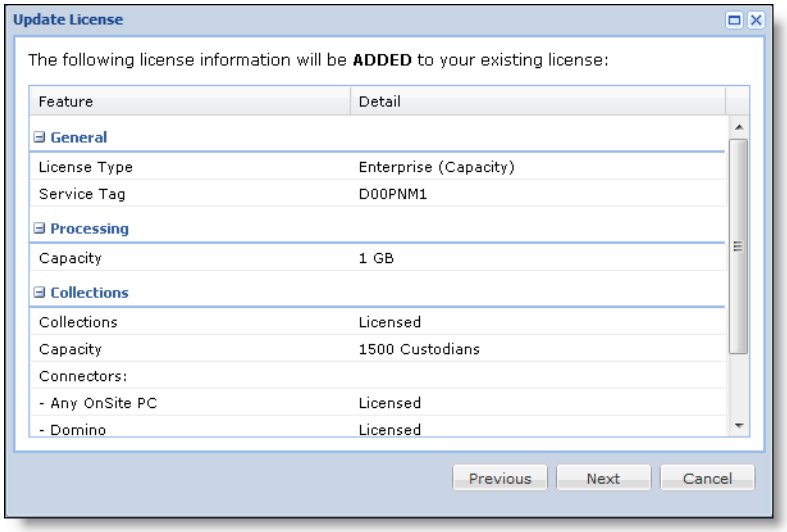
Click **Next**.

6. Review the license information to be applied (*replacing* or *adding* to your existing license).

   A. If you copy/pasted in your license (you received a license.txt file via email), note that the information, as shown, will *replace* your existing license:

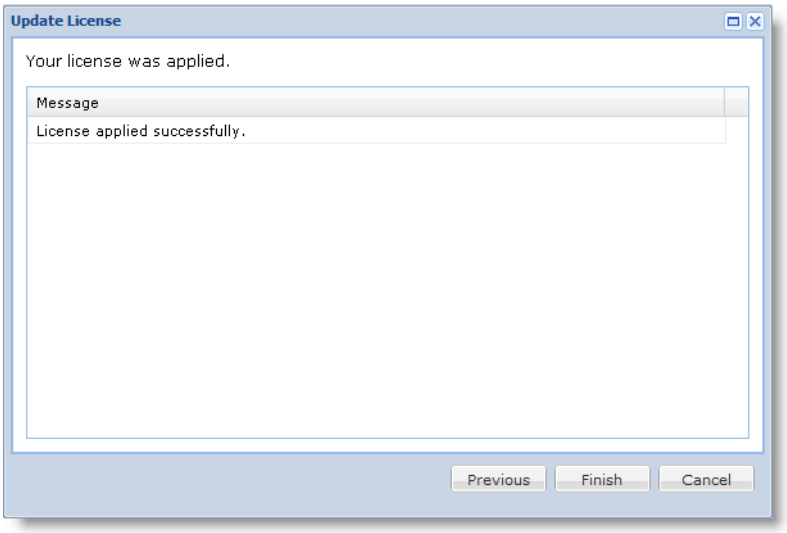


   B. If you uploaded your license (from a ZIP or SLF file), note that the information, as shown, will be *added to* your existing license:



   To confirm and continue, click **Next**. (Alternatively, click **Previous** to re-apply the license information.)

7. The final screen of the Wizard displays a message reflecting your license status.



Click **Finish**. (Alternatively, click **Previous** to re-apply the license information.)

Additional Collections Admin Tasks

The following table summarizes additional tasks that Veritas eDiscovery Platform Administrators managing collections can perform.

Summary of Additional Collections Tasks

Task	Description
Defining Collection Admin Accounts	A user's account and its associated user role determine the system administration tasks the user can perform, and the cases the user can search and/or administer. In addition, an access profile can override the case privileges in a user's role, and limit document visibility within a case to specific folders and/or a specific date range. See *"Defining Collections Administration User Accounts" on page 178*.
Managing Task Collections	Data collections can be scheduled to occur automatically. See *"Run or Schedule a Collection Task" on page 126*. (Tasks can be stopped and started as needed.)
Backing Up Data Map and Collections	Data Maps and Collections should be backed up periodically to minimize data loss in the event of a system failure. See *"Creating Collections Backups" in the System Administration Guide*.
Managing Licenses	You can view and update the Collections license. See *"Managing Your Collections License" on page 194*.
Extend Collection Search and Retrievals to multiple servers (Enterprise Vault)	(For Veritas Enterprise Vault Storage Servers only): If you have more than one server to be used for collections from one or more Enterprise Vault sources, you can perform search and retrieval on multiple servers simultaneously to optimize input/output distribution.
Troubleshooting	System logs can be uploaded to Technical Support for analysis. (Refer to *"Troubleshooting" in the System Administration Guide*). For information about troubleshooting collections from a specific source type, see *"Troubleshooting" on page 201*.

About Collections Backups

For information about collection backups, configuring the collections backup location, or running on-demand or scheduled backups on collections, refer to the section *"Backup and Restore" in the System Administration Guide*.

Troubleshooting

This section provides tips and techniques for resolving issues you may encounter with sources or accounts associated with your data map on your appliance.

Topics in this section:

Troubleshooting the collection task failures

If your collection tasks fail and if you see the following type of error logs in Windows Event Viewer, then a possible cause might be related to User Account Control (UAC) settings on your appliance. To troubleshoot this issue, the system administrator must first deactivate UAC settings on the appliance, and then restart the appliance.

Event Logs (an example):

```
Faulting application name: conhost.exe, version: 6.3.9600.17415, time
stamp: 0x5450410b
Faulting module name: USER32.dll, version: 6.3.9600.18202, time stamp:
0x569e7d02
Exception code: 0xc0000142
Fault offset: 0x00000000000ecdd0
Faulting process id: 0x1cb4
Faulting application start time: 0x01d1ad09184a5a20
Faulting application path: C:\Windows\system32\conhost.exe
Faulting module path: USER32.dll
Report Id: 56528905-18fc-11e6-80ef-005056aa3a0d
Faulting package full name:
Faulting package-relative application ID:

--------------
Faulting application name: cmd.exe, version: 6.3.9600.17415, time stamp:
0x545042b1
Faulting module name: KERNELBASE.dll, version: 6.3.9600.18202, time stamp:
0x569e7d02
Exception code: 0xc0000142
Fault offset: 0x00000000000ecdd0
Faulting process id: 0x1ca4
Faulting application start time: 0x01d1ad091847749e
Faulting application path: C:\Windows\system32\cmd.exe
Faulting module path: KERNELBASE.dll
Report Id: 934dea14-18fc-11e6-80ef-005056aa3a0d
Faulting package full name:
Faulting package-relative application ID:
```

