Veritas eDiscovery Platform™

Identification and Collection Guide

10.2

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: 2022-9-3.

Legal Notice

Copyright © 2022 Veritas Technologies LLC. All rights reserved.

Veritas and the Veritas Logo are trademarks or registered trademarks of Veritas Technologies LLC or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This product may contain third-party software for which Veritas is required to provide attribution to the third party ("Third-Party Programs"). Some of the Third-Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Refer to the Third-Party Legal Notices for this product at: https://www.veritas.com/about/legal/license-agreements

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Veritas Technologies LLC and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. VERITAS TECHNOLOGIES LLC SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Veritas as on premises or hosted services. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054
http://www.veritas.com

Contents

About This Guide 9

Related Documents 9
Revision History 10
Technical Support 16
Documentation 16
Documentation Feedback 16

Getting Started 17

About Data Identification and Collection 17
Identification and Collection Module User Interface 18
Checklist: Before You Begin... 19
Logging On 19
Collection Workflow 20

Network and Data Map Setup 23

About Data Mapping 23
Supported Source Types 23
Best Practices 24
Network Impact and Performance 24
Veritas eDiscovery Platform Collection Methodology and Setup 24
Tips, Troubleshooting, and Technical Support 25
Setting Up Your Data Map 26
Before You Begin... 26
Source Account Overview 26
Verify Network Setup by Data Source 27
Adding a Source Account 30
Define Source Groups (Optional) 31
Securing source account credentials 32
Data Discovery Overview 35
Mapping Employee Attributes 36
Importing Custodians to Your Data Map 37
Adding Locations for Collected Data 46

Setting up Data Sources 49

About Adding (or Importing) Sources to Your Data Map 49
Required Source Information 51
Import Sources from CSV or Script 52
Local Domain Exchange Setup 56
Step 1: Create a New Domain Admin Account 57
Step 2: Perform Active Directory Discovery and Import Custodians 60
Step 3: Add Exchange Source to the Data Map 61
Step 4: Test an Exchange Mailbox Collection 62
Lync 2013 Setup 63

Microsoft 365 Setup 64
Exchange and OneDrive 64
Prerequisites 65
Setting up Microsoft 365 65
Best Practices 72
Limitations in Microsoft 365 collection 72
Collections from Microsoft 365 source through a proxy 73
Microsoft Teams 74
Prerequisites 74
Installing and Configuring the Merge1 Application 76
Configuring eDiscovery Platform for Microsoft Teams data collection 77
Turning the automatic download feature OFF 77
Configuring Rich Email Application 78
Adding a new collection task for Microsoft Teams collection 78
Creating a new collection set for Microsoft Teams collection 79
Processing collected PST files 80
Performing analysis and review of the collected PST files 81
Lotus Domino® Server Setup 82
Step 1: Perform Domino Server Discovery 82
Step 2: Add the Domino Source 83
SharePoint Source Setup 84
Add the SharePoint Source 84
File Share and Windows PC Setup 86
Add File Share (or PC) Source 86
Veritas Enterprise Vault 87
Enterprise Vault Source Considerations Before Setup 87
About Enterprise Vault Discovery 90
Step 1: Perform Enterprise Vault Discovery/Vault Administration 90
Step 2: Add Enterprise Vault Sources 94
Step 3: Update your License 95
EV.cloud 96
About EV.cloud Discovery 96
Step 1: Perform EV.cloud Discovery 96
Step 2: Add EV.cloud Sources 97
Step 3: Update your License 98

Creating and Managing Collections 99

About Collection Activities 99
About OnSite Collections 100
Creating a Collection and Running Tasks 102
Process Overview 102
Create/Add a New Collection 102
Add Tasks to a Collection 103
Copy a Collection, EV Search, or EV Hold Task 115
Filtering Best Practices for Microsoft 365 Exchange and OneDrive 116
Filtering Best Practices (for Enterprise Vault Sources) 118
Archive Selection 118
Search Techniques 121
Using special characters in the directory path 126
Using custom attributes in the Traits filter for Enterprise Vault 127

Keyword-Based Collection (Non-Enterprise Vault Sources) 129
Include/Exclude Directories 130
Enable Compression for OnSite Collection Tasks 136
Create a Collection Template 136
Run or Schedule a Collection Task 137
Schedule a Recurring Collection Task 139
Rerunning a Collection Task 140
Re-running a Collection Task for Microsoft 365 142
Retrying a Failed Collection Task (for Enterprise Vault and EV.cloud Sources) 144
Move Collected Data to Another Location 146
Running Custodian Assignments 148
Enterprise Vault Considerations 148
Performing OnSite Collection Tasks 150
Running Collection Reports 150
Collection Reports 150

Creating and Managing Search Tasks 153

About Enterprise Vault Search Task Activities 153
Prerequisites 153
Creating and Managing Search Tasks 154
Create a Search 154
Schedule a Search (or Run On-Demand) 158
View/Edit Search Tasks 159
Copy a Search Task 159
Analyze Results 160
Sample Preview 161
Run a Report 161
Delete a Search Task 162

Creating and Managing Hold Tasks 163

About Enterprise Vault Hold Activities 163
Prerequisites 163
Creating and Managing Hold Tasks 164
Create a Hold 164
Schedule a Hold 167
Create a Hold and Collection Task 169
View/Report Hold Statistics 170
Edit/Re-Apply a Hold Task 171
Copy a Hold Task 172
Release a Hold 173
Retry Release Hold 173
Enterprise Vault Hold Tasks and Release Guidelines 174

Creating, Analyzing and Processing Collections 175
About Collection Sets 175
Managing Collection Sets 175
Creating a collection set 176
Managing default type of collection sets 180
Changing Collection Settings 181
Processing Collection Sets 182
Analyzing Data (Across Your Case) 184
Viewing Processed Data 184

Collection Administration and Maintenance 189
Managing Collection User Accounts 189
Defining Collections Administration User Accounts 190
Viewing the Collections Admin Role 192
Managing Access Groups Permissions 193
Managing Custodians (Across a Case) 199
Archiving, Restoring, and Deleting Collections 203
Archiving versus Deleting Collections 203
Restoring an Archived Collection 205
Managing Your Collections License 206
About Reusable Licenses 206
Updating Your License 207
Additional Collections Admin Tasks 212
About Collections Backups 212

Troubleshooting 213
Troubleshooting the collection task failures 214
Troubleshooting Exchange collections 216
Troubleshooting Exchange collections failure in a cross-domain environment 217
Troubleshooting Exchange 2013 collections 218
Troubleshooting File Server or PC collections 221
Performing Collections on a File Share Source 222
Troubleshooting SharePoint collections 223
Troubleshooting Collector Sources 224
Enabling Scaleout Mode (for Enterprise Vault Collection) 225
Enable Scaling to Multiple Enterprise Vault Servers 225
Enable Multiple PST Creation 226
Troubleshooting the EV.cloud discovery 227
Troubleshooting Enterprise Vault Retry Failures 227
Improving the Enterprise Vault collection task concurrency 228
Custodian assignment for Enterprise Vault User Mailbox Archives 229

Changing Source Accounts **231**
Troubleshooting the Microsoft 365 collections **231**
Microsoft 365 Collection Performance Tuning **233**
Troubleshooting Microsoft Teams collections **236**
Technical Support **238**

Appendix A: Using Merge1 with eDiscovery Platform **239**

Appendix B: Product Documentation **241**

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" in the next section*
- *"Related Documents" on page 9*
- *"Revision History" on page 10*
- *"Technical Support" on page 16*
- *"Documentation" on page 16*
- *"Documentation Feedback" on page 16*

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 2022	• Updated version for release 10.1.2 • Added the information to refer to Merge1 documentation for steps to access privilege Graph APIs for tenant for collection from Microsoft Teams. See *"Microsoft 365 Setup" on page 64*. • Updated the image about Analysis & Review module to review PST files as per change in UI. See *"Performing analysis and review of the collected PST files" on page 81*.
February 2022	• Updated version for release 10.1.1 • Added the content for permission required for OneDrive collection. See *"To assign the Microsoft Graph API permissions to App ID" on page 68*. • Added the solution for Exchange collections failure in a cross-domain environment. See *"Troubleshooting Exchange collections failure in a cross-domain environment" on page 217*. • Documented the change in property required for Govcloud O365 collection. See *"Specify a connection URL to get an authentication token for O365 Discovery" on page 233*.
December 2021	• Added information on additional permission required for OneDrive collection using keyword filter. See *"To assign the Microsoft Graph API permissions to App ID" on page 68*. • Added content—for Microsoft Teams, manage proxy configuration on Merge1. See *"Collections from Microsoft 365 source through a proxy" on page 73*. • New section on setting up Microsoft Teams for data collection. See *"Microsoft Teams" on page 74*. • Added a note related to Exchange collections failure due to server not having a trusted CA signed certificate. See *"Troubleshooting Exchange collections" on page 216*. • Troubleshooting information. See *"Troubleshooting Microsoft Teams collections" on page 236*.
July 2021	• Added support for SharePoint 2019. • Updated information on the supported versions of Enterprise Vault. • Added information on collections from Microsoft 365 source through a proxy. • Updated Appendix A: Using Merge1 with eDiscovery Platform
March 2021	• Updated information about OnSite collections • Minor edits

Revision Date	New Information
September 2020	• Added information related to Office® 365 – Supported source types. See *"Supported Source Types" on page 23*. – Best practices. See *"Veritas eDiscovery Platform Collection Methodology and Setup" on page 24*. – Mapping Employee Attributes. *"Mapping Employee Attributes" on page 36*. – Import custodians to your data map. *"Importing Custodians to Your Data Map" on page 37*. – Add or importing sources to your data map. *"About Adding (or Importing) Sources to Your Data Map" on page 49*. – New topic on setting up Office® 365. *"Microsoft 365 Setup" on page 64*. – Add tasks to a collection. *"Add Tasks to a Collection" on page 103*. – Filter data while adding a collection task: *"Filtering Best Practices for Microsoft 365 Exchange and OneDrive" on page 116* – Run or schedule a collection task. *"Run or Schedule a Collection Task" on page 137* – Troubleshooting information. *"Troubleshooting the Microsoft 365 collections" on page 231* – Improve the collection performance: *"Microsoft 365 Collection Performance Tuning" on page 233* • Removed the following information; if you needs to see these sections, refer to the *9.5 version of the Identification and Collections Guide*. – Information related to legacy MAPI-based Office® 365 and BPOS data sources. – Information related to Documentum, Livelink, and FileNet data sources.
March 2020	• Minor edits
October 2018	• Added information related to – Advanced search functionality for the Enterprise Vault Keyword filter. See *"Search Techniques" on page 121*. – Custom attributes search for the Enterprise Vault Traits filter. See *"Using custom attributes in the Traits filter for Enterprise Vault" on page 127*. – Enhancements in custodian assignment for Enterprise Vault User Mailbox Archives. See *"Custodian assignment for Enterprise Vault User Mailbox Archives" on page 229*. • Minor edits throughout the guide
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

Revision Date	New Information
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
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

Revision Date	New Information
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
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 *“Trouble-shooting” on page 213*.)

Revision Date	New Information
September 2012	• Added source support for: – Four new collectors (See *"Supported Source Types" on page 23*.) – 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
May 2011	• Documented OnSite Collector secure encryption option
February 2011	• Added support for: – SharePoint with proxy – MAC (for OnSite) collection • Documented Folder Exclusion feature

Revision Date	New Information
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" in the next section*
  - *"Identification and Collection Module User Interface" on page 18*
- *"Checklist: Before You Begin..." on page 19*
- *"Logging On" on page 19*
- *"Collection Workflow" on page 20*

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, Microsoft 365 (Formerly Office 365) Exchange and OneDrive, 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**:

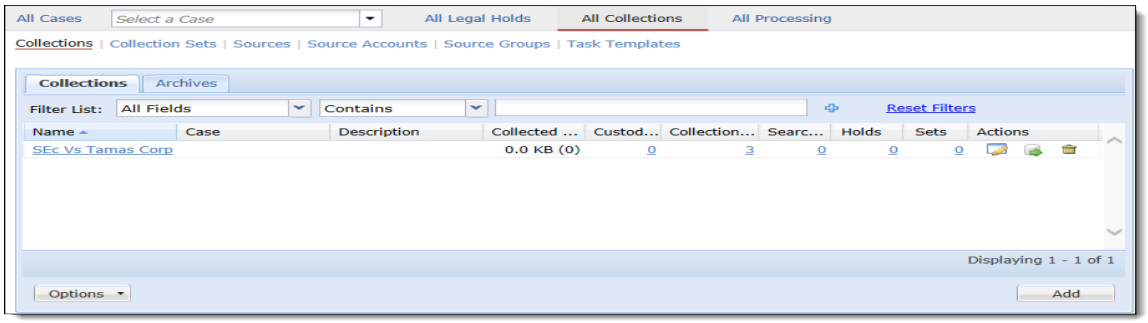


Figure: Identification and Collection Module: All Collections view

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**.

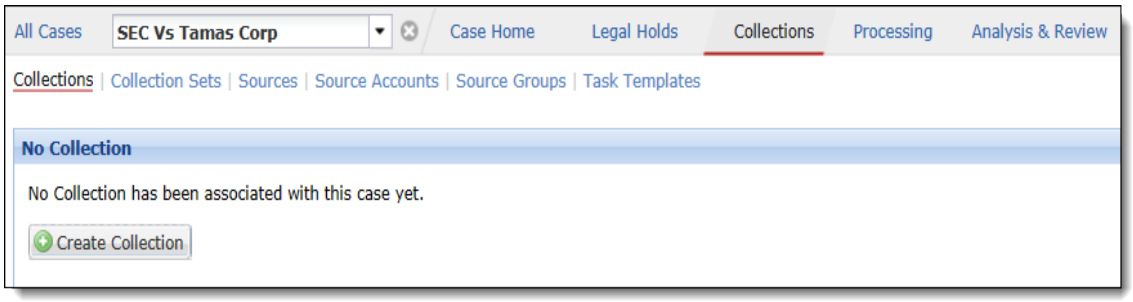


Figure: Identification and Collection Module: Within a Selected Case (No Collections)

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 102*.

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 23* 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 206* 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.

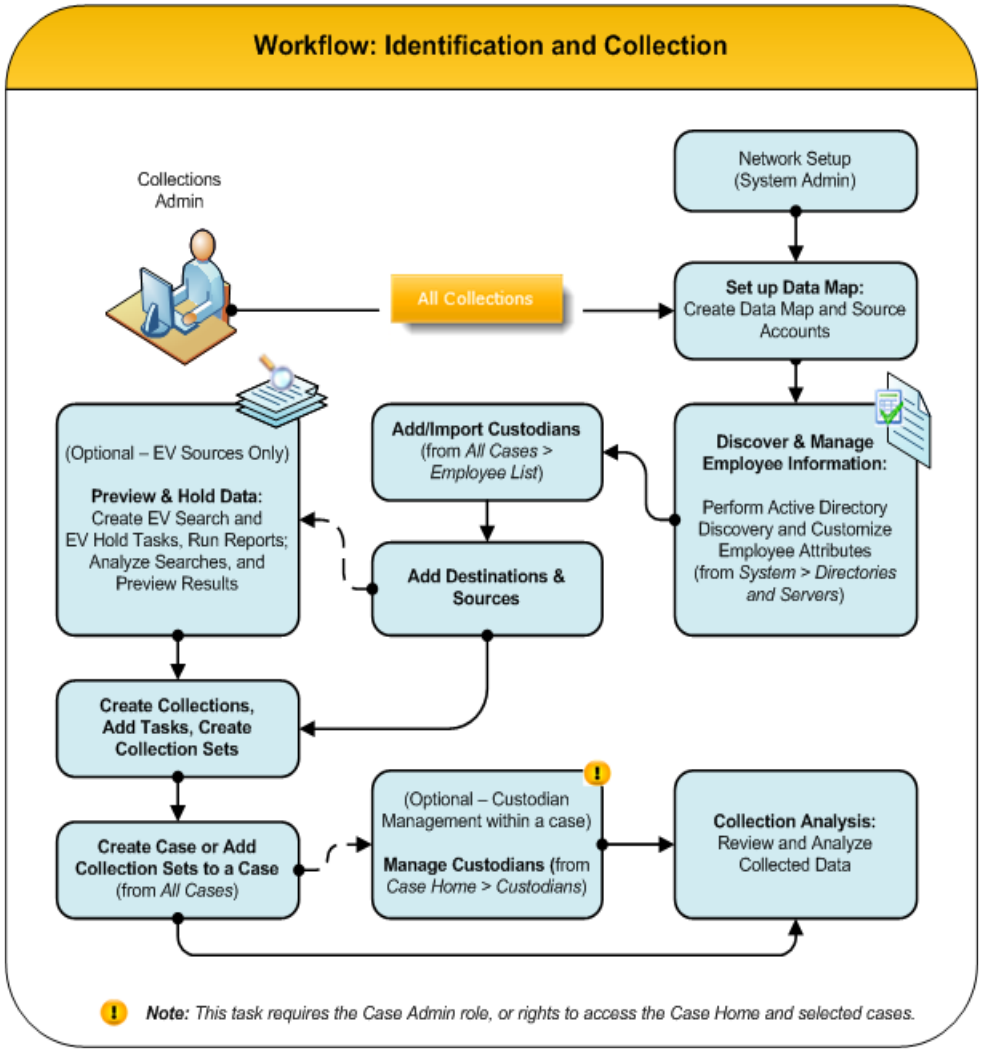
   Note: The password is the same on every appliance. Leaving the default password opens your system up to vulnerabilities.

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 23*.)
- **Discovery, Employee & Custodian Management, Sources**. Discover and customize employee information, add/import custodians, and add sources. (See *"Mapping Employee Attributes" on page 36*, and *"Importing Custodians to Your Data Map" on page 37*. To manage custodians within a specific case, see *"Managing Custodians (Across a Case)" on page 199*.)
- **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 153*, and *"Creating and Managing Hold Tasks" on page 163*, or *"Creating and Managing Collections" on page 99*.) 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 175*.)

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 189*.

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" in the next section*
- *"Best Practices" on page 24*
- *"Setting Up Your Data Map" on page 26*

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.

Note: Starting with 9.5.1, Documentum, Livelink, and FileNet data sources are not supported.

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, 2019	
Microsoft 365	Exchange and OneDrive	Connected using Microsoft Graph APIs and OAuth2 authentication
	Microsoft Teams	Collected using Merge1
SharePoint®	2007, 2010, 2013, 2016, 2019 SharePoint Online (as part of an Microsoft 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	

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 23*).

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
Microsoft 365	• 2 max parallel tasks, configurable number of threads per tasks	• Multiple user's data is collected with parallel threads running simultaneously. The number of parallel threads per user is configurable. *See "Microsoft 365 Collection Performance Tuning" on page 233*
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	• Number of threads is dynamically configured based on the number 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

Tips, Troubleshooting, and Technical Support

For troubleshooting information in this guide, see *"Troubleshooting" on page 213*, 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 24* for setting up your network.
  - See *"Troubleshooting Exchange collections" on page 216*
- 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 27*
  - See *"Adding a Source Account" on page 30*
  - See *"Define Source Groups (Optional)" on page 31*
  - See *"Securing source account credentials" on page 32*
  - See *"Data Discovery Overview" on page 35*
- As needed, map, add (or import) custodians, and specify locations and policies:
  - See *"Mapping Employee Attributes" on page 36*
  - See *"Importing Custodians to Your Data Map" on page 37*
  - See *"Adding Locations for Collected Data" on page 46*

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 27*.

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 32*.
☑	**Microsoft 365**	• Application and Site delegated permissions must be provided to the Application ID.	• See *"Prerequisites" on page 65*.

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*** property 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 32*.
☑	**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 sub folders 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.

Data Source Setup Checklist

Check	Supported Source Type	Source Account Requirements	Notes
☑	**Mac (for OnSite Collection)**	• [No additional setup required]	
☑	**Veritas Enterprise Vault**	• **Check Veritas Enterprise Vault API Runtime version**. Upgrading to Veritas eDiscovery Platform 10.0 automatically installs Enterprise Vault 12.4.0 API Runtime client. If you want to use a different certified version instead of Enterprise Vault 12.4.0, you can avoid installing Enterprise Vault 12.4.0 by clearing the check box for Enterprise Vault 12.4.0 on the "Select Features" screen of the InstallShield Wizard while upgrading to Veritas eDiscovery Platform 10.0. If you already have installed Enterprise Vault 12.4.0 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. • Refer to the *Veritas eDiscovery Platform™ Compatibility Charts* guide to know the certified versions of Enterprise Vault. • After upgrading to 10.0, 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 189*. • 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.

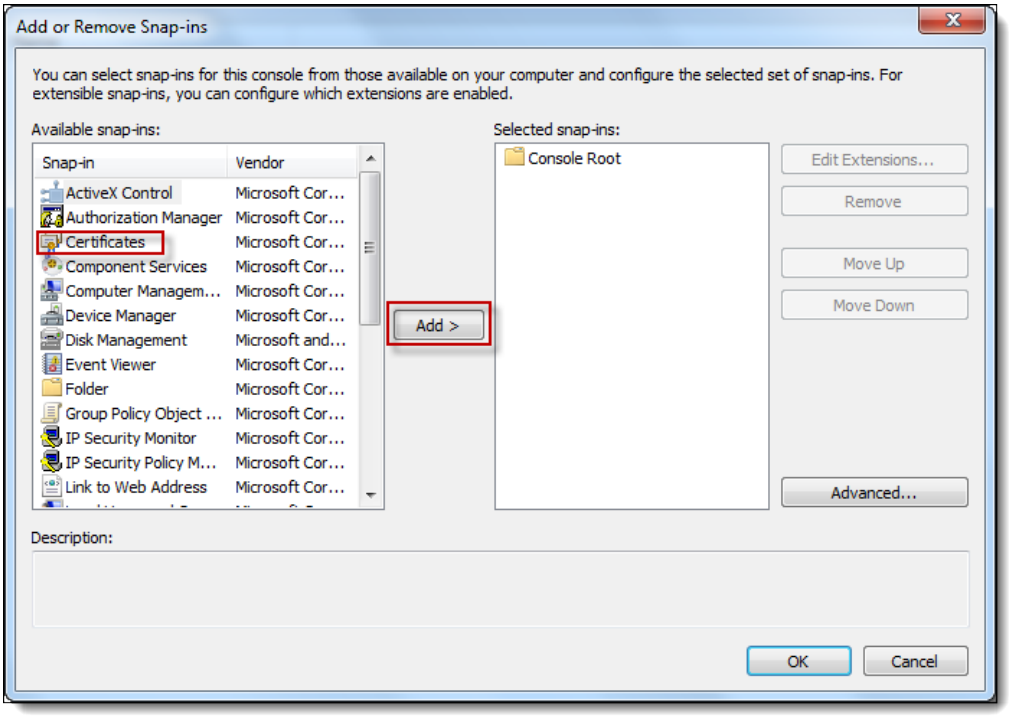
    C. Copy the Valid Certificate Where Needed.

    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.

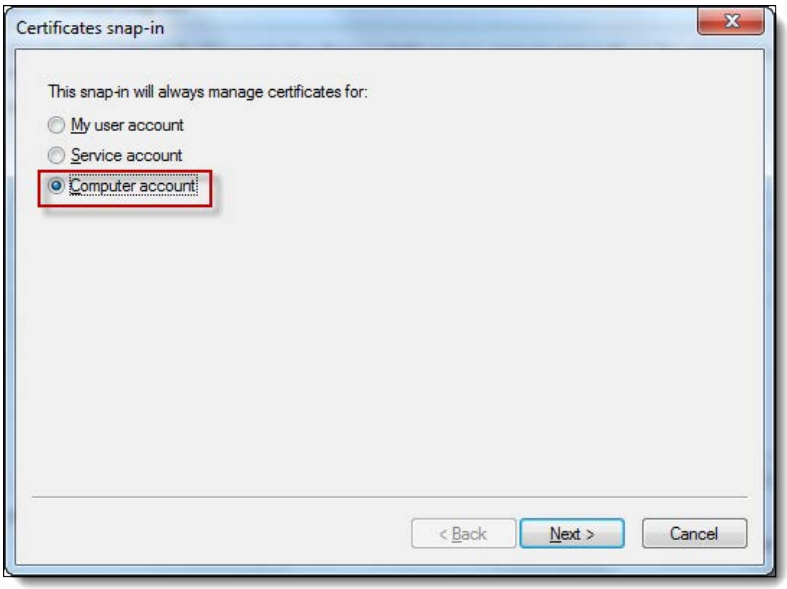
If Active Directory discovery or collection fails or a certificate gets expired or corrupt, users can see details in the server logs.