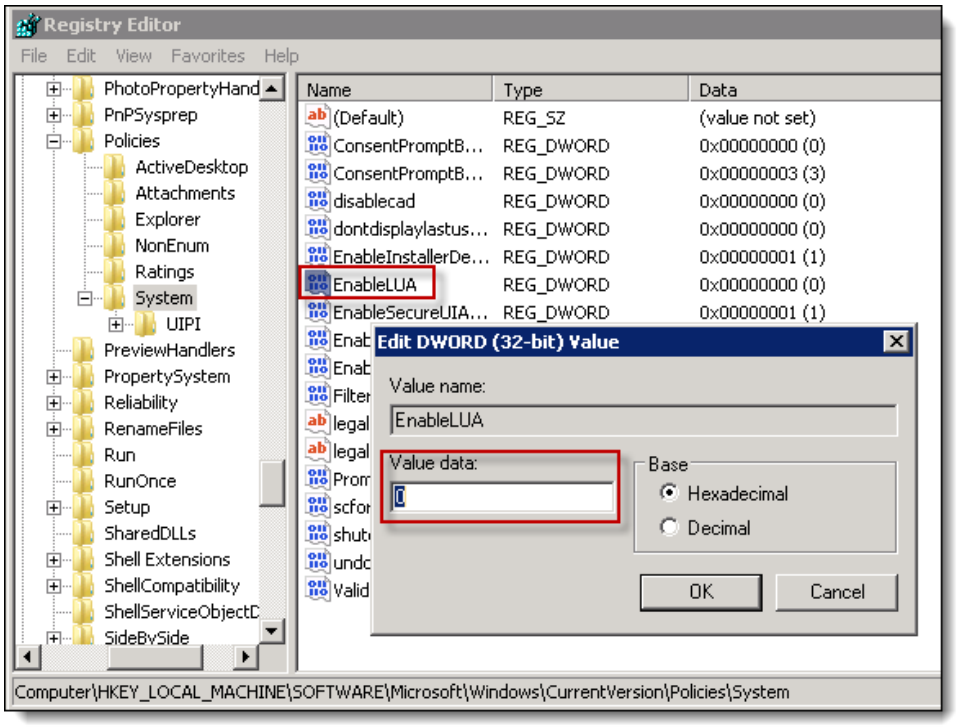
How to deactivate UAC on your appliance:

Before making any changes to registry, it is recommended to take a Registry Backup: Right-click > **Export** > Save it at a desired location.

While UAC can be disabled by selecting “Never Notify” from **Action Center** > **Change User Account Control settings**; the system administrator must deactivate it by modifying the registry key.

You can turn off UAC via registry by changing the DWORD "**EnableLUA**" from 1 to 0 in "*HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system*".

A notification to reboot the appliance is displayed. After the reboot, UAC is disabled.



Troubleshooting Exchange collections

If you are unable to see the mailbox or Exchange server, or you are having difficulty collecting from Exchange, follow the steps below to troubleshoot the issue. Continue in order until the issue has been resolved.

To troubleshoot Exchange Server collection

1. Download Active Directory explorer (AD explorer) from Microsoft® Sysinternals™

   Web site: http://technet.microsoft.com/en-us/sysinternals/default.aspx

2. Launch AD explorer, and run it as the *EsaApplicationService* account. You should be able to see the Exchange server and mailboxes in the AD Forest.

3. Launch Outlook from the appliance, and log on as the same Source account you use for the Exchange server source in your Data Map. Specify the mailbox and Exchange server name. You should be able to open the mailbox.

4. Check your security settings for the mailbox. The security settings may be preventing mailbox access.

Troubleshooting Exchange 2013 collections

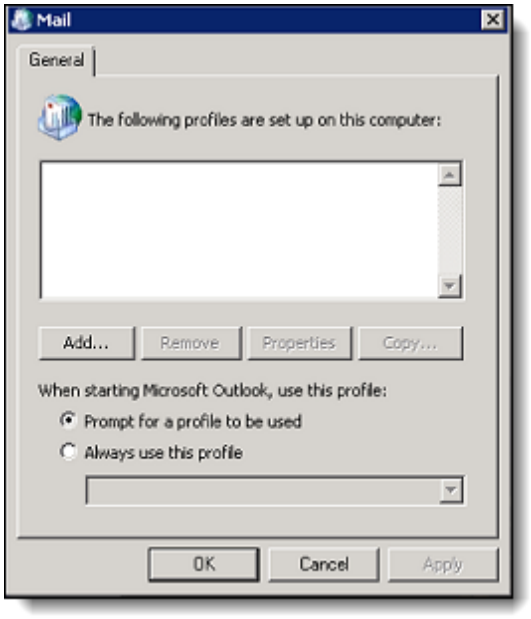
The Exchange 2013 mailbox uses the built-in Auto-discover feature which automatically detects your Microsoft Outlook settings. Your collection task to collect from the Exchange 2013 mailboxes may fail if the profile information for your Exchange server is not retrieved correctly.

If your collection task fails, you may check the *ExchangeAutoDiscovery_output.log* that shows the error messages: *Profile info for Exchange server "Server name" could not be retrieved from any of the GCs*.

To troubleshoot the issue, you must follow the steps below to configure the Outlook template profile for the user mailbox.

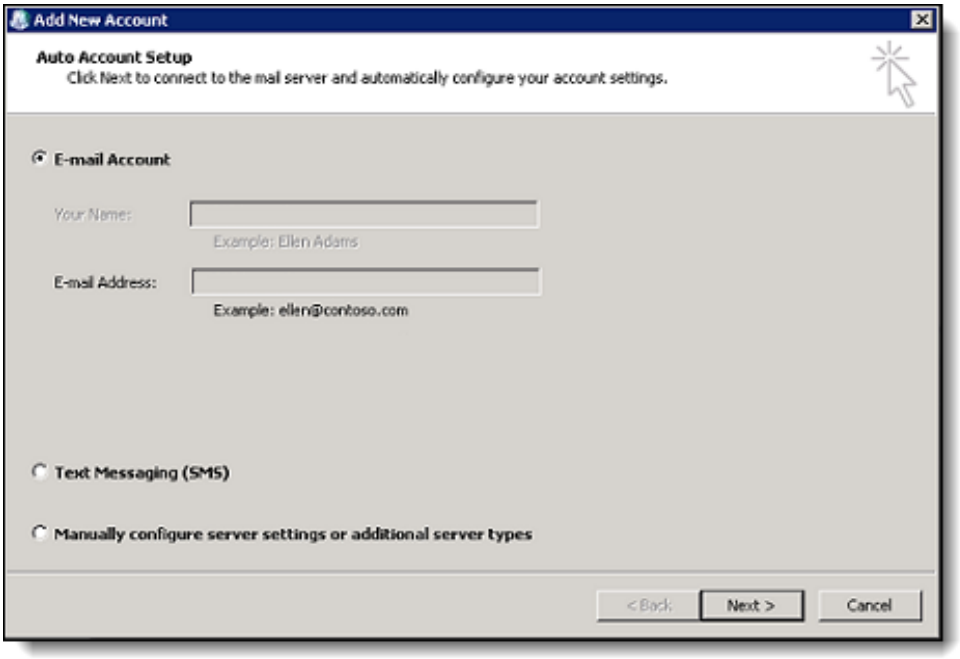
To configure the Outlook template profile