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.

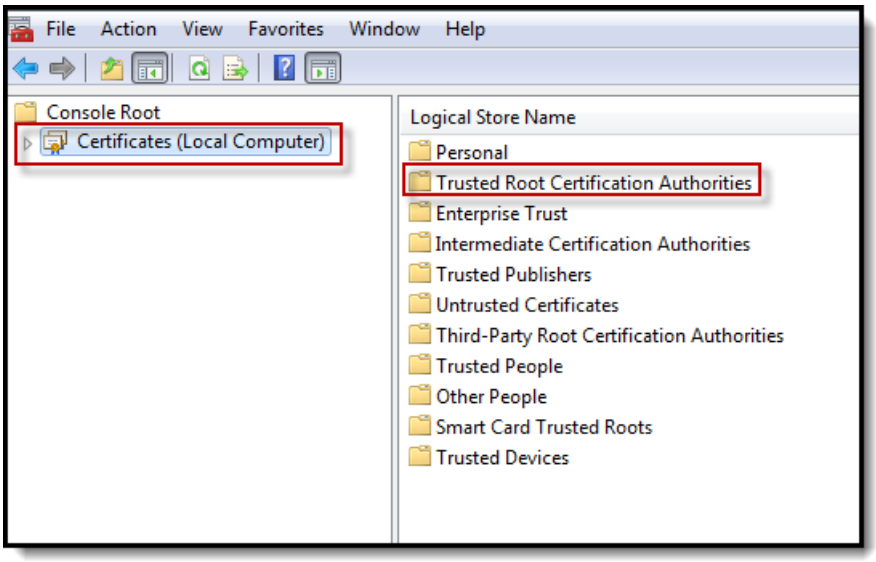


4. Select **Certificates** from the Available snap-ins section, and then click **Add**. The Certificates snap-in window appears.

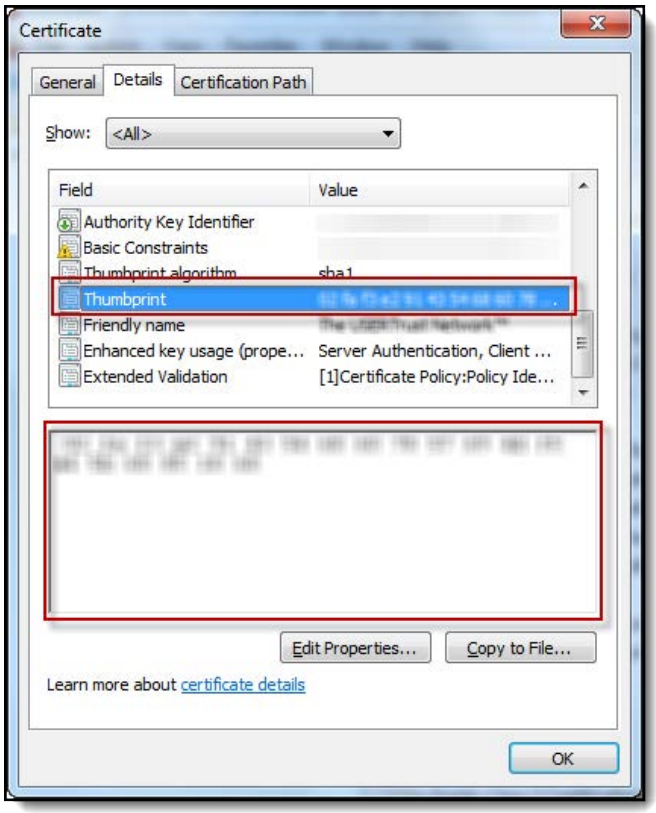


5. Select **Computer account**, and then click **Next**.
6. Click **Finish**, and then click **OK**.

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:

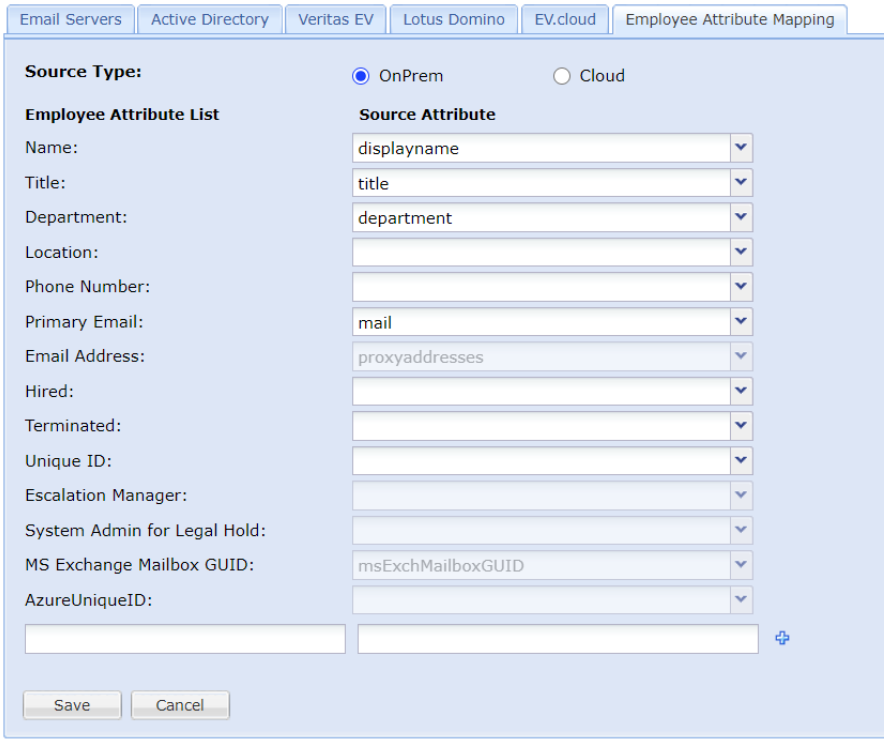
- **Email Servers**
  - Shows a repository of all discovered Exchange servers, Domino Servers, and Enterprise Vault Stores
- **Active Directory**
  - Shows domain sources available for on-premise discovery (or click to add a domain if the domain source exists, but does not appear on the list.) Verify that the sources to be added are part of your Active Directory Forest.
  - Shows tenants available for cloud discovery for Microsoft 365 (or click to add a tenant if it does not appear on the list).

  See *"Setting up Data Sources" on page 49* for detailed steps to perform discovery depending on the source type.
- **Veritas Enterprise Vault**
  - Shows results for all Enterprise Vault sources and archives from discovery. To discover a new Enterprise 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 49* 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 on-premise Active Directory (AD) or cloud Active Directory (for Microsoft 365) 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 44*.
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 on-premise Active Directory for the sources other than Microsoft 365 or cloud Active Directory for Microsoft 365
- add individually
- import from a CSV or Script file
  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 199*.

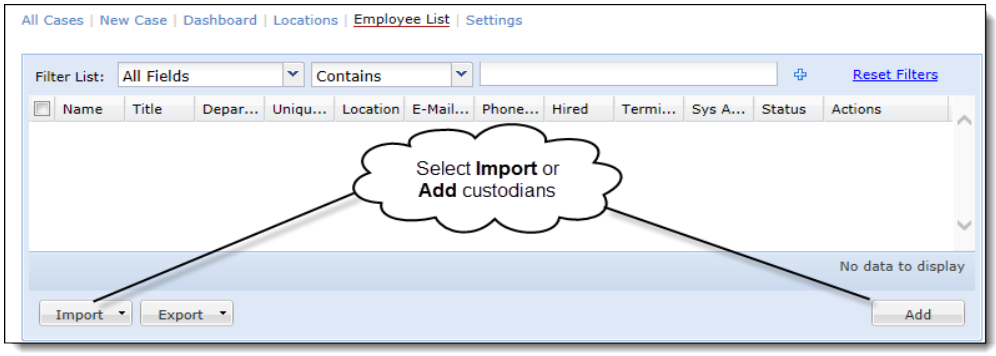
About Merging/Unmerging Custodians

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 38*.

   B. **Add** custodians individually. See *"To add a custodian individually (option B)" on page 44*.

To import custodians (option A)

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

   – **Synchronize Now with the Active Directory**. This submits an "Employee Synchronization Job" which checks Active Directory for any new or modified custodian data of on-premise users. Click **OK** at the prompt, then check the **Jobs** window for results. (See *"Synchronize with Active Directory" on page 39*.)

   – **Synchronize Now with the Cloud AD**. This option should be used for Microsoft 365. This submits an "Employee Synchronization Job" which checks Cloud Active Directory for any new or modified custodian data of cloud users. Click **OK** at the prompt, then check the **Jobs** window for results.

   Note: Only those users that have the **Directory synced** attribute set to **No** on Azure AD are synchronized after performing cloud AD. Also, users that are deleted from Azure will not be discovered.

   Note: Veritas eDiscovery Platform performs an Active Directory discovery to synchronize Active Directory domains/tenants, 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 39* for format requirements).

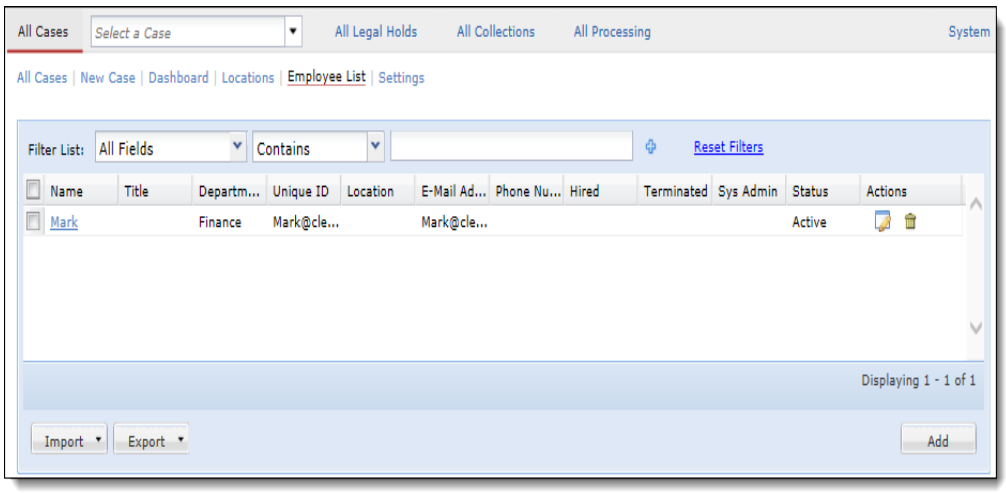
2. If your import/synchronization was successful, all new or updated custodians appear in the employee list.

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
AzureUniqueID	UTF-8	100	1133 **Note:** Required only for Microsoft 365.

CSV Import Format Requirements

Column Name	Format	Max Limit	Example
AzureID	UTF-8	100	1133 **Note:** Required only for Microsoft 365.
AzureUPN	UTF-8	100	1144 **Note:** Required only for Microsoft 365.
[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**: *Existing entry in Employee List*: Name: John Doe; Email: JohnDoe@JohnDoe.com; Unique ID: 1 *New entry from CSV*: Name: Johnnie Doey; Email: JohnnieDoey@JohnnieDoey.com; Unique ID: 1 *Resulting entry*: Name: Johnnie Doey; Email: JohnDoe@JohnDoe.com, JohnnieDoey@JohnnieDoey.com; Unique ID: 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
AzureUniqueID	UTF-8	100	1133 **Note:** Required only for Microsoft 365.
AzureID	UTF-8	100	1133 **Note:** Required only for Microsoft 365.
AzureUPN	UTF-8	100	1144 **Note:** Required only for Microsoft 365.
[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.

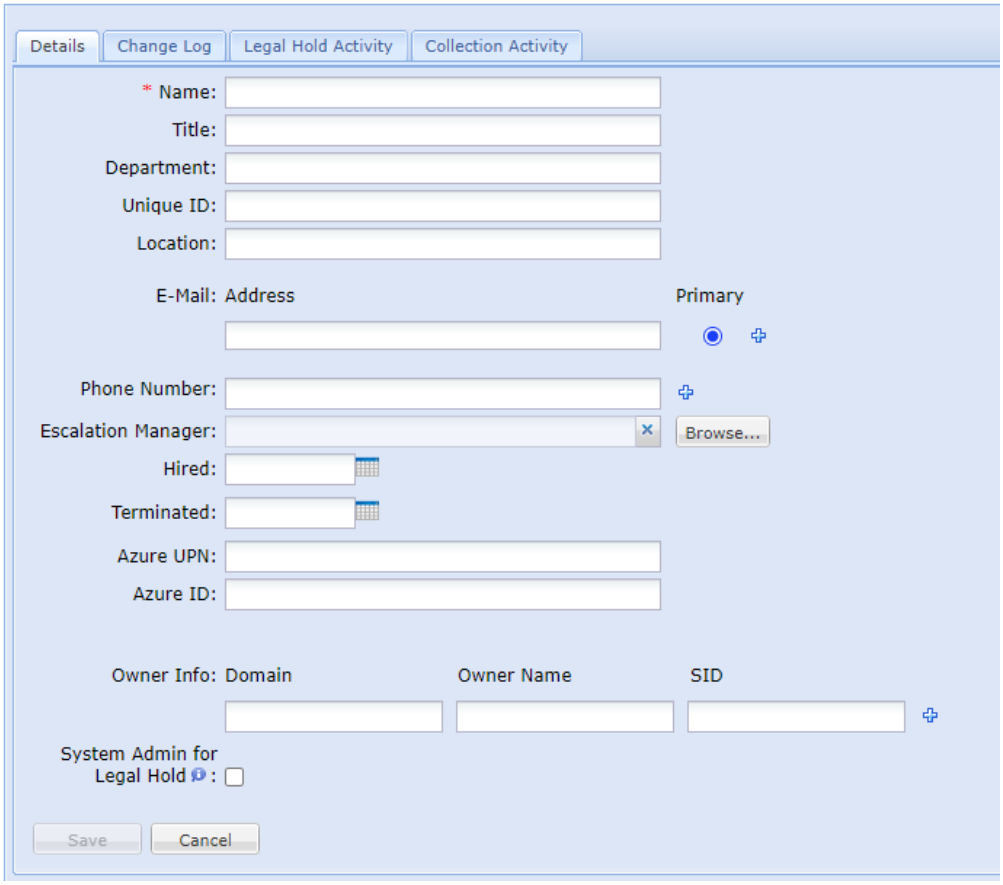
Note: Unless the file is an executable (.exe), then it should contain the location of the executable used to run it (as shown in the first line of the following example).

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.
Azure UPN	Enter the UPN that can be used by Azure ID to allow users to sign-in. **Note:** Required only for Microsoft 365.
Azure ID	Enter the Azure Object ID of the user. **Note:** Required only for Microsoft 365.
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 199*.

Adding Locations for Collected Data

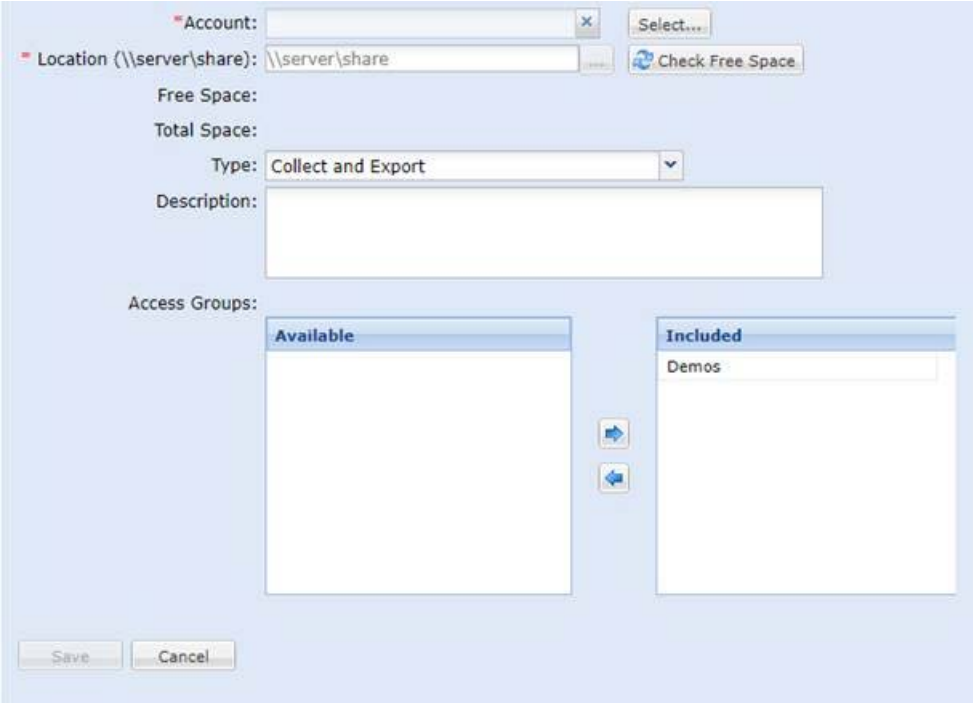
After setting up an authentication account, add a *Preservation Destination*, the location where you want collected data to be copied. You can add multiple locations to manage storage across geographical locations and by priority.

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 146*.

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.
Location (\\server\share)*	Enter the path to the location in the UNC format (\\servername\folder) 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 51*
  - *"Import Sources from CSV or Script" on page 52*

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

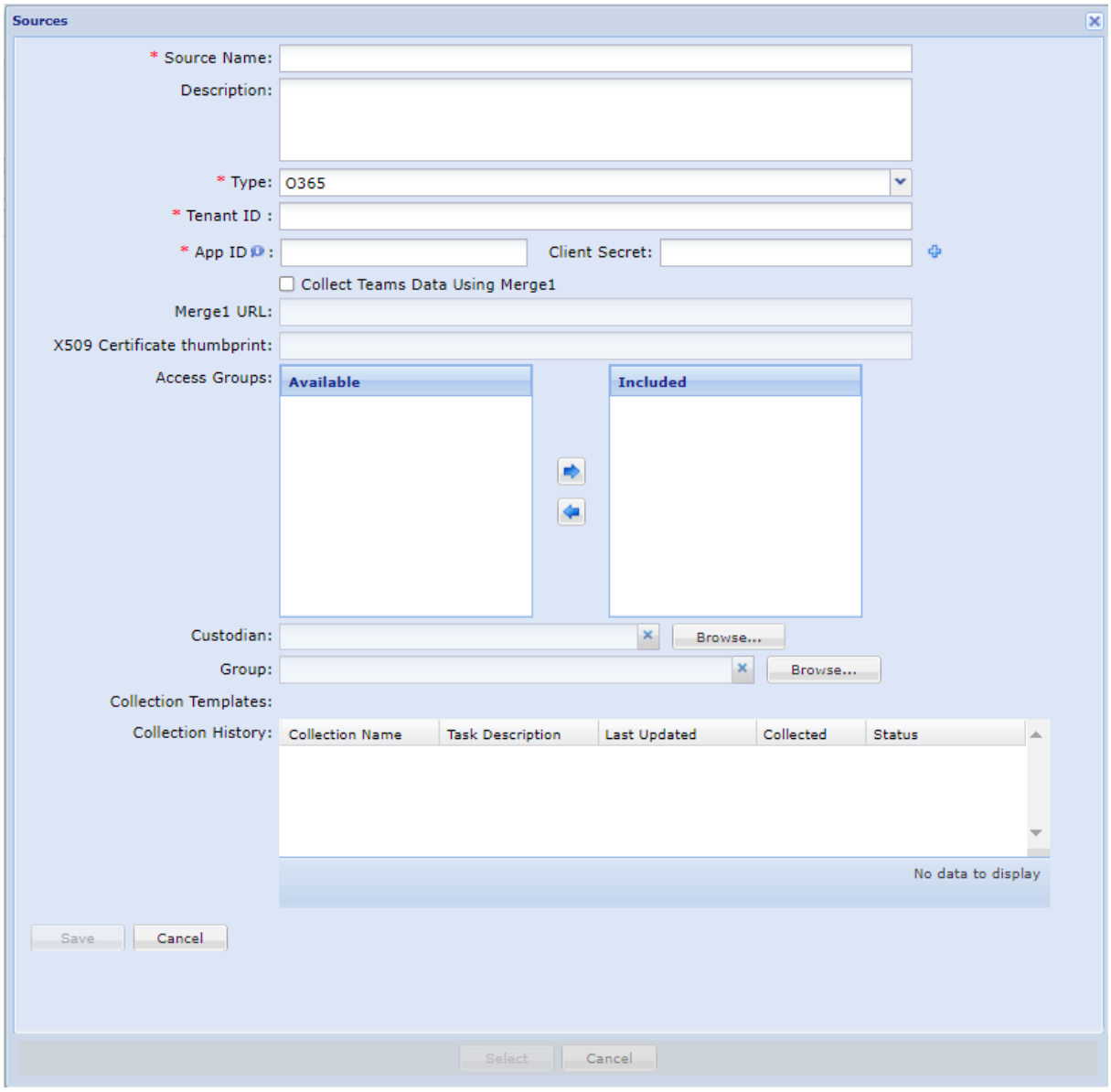
- *"Local Domain Exchange Setup" on page 56*
  - *"Lync 2013 Setup" on page 63*
- *"Microsoft 365 Setup" on page 64*
- *"Microsoft Teams" on page 74*
- *"Lotus Domino® Server Setup" on page 82*
- *"SharePoint Source Setup" on page 84*
- *"File Share and Windows PC Setup" on page 86*
- *"Veritas Enterprise Vault" on page 87*
- *"EV.cloud" on page 96*

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, Microsoft 365, Exchange Servers, SharePoint, Lotus Domino Servers, Enterprise Vault, EV.cloud, or remote locations such as a personal computer.

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.

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".

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 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.
*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.
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.
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.
*Tenant ID	(For Microsoft 365 source): Enter the Azure Tenant ID, the ID of the Azure Active Directory (Azure AD) in which you created the application.

Source Data (Continued)

Field	Description
*App ID Client Secret	(For Microsoft 365 source): Enter the App ID and the corresponding Client Secret generated while registering the application on Azure Active Directory. **Note:** A maximum of 3 App IDs can be added that can improve the collection performance.
Collect Teams Data Using Merge1	(For Microsoft Teams): Select this check box to collect Microsoft Teams chats and channels data using Merge1.
Merge1 URL	(For Microsoft Teams): Enter the Merge1 URL.
X.509 Certificate thumbprint	(For Microsoft Teams): Enter the X.509 certificate thumbprint. For details on how to get the Merge1 URL and X.509 Certificate thumbprint, refer to the *Merge1 User Guide*.
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 55*.)

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.

Note: Microsoft 365 sources cannot be imported from CSV or script.

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.

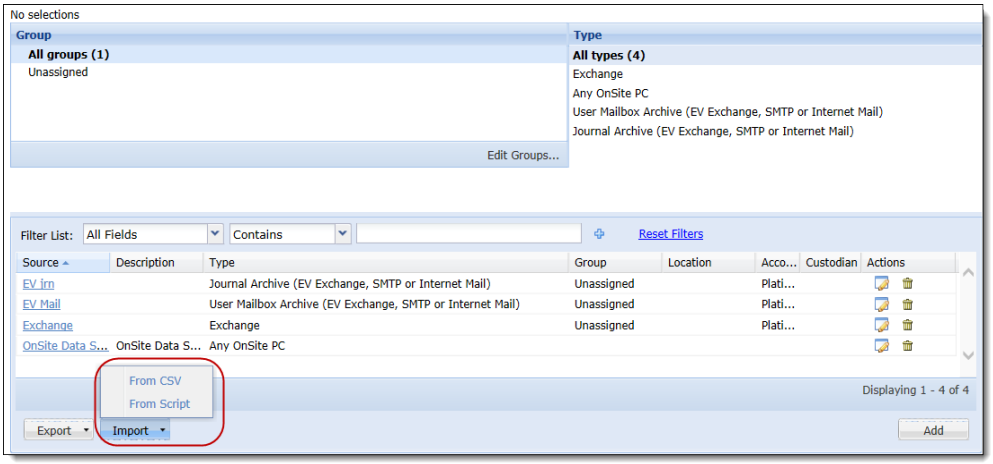
Source Import File Format Requirements

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

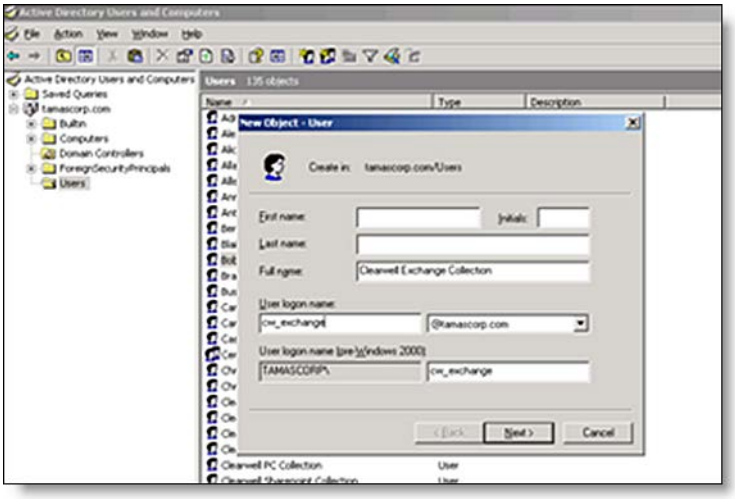
- *"Step 1: Create a New Domain Admin Account" in the next section*
- *"Step 2: Perform Active Directory Discovery and Import Custodians" on page 60*
- *"Step 3: Add Exchange Source to the Data Map" on page 61*
- *"Step 4: Test an Exchange Mailbox Collection" on page 62*

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 63*.

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.

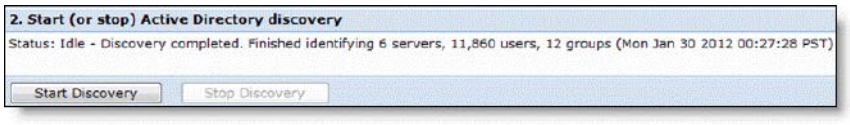
Note: It is recommended to provide credentials for a domain user account which has permissions to read the domain users as well as permissions to read the deleted objects container in Active Directory. This is required to mark correct status such as “Active” and “Inactive” for custodians as displayed 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, and then click **On-Prem Discovery**.
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.



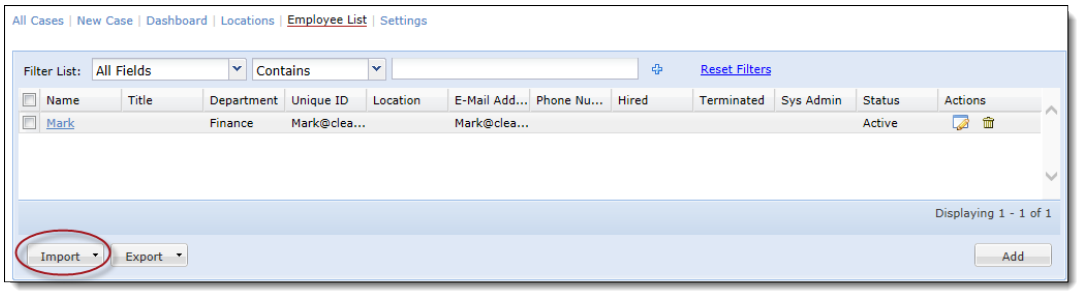
   Technical Note: This function checks for domains which contain the appliance. Once the domain is detected, Veritas eDiscovery Platform used the logged in account ("Admin Account") to discover servers, mailboxes, and groups from Active Directory. Typically, this should automatically discover the same 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 Now with the Active Directory** (imports all custodians at once).

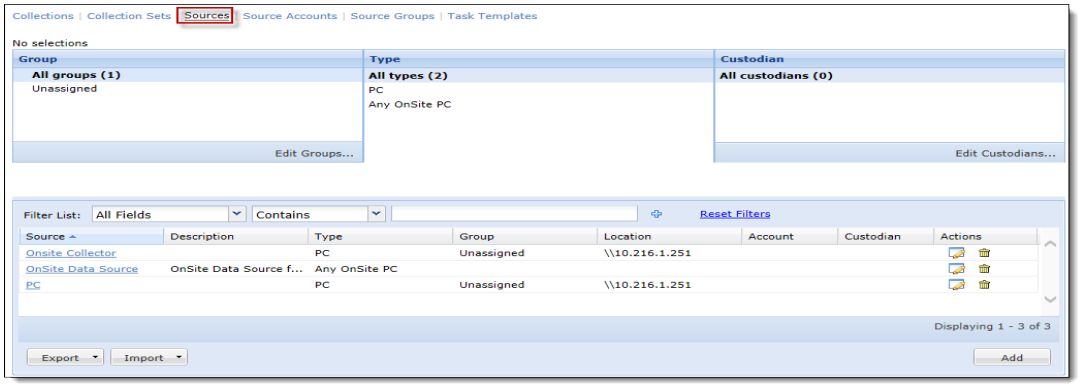
   Note: After import, use the Filter List menu to view by Name, User Name, or E-Mail Address and apply additional filter parameters.

For more details, refer to the section *"Importing Custodians to Your Data Map" on page 37*.

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 57*.
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 99*.

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

Microsoft 365 Setup

Exchange and OneDrive

Note: Use the information in this section if you are using Microsoft Graph API-based Microsoft 365. If you are using the legacy Microsoft 365 setup in MAPI-based environment, follow the steps described in the *9.5 version of the Identification and Collections Guide*.

Starting with release 9.5.1, eDiscovery Platform supports the identification and collection of data from Microsoft 365® (formerly Office® 365®) Exchange and OneDrive. Microsoft 365 now utilizes enhanced security by using Microsoft Graph APIs and OAuth2 authentication.

Release 9.5.1 changes how the collection from Microsoft 365 Exchange is done and how the custodian assignment is done. The collection from Microsoft 365 also supports federated collection with rich server-side filtering capabilities.

For Microsoft 365 sources, a collection task can collect data from the main mailbox and its dumpster.

Starting with release 10.1, eDiscovery Platform supports collection of Microsoft Teams chats and channels using Merge1. To collect from Microsoft Teams, refer to the Merge1 documentation for steps to access privilege Graph APIs for your tenant.

Some considerations about collection from Microsoft Teams:

- Each Microsoft Teams message is collected in Merge1 JSON file format. These messages are then converted into an EML for each day of messages per room. Multiple EMLs related to a room are bundled into a PST container for faster processing downstream.
- The Chat initiator participant is inserted into the “From” field, and the rest of the participants are inserted into the “To” field. All emails have a subject starting from “TeamsChat” for a chat conversation and “TeamsChannel” for a channel conversation.
- Reactions added in Microsoft Teams messages are not retained when these messages are converted into emails.
- When a collection runs, the eDiscovery Platform shows the number of downloaded JSON messages. After the collection is completed, these loose JSON messages are converted into emails. So the count of collected items as well as the size of the download varies during and post collection.

Prerequisites

To collect data from an Microsoft 365 source, the user should have a valid license for one or more of the following:

- Microsoft 365 Exchange
- Microsoft 365 OneDrive
- Microsoft Teams

Microsoft 365 Discovery is used to get the user accounts and collect data from their mailboxes, OneDrive files in Microsoft 365, and Microsoft Teams Chats and Channels.

For Microsoft 365 Exchange and Microsoft 365 OneDrive:

Azure Active Directory (AD) application authentication requires creating and registering an application with Azure AD. Microsoft 365 collections need the following values to run the AD discovery and collection successfully:

- Tenant ID
- App ID
- Client secret

Additionally, for Microsoft Teams Chats and Channels:

You must have installed Merge1 software on a server other than the server where eDiscovery Platform is installed. You must have a valid Merge1 license.

You must have Merge1 URL and the X.509 Certificate thumbprint ready to be used while creating a data source in eDiscovery Platform. For details on how to get the Merge1 URL and X.509 Certificate thumbprint, refer to the *Merge1 User Guide*.

Setting up Microsoft 365

This section explains how to create and register the eDiscovery Platform setup in Azure Active Directory, and then authorize it to access the Exchange and OneDrive database of the tenants. During this setup, you need to assign correct permissions to the users. Users with these permissions can collect the Exchange and OneDrive data by using the eDiscovery Platform.

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

1. Make sure you possess the required licenses for Microsoft 365 Exchange or Microsoft 365 OneDrive.
2. Register App ID on Azure Portal. See *"Registering App ID on Azure Portal" on page 66*.
3. Generate a new client secret. See *"Generating a new client secret" on page 67*.
4. Assign the Microsoft Graph API permissions to App ID. See *"Assigning the Microsoft Graph API permissions to App ID" on page 68*.
5. Synchronize Cloud Active Directory for Microsoft 365 accounts. See *"Synchronizing Cloud Active Directory for Microsoft 365 accounts" on page 70*.
6. Add the Microsoft 365 source to your data map. See *"Adding the Microsoft 365 Source to your Data Map" on page 71*.

Note: Once you complete your Microsoft 365 setup successfully, and before you start collecting data, make sure you understand the best practices and limitations. See *"Best Practices" on page 72* and See *"Limitations in Microsoft 365 collection" on page 72*.

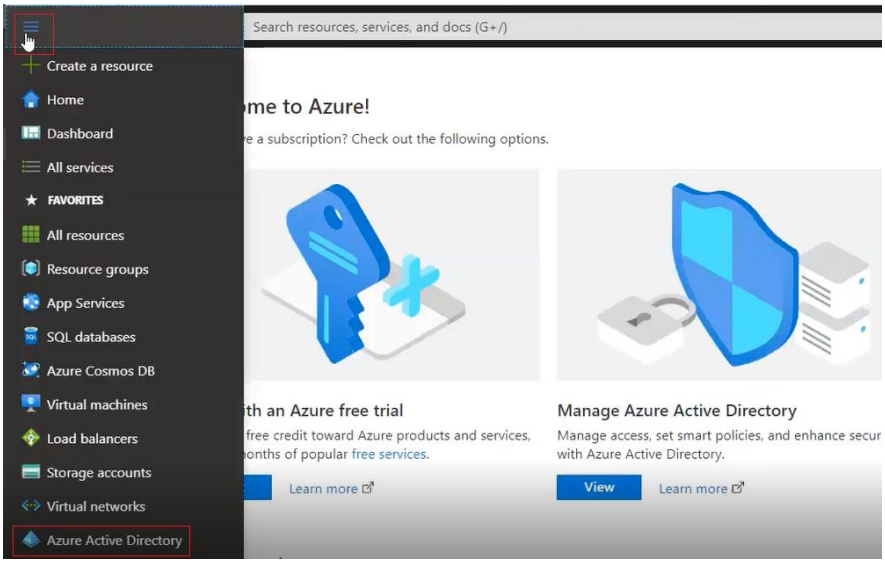
In case your environment requires to use a proxy while collecting data from an Microsoft 365 source, see *"Collections from Microsoft 365 source through a proxy" on page 73*.

Registering App ID on Azure Portal

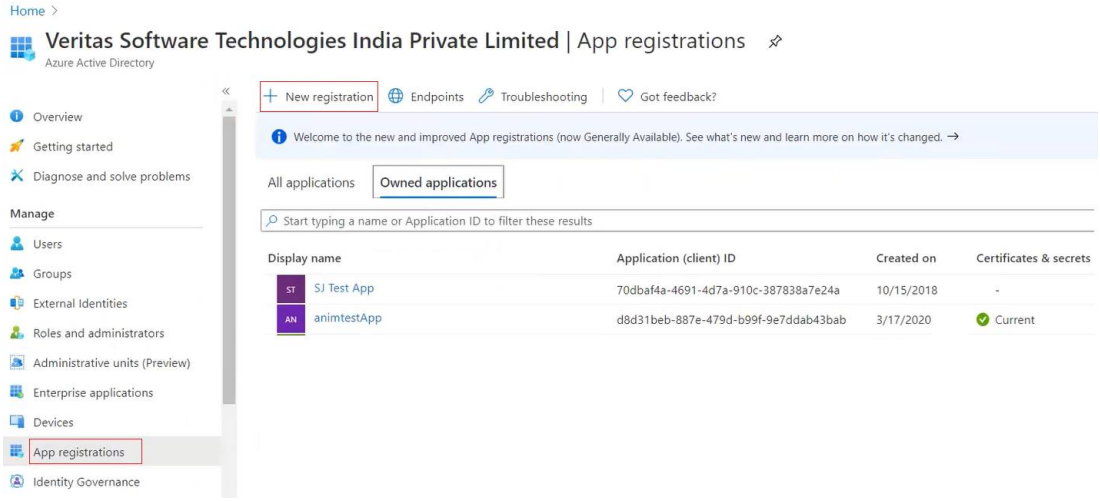
You need to register the application on Azure Active Directory to generate an App ID. This App ID is required when you create a new Microsoft 365 source in eDiscovery Platform. You must have administrator permissions to register the App ID.

To register the App ID on Azure Portal

1. Sign in to the Microsoft Azure Portal.
2. Navigate to and open the Azure Active Directory page.



3. In the left navigation pane, under **Manage**, select **App registration**, and then click **New registration**.



4. Specify a unique application name and click **Register**.

   The application displays all the registered applications. To view owned applications, select the **Owned Application** tab. After activation of the application, save the following:

   – App ID

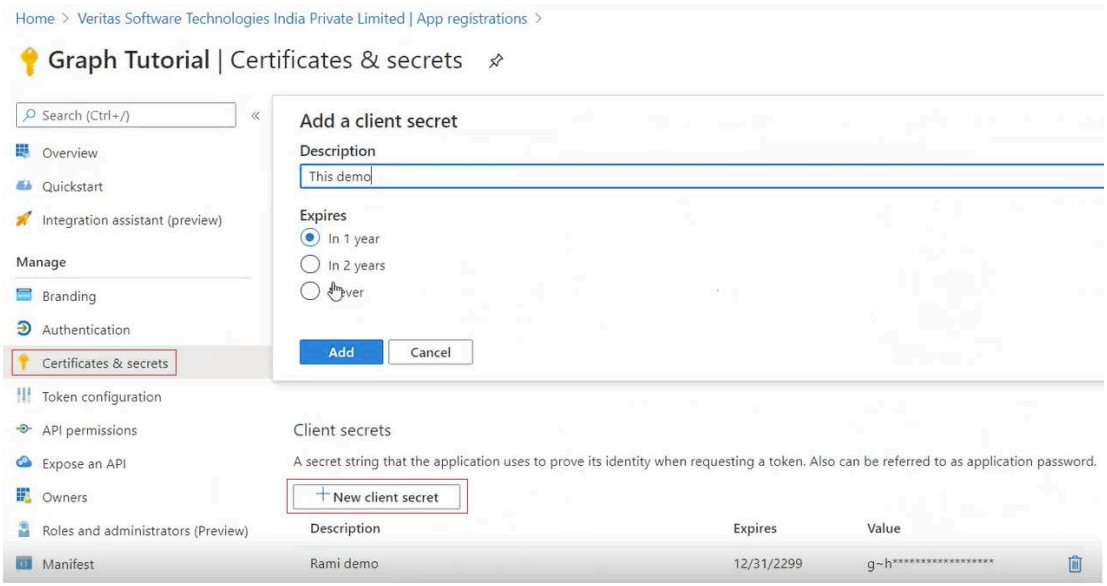
   – Directory (tenant) ID

Generating a new client secret

When you create a new source for Microsoft 365 collection, you need an App ID and the corresponding client secret. You can generate several client secrets for a single App ID, whenever required.

To generate a new client secret for App ID

1. Open the newly registered application.
2. In the left navigation pane, under **Manage**, select **Certificates & secrets**.



3. Click **New client secret**.
4. Provide a description text for the client secret and specify the expiry duration.
5. Click **Add**.

   The application displays all the secrets under the **Client secrets** section. Wait till this newly created client secret is generated and activated.

Note: After generating the secret key, save the client secret for further use. The client secret is only visible when it is created and will be obfuscated after.

Assigning the Microsoft Graph API permissions to App ID

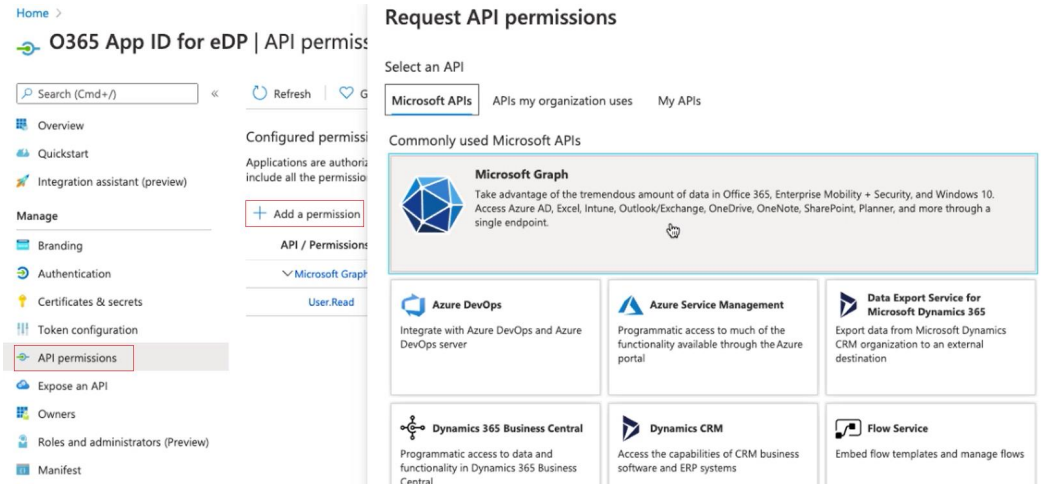
You need to assign the required Microsoft Graph API permissions to the application users to allow or restrict collecting the Exchange and OneDrive data.

Note: Application and Site delegated permissions must be provided to the Application ID.

You can associate the delegation-specific permissions and the application-specific permissions. If you want your application to access API as the signed-in user, set the delegation-specific permissions. If you want your application without a signed-in user, set the application-specific permissions in an automated way. To understand all the permissions in detail, see https://docs.microsoft.com/en-us/graph/permissions-reference.

To assign the Microsoft Graph API permissions to App ID

1. Open the newly registered application.
2. In the left navigation pane, under **Manage**, select **API permissions**.



3. Click **Add a permission**, and select **Microsoft Graph**.

   The application displays the Delegation permissions and the Application permissions.

4. Select Application permissions and then select the following permissions.

Permission	Purpose
Calendar.Read	Allows for reading and download of calendars.
Contacts.Read	Allows for reading and download of contacts.
Directory.Read.All	Allows for Active Directory sync of all the users and mailboxes within the active directory.
Files.Read.All	Allows for reading and download of documents stored in OneDrive.
Mail.Read	Allows for reading and download of all emails within the mailboxes.
Channel.ReadBasic.All	Allows reading the names and descriptions of all channels.
ChannelMember.Read.All	Allows reading the members of all channels.
ChannelMessage.Read.All	Allows reading all channel messages.
Chat.Read.All	Allows reading all chat messages.
Chat.ReadBasic.All	Allows reading names and members of all chat threads.
ChatMember.Read.All	Allows reading the members of all chats.
ChatMessage.Read.All	Allows reading all chat messages.
Files.Read.All	Allows reading files in all site collections.
Group.Read.All	Allows reading all groups.
Team.ReadBasic.All	Allows to get a list of all teams.
User.Read.All	Allows reading all users' full profiles.
Sites.Read.All[#]	Allows for reading documents and list items in all site collections.

The permission is required only for OneDrive collection.

5. For OneDrive collection using keyword filter, select additional permission: Sites.Read.All
6. Click **Add permissions**.
7. Click **Grant admin consent**.

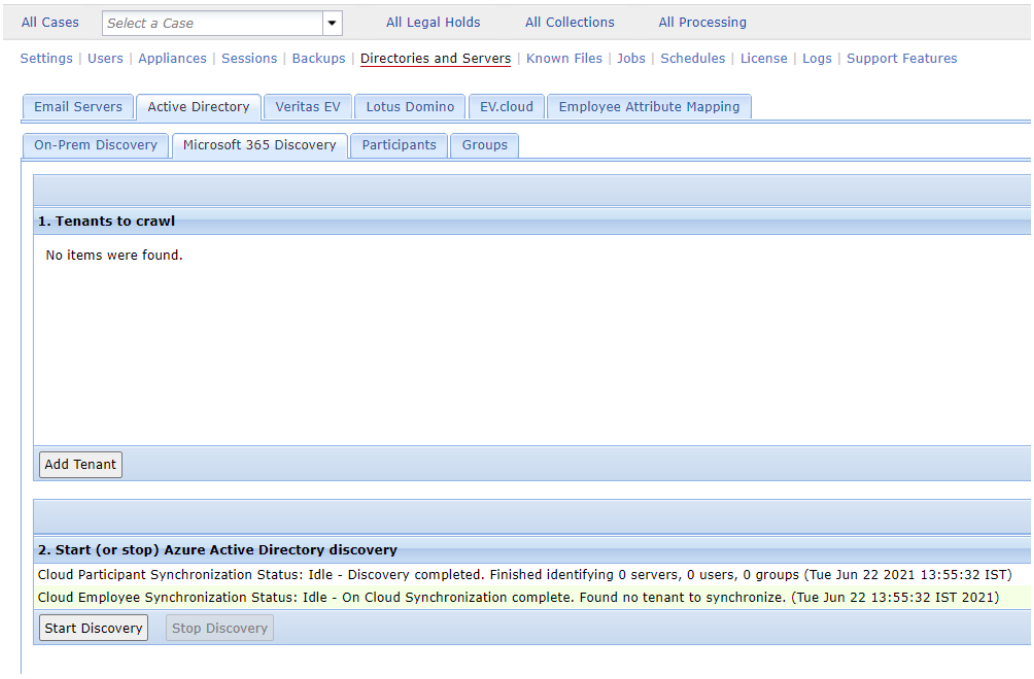
   Note: If you have the right permissions to grant consent, click **Grant admin consent**. If you do not have permissions, request the authorized administrator to grant permissions for you.

Synchronizing Cloud Active Directory for Microsoft 365 accounts

The Microsoft 365 Azure Active Directory (AAD) crawler discovers your Microsoft Exchange servers and OneDrive services, the mailboxes on each server, and your organizational data, such as physical locations and departments (groups).

To perform cloud active directory sync

1. On the top navigation bar, click **System** > **Directories and Servers**, and select the **Active Directory** tab.
2. To add a new tenant for cloud discovery, on the **Microsoft 365 Discovery** tab.



3. Click **Add Tenant**. Specify the following information and click **Save**.

Field	Description
Tenant Name	Specify the tenant name.
Azure Tenant ID	Type the Azure tenant ID.

Field	Description
Azure Tenant Client Secret	Type the Azure Tenant Client Secret.
Azure APP ID	Specify the Azure App ID.

4. After adding the tenant, click **Start Discovery** to perform Microsoft 365 Active Directory discovery. eDiscovery Platform displays the number of users added, deleted, updated, truncated (reducing user's number of aliases to 20), and restored.