1. Log on to the box as the Exchange Source Account. If any jobs are running, these steps should be done when jobs are completed and all Veritas services that require MAPI are stopped (*PSTCrawler* and *PSTRetriever*). When a MAPI process is running, profile databases are locked and cannot be configured.
2. Go to **Control Panel**, click **Mail (32-bit)**. The **Mail** dialog appears.



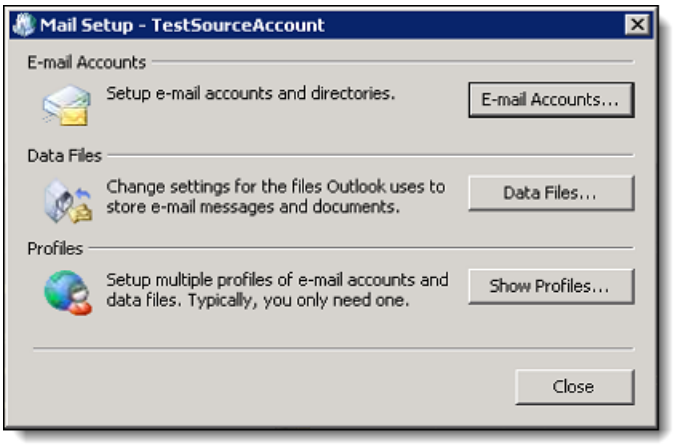
3. Click **Add**. The **New Profile** dialog appears.

4. Enter a name for the profile in the **Profile Name** field.
5. Click **OK**. The **Add New Account** dialog appears.

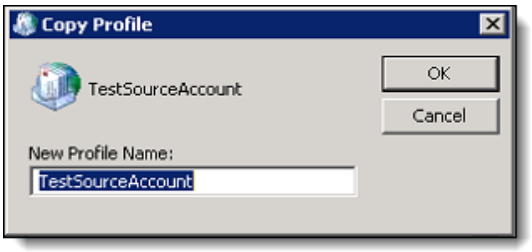


6. Click **Next**.
7. Ensure that MS Outlook is able to resolve the email address of the logged on user. Click **Next**.
8. If prompted for credentials, then provide the correct email address and password to log on to the Exchange account.
9. Once the above step is successful, click **Finish**.
10. Click **OK** on the **Mail** dialog.
11. Launch the Outlook client using the above created profile using the **Choose Profile** dialog.
12. Close the Outlook client.

13. Go to the **Control Panel** > **Mail (32-bit)**. The **Mail Setup** dialog appears.



14. Click **Show Profiles**. The **Mail** dialog appears.
15. Select the above created profile and then select **Copy**. The **Copy Profile** dialog appears.



16. In the **New Profile Name** field, enter the profile name as **ExchangeServerName-TemplateProfile-Do not Delete**, where **ExchangeServerName** must be replaced with your Exchange server name.
17. Click **OK**.
18. Click **Properties**. The **Mail Setup** dialog appears.
19. Click **E-mail Accounts**. The **Account Settings** dialog appears.
20. Click the email address displayed. The **Change Account** dialog appears.
21. Clear the **Use Cached Exchange Mode** check box.

    CAUTION: Never select **Check Name**. If you clicked **Check Name** unintentionally, then be sure to remove the **ExchangeServerName-TemplateProfile-Do not Delete** profile and add a profile with the same name.
22. Click **Next** > **Finish** > **Close**.
23. Click **Close.**
24. Click **OK**. The Outlook profile required to collect data is created.

Troubleshooting File Server or PC collections

If you are encountering issues with collecting data from a File Server or PC source, follow the steps in this section to troubleshoot the issue. This procedure replicates the network collection process in order in attempt to help you diagnose and resolve the issue.

To troubleshoot File Server or PC collection

1. Determine the user account to be used for access to the source file system. (This is either the account assigned to the source, or the user being run by EsaApplicationService.)
2. Determine the path that will be used to mount the source.
   A. For File Server sources, this is the source locator.
   B. For a PC source, this is the locator preceded by "\\" followed by "\" then the directory from where you want to collect the data.
      For example, if you want to collect "abcdata#" from a PC source whose hostname is "jsmith123", the path is: \\jsmith123\abcdata#
3. While logged in to the appliance as the EsaApplicationService user, type the following command at the command prompt:
   `net use [path] /user:[domain\user]`
   where **`[path]`** is the path you determined in step 2, and **`[domain\user]`** is the account you determined in step 1.
   – If you receive an error at this point, it could indicate one of the following cases:
      › You may need to adjust the permissions on the file system you are trying to collect data from, and/or adjust the permissions on the share itself.
      › If you are attempting to collect across domains, the domains may not be configured correctly to allow access.
   Continue to step 4 to test these cases and try to resolve the issue.
4. To troubleshoot the error complete the following steps in order until the issue is resolved:
   A. Try browsing to the path in Windows Explorer. If this is successful, you should be able to collect from the source(s).
   B. To remove the mounting you just added, type the following:
      `net use path /delete`
   C. If you still cannot collect, wait until there are no collection or processing jobs running. Then select and run the support feature **Unmount all file systems mounted**. (From the **System** view, select **Support Features**.)
   D. Try collecting from the source once again.
5. If the issue persists, contact Customer Support.