   Note: Only those users that have the **Directory synced** attribute set to **No** on Azure AD are synchronized after synchronizing the cloud AD. Also, if the user was deleted from Azure, that user will be discovered after synchronizing the cloud AD.

5. When the Active Directory discovery is complete, do the following:
   - To view and search for the associated individuals of the active directory, click the **Participants** tab.
   - To view and search for the associated groups of the active directory, click the **Groups** tab.

Adding the Microsoft 365 Source to your Data Map

To add Microsoft 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 Microsoft 365 source.
Description	Enter a description of the source (up to 255 characters).
*Type	Select O365 as the source type.
*Tenant ID	Type the Azure tenant ID.
*App ID	Specify the Azure App ID and the Azure Tenant Client Secret. **Note:** A maximum of 3 App IDs can be added that can improve the collection performance.
*Client Secret	
Collect Teams Data Using Merge1	(For Microsoft Teams): Select this check box to collect Microsoft Teams chats and channels data using Merge1.
Merge1 URL	(For Microsoft Teams): Enter the Merge1 URL.
X.509 Certificate thumbprint	(For Microsoft Teams): Enter the X.509 certificate thumbprint. For details on how to get the Merge1 URL and X.509 Certificate thumbprint, refer to the *Merge1 User Guide*.

Source Data (Continued)

Field	Description
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**.

Best Practices

eDiscovery Platform has several properties that you can use to improve the performance of data collection from Microsoft 365 Exchange and OneDrive.

Based on your requirements and setup, you should consider setting the properties listed in the section *"Microsoft 365 Collection Performance Tuning" on page 233*.

Best practices related to filtering in collection tasks are listed in *"Filtering Best Practices for Microsoft 365 Exchange and OneDrive" on page 116*.

Also, note that eDiscovery Platform collects data from the files shared in a private chat or a chat during a meeting or call that is uploaded and stored in the OneDrive for the Business account of the user who shares the file.

Limitations in Microsoft 365 collection

While collecting data from Microsoft 365 Cloud Apps, such as Exchange and OneDrive that uses Microsoft Graph APIs and OAuth2 authentication for connection, consider the following limitations. Check the future releases of eDiscovery Platform that might provide fixes for these limitations:

- Keyword search in Contact and Calendars in Exchange is not supported. Keyword search works incorrectly for contacts and does not work entirely for calendars.
- If Microsoft 365 collection is run using the participant filter, then the search returns only data related to Exchange mails and does not return data for calendars and contacts.
- Size of the collection data is shown differently on the Collection Task page and the Collection Activity under Employee List. The Collection Task page shows the correct size of the collection.
- Only 500 users are displayed while selecting owners on the Filter page. It is recommended to provide more letters of the user while searching mailboxes to narrow down the search.
- Scanned size of the collection on the collection task page is always displayed as zero.

- If a job is started and immediately stopped by the user, it goes into the failure state, and not in the stopped state.
- If a OneDrive file name has a special character in it that is not supported by Windows file names, then eDiscovery Platform replaces that special character with its ASCII value while saving the file on a disc.
  For example, a OneDrive file with name ~text.txt will be changed to _126_text.txt while saving on disk when an Microsoft 365 collection collects it.
- Additionally, Microsoft Graph-related limitations also limit the Microsoft 365 collections:
  - Collection from Archive Mailboxes and inactive mailboxes is not supported.
  - Keyword search fetches items only from the data that is indexed by Microsoft 365. Items, such as password-protected files that might not have been indexed on Microsoft 365 are not fetched when a keyword search is used.
  - If Microsoft 365 collection is run with the attachment filter set, then the search will return data only related to Exchange emails. It will not search for calendars and contacts.
  - Wildcards (for example, *,?) in keyword search for OneDrive are not supported.
  - Keyword search with the NEAR operator is not supported for OneDrive. It works only for Exchange.
- Keyword search option is not provided for Teams collection.
- Teams data is collected in the form of messages (one JSON per message). When a collection is running, UI will show the number of messages downloaded. Once a collection is over, the number of messages will be reduced drastically and aggregation of many JSON messages will constitute a single email file.
- In-line images that are embedded by participants into Teams chat by copying web references are automatically downloaded while rendering Teams chat email in the Analysis and Review module of eDiscovery.
- Veritas eDiscovery Platform 10.1 supports collection of information from one Merge1 server at a time.

Collections from Microsoft 365 source through a proxy

Veritas eDiscovery Platform does not support collections from a Microsoft 365 source through a proxy by default. The system administrators can enable collection from Microsoft 365 through a proxy by configuring the following system properties using **System** > **Support Features** > **Property Browser**.

These properties are only applicable for Microsoft 365® Exchange and OneDrive. For Microsoft Teams, you need to manage your proxy configuration on Merge1. For details, refer to the *Merge1 User Guide*.

Property	Value
esa.o365.collection.proxy.enabled	True to enable the proxy. False to disable the proxy.
esa.o365.collection.proxy.ip	Proxy server host name or IP address

(Continued)

Property	Value
esa.o365.collection.proxy.port	Proxy server port
esa.o365.collection.proxy.username	Proxy server username
esa.o365.collection.proxy.password	Proxy server password

Note: While collecting data from Microsoft 365 through a proxy, there would be a marginal performance degradation.

Microsoft Teams

Starting eDiscovery 10.1, the eDiscovery Identification and Collection module can now be used to collect from Microsoft 365 Teams (chats - group or individual - and channels). Ability to collect from Microsoft 365 Exchange and OneDrive was added in v10.0.

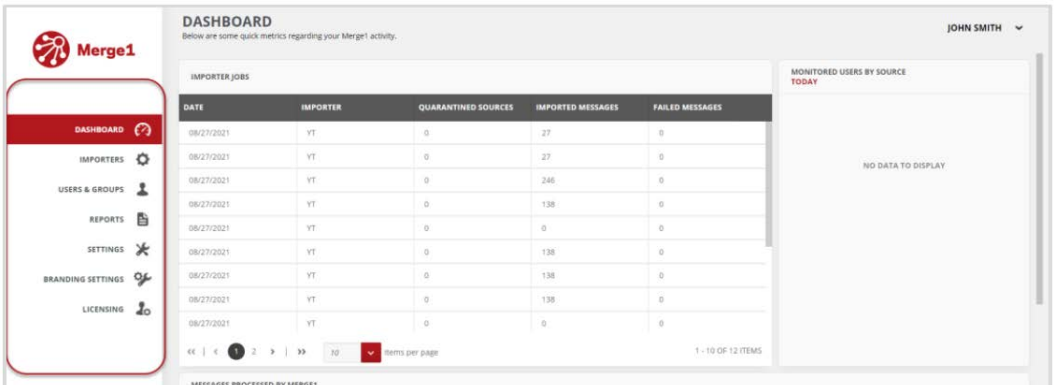
The new Teams collection feature shares the same user interface as the Exchange and OneDrive collection but uses Merge1 in the background as a conduit to collect from Microsoft 365 using Graph APIs. Accordingly, Merge1 licenses need to be purchased to collect from Teams.

Prerequisites

Before you proceed to collect Microsoft Teams data, you need to perform the following activities.

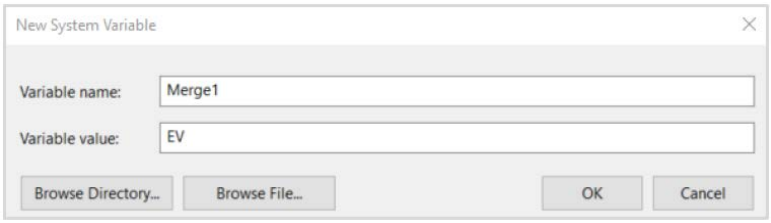
- Creating a Microsoft Azure App for permissions to collect from Microsoft Teams
  - Noting down the Tenant ID, APP ID, and Client Secret
- Performing Active Directory (AD) synchronization
- Installing and configuring the Merge1 application
  - Creating a Merge1 application to connect with the eDiscovery Platform
  - Activating API Clients in the Merge1 UI (This step is required to get Merge1 Application ID and Merge1 Client Secret)

  Note: API Clients section is hidden from the Merge1 UI.



To view the API Clients section in the navigation pane:

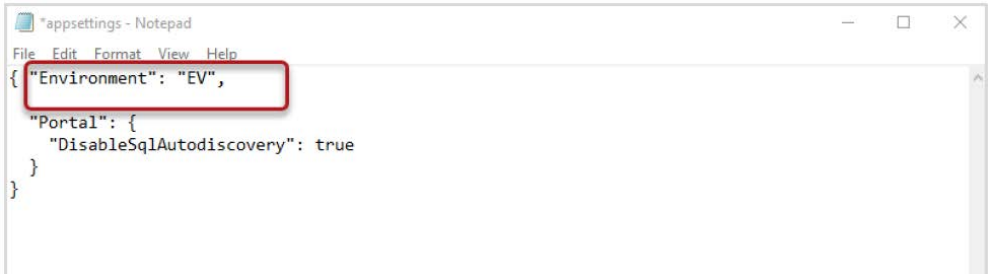
1. Go to **System Properties** > **Environment Variables** > S**ystem Variables**.
2. To open the **New System Variable** window, click **Add new**.



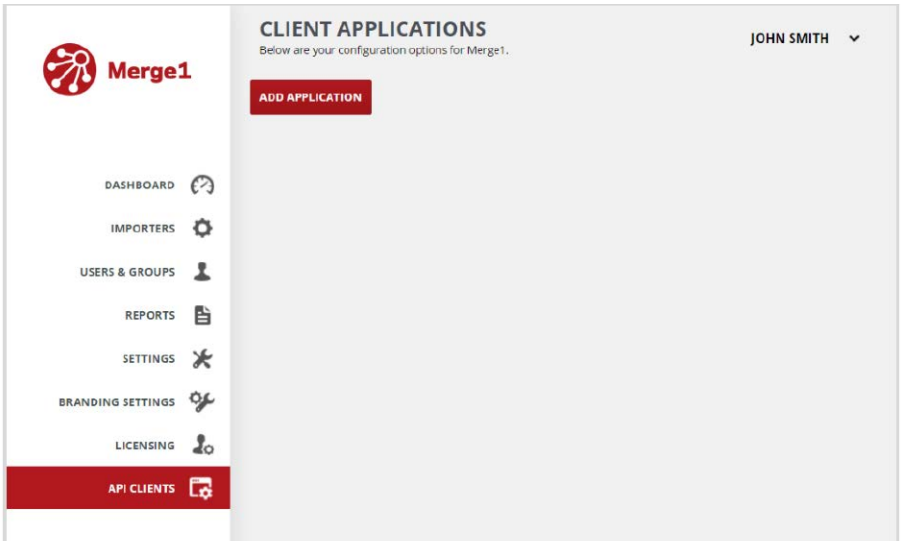
3. Type **`Merge1: Environment`** in the **Variable name** field and **`EV`** in the **Variable value** field.
4. Restart **IIS**.

   Or

1. Go to *C:\Program Files\Globanet Consulting Services\Merge1 6.0\Bin\Configuration*.
2. Open **appsettings.json** file.
3. Add **`"Environment": "EV"`** in the file.



After adding the variable, the API Clients section will be added to the navigation pane.



  - Note down the following:
    - Merge1 Server URL
    - X509 certificate thumbprint
    - Merge1 Application ID
    - Merge1 Client Secret

- Configuring the M365 collection source within the Identification and Collection module of the eDiscovery Platform
- Ensuring the eDiscovery Platform, Merge1, and collection destination are in same domain
- Ensuring that the collection destination has read/write permission

Installing and Configuring the Merge1 Application

Merge1 is a Veritas product that needs to be installed and configured for Teams data collection. For more details, refer to the *Merge1 Installation Guide*. After installing and configuring Merge1, do the following:

1. In eDiscovery Platform, select **System** > **Support Feature** > **Properties Browser**.
2. Configure the following properties in eDiscovery Platform.
   - `esa.M365.collection.teams.logFolder` to specify location of the Merge1 log folder.
     For example, C:\\Merge1Logs
   - `esa.M365.collection.teams.localUsername` to specify the local user on the Merge1 system.
     For example, NDDOMAIN\\evuser
   - `esa.M365.collection.teams.localCred` to specify the local user's password on the Merge1 system.
     For example, admin@123

Configuring eDiscovery Platform for Microsoft Teams data collection

You must configure the following properties in eDiscovery Platform. The configuration procedure is explained below.

Property Name	Description	Level	Default Value
`esa.o365.collection.teams.localUsername`	Merge1 system's local user name through which all Merge1 operations are to be done.	System	No default value
`esa.o365.collection.teams.localCred`	Merge1 system's local password through which all Merge1 operations are to be done.	System	No default value
`esa.o365.collection.teams.filtersProcessingType`	Filters applied to all ("MatchAll") or any ("MatchAny") provided filters.	System	MatchAny
`esa.o365.collection.teams.processType`	Collect only new ("New"), failed ("Failed") or both ("New, Failed").	System	New, Failed
`esa.o365.collection.teams.noteAttachmentMissing`	Specify the message shown to user if attachment is missing while collecting Teams data.	System	This message..
`esa.o365.collection.teams.noteDisclaimerMissing`	Merge1 Importer disclaimer missing message	System	This message..
`esa.o365.collection.teams.logFolder`	Merge1 log folder location	System	C:\\Merge 1Logs

Turning the automatic download feature OFF

Automatic download feature for in-line images is turned ON by default. You may consider it as a security risk and want to disable the feature. To turn the automatic download feature OFF, complete the following steps:

A. Stop PrizmDoc server using EsaPrizmDocServer Windows service.

B. Change the property "**security.htmlRendering.blockExternalContent**" value from "true" to "false" in *D:\Prizm\Server\prizm-services-config.yml*.

   For details about the property, see *https://help.accusoft.com/PrizmDoc/v13.17/HTML/central-configuration.html?highlight=htmlrendering%2C*

C. Delete all the subdirectories in *D:\Prizm\Server\cache*.

D. Restart PD server from Windows service.

E. Clear browser cache.

Configuring Rich Email Application

eDiscovery Platform converts Microsoft Teams conversation chats into emails, and archive it as the PST files. While converting emails, a few parameters can change the behavior of email conversion.

Note: Configuring Rich Email application is a general customization activity, and is entirely optional step.

To configure Rich Email application,

1. Access the *3rdparty\vtas\ConversionUtilities* on the eDiscovery server.
2. Update the parameters provided in the `Mapping.properties` files.

   All parameters in this file are self-explanatory. Some important parameters are listed below.

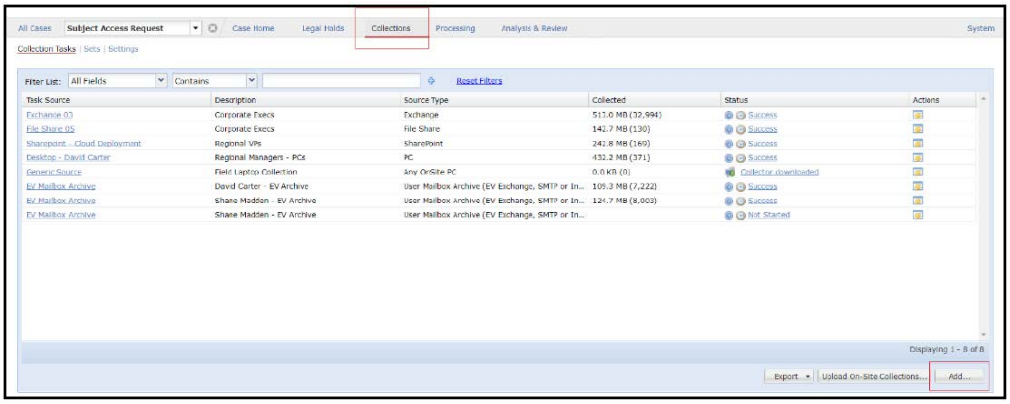
   – **IS_VCJ_ATT_ENABLE** - Set this value as true if you want to collect VCJ files (JSONs from Merge1) of original chat conversation as an attachment to the emails. This may be required by some users for legal or compliance matters.

   – **DEFAULT_TIME_ZONE** - Select your time zone.

Adding a new collection task for Microsoft Teams collection

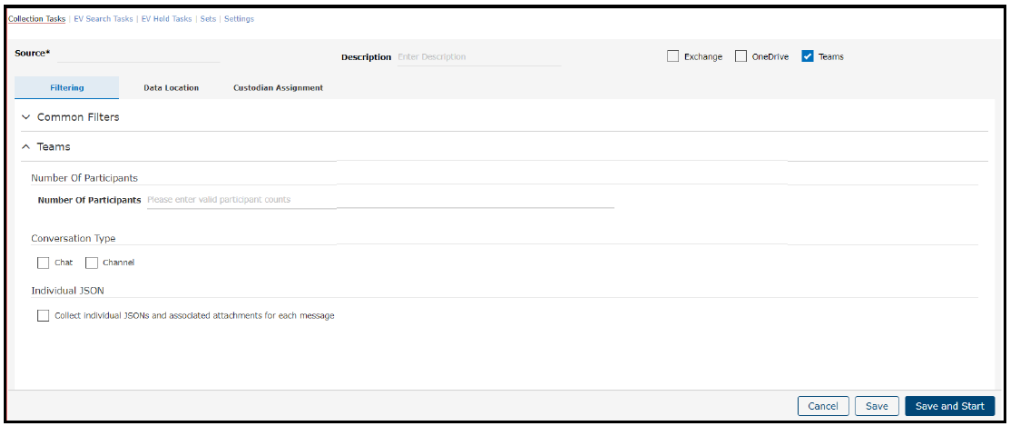
To add a new collection task for Teams collection

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



2. On the **Collection Tasks** screen, click **Add**.
3. Select the source you want to use to run your task, and click **Select**.
4. The **Collection Tasks** screen displays the name of the source. Enter a description for the collection task.
5. Select the **Teams** check box.

6. On the **Filtering** tab, expand **Common Filters** to specify dates and participants. An asterisk (*) indicates a required field. Keyword are not supported for Teams because the resulting data will provide no context to what was sent before or after.



   Additionally, expand the Teams dropdown to:

Number of participants	Specify the exact number of participants in the Teams conversation.
Conversation type	Specify whether you want to filter only Chats, only Channel communication, or both.
Individual JSON	Select the check box if you want to collect individual JSONs and associated attachments for each conversation. These will not be available to download as native files in PPAR.

7. Select the **Data Location** tab to see the default location where the collection will be stored.

8. Select the **Custodian Assignment** tab to choose whether to assign to custodian based on associated email addresses or file owners or create a new custodian using the associated email addresses.

9. Click **Save** to save the task, or click **Save and Start** to add, and immediately start running the new task.

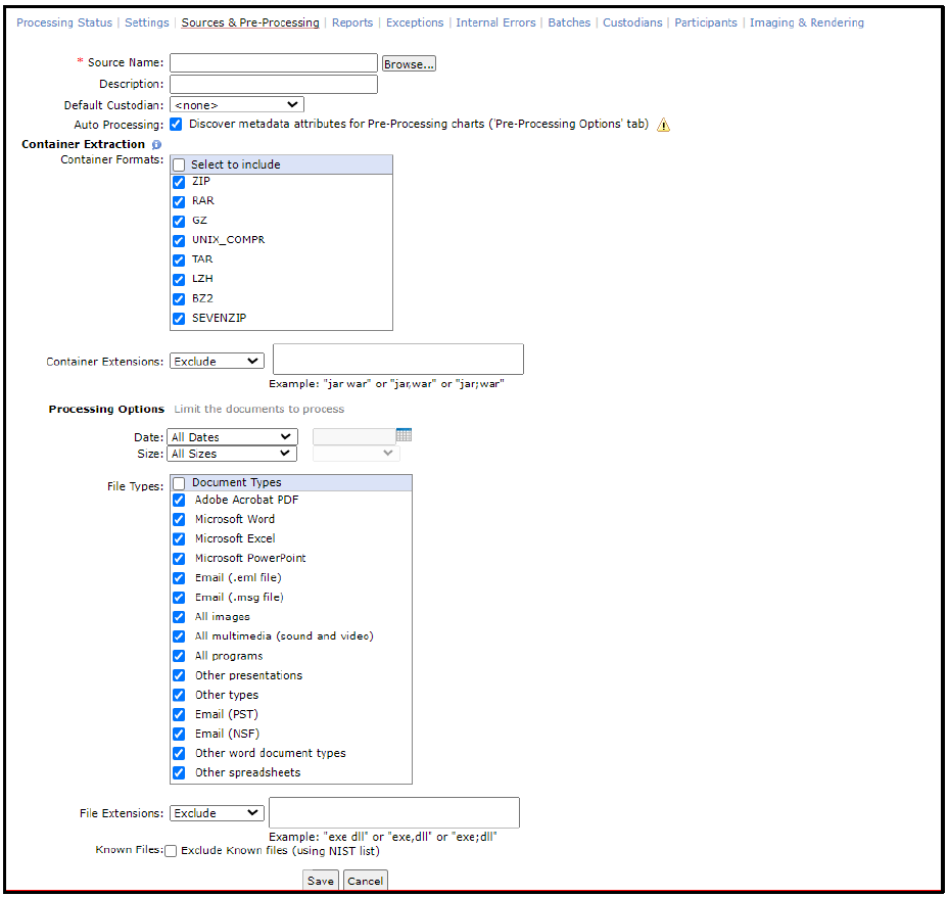
Creating a new collection set for Microsoft Teams collection

Create collection set for data that is collected through Microsoft Teams collection.

For the general information about creating collection sets, see *"Managing Collection Sets" on page 175*.

Processing collected PST files

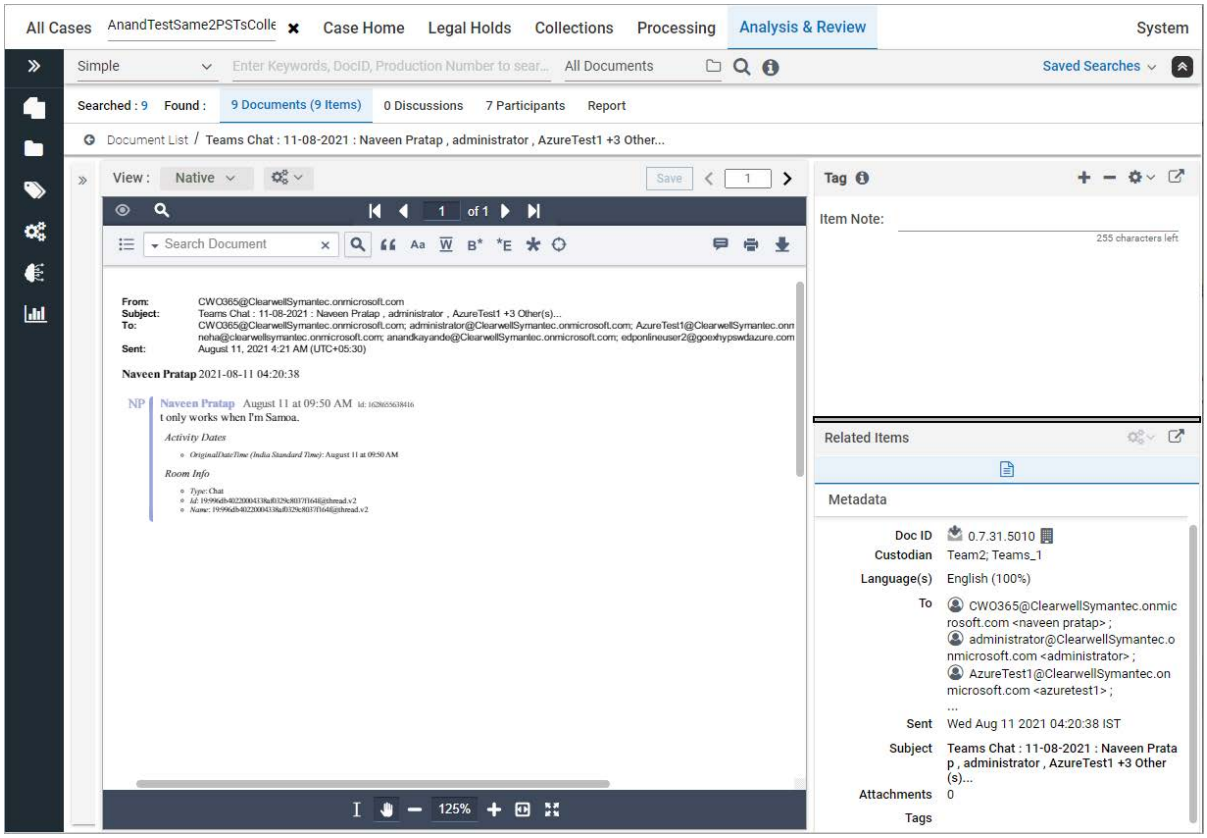
To process the collected PSTs of Microsoft Teams collection, use standard processing workflows.