Performing Collections on a File Share Source

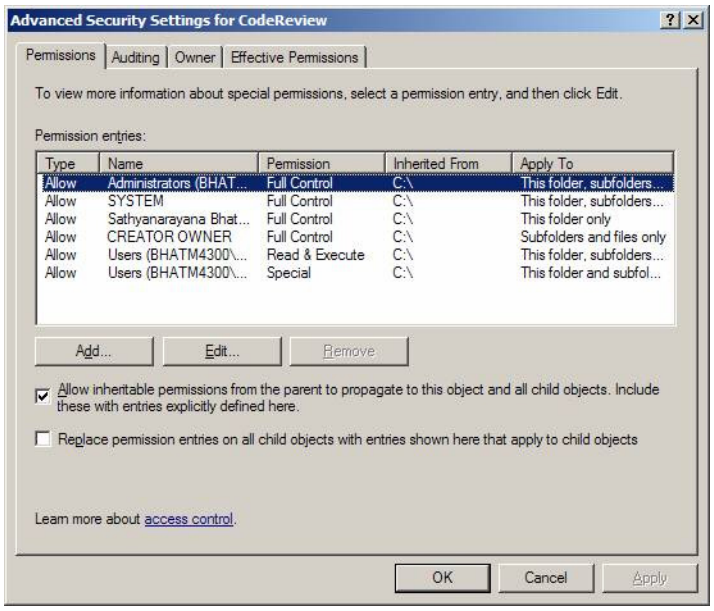
To perform the collection, run Microsoft's "net use" command, which requires 'RunAs' privileges, and do the following:

- Confirm with IT that your Group Policy Object (GPO) Software Restriction has not disabled 'RunAs.exe' for the appliance or <EsaApplicationService User>
- To test this, log on to Veritas as <EsaApplicationService User> and run the following command with Source account in a CMD shell.

```
RunAs /profile /user:domain\sourceuser cmd.exe
```

If successful, this launches another CMD.EXE shell as 'domain\sourceuser'

Also ensure that the 'domain\sourceuser' has inherited subdirectory permissions. In Windows Explorer, right-click the source directory and select **Security > Advanced > Permissions**.



Ensure that the **Allow inheritable permissions from the parent…** option is enabled.

Note: (For File Share Sources Only)

For File Share sources, the Veritas eDiscovery Platform application uses the Source Account, and performs a collection by using the RunAs service.

For more information, refer to the Microsoft Support Knowledge Base article: http://support.microsoft.com/kb/294676

In some configurations, a customer's Group Policy Object (GPO) will have to be adjusted such that it allows RunAs. Refer to the Administrator's Tip in: http://www.windowsnetworking.com/kbase/WindowsTips/Windows2003/AdminTips/Admin/DisablingtheRunAsCommand.html

With appropriate permission rules, the collection is similar to reading/opening a file over the network. You can simply copy/paste that file to another location (the preservation destination).

Troubleshooting SharePoint collections

If you encounter issues while adding a source for SharePoint 2007, 2010, 2013, and SharePoint Online or while running a collection task for these sources, see if you get the below error message in ICP logs:

"*No appropriate protocol (protocol is disabled or cipher suites are inappropriate)*"

This might happen because the SSL protocol used on your SharePoint server differs than the default TLSv1.2 protocol used on your eDiscovery Platform appliance.

By default, the SSL configuration in the eDiscovery Platform is set to accept 128-bit or greater ciphers and requires the use of the TLSv1.2 protocol. SSLv2, SSLv3.0, TLS1 and TLS1.1 are all disabled. The set of supported ciphers and protocols can be modified if needed. Consult your IT department's security specialists to determine secure settings.

Note: If your policies require the use of TLSv1.2, certificates for all appliances must be issued by an external certificate issuing authority and installed on your servers by your own IT department. For details on how to work with SSL backward compatibility, see Tech Note 226376: http://www.Veritas.com/docs/TECH226376.

You can reconfigure the SSL/TLS protocol used on your appliance. However, you should first check with your IT department before performing the following steps. It is also recommended to consider the vulnerability associated with SSL protocols, refer to http://www.Veritas.com/connect/blogs/poodle-vulnerability-old-version-ssl-represents-new-threat.

To reconfigure SSL protocol:

1. Check which protocol you are using on your SharePoint server.
2. Logon to your appliance as an administrator.
3. From the **System** > **Support Features** screen, select the **Property Browser** feature.
4. Enter the following property in the **Name of property to change** field.

   esa.icp.sharepoint.ssl.supportedProtocols

5. Modify the values in the New value (leave blank to remove) field:

   TLSv1.2,NewValue1,NewValue2

   Note: Do not remove the default value TLSv1.2 from the value list. Add the new values separated by comma.

6. Select the **Confirm change. Are you sure?** check box.
7. Click **Submit**.

Troubleshooting Office® 365 collections

Troubleshooting collection tasks failures caused by OpenMsgStore error

When collection tasks targeted Office® 365 source fails with an error "*Could not OpenMsgStore for profile*," perform the following steps:

To re-synchronize all mailboxes:

1. Logon to your appliance as a source account user.
2. Close the Outlook Client if it is open.
3. Open the Outlook Client from **Start** > **All Programs** > **Microsoft 2013** > **Outlook 2013**.
4. On the **Choose Profile** dialog, select the Outlook profile used, and then click **OK**.

   You should perform this step for "*eDP-O365-MapiHttp-TemplateProfile-Do not Delete*" profile. If you have configured the "*BPOSExchangeTemplateProfile-OL2013-Do not Delete*" profile, then you should perform this step for both profiles.
5. While opening the Outlook Client, all associated mailboxes will get synchronized.
6. Make sure that all associated mailboxes appear in the left panel.

Rerun the collection task. If the collection task still fails, contact your system administrator.

Troubleshooting template profile configuration error

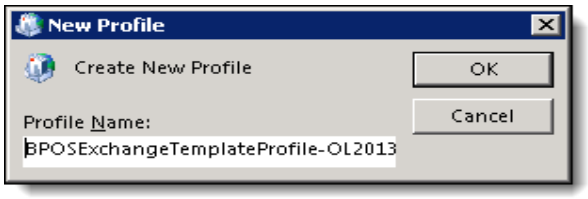
If your collection task fails, you should first check the *ExchCollection_output.log* available at *D:\CW\V90\logs* that might show the following error messages:
"*Please verify that "BPOSExchangeTemplateProfile-OL2013-Do not Delete" profile is correctly configured. Reconfigure this Outlook profile using manual configuration option and then retry the collection tasks."*

If the above error message is seen, then the system created profile "*eDP-O365-MapiHttp-TemplateProfile-Do not Delete*" seems to have configuration issues.
To resolve this issue, you need to create the outlook profile manually with the name "*BPOSExchangeTemplateProfile-OL2013-Do not Delete*" using the steps mentioned below.

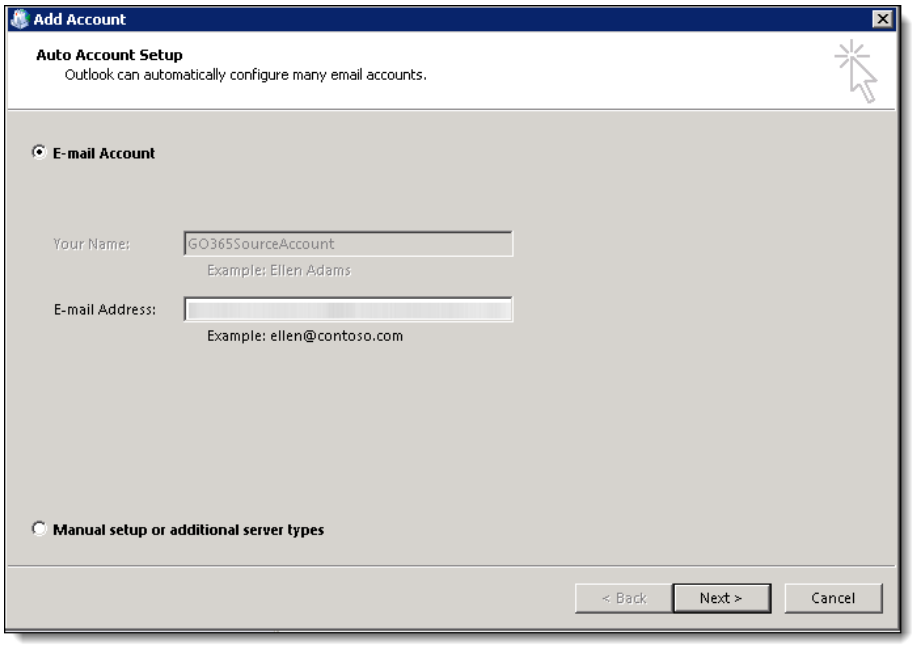
To configure the Outlook template profile

1. Log on to the box as the Exchange Source Account.
2. Go to **Control Panel**, and then click **Mail (32-bit)**. The **Mail** dialog appears.
3. If the profile with the "*BPOSExchangeTemplateProfile-OL2013-Do not Delete*" name already exists, then remove that profile.
4. Click **Add**. The **New Profile** dialog appears.