For the general information about Processing Collection Sets, see *"Managing Collection Sets" on page 175*.

Performing analysis and review of the collected PST files

After processing the PST files of Microsoft Teams conversations, you can view these files in the **Analysis & Review** UI. You can redact, print, and export the files as required.



Lotus Domino® Server Setup

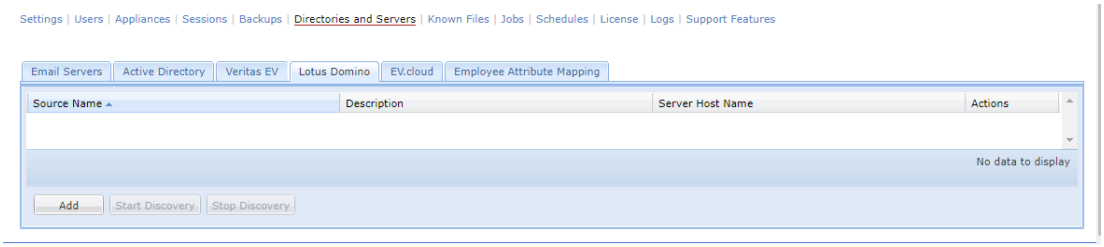
Follow the steps below to set up your Lotus Domino Server as a source for collection:

- *"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 221*.

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. For up-to-date information on the supported versions, see the *Veritas eDiscovery Platform™ Compatibility Charts* guide.

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.

Starting with release 9.5.1, eDiscovery Platform now converts the EML files that are collected from all Enterprise Vault archives, such as Exchange, SMTP, and IMAP into MSG files that are stored in PST files. This results in faster collection and processing of data from Enterprise Vault and enhanced usability in dealing with a PST file instead of individual loose EML files.

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 90*
- *"Step 1: Perform Enterprise Vault Discovery/Vault Administration" on page 90*
- *"Step 2: Add Enterprise Vault Sources" on page 94*
- *"Step 3: Update your License" on page 95*

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.

Enterprise Vault Index Levels

Index Level	Description
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 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).

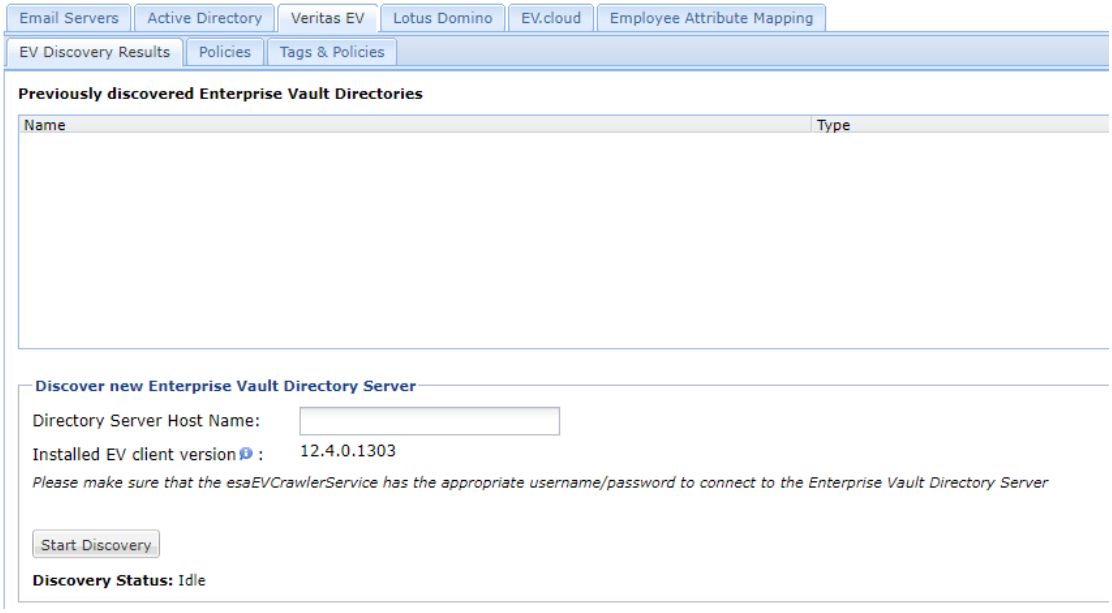
About Enterprise Vault Policies

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, 10.0 automatically installs Enterprise Vault 12.4.0 API Runtime on the appliance. To connect to other certified versions of Enterprise Vault, follow the steps to uninstall 12.4.0, 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 27*.

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.



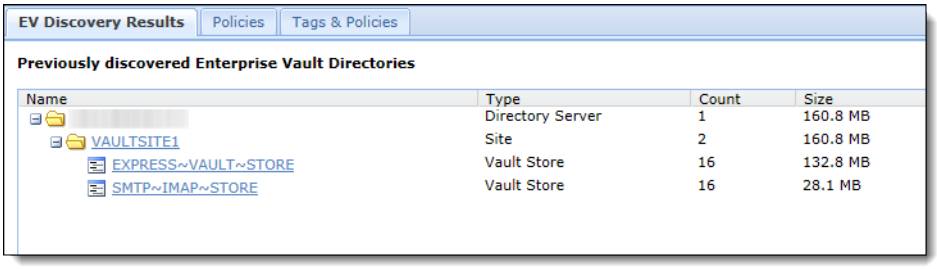
Under the "**EV Discovery Results**" tab appears either a blank field, or list of any previously discovered Enterprise Vault directories.

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 directories that have been discovered.



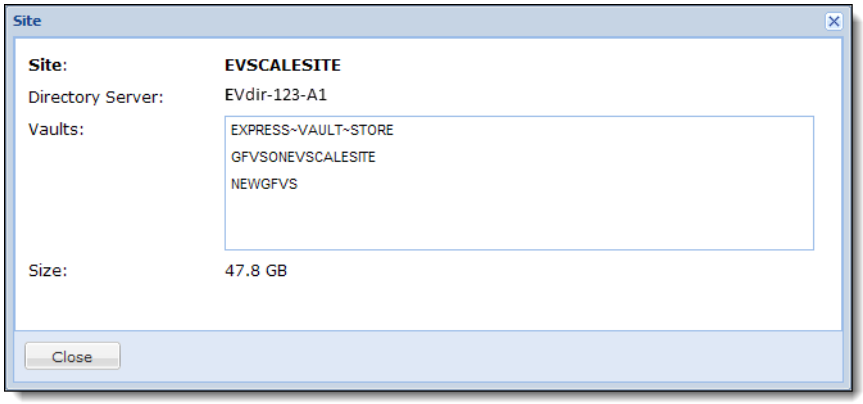
Troubleshooting: If you encounter issues during discovery, check the server logs, including output from the *EsaEVCrawlerService*. Any archives that were dropped for any reason are not reported through the Veritas eDiscovery Platform user interface. Be sure to check these logs first to determine what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

6. Continue with *"Step 2: Add Enterprise Vault Sources" on page 94*. Alternatively, continue to the next set of steps to view statistics on your discovered directories.

To view vault directory statistics

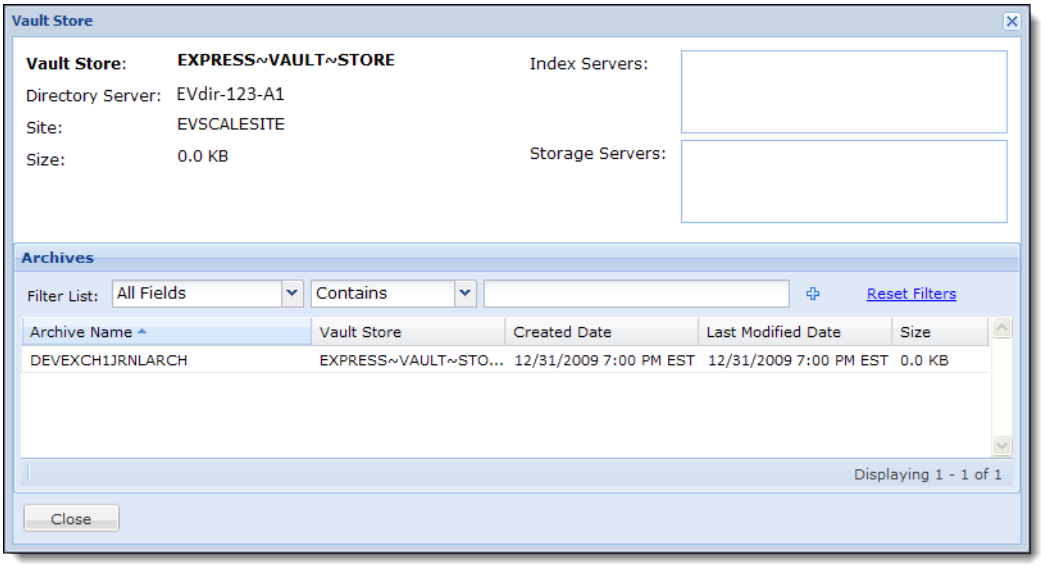
1. Click any link displayed in your discovery results to view statistics about that site and/or its vault stores and associated archives.

   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.

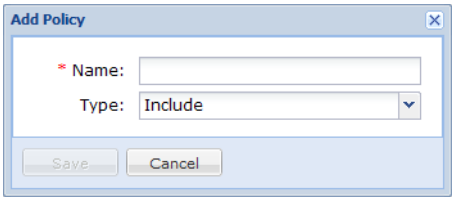


The Archives section displays all associated archives, including its *Vault Store*, *Created Date*, *Last Modified Date*, and *Size*. Click on an archive to view these same statistics, plus view its *Index* status in a new window.

2. Continue with *"Step 2: Add Enterprise Vault Sources" on page 94*. 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 206*.

   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 9.1 version license. If you are upgrading your appliance to 9.1, 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 189*.

Continue to *"Creating and Managing Collections" on page 99* 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

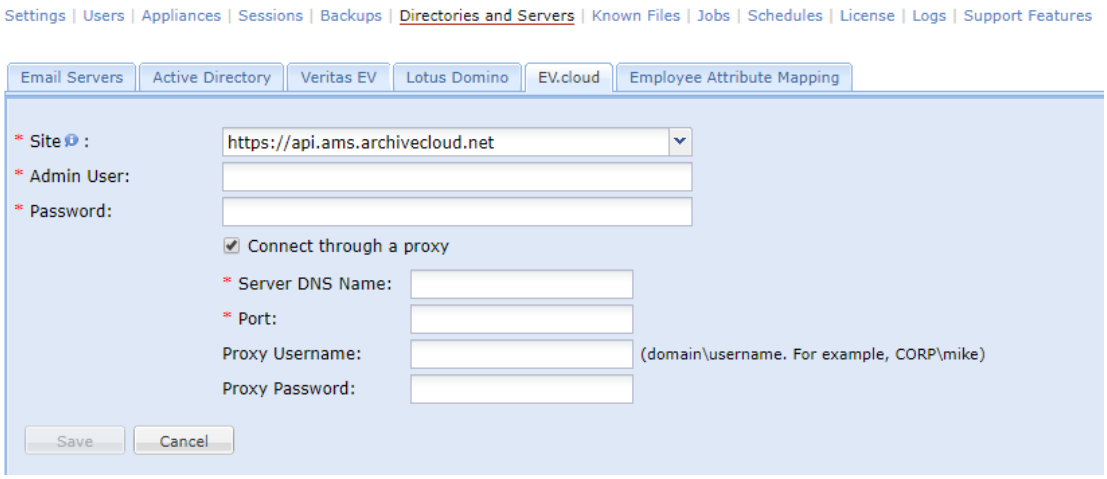
Please contact your EV.cloud administrator if you do not have this information.

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 206*.

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	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. 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 9.1 version license. If you are upgrading your appliance to 9.1, be sure to update your license. Go to **System > License** to see the available licenses. For details, see *"Collection Administration and Maintenance" on page 189*.

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

Creating and Managing Collections

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

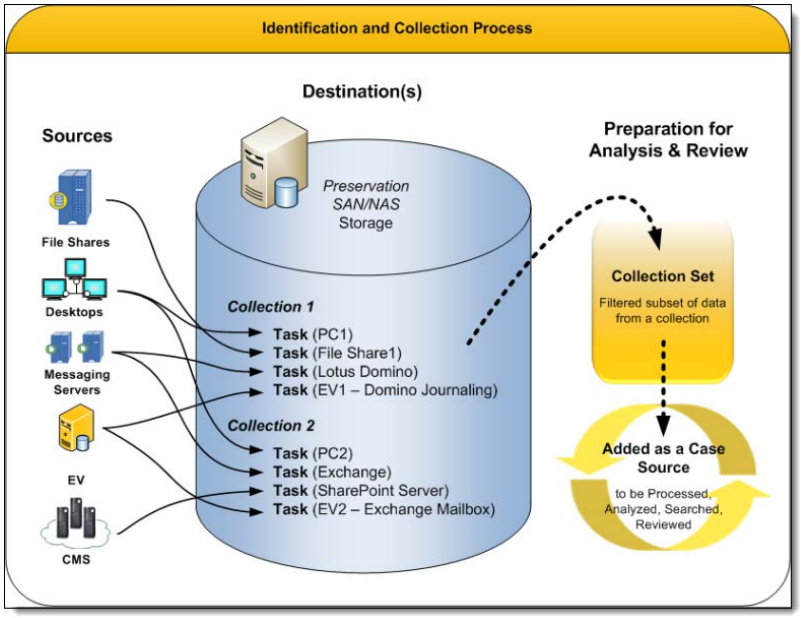
- *"About Collection Activities" in the next section*
- *"About OnSite Collections" on page 100*
- *"Creating a Collection and Running Tasks" on page 102*
  - *"Process Overview" on page 102*
  - *"Create/Add a New Collection" on page 102*
  - *"Add Tasks to a Collection" on page 103*
    - *"Add Tasks To a Collection" on page 103*
    - *"Add Tasks To a Collection (For Microsoft Graph API-based Microsoft 365 Source)" on page 113*
  - *"Copy a Collection, EV Search, or EV Hold Task" on page 115*
  - *"Filtering Best Practices for Microsoft 365 Exchange and OneDrive" on page 116*
  - *"Filtering Best Practices (for Enterprise Vault Sources)" on page 118*
  - *"Keyword-Based Collection (Non-Enterprise Vault Sources)" on page 129*
  - *"Include/Exclude Directories" on page 130*
  - *"Enable Compression for OnSite Collection Tasks" on page 136*
  - *"Create a Collection Template" on page 136*
  - *"Run or Schedule a Collection Task" on page 137*
  - *"Schedule a Recurring Collection Task" on page 139*
  - *"Rerunning a Collection Task" on page 140*
  - *"Re-running a Collection Task for Microsoft 365" on page 142*
  - *"Retrying a Failed Collection Task (for Enterprise Vault and EV.cloud Sources)" on page 144*
  - *"Move Collected Data to Another Location" on page 146*
- *"Running Custodian Assignments" on page 148*
  - *"Enterprise Vault Considerations" on page 148*
- *"Performing OnSite Collection Tasks" on page 150*
- *"Running Collection Reports" on page 150*
  - *"Collection Reports" on page 150*

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 175*.)



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 102*.

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 130*.

Note: Starting with release 10.0, the option to securely encrypt the collected data is not available.

A programmatic way is available to run OnSite Collector in hidden mode without the need of any user intervention. For details, 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 118*.

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 102*
2. Add Tasks to the collection.
   See *"Add Tasks to a Collection" on page 103*.
3. Run or Schedule a Task in the collection.
   See *"Run or Schedule a Collection Task" on page 137*.

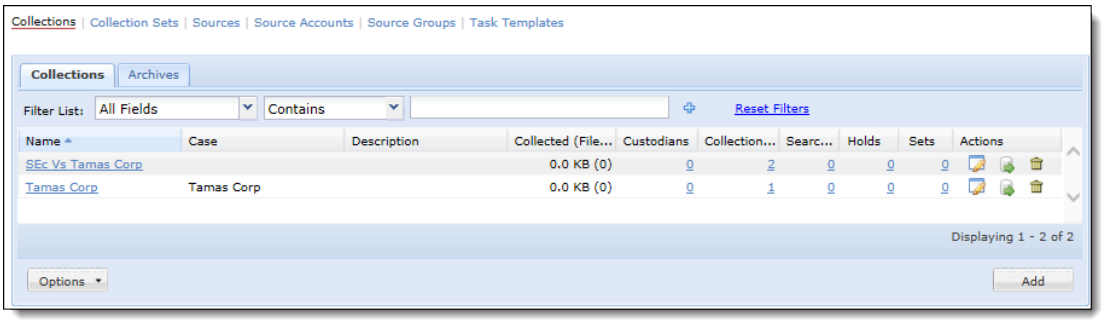
Create/Add a New Collection

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. Starting with release 9.0.2, collection name can include letters, numbers, underscores, spaces, hyphens, and dashes.
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 46* 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 136*.

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**.

Add Tasks To a Collection

Use the instruction in this section if you are collecting data from sources other than Microsoft Graph API-based Microsoft 365.

If you are collecting data from Microsoft Graph API-based Microsoft 365 source, see *"Add Tasks To a Collection (For Microsoft Graph API-based Microsoft 365 Source)" on page 113*.

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 150*.

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 172*.

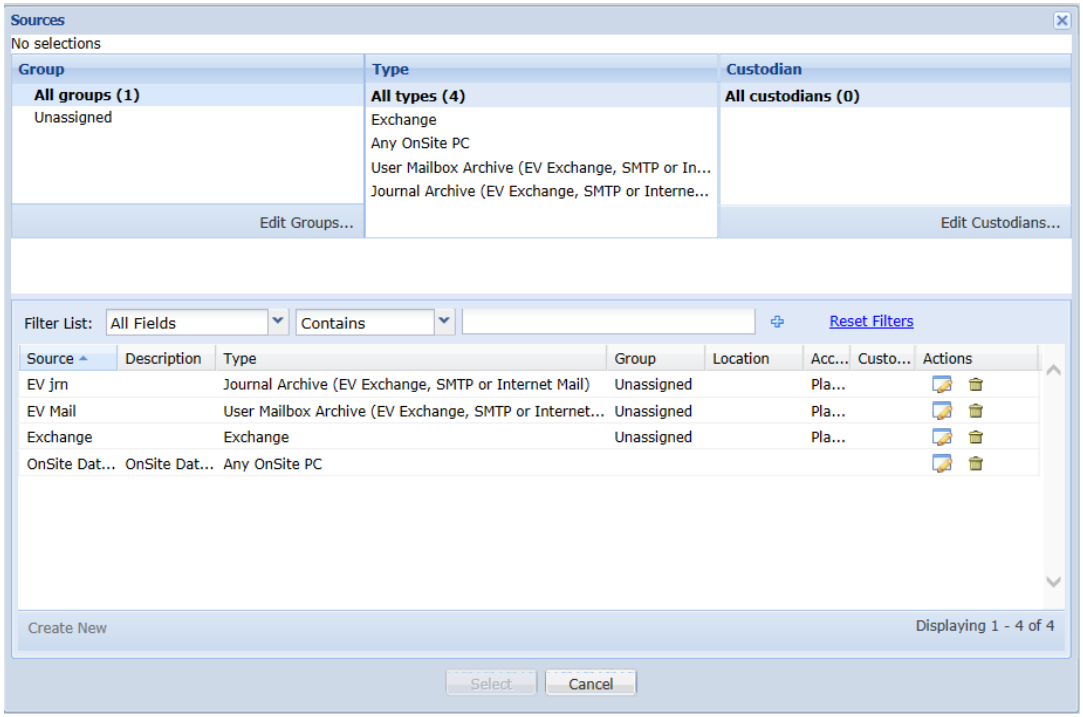
To add a task (to an existing collection)

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.

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 118*. **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 150*. 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 118* 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 130*. 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 148*. (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, DXL, or SMTP. 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. See *Using custom attributes in the Traits filter for Enterprise Vault*. 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.) For Enterprise Vault sources, the Simple search provides the option of listing any, all, or none of the phrases entered. All three categories can be grouped together by an AND expression. Release 9.1 provides an **Advanced** search option to use AND, OR, NOT, and NEAR operators for Enterprise Vault sources. See *Keyword Search*. See *"Filtering Best Practices (for Enterprise Vault Sources)" on page 118*.

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. 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 130*.

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 136*. (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 137*.

Add Tasks To a Collection (For Microsoft Graph API-based Microsoft 365 Source)

Starting with release 9.5.1 of eDiscovery Platform, a new user interface is provided to capture all details related to the collection from Microsoft 365 Exchange and OneDrive.

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

1. Select the collection you just created to view the *Collection Tasks* screen.
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 Microsoft 365 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 172*.

To add a task (to an existing Microsoft 365 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.
3. Select the source you want to use to run your task, and click the **Select** button.
4. The Collection Tasks screen displays the name of the source. Enter a description for the collection task.
5. Select the required options:
   – **Exchange** if you are collecting from Microsoft 365 Exchange
   – **OneDrive** if you are collecting from Microsoft 365 OneDrive
   – **Teams** if you are collection from Microsoft Teams

   You can select multiple options if you are collecting from multiple sources. Depending on your selection, the options under the **Filtering** tab are displayed.

6. Select the **Filtering** tab, and then specify the following information. An asterisk (*) indicates a required field.
   See *"Filtering Best Practices for Microsoft 365 Exchange and OneDrive" on page 116*.

Add Task Filter Options

Field	Description
Common Filters	
Date	Specify the sent date for Exchange or creation date for OneDrive (according to time zone shown). You can reset the Date filters by selecting All Dates. To change the time zone, go to **System** > **Settings**.
Keywords	Filter documents that contain only certain keywords. Enter one or more keywords. **Note:** The Keywords filter is not available for Microsoft Teams.
Owners/ Participants	(Mandatory) Click **Add Owner(s)/Participant(s)** to add emails or names of the custodians or participants. On the Add Owners dialog, select one or multiple owners/participants and then click **OK**. You can add all owners/participants by clicking **Select All From Organization**. If required, you can remove an individual owner/participant or remove all owners/ participants by clicking **Remove All**. **Note:** To be able to collect Microsoft 365 user's data, you must first discover the cloud mailboxes by running On-Prem Active Discovery or Microsoft 365 Active Discovery Sync.
Exchange	
Document Type	Filter emails based on the documents type. Options available are Emails, Calendars, and Contacts.
Participants	Filter emails based on participants using from, to, cc, bcc fields.
Attachments	Filter emails based on attachments. You can choose to include emails with or without attachments, or both.
OneDrive	
File Extensions	Filter files based on their file extension. You can include files with specific extensions. For example, .doc
Date Modified	Filter files based on modification date. Available options are: • All Dates • Dates On or After • Dates On or Before • Dates Between
Teams	
Number of Participants	Enter a valid participant count if you want to filter Teams messages based on the number of participants that stay at the conversation end. If no value is entered, the participant count is ignored and all Teams messages are collected.
Conversation Type	Select the appropriate conversation type: Chat, Channel, or both (default). **Note:** You must select at least one of these conversation types.

7. Select the **Data Location** tab to see the default location where the collection will be stored.
8. Select the **Custodian Assignment** tab to choose whether to assign to custodian based on associated email addresses or file owners, or create a new custodian using the associated email addresses. To assign custodians, specify the following information.

Custodian Assignment Details for Microsoft 365

Option / Sub-Options		Description
Assign items to the Source default custodian (Common Source)		(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 to a custodian based on the associated email addresses (for Exchange) and file owners (for OneDrive)		Select to assign custodian only if the email address (for Exchange) is matched with the email addresses in the Employee List or the file owner name for OneDrive.
If no match is found:		
	Create a new custodian using the associated email address (for Exchange) and file owners (for OneDrive)	If no match (or in cases where a mismatch has occurred), create the custodian using the associated email address or file owner.
	Assign the custodian	Type a specific custodian you want to assign, or click **Select** 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. **Note:** This is the default option for Teams.

9. 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. If you have used the **Save Progress** option, you can start the task at any time or you can also schedule the collection task.

Copy a Collection, EV Search, or EV Hold Task

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

To copy a Collection, EV Search, or EV Hold 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.

Note: Starting with 9.1, when you create a new task either by using the "Copy from the parent task" operation or by applying a template from the **Actions** > **Load Collection Template** option, the disabled archives from the Enterprise Vault source are filtered out.

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 102*.

   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 164*.

Filtering Best Practices for Microsoft 365 Exchange and OneDrive

Refer to this section for tips and guidance when filtering criteria on Microsoft 365 Exchange and OneDrive source data.

Keywords search

- Only operators allowed for searching are AND, OR, NOT, NEAR (in capital letters)
- Logical operators should be in the capital letter only. Otherwise, they will be treated as keywords.
- If space is used between words, they are considered separate words and not as a phrase. For example, Adam Eve will be considered as Adam AND Eve. Here, the search will fetch items that have both Adam and Eve words. The positioning of these words doesn't make any difference.
- Do not use extra spaces, and do not press Enter to move to the next line.
- No special characters are allowed except * (asterisk), ? (question mark), and parentheses. * is a wildcard character that searches for one or more characters after the provided text. A question mark searches for any one character.
- If no operator is used between two keywords, then it will be considered as a phrase search.
- Order of precedence is Parentheses > NOT > AND > OR, where Parentheses has the highest priority and OR has the lowest priority.
- For filters, the search logic would be used in the following manner:
  (Common filters AND Exchange filters) OR (Common filters AND OneDrive filter)

Example:

Emails resided on a specific mailbox are:

- Keyword: Creta
  Subject-Mail1
- Keyword: Aspire
  Subject-Mail2
- Keyword: Creta Aspire
  Subject-Mail3
- Keyword: Carnival
  Subject-Mail4

In this case, below are the search queries and their search results:

Keywords	**Search Results**
(Creta OR Aspire) AND (Carnival OR Creta Aspire)	Mail3
Creta OR Aspire AND Carnival	Mail3, Mail1
Creta AND Carnival OR Aspire	Mail3, Mail2
Creta AND (Carnival OR Aspire)	Mail3
Carnival OR Creta AND Aspire	Mail3, Mail4
Creta AND Carnival NOT Creta	Empty response
(Creta OR Aspire OR Carnival) AND (Carnival OR Creta AND (Carnival))	Mail4

File Extension search

Use a comma to separate the file extensions. For example: .txt, .doc, .pdf

Participants search

- Participants can be searched for from, to, cc, bcc.
- Only logical operators allowed for searching are AND, OR, NOT (in uppercase).
- No special characters are allowed except * (asterisk), ? (question mark), and parentheses. * is a wildcard character that searches for one or more characters after the provided text. A question mark searches for any one character.
- No space should be added between to/from/cc/bcc and actual search email.

  Example:

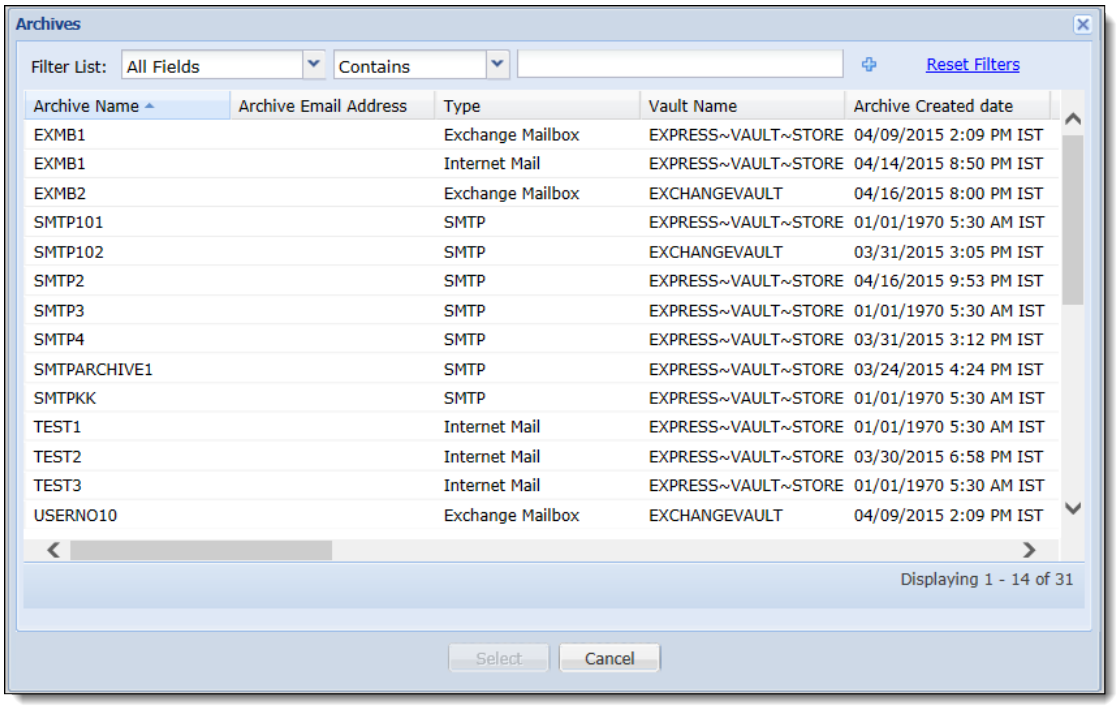
  - from:pqr@kmail.com AND cc:abc@kmail.com OR bcc:xyz@kmail.com NOT to:ghi@kmail.com
  - from:pq*

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

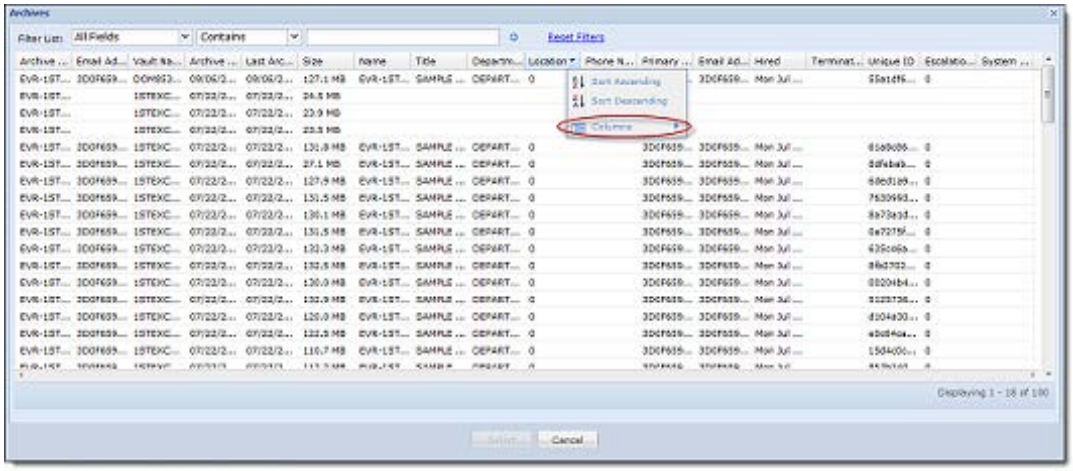
When you add an archive from your collection task "**Archives**" tab filter, the Archives window opens allowing you to select from all discovered archives for the selected source.



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.

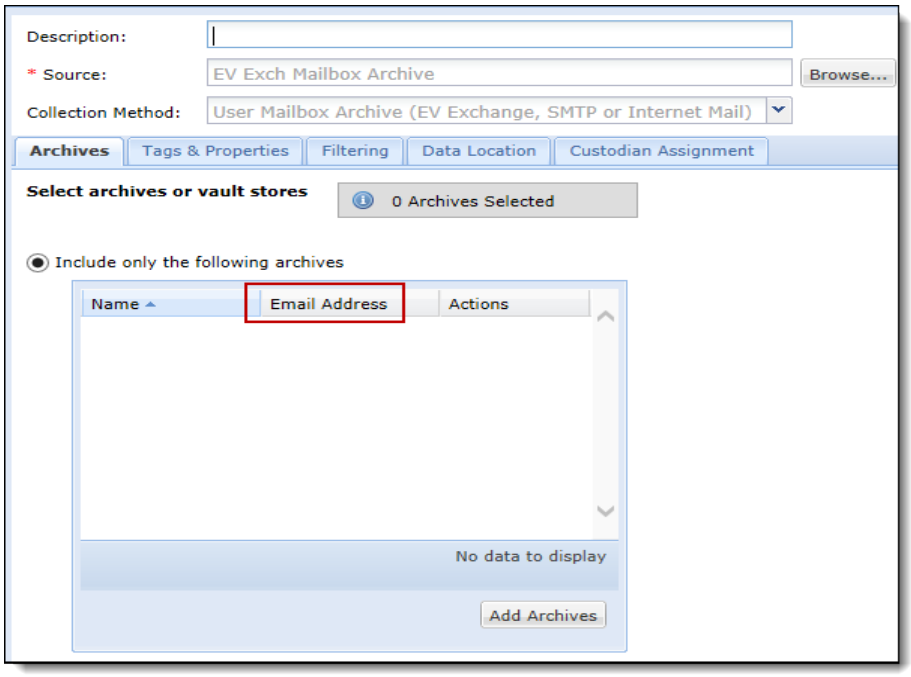
Email Address Selection

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.

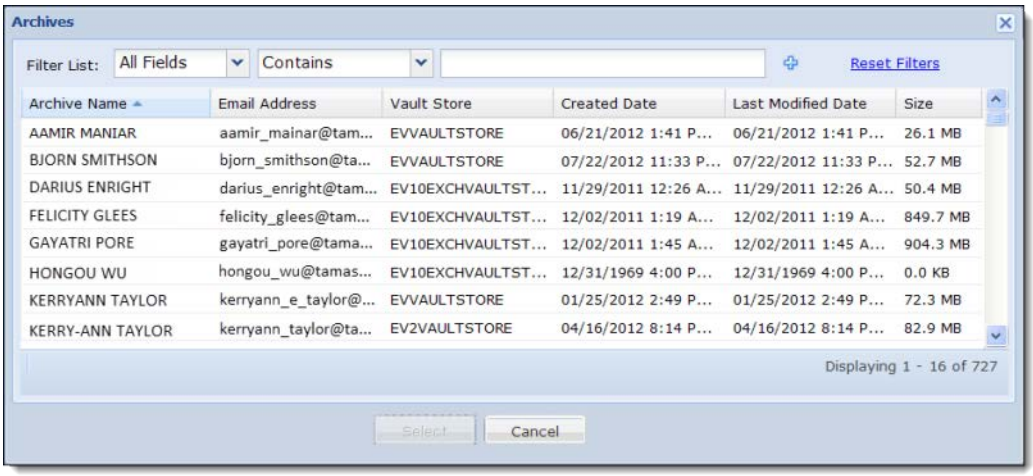
From **All Collections**, when creating (or editing) a collection task (for an Enterprise Vault Archive, Domino, or Exchange mailbox source), the **Archives** tab automatically shows the Email Address column.

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.

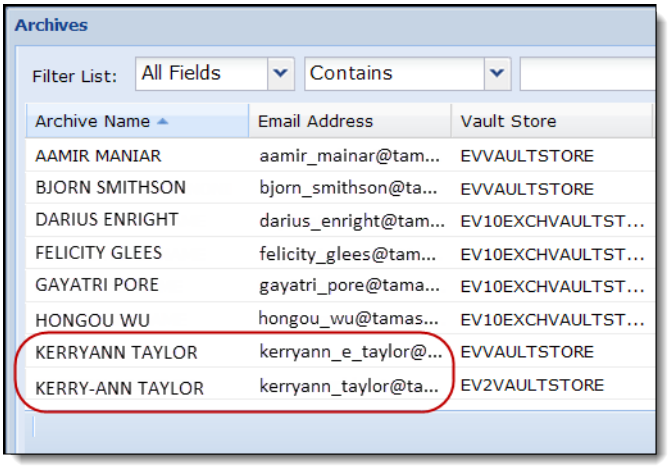


Click **Add Archives** to select from archive names that have an Email Address.

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 150*.

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**, **Keywords**, and **Traits** 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 Platform User Guide*.

Keyword Search

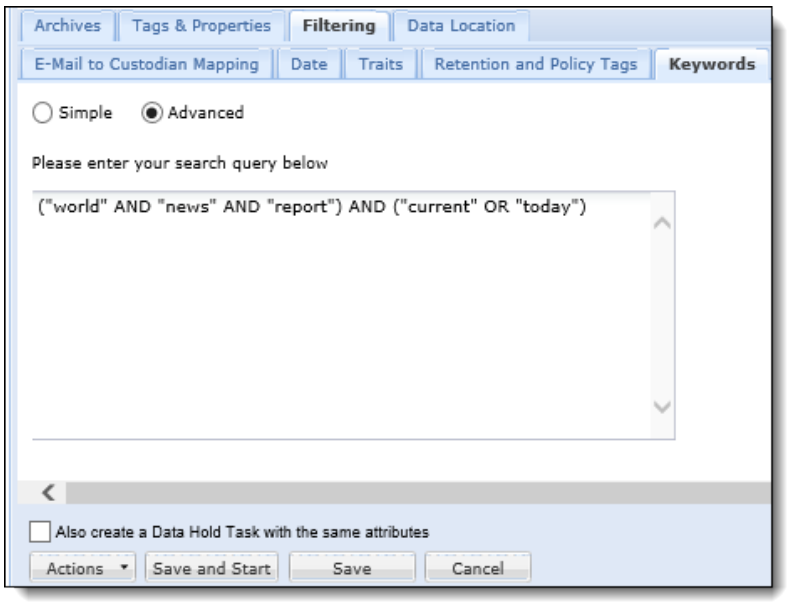
Starting with 9.1, users can use the Enterprise Vault keyword search in two ways:

- Advanced Search
- Simple Search

Advanced search

Starting with 9.1, users can use AND, OR, and NOT Boolean operators to define a content-based search query. Users can also use the NEAR operator to search the files based on the proximity of two keywords.

Note: The advanced search query must be entered in the specified format. If the syntax is incorrect, you will either get an error on the UI or the collection task will fail to retrieve the results from Enterprise Vault. See the guidelines listed below before you start using the advanced search technique.



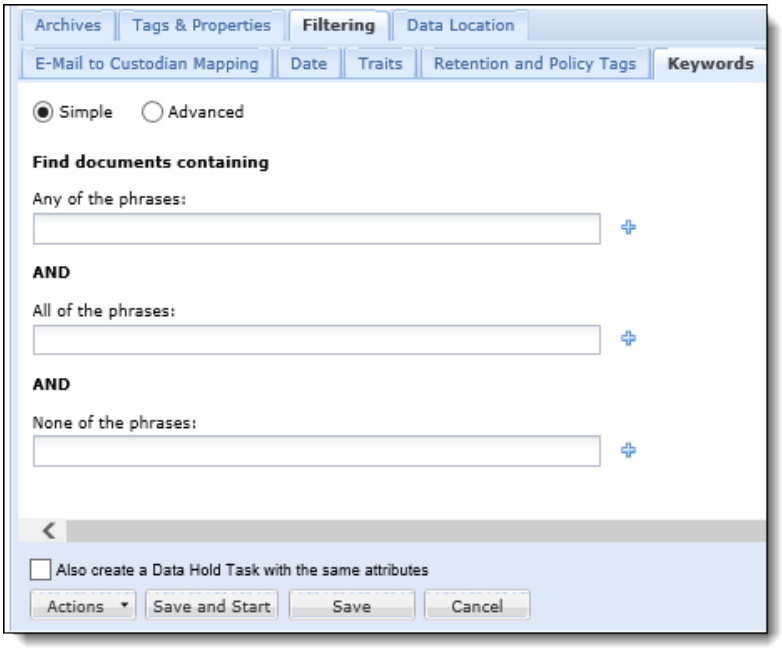
Guidelines for writing an advanced search query for Enterprise Vault sources:

- Each keyword must be enclosed within double quotes (“”).
  For example:
  Correct Syntax: “world report” OR “news”
  Incorrect Syntax: “world report” OR news
- Wild cards * and ? are supported.
  For example: (“wor*” AND “new?”), where * will search for all phrases starting with *wor* and *?* will search for all words starting with new and in addition will have one more character that will substitute *?*
- Parenthesis must be used if different operators are used in a single query.
  For example:
  Correct Syntax:
  “world” AND “news” AND “report”
  (“world” AND “news”) OR (“Report”)
  Incorrect Syntax: “world” AND “news” OR “report”
- Each criterion must be enclosed within parenthesis marks even if it contains a single keyword.
  For example:
  Correct Syntax: (“world” AND “news”) OR (“Report”)
  Incorrect Syntax: (“world” AND “news”) OR “Report”
- Operators are not case-sensitive. For example, both ‘AND’ or ‘and’ are treated as same. It is a good practice to write out the operator in all capitals to distinguish them from the terms.

- A set of criteria within one parenthesis set can only have the same operator. All terms within a parenthesis set will serve as one set of criteria and the terms within the other set of parenthesis as another. The operator between these sets of parenthesis is used in the search to get the overall results.
  For example:
  Correct syntax: (“world” OR “news” OR “report”) AND (“current” AND “today”)
  Incorrect syntax: (“world” AND “news” OR “report”) AND (“current” OR “today”)
- ALL operators should always be used as binary operators.
  For example:
  Correct Syntax:
  “world” NOT “news”
  “world” AND “news”
  Incorrect Syntax:
  NOT (“world” AND “News”)
  NOT “world”
  AND “world”
- NEAR operator can be used to search files where two keywords/phrases appear within 10 words of each other (both inclusive). The proximity of the number of words is not configurable.
  Example: “world” NEAR “news”
- NEAR operator can also be used in combination to the logical AND/OR/NOT operators.
  Example: (“world” NEAR “news”) OR (“report” NEAR “current”)
- Multiple proximity searches cannot occur against each other.
  For example:
  Incorrect Syntax:
  (“world” NEAR “news”) NEAR (“report”)
  “world” NEAR “news” NEAR “report”

Simple search

This is an existing keyword search technique. Content of a single row is considered a full phrase. You do not need to use quotes or double quotes. Phrases can include wildcards. An asterisk character ("*") substitutes for any zero or more characters, and the question mark ("?") substitutes for a single character.



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.

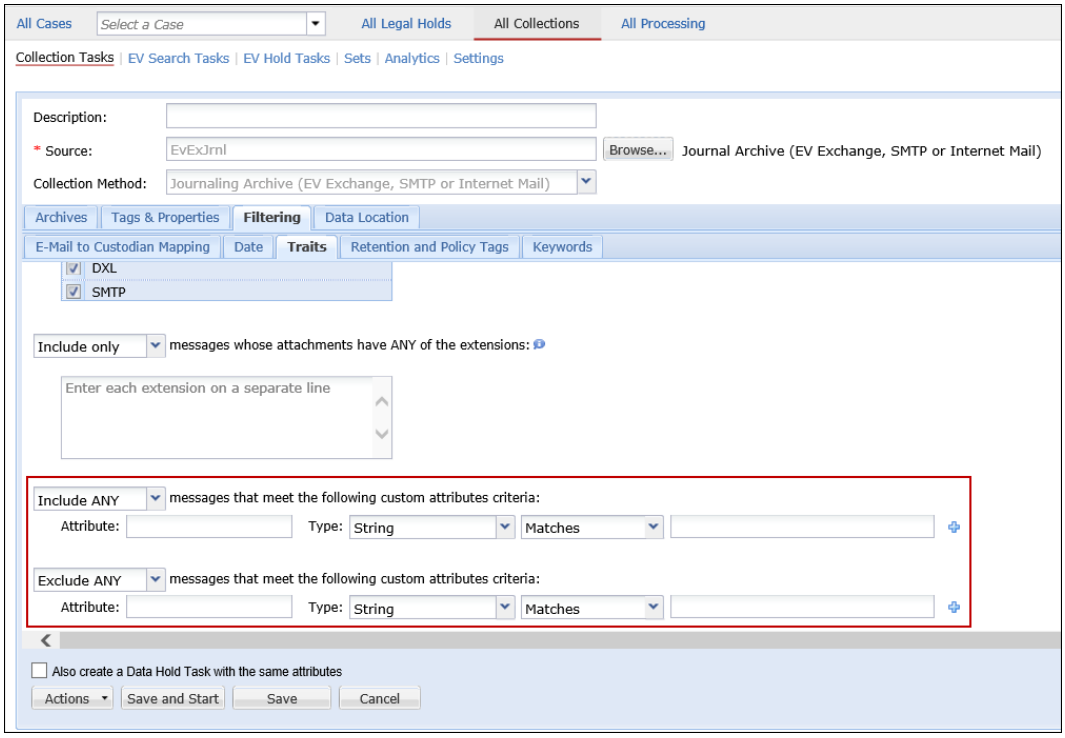
However, this over- or under-collection will not happen if the folder names are "fol_der1" and "folder$1" as the position of the special characters in the name is different.

Using custom attributes in the Traits filter for Enterprise Vault

With the enhancements made in release 9.1, users can use custom attributes in the Traits filter for Enterprise Vault Exchange and Enterprise Vault Domino sources.

Following options are available for the Traits filter:

- Include ALL/ANY:
  - Include ALL: Collect files which satisfy ALL the custom attributes specified by the user.
  - Include ANY: Collect files which satisfy ANY of the custom attributes specified by the user.
- Exclude ALL/ANY:
  - Exclude ALL: Exclude files which satisfy ALL the custom attributes specified by the user.
  - Exclude ANY: Exclude files which satisfy ANY of the custom attributes specified by the user.
- Contains: Provide a substring of the required phrase. The Contains option is available for String attributes type only.



The Attribute name field is case sensitive. Refer to the Enterprise Vault documentation for the exact names of the custom and standard attributes.
Text entered in the custom attribute value text box is considered as a phrase even if the text is not enclosed in double quotes.
Wildcard characters such as * and ? are supported for the attribute values of type "*String*".

See the following examples of search queries using custom attributes in the Traits filter.