5. Create a new profile with the profile name as "*BPOSExchangeTemplateProfile-OL2013-Do not Delete*".

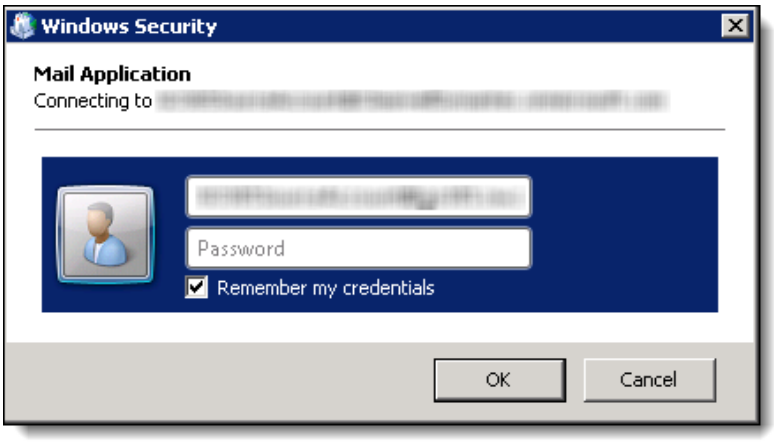


6. Click **OK**. The **Add New Account** dialog appears.

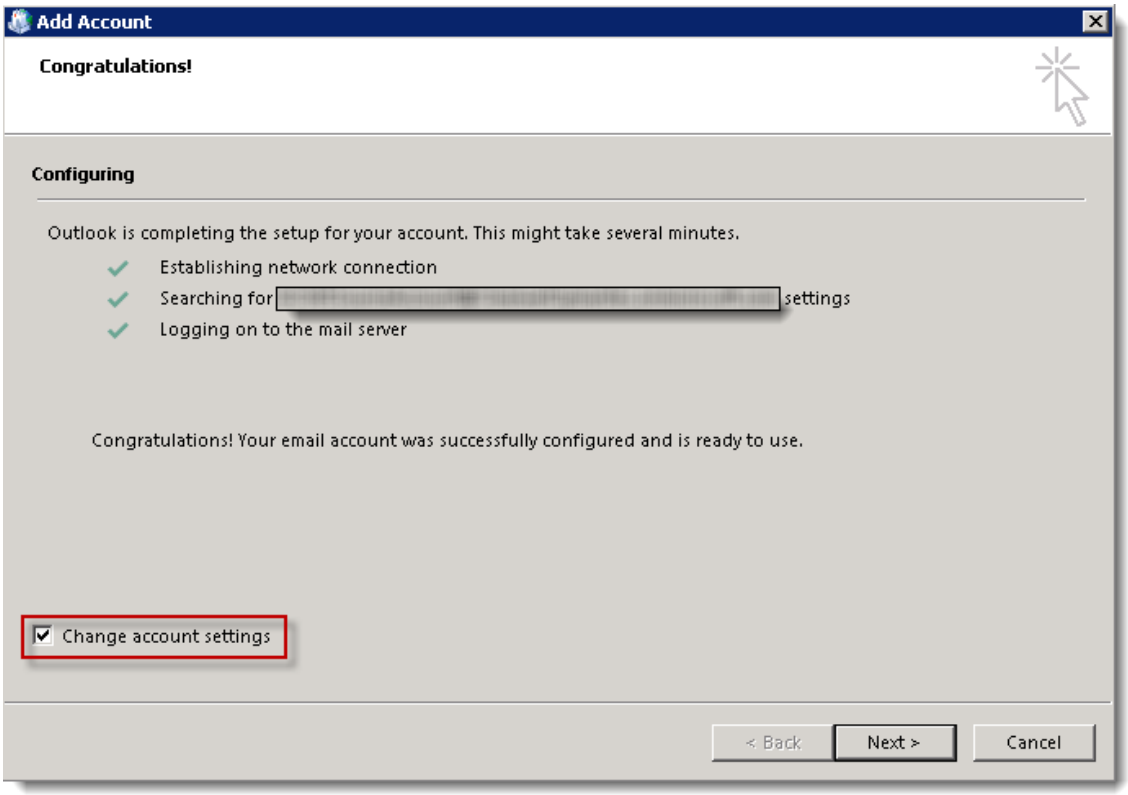


7. Keep the default selections under E-mail Account.
8. Click **Next**. Windows Security dialog appears.

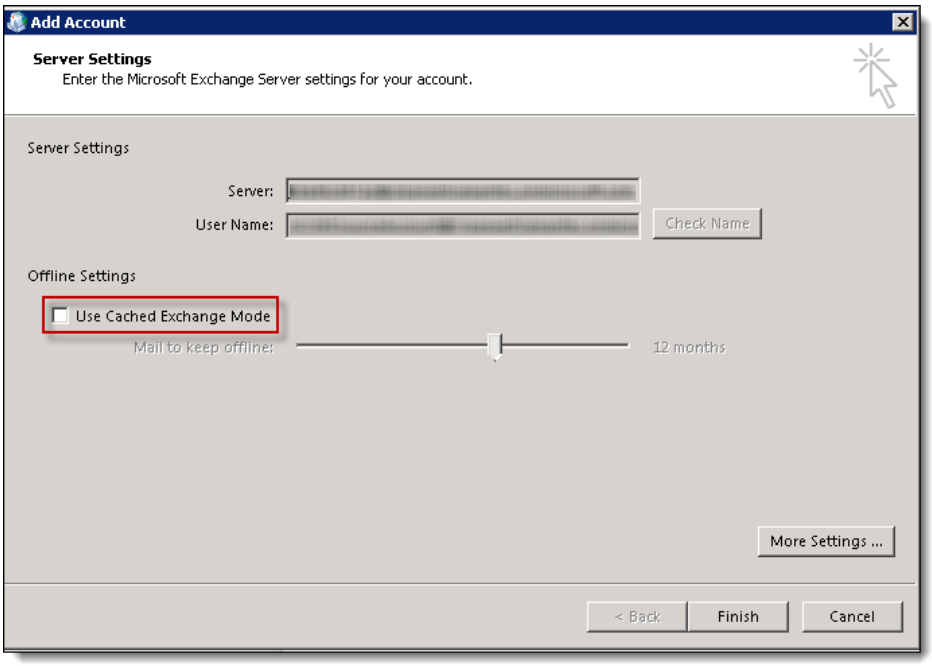
9. Enter the Exchange source account credentials and select the **Remember my credentials** check box. Click **OK**. The Add Account screen appears.



10. Select the **Change account settings** check box. Click **Next**.



11. Clear the **Use Cached Exchange Mode** check box.



12. Click **Finish**. The Outlook profile required to collect data is created.

After you perform the above troubleshooting steps for the Outlook template profile creation, you should be able to collect data from your Office® 365 mailboxes.

If you still fail to collect data, perform the following additional troubleshooting steps:

1. Set the value for the property ***esa.icp.collection.exchange.RetrieveHomeServerDetails*** as **True** by using **System** > **Support Features** > **Property Browser**.
2. Make registry key changes:
   A. Log on to the box as the Exchange Source Account.
   B. Close all Microsoft applications.
   C. Start Registry Editor: **regedit.exe**
   D. Enable Autodiscover service for non-Outlook applications:
      I. Select the following registry key:

         HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Cached Mode

      II. On the **Edit** menu, point to **New**, and then select **DWORD Value**.
      III. Enter *AllowAutoDiscoverForNonOutlook*, and then press **Enter**.
      IV. In the **Details** pane, press and hold (or right-click) *AllowAutoDiscoverForNonOutlook*, and then select **Modify**.
      V. In the **Value** data box, enter **1**, and then select **OK**.

E. Configure Outlook behavior to allow HTTP redirection:
   I. Select the following registry key:

      HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\AutoDiscover\RedirectServers

      You can also use the following registry subkey:

      HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\15.0\Outlook\AutoDiscover\RedirectServers
   II. Click the **Edit** menu, point to **New**, and then click **String Value**.
   III. Type the name of the HTTPS server to which AutoDiscover can be redirected without prompting for confirmation from the user, and then press **ENTER**.

      For example, to allow redirection to *https://autodiscover-s.outlook.com*, the first **String Value** (REG_SZ) name would be: *autodiscover-s.outlook.com*
   IV. There is no need to add text to the **Value data** box. The Data column should remain empty for the string values that you create.
   V. To add additional HTTPS servers to which *AutoDiscover* can be redirected without displaying a warning, repeat steps b, c, and d for each server.

F. Exit Registry Editor.

Troubleshooting Office 365 collection failures

If you encounter issues where Office 365 collection fails to collect data when the mailbox is present on a different domain. To fix this issue, you should set the following property using **Support Feature** > **Property Browser**.

Property: ***esa.icp.exchange.online.sao365emailId.User_Name***

Value: Email address of the source account from where you would be running the collection

For example:

Property: ***esa.icp.exchange.online.sao365emailId.go365sourceaccount***

Value: ***go365sourceaccount@xyz.com***

Troubleshooting Collector Sources

If you encounter issues attempting to add a collector or run a collection task from a collector source, review the following checklist first. Check your setup against these frequently encountered issues to verify your collector source status before contacting Customer Support for assistance.

Do you have the right credentials?

Check which credentials you are using and double-check how you entered Account information on the **Sources** > **Add** screen.

- Note that leaving the Account field blank will default to the current logged-on Veritas eDiscovery Platform ESA services user account credentials. You may need to enter a different account, as specified for the collector you are adding.
- If you are attempting access through a browser, try accessing the data source (Documentum, Livelink, or FileNet) directly, not through the Veritas eDiscovery Platform browser.
- Check how you are entering the credentials - *username* versus *domain\username* versus *username@domain*
- Is your collection task trying to write the results to a location? Is the location accessible? Are the credentials correct for accessing this location? Try browsing to the location through Windows Explorer from the appliance.

Are there documents to collect?

For these ECM data sources, Veritas eDiscovery Platform may only collect documents, but not other data types (such as calendar items, and plug-in widgets).

Are the documents getting filtered out?

Check all the filters that you specified and ensure that the documents which are not being collected are not part of other filter criteria (date, author, folder, file type/extension, keywords).

Was Veritas eDiscovery Platform not able to collect all the documents?

Most likely, the cause could be that either access is denied (to either a file or directory), or by a locked file (because its open or is being used by a process).

- If a file cannot be downloaded from within the UI of a collector, then Veritas eDiscovery Platform is not able to collect the data.
- Check the *Uncollected.csv* and *Validation.csv* files in the job log to find the filenames and paths.

Configuring SSL-enabled CMIS compliant content management repositories

While creating a source for CMIS-compliant Documentum, Livelink, and FileNet data sources, the Fetch Repositories functionality doesn't work due to errors in connection to the CMIS repository. The server log file shows the *SSLHandshakeException* exception.

This happens because a valid Root Certificate Authority (CA) certificate is not installed on JRE's default keystore. When the host's certificate does not have a valid trust chain, i.e if a certificate signed by private CA or a self-signed certificate is used, then the connection to the specified CMIS repository fails.

If a certificate signed by private CA or a self-signed certificate is used, you will need to import the hosts's Root CA certificate into the JRE's default keystore. It is recommended to contact your CA for a valid Root CA certificate.