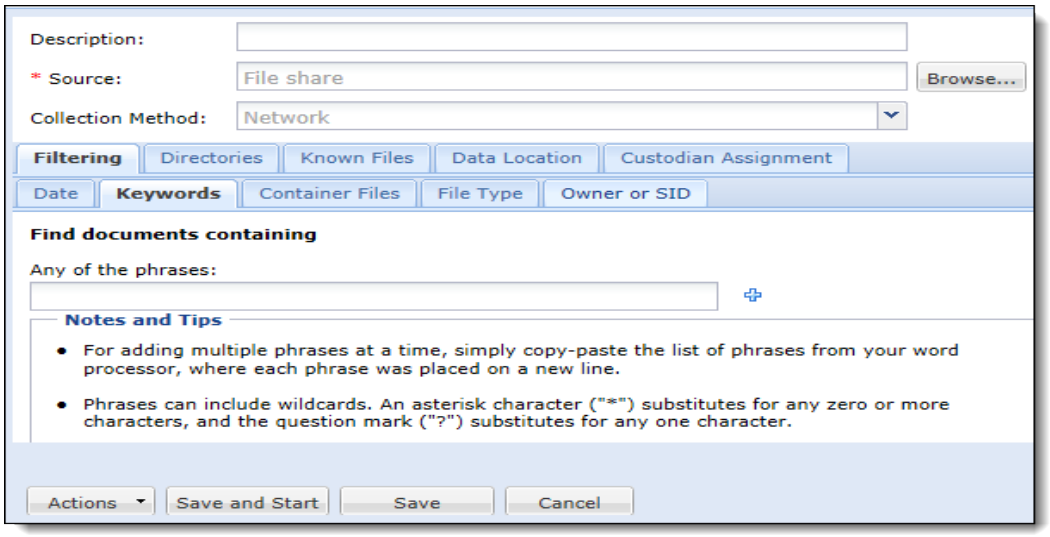
Examples:

Include/ Exclude	Any/ All	Contains /Matches	Attribute name, value pairs	Expected behavior
Exclude	ANY	Contains	subj : veritas	Exclude all the emails where subject contains ANY of the attribute values, i.e. veritas and test.
			subj : test	
Exclude	ALL	Contains	subj : veritas	Exclude all the emails where subject contains ALL of the attribute values, i.e. *veritas* and *test*.
			subj : test	
Include	ANY	Contains	subj: shares	Include all the emails which contain *shares* OR *rates* in the subject.
			subj: rates	
Include	ALL	Contains	subj: shares	Include all the emails which contains *shares* in the subject AND have the msgType as *exch*.
			Vault.msgType: EXCH	
Exclude	ALL	Contains	subj : undeliverable attachments	Exclude all emails which contain the phrase "undeliverable attachments" AND the phrase “Town Hall Meeting“ in the subject. The entire text would be considered as a phrase with or without enclosing the text in double quotes.
			subj : “Town Hall Meeting”	
Exclude	ANY	Contains	subj : undeliverable attachments	Exclude all emails which contain the phrase "undeliverable attachments" OR the phrase “Town Hall Meeting“ in the subject. The entire text would be considered as a phrase with or without enclosing the text in double quotes.
			subj : “Town Hall Meeting”	
Include	ALL	Contains	subj : undeliverable attachments	Include all emails which contain the phrase "undeliverable attachments" AND the phrase “Town Hall Meeting“ in the subject. The entire text would be considered as a phrase with or without enclosing the text in double quotes.
			subj : “Town Hall Meeting”	
Include	ANY	Contains	subj : undeliverable attachments	Include all emails which contain the phrase "undeliverable attachments" OR the phrase “Town Hall Meeting“ in the subject. The entire text would be considered as a phrase with or without enclosing the text in double quotes.
			subj : “Town Hall Meeting”	
Include	ALL	Contains	subj : "email with attachments"	Include all emails which contain the phrase "*email with attachments*" and *Undeliverable* keyword in the subject.
			subj : undeliverable	
Exclude	ANY	Matches	subj : veritas	Exclude all the emails where subject matches ANY of the attribute values, i.e. veritas and test.
			subj : test	
Include	ALL	Matches	subj: shares	Include all the emails where subject matches *shares* and *rates* in the subject.
			subj: rates	

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, SharePoint, Domino, EV.cloud, On-site PC and On-site Macintosh.

Note: For Microsoft 365 sources, see *"Filtering Best Practices for Microsoft 365 Exchange and OneDrive" on page 116*.



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 Microsoft 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 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.

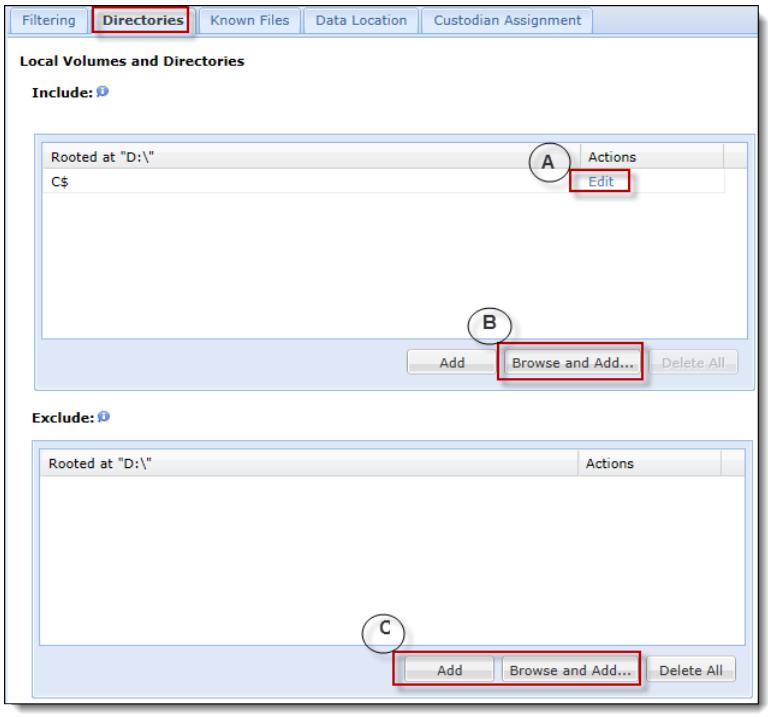
CAUTION! You must have sufficient permissions for browsing/selecting directories. (The logged on user account is shown at the bottom of the Source Directories window.) Ensure that you are logged on with the correct account user and role. Veritas strongly recommends logging on with the correct account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

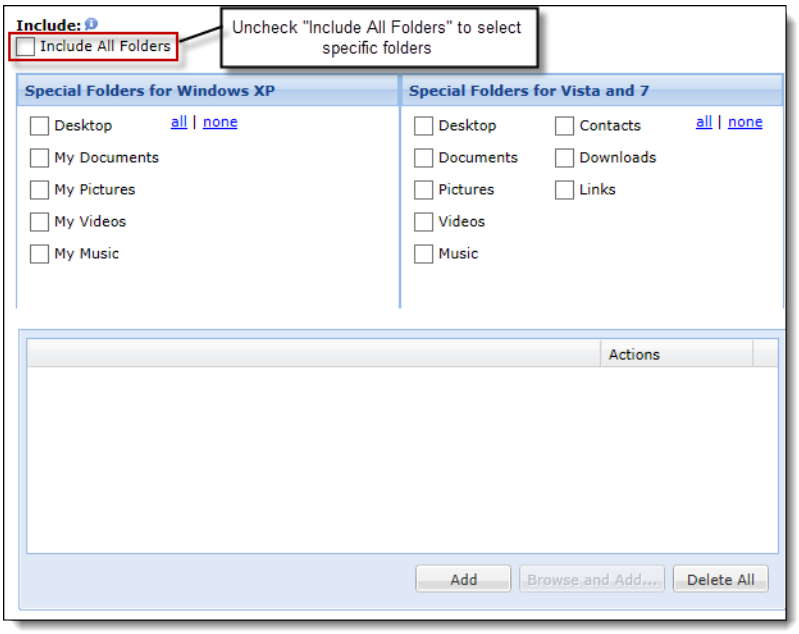
   Note: Excluded folders must be in one of the specified directories in your "Include" list above. If a selected folder is not in one of the "Include" folders, the collection task will ignore the entry.

   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 103*.

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 103*.

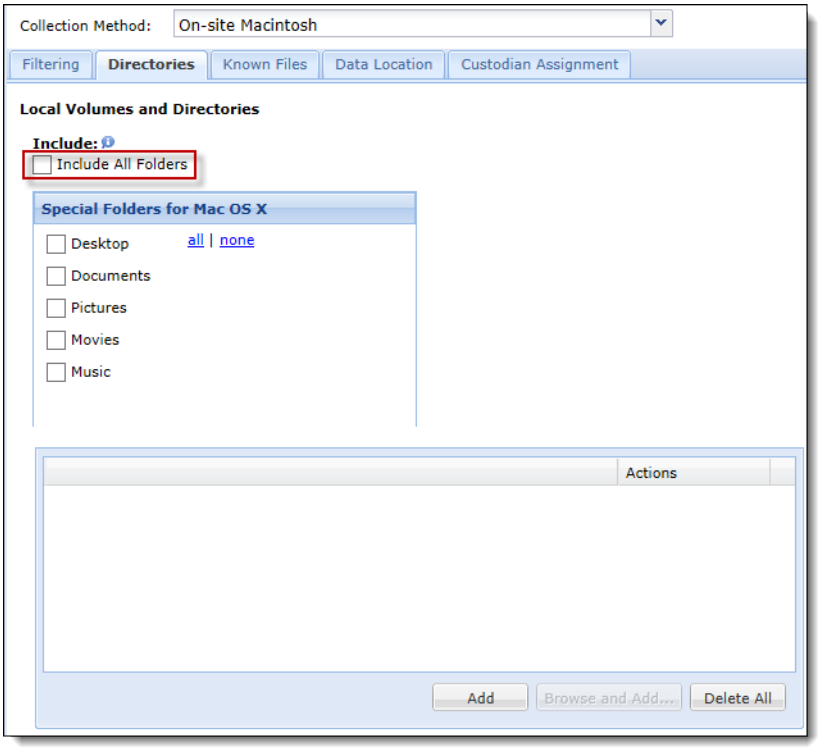
To include/exclude directories for an OnSite Macintosh

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 103*.

OnSite Mac Collection Considerations

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

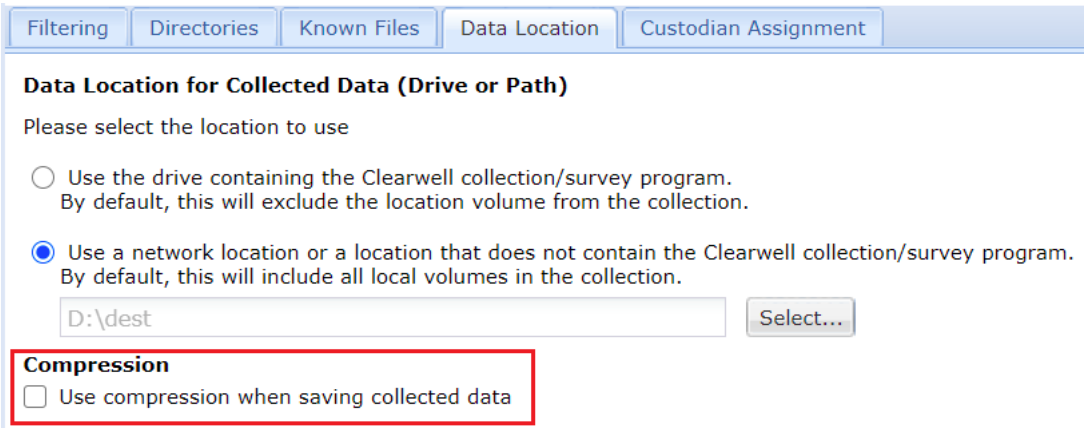
- **Invalid Character handling—**Backslashes, colons, forward slashes: Unlike for PC collection, in which all files with invalid characters for Windows except for the backslash (\) are collected when compression is off, for OnSite Mac collection, users can create files and folders with forward slashes (/), 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 hard disks 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.

Enable Compression for OnSite Collection Tasks

To compress the collected data, you can enable compression on the **Data Location** tab.



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: Saving and loading of collection templates are not supported for an Microsoft 365 Collection task. Instead, an existing collection task can be copied using the **Actions** column.

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.
Collection Method	(Default is "Network"), or click **Cancel** to collect data from a non-network source. See *"Performing OnSite Collection Tasks" on page 150*.

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.

Run or Schedule a Collection Task

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):

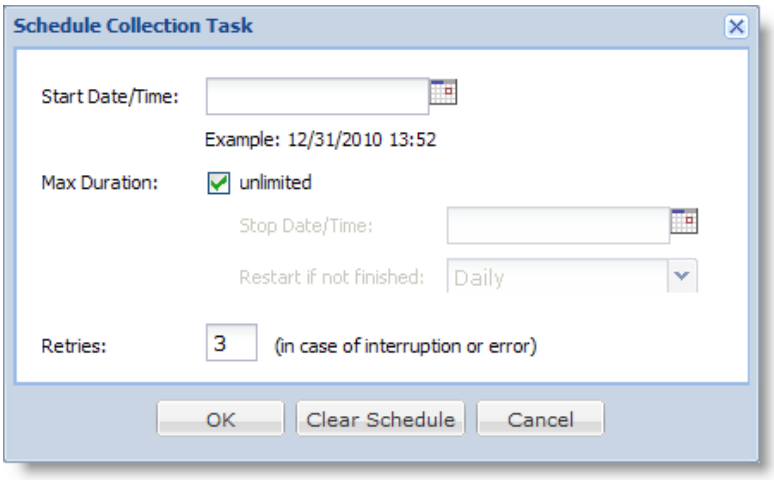
   – To run a task, from the **Collection Tasks** screen, click the icon to start running the task.

   – 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 139*.

  › 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*.)

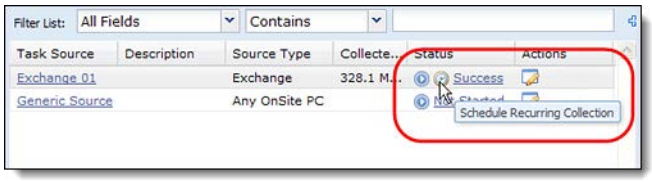
   C. To delete the task, click the icon.

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.

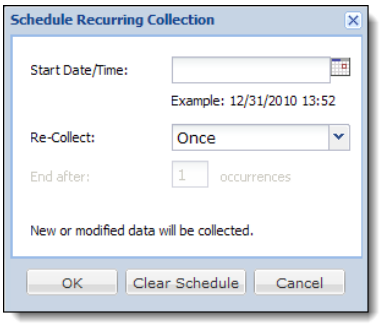
To run a recurring collection task

1. Follow the steps in *"Run or Schedule a Collection Task" on page 137*, 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.

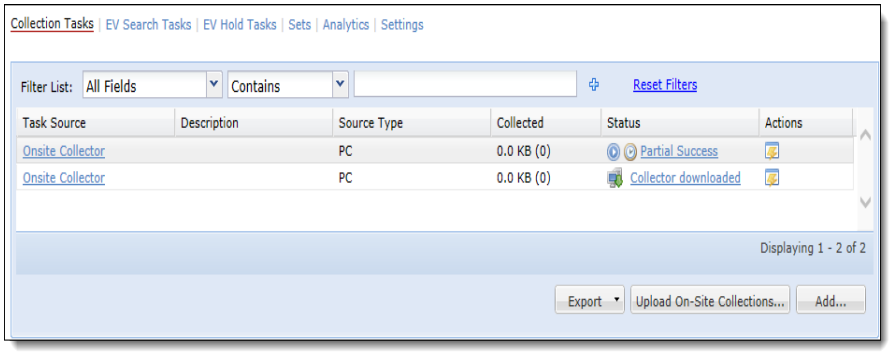
Note: For Microsoft 365 tasks, see *"Re-running a Collection Task for Microsoft 365" on page 142*.

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.
- 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.

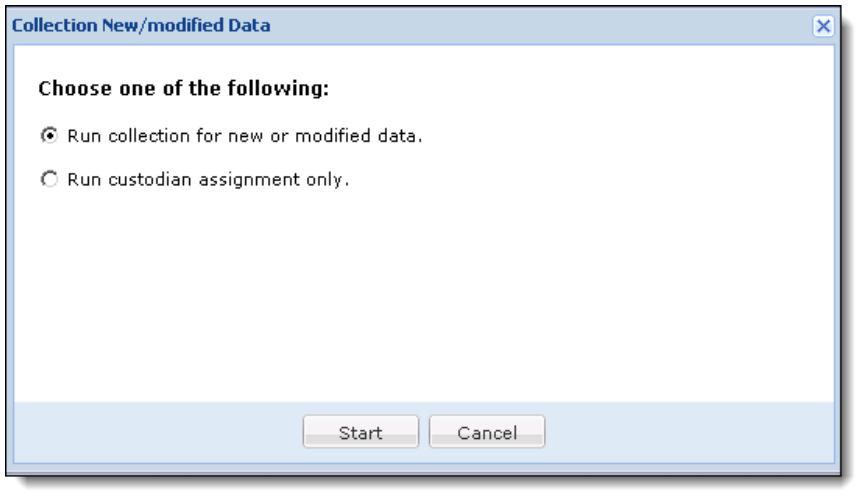


2. From the Collection New/modified Data window, select one of the following option, and then click **Start.**

   – 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 148* 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.

Re-running a Collection Task for Microsoft 365

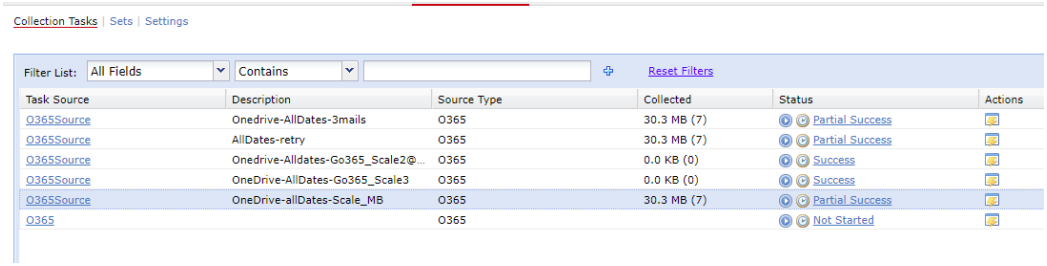
For Microsoft 365 collections, re-running or scheduling a collection works in the following manner:

- Re-running a collection task with Not Started, Stopped, or Failure status will resubmit the collection task to collect the data.
- Scheduling a collection task with Not Started, Stopped, or Failure status will resubmit the collection task to collect the data.
- Re-running a collection task with Success status will schedule a recurring collection to collect new or modified data.
- Scheduling a collection task with Success status will schedule a recurring collection to collect new or modified data.
- Re-running a collection task with Partial Success status will schedule a recurring collection to collect new or modified data and the previously failed items.
- Scheduling a collection task with Partial Success status will schedule a recurring collection to collect new or modified data and the previously failed items.

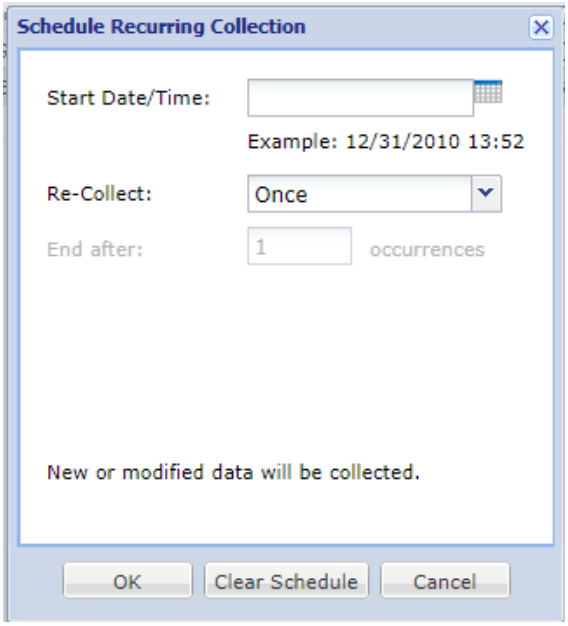
Note: If the data was collected completely when the task was run the last time, and there is no new or modified data available, then re-running a collection task does not collect any new items.
Re-running a collection task does not collect the old data that was not collected previously. To get this data, a new collection task must be created. However, new or modified items will be collected.

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. 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.



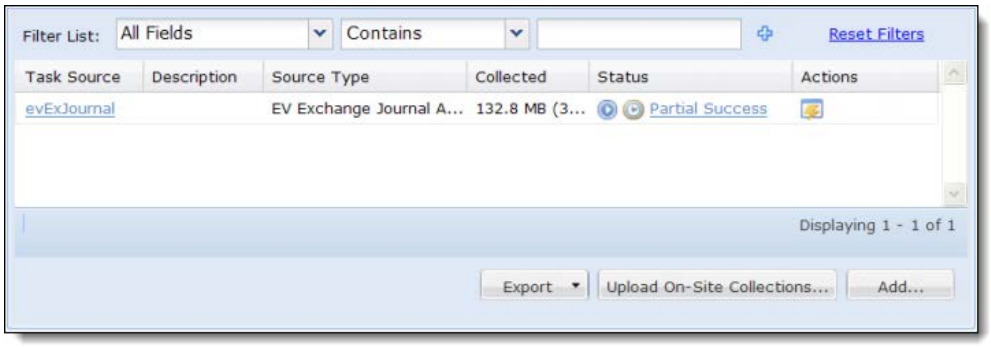
3. Click **OK** to schedule, or **Clear Schedule** to discard changes and reschedule.

   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.

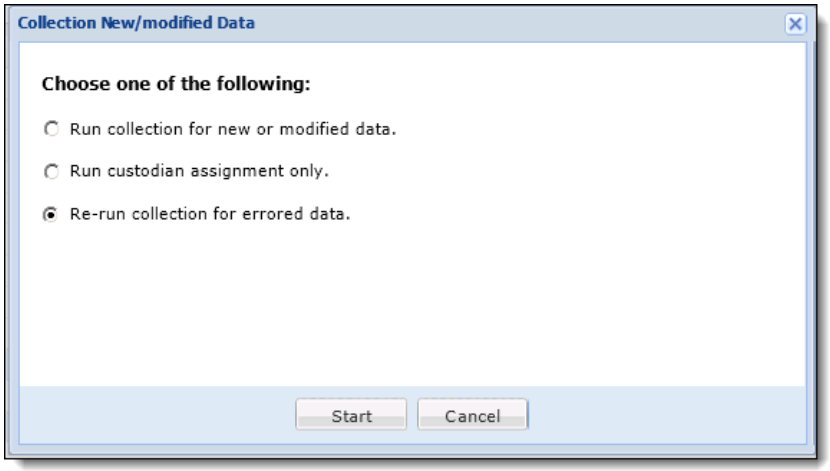
Retrying a Failed Collection Task (for Enterprise Vault and EV.cloud Sources)

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.

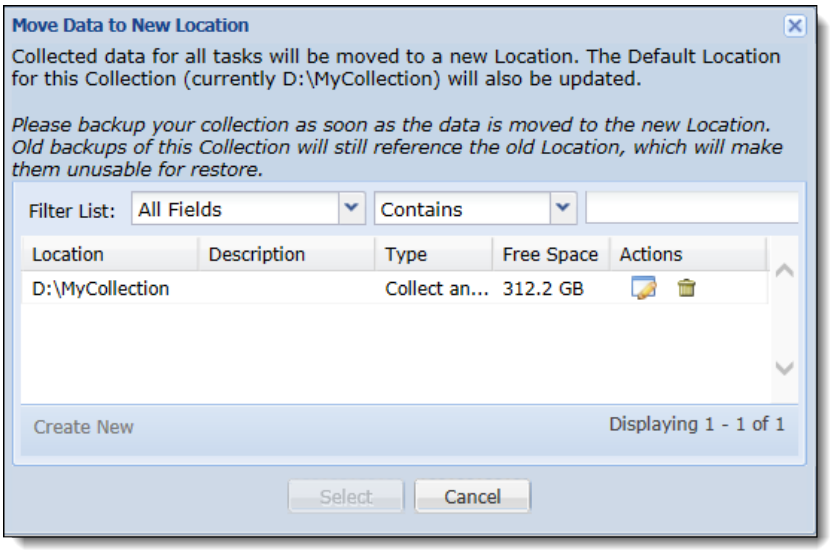
Move Collected Data to Another Location

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: For Microsoft 365 sources, see *"Custodian Assignment Details for Microsoft 365" on page 115*.