The hostname used in the CMIS repository URL should be same as Common Name (CN) specified in the certificate. For example, if the certificate has CN as "testserver.com", then the URL should be like *https://testserver.com:<port no>/url*. Make sure that the hostname should be resolvable from the eDiscovery Platform appliance.

Following are just example procedures for your reference. You must consult your own IT department before you perform the steps that fit in your environment.

To import the root certificate:

1. Go to the JDK directory.

   cd C:\jdk-8u121-windows-x64\jre\lib\security\

2. Run the keytool command.

   > c:\jdk-8u121-windows-x64\bin\keytool.exe -import -trustcacerts -alias CMISRootCA -file c:\temp\CMIS_rootCA_cert.crt -keystore cacerts

   where, c:\temp\CMIS_rootCA_cert.crt is the file path of your Root CA certificate.

3. Enter the keystore password.

(If applicable) To import the intermediate certificate

1. Go to the JDK directory.

   cd C:\jdk-8u121-windows-x64\jre\lib\security

2. Run the keytool command.

   > c:\jdk-8u121-windows-x64\bin\keytool.exe -import -trustcacerts -alias CMISIntermediateCA -file c:\temp\CMIS_intermediateCA_cert.crt -keystore cacerts

   Where, c:\temp\CMIS_intermediateCA_cert.crt is the file path of your intermediate certificate.

3. Enter the keystore password.

Enabling Scaleout Mode (for Enterprise Vault Collection)

Use properties described in this section to configure multiple appliances to distribute, search, collect, or hold tasks against Veritas Enterprise Vault sources.

- *"Enable Scaling to Multiple Enterprise Vault Servers" in the next section*
- *"Enable Multiple PST Creation" on page 218*

Enable Scaling to Multiple Enterprise Vault Servers

Searches, holds, and collections from Enterprise Vault sources can be distributed across multiple appliances in order to increase speed and scale to larger Enterprise Vault deployments. Appliances which are already clustered (for Processing, Analysis & Review purposes) will automatically distribute search, hold and collection tasks against Enterprise Vault sources across all appliances.

For non-clustered environments, or if there is a need to manually override the appliances to be used for Identification and Collection in a clustered environment (such as when only using four out of five appliances in a cluster for collection), use the steps below.

For example, if an environment consists of 50 Enterprise Vault servers and four appliances named *Veritas_Appliance_Master*, *CWA_Node1*, *CWA_Node2*, and *CWA_Node3*, the Veritas_Appliance_Master can be configured to distribute all search, hold, and collection jobs against Enterprise Vault sources across the three nodes. To do so, the following property must be set on the master appliance to indicate which are the node appliances.

Note: Search, hold, and collection jobs created manually on any of the node appliances will only run locally (they will not be distributed).

To scale Enterprise Vault collection to two or more servers

1. From the **System** view, click **Support Features**, and select **Property Browser**.
2. (Using the above example) Set the property: **esa.icp.collection.scaleout.remote_nodes= *[CWA_Node1,CWA_Node2,CWA_Node3]***

   where ***CWA_Node1,CWA_Node2,CWA_Node3*** are the hostnames or IP addresses of the node appliances.
3. Click **Submit**.

   To check if scalability has been enabled, navigate to **All Collections > Collect > Status** and open the Job status log for any tasks targeting Enterprise Vault sources.

   Note: You must restart all ongoing search, hold, and collection tasks against Enterprise Vault sources for scaleout mode to take effect.

You can disable distributed search, holds, and collection tasks at any time by following the steps above, and leaving the Value field blank.

Note: The location for the collection should be on a shared location and should be accessible to all nodes. If the location is local to the master appliance, or on a location that is not visible to one or more nodes, those nodes will not be used for scaling-out.

For Exchange-based Archive Collection, the above configuration needs to be done on all nodes.

For task restart ability, mapping about nodes and the sub-tasks they perform should be maintained within a task so that upon restart, each node is given the sub-task it was performing earlier. Even if one mapped node is down after restarting a task, the task fails giving a proper error message.

When a stopped task is deleted, the temporary data on all nodes used for that task is also deleted.

Enable Multiple PST Creation

Note: (For Exchange-based Enterprise Vault Collection Only)

This section applies only to Enterprise Vault collection from Microsoft Exchange archives (not NSF or Exchange Mailboxes).

Due to a limitation that exists with Microsoft's MAPI protocol, a user can write only one PST at a time. However, if you need to support the model of multiple PST creation, you can create multiple Local User accounts. Each user would then be able to create one PST at a time. Multiple users allows for concurrent PST creation.

Follow the steps to create as many users as needed for concurrent PST creation.

To enable multiple PST creation on the appliance

1. Create more than one Local User on the appliance (one for each additional PST creator) and add them to the Local Administrators group.
2. From the System view, click **All Collections > Source Accounts**. Create a source account for each Local User created in step 1.
3. From the **System** view, click **Support Features**, and select **Property Browser**.
4. Enter the property:
   esa.collection.ev.pst_writer_ic_source_accounts=*[user1,user2,user3]*

   where ***user1***, ***user2***, ***user3*** are the Source Account names created in step 2 (comma separated). Include all accounts created for each user.
5. Click **Submit**.

You can disable this at any time by entering the property and leaving the field blank.

Only the collection processes that have started after setting this property will support parallel creation of PSTs. Existing collections will need to be stopped and restarted.

Troubleshooting the EV.cloud discovery

When you discover an EV.cloud site for the first time, all EV.cloud accounts are discovered. However, when you re-discover the EV.cloud site, only new or modified accounts are discovered. After discovering an EV.cloud site, you can see the number of discovered accounts on the **System** > **Directories and Servers** > **EV.cloud** page. You can choose to discover all accounts in addition to the new or modified accounts even when you re-discover the EV.cloud site. To achieve this, you only need to do a full synchronization of the EV.cloud accounts.

To apply a full synchronization for the EV.cloud accounts:

1. From the **System** view, click **Support Features**.
2. Select **Property Browser**.
3. Enter the property: **esa.evcloud.evcloud_discovery_force_full_synch**
4. Set the value to **True**. By default, this property is set to **False.**
5. Click **Submit**.

When you re-discover the EV.cloud site, the system will discover all accounts that are available on the EV.cloud site.

Troubleshooting Enterprise Vault Retry Failures

Retry failure due to storage server connectivity:

A retry task may fail due to server connectivity issues, such as the storage server or the Enterprise Vault server being down. When content retrieval fails, you can set two new properties using **System** > **Support Features** > **Property Browser** to configure the number of retry attempts and the interval between two retry attempts.

- **esa.icp.collection.ev.ContentRetriever.RetryCount=12**
- **esa.icp.collection.ev.ContentRetriever.WaitBetweenRetries.Minutes=5**

Retry task will fail only after all retry attempts configured as mentioned above are exhausted.

Retry failure due to Index Server connectivity:

A retry task may fail when there is a connectivity issue with the Index Server. You might receive the following error codes due to the Index Server connectivity issues:

- E_SERVER_UNAVAILABLE 0x800706BA
- INDEXING_W_CANT_ACCESS_DIRECTORY 0x80041C11
- INDEXING_W_INDEXDISABLED 0x80041C84
- INDEXING_W_SERVICE_BUSY 0x80041C86
- INDEXING_W_SERVER_STOPPING 0x80041C1A
- INDEXING_W_SERVICE_STOPPING 0x80041C47

- INDEXING_W_SEARCH_WOULD_BLOCK 0x80041C70
- INDEXING_W_SEARCH_TIMEDOUT 0x80041C71
- INDEXING_E_FAILED_SEARCH_REQUEST 0xC0041C67
- INDEXING_E_INDEX_SEARCH_FAILED 0xC0041C0E
- EV_INTERNAL_ERROR 0xc0041c09

You can set the following properties using **System** > **Support Features** > **Property Browser** to configure the number of retry attempts and the interval between two retry attempts:

- **esa.icp.collection.ev.EVSearcher.WaitBetweenRetries.Minutes=5**
- **esa.icp.collection.ev.EVSearcher.SearcherRetryCount=12**
- **esa.icp.EVSearcher.ErrorCode=0x800706BA,0x80041C11,0x80041C84,0x80041C86,0x80041C1A,0x80041C47,0x80041C70,0x80041C71,0xC0041C67,0xC0041C0E,0xc0041c09**

  where,
  0x800706BA,0x80041C11,0x80041C84,0x80041C86,0x80041C1A,0x80041C47,0x80041C70,0x80041C71,0xC0041C67,0xC0041C0E,0xc0041c09 are the error codes.

Retry task will fail only after all retry attempts configured as mentioned above are exhausted.

Retry failure due to disk space:

A retry task may fail when there is no enough space that is required to retrieve the batch on the scratch temp folder.

You can set the following properties using **System** > **Support Features** > **Property Browser** to configure the number of retry attempts and the interval between two retry attempts:

- **esa.icp.collection.ev.ContentRetriever.ScratchSpaceCheck.WaitBetweenRetries.Minutes=5**
- **esa.icp.collection.ev.ContentRetriever.ScratchSpaceCheck.RetryCount=12**

Retry task will fail only after all retry attempts configured as mentioned above are exhausted.

Changing Source Accounts

If you change the Source Account (for source password) that is associated with a Source or a Location, you may have to refresh the appliance before the new Account settings take effect.

To refresh the appliance

1. From the **System** view, select **Support Features**.
2. Select the support feature **Unmount all UNC paths mounted by Clearwell appliance**.
3. Click **Submit**.

   This will clear out the old Account settings, which may have been cached.

Technical Support

To contact Veritas Technical Support, use any of the following methods:

- **MyVeritas Technical Support Portal**
  - *https://my.Veritas.com*

  Note: Access to the MyVeritas Technical Support Portal requires a SymAccount. If you do not already have on, register for a new SymAccount from the MyVeritas Technical Support Portal.
- **Phone** — Toll-Free (North America):
  - 1-800-342-0652
    For regional contact numbers: *http://www.Veritas.com/business/support/techsupp_contact_phone.jsp*

For additional information about Technical Support, Licensing, Customer Service, and to view a list of information to have available when contacting Technical Support, see *"Technical Support" on page 14*.

Appendix A: Product Documentation

The table below lists the administrator and end-user documentation that is available for the Veritas eDiscovery Platform product.

Veritas eDiscovery Platform Documentation

Document	Comments
Installation and Configuration	
Installation Guide	Describes prerequisites, and how to perform a full install of the Veritas eDiscovery Platform application
Upgrade Overview Guide	Provides critical upgrade information, by version, useful prior to upgrading an appliance to the current product release
Upgrade Guide	Describes prerequisites and upgrade information for the current customers with a previous version of the software application
Utility Node Guide	For customers using utility nodes, describes how to install and configure appliances as utility nodes for use with an existing software setup
Native Viewer Installation Guide	Describes how to install and configure the Brava Client for native document rendering and redaction for use during analysis and review
Distributed Architecture Deployment Guide	Provides installation and configuration information for the Review and Processing Scalability feature in a distributed architecture deployment
Getting Started	
Navigation Reference Card	Provides a mapping of review changes from 8.x compared to 7.x and the user interface changes from 7.x compared to 6.x
Administrator's QuickStart Guide	Describes basic appliance and case configuration
Reviewer's QuickStart Guide	A reviewer's reference to using the Analysis & Review module
Tagging Reference Card	Describes how tag sets and filter type impact filter counts
User and Administration	
Legal Hold User Guide	Describes how to set up and configure appliance for Legal Holds, and use the Legal Hold module as an administrator
Identification and Collection Guide	Describes how to prepare and collect data for processing, using the Identification and Collection module
Case Administration Guide	Describes case setup, processing, and management, plus pre-processing navigation, tips, and recommendations. Includes processing exceptions reference and associated reports, plus file handling information for multiple languages, and supported file types and file type mapping
System Administration Guide	Includes system backup, restore, and support features, configuration, and anti-virus scanning guidelines for use with Veritas eDiscovery Platform
Load File Import Guide	Describes how to import load file sources into Veritas eDiscovery Platform
User Guide	Describes how to perform searches, analysis, and review, including detailed information and syntax examples for performing advanced searches

Veritas eDiscovery Platform Documentation

Document	Comments
Export and Production Guide	Describes how to use, produce, and troubleshoot exports
Transparent Predictive Coding User Guide	Describes how to use the Transparent Predictive Coding feature to train the system to predict results from control data and tag settings
Audio Search Guide	Describes how to use the Audio Search feature to process, analyze, search and export search media content
Reference and Support	
Audio Processing	A quick reference card for processing multimedia sources
Audio Search	A quick reference card for performing multimedia search tasks
Legal Hold	A quick reference card of how to create and manage holds and notifications
Collection	A quick reference card of how to collect data
OnSite Collection	A quick reference for performing OnSite collection tasks
Review and Redaction	Reviewer's reference card of all redaction functions
Keyboard Shortcuts	A quick reference card listing all supported shortcuts
Production	Administrator's reference card for production exports
User Rights Management	A quick reference card for managing user accounts
Online Help	
Includes all the above documentation (excluding Installation and Configuration) to enable search across all topics. To access this information from within the user interface, click **Help**.	
Release	
Release Notes	Provides latest updated information specific to the current product release