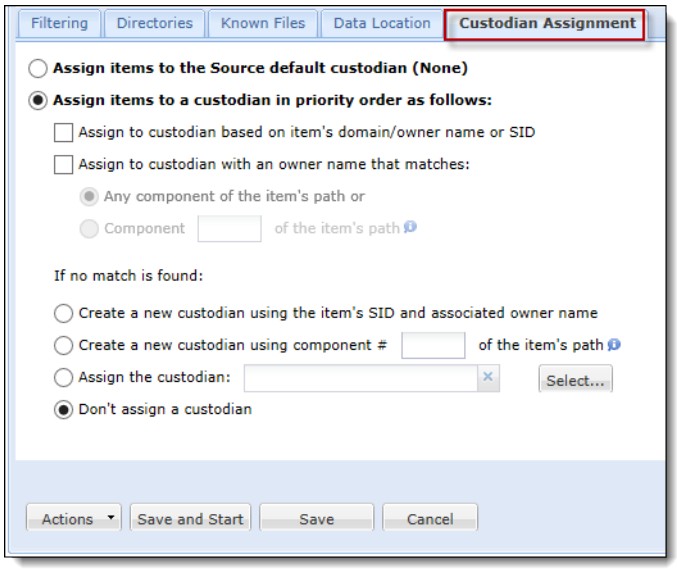
Note: If your task contains uploaded data from an OnSite collection, Veritas eDiscovery Platform will only retain custodian assignment options if the parent task is also part of the same collection. For more information, see *"Performing OnSite Collection Tasks" on page 150*.

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 103*. (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 136*.

   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 130*.

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.

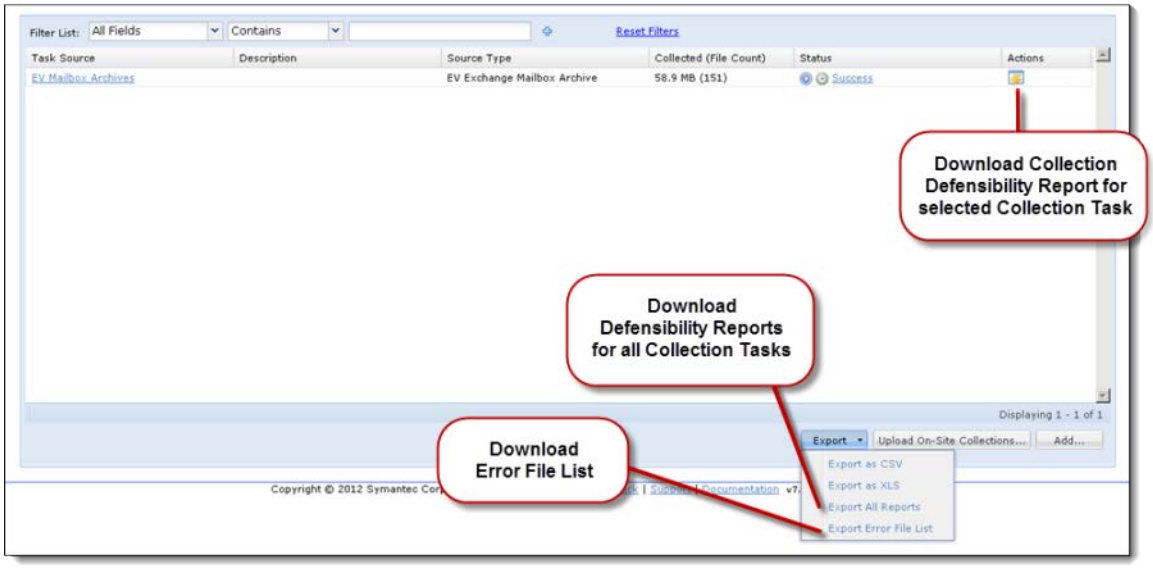
Collection Reports

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.

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" in the next section*
- *"Prerequisites" on page 153*
- *"Creating and Managing Search Tasks" on page 154*

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 158*
- *"View/Edit Search Tasks" on page 159*
- *"Copy a Search Task" on page 159*
- *"Analyze Results" on page 160*
- *"Sample Preview" on page 161*
- *"Run a Report" on page 161*
- *"Delete a Search Task" on page 162*

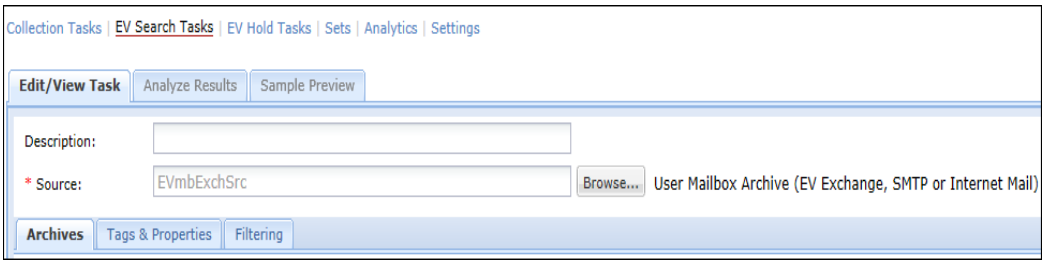
Create a Search

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 169*.

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 102*.)
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 118* 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 "$", "_", and so on in the folder or directory path. Click Add to add the directories. See *"Using special characters in the directory path" on page 126*.
	Folders	(For Enterprise Vault SharePoint Archive source only) Specify the folders you want to include or exclude. Ensure that you do not use special characters such as "$", "_", 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 126*.

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, DXL, or SMTP. 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. See *Using custom attributes in the Traits filter for Enterprise Vault*. 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, the Simple search provides the option of listing any, all, or none of the phrases entered. All three categories can be grouped together by an AND expression. Release 9.1 provides an Advanced search option to use AND, OR, NOT, and NEAR operators for Enterprise Vault sources. See *"Keyword Search" on page 121*.

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 160*.

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 139*.

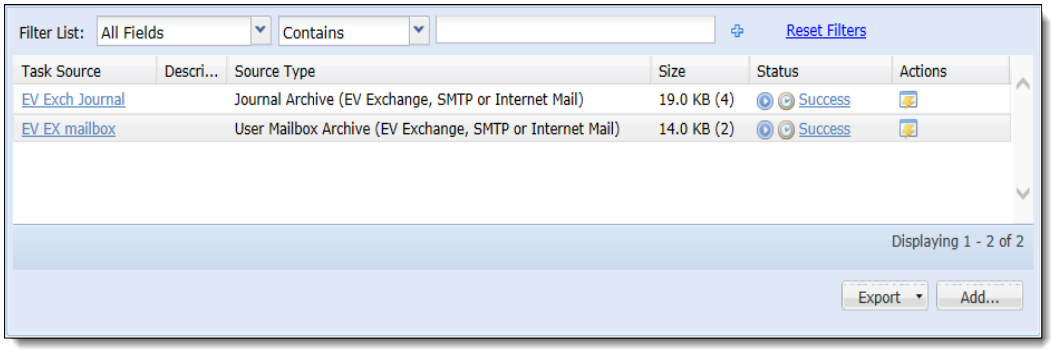
3. Click **OK** to schedule, or **Clear Schedule** to discard changes and reschedule. The date and time when the search is scheduled to run appears in the Status column.

   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

See *"Copy a Collection, EV Search, or EV Hold Task" on page 115*.

Analyze Results

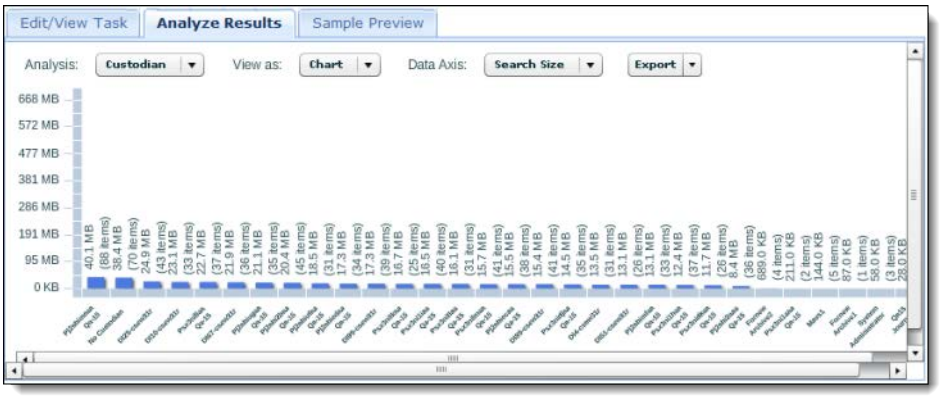
After running a search task, you can view and analyze the results. (The **Analyze Results** tab becomes available only after a search completes successfully.)

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" in the next section*
- *"Prerequisites" on page 163*
- *"Creating and Managing Hold Tasks" on page 164*
- *"Retry Release Hold" on page 173*

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:

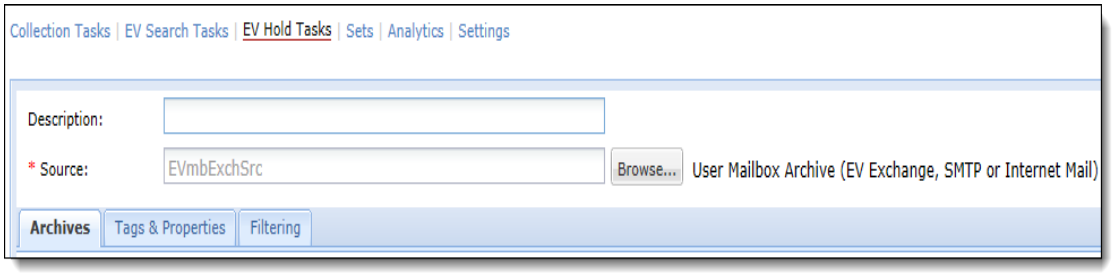
- *"Create a Hold" in the next section*
- *"Schedule a Hold" on page 167*
- *"Create a Hold and Collection Task" on page 169*
- *"View/Report Hold Statistics" on page 170*
- *"Edit/Re-Apply a Hold Task" on page 171*
- *"Copy a Hold Task" on page 172*
- *"Release a Hold" on page 173*

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 169*.

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 169*.)
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 118* 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 "$", "_", and so on in the folder or directory path. Click **Add** to add the directories. See *"Using special characters in the directory path" on page 126*.
	Folders	(For Enterprise Vault SharePoint Archive source only) Specify the folders you want to include or exclude. Ensure that you do not use special characters such as "$", "_", 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 126*.

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, DXL, or SMTP. 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. See *Using custom attributes in the Traits filter for Enterprise Vault*. 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, the Simple search provides the option of listing any, all, or none of the phrases entered. All three categories can be grouped together by an AND expression. Release 9.1 provides an Advanced search option to use AND, OR, NOT, and NEAR operators for Enterprise Vault sources. See *"Keyword Search" on page 121*.

Add Task Filter Options (Continued)

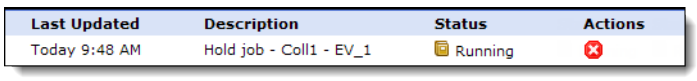
Field	Description	
	Date	Filter by Date. Click the drop-down menu to select a filter type, and if applicable, enter or select a date. **Note:** Indexes of an archive are usually spread across multiple index volume sets. In earlier releases of Veritas eDiscovery Platform, when a date range filter is used 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 169*.)

   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 173*.

   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 172*.

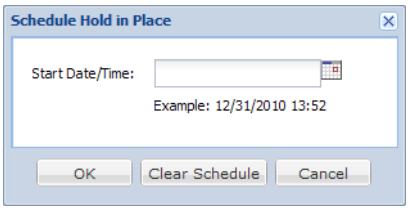
Schedule a Hold

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 171*.) Scheduling recurring runs allows you to place new items on hold in tasks that have already completed successfully.

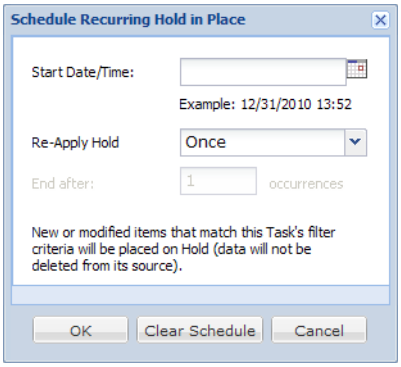
To schedule a hold task

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 139*.

   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 171* and *"Copy a Hold Task" on page 172*.)

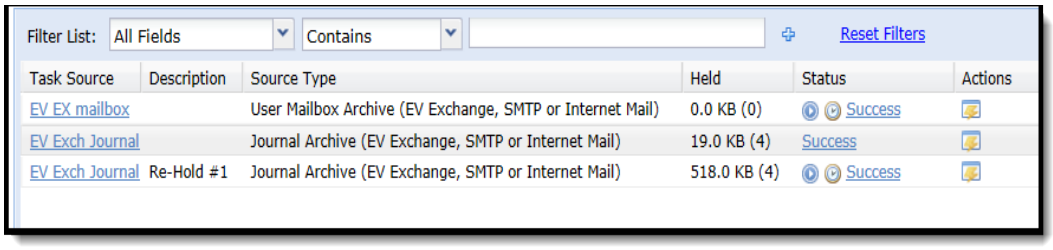
To create a hold and collection task

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 167*.

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 169*.

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

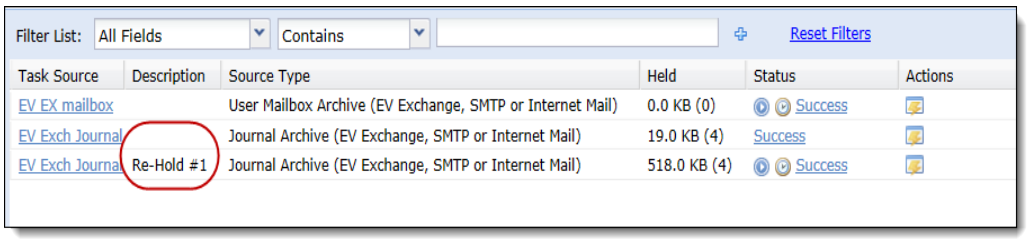
   - Create a new collection or data hold task using the same attributes. Follow steps 4-5 in *"Create a Hold and Collection Task" on page 169*.

     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.

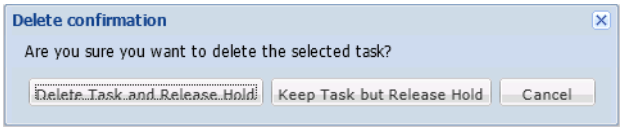
Copy a Hold Task

See *"Copy a Collection, EV Search, or EV Hold Task" on page 115*.

Release a Hold

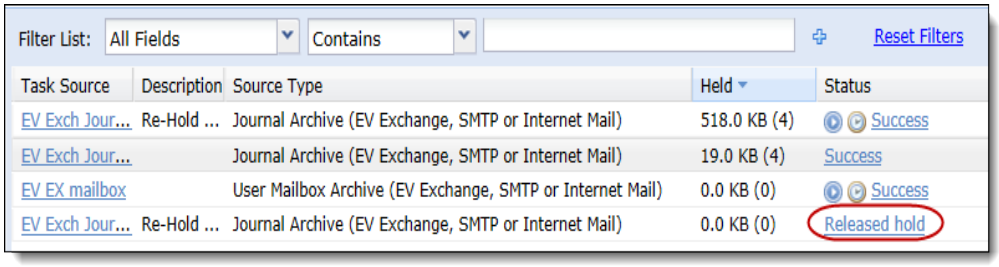
To release a hold

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 173*.) 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 172*.)

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" in the next section*
- *"Managing Collection Sets" on page 175*
- *"Changing Collection Settings" on page 181*
- *"Processing Collection Sets" on page 182*
- *"Analyzing Data (Across Your Case)" on page 184*
  - *"Viewing Processed Data" on page 184*

About Collection Sets

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 153*.

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 9.1, 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.

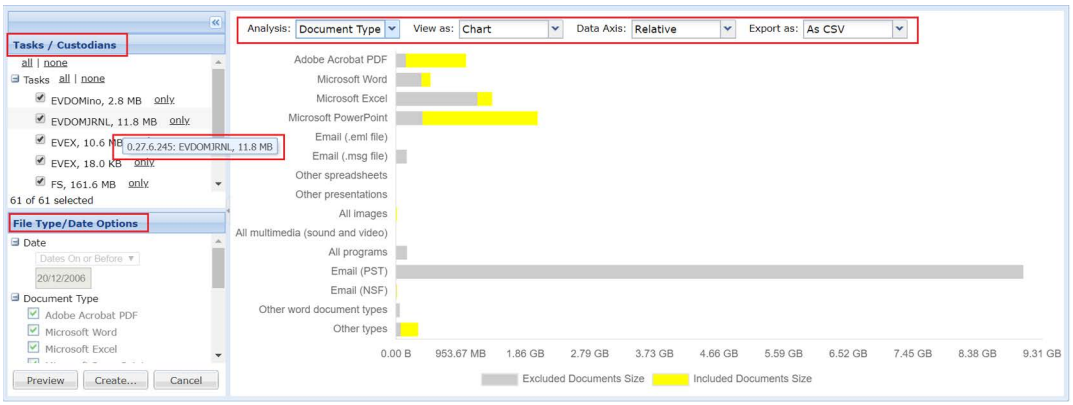
Creating a collection set

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	View data as a high-level summary, by the type of documents collected, by custodian. **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.
(View As:) Chart, or Table	Change the output view of the data formatted as a graphic chart or in table form.
(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.

5. Select options to include in, or exclude from your collection set:

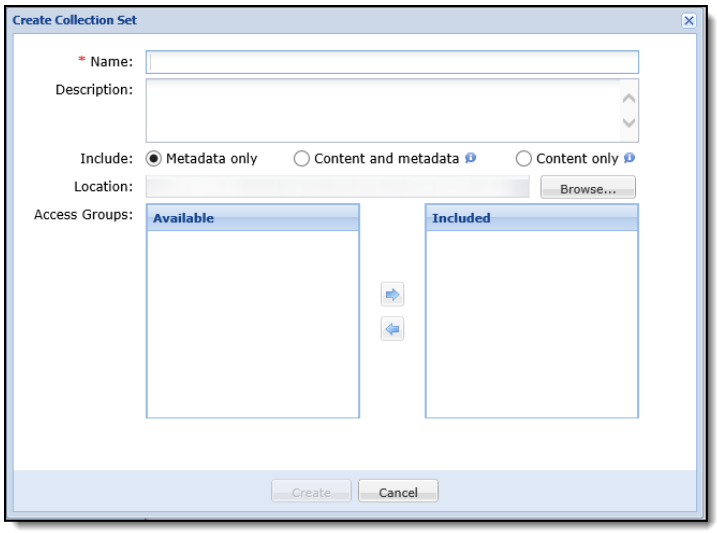
   A. Choose data types to include in your collection set by using the following filter options.

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 194*. **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:

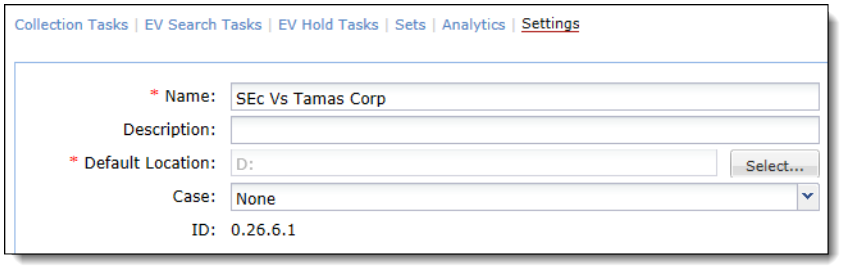
METADATA_ONLY: To create "Metadata only" collection set by default.

METADATA_AND_CONTENT: To create "Content and metadata" collection set by default.

CONTENT_ONLY: To create "Content only" collection set by default.

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.

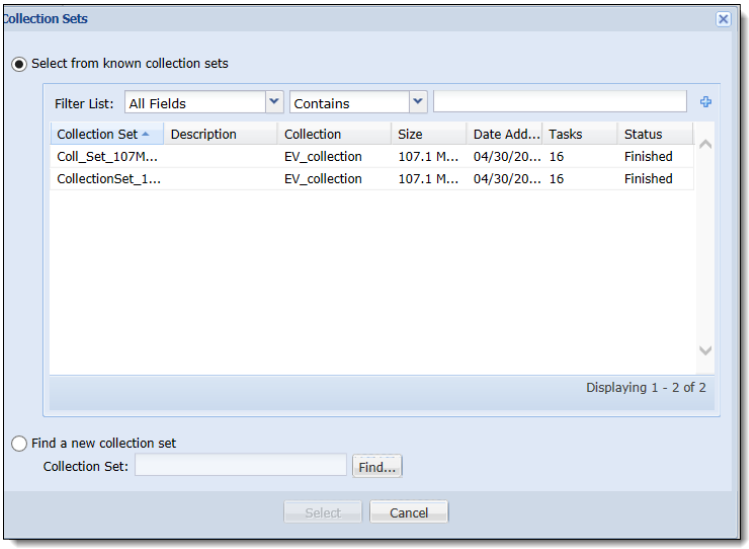
2. To add a collection set to your case:

   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

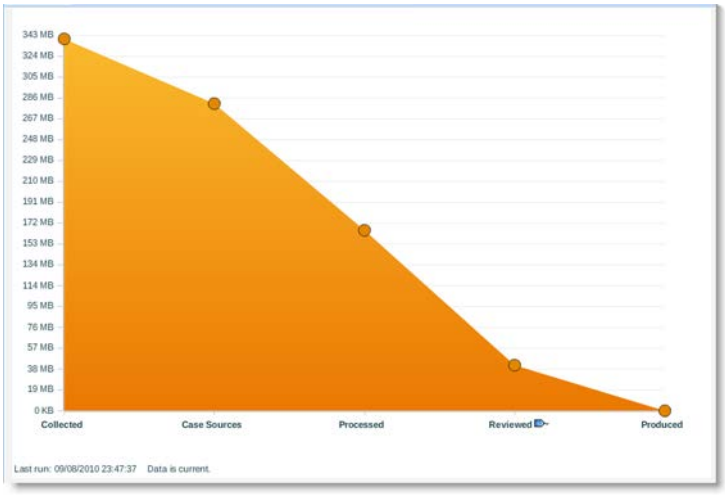
To view your processed data

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

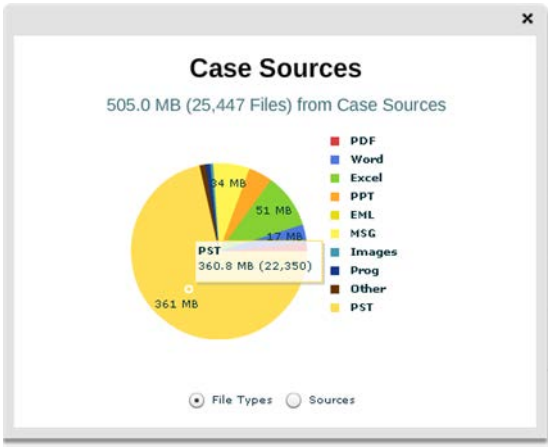


   This overall view of the data is defined by collected data (sources added to be processed), to what was actually processed; to later, what has been reviewed, and produced.

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 185*.

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 186*.

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 186*.

Collection Administration and Maintenance

This section describes how to manage and maintain your collected data in Veritas eDiscovery Platform.

- *"Managing Collection User Accounts" in the next section*
  - *"Defining Collections Administration User Accounts" on page 190*
  - *"Viewing the Collections Admin Role" on page 192*
  - *"Managing Access Groups Permissions" on page 193*
    - *"Planning for access group deployments" on page 194*
    - *"An example of access group mapping:" on page 194*
    - *"Adding an Access Group" on page 197*
    - *"Deleting an access group" on page 198*
- *"Managing Custodians (Across a Case)" on page 199*
- *"Archiving, Restoring, and Deleting Collections" on page 203*
- *"Managing Your Collections License" on page 206*
  - *"About Reusable Licenses" on page 206*
  - *"Updating Your License" on page 207*
- *"Additional Collections Admin Tasks" on page 212*
- *"About Collections Backups" on page 212*

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" in the next section*
- *"Viewing the Collections Admin Role" on page 192*
- *"Managing Access Groups Permissions" on page 193*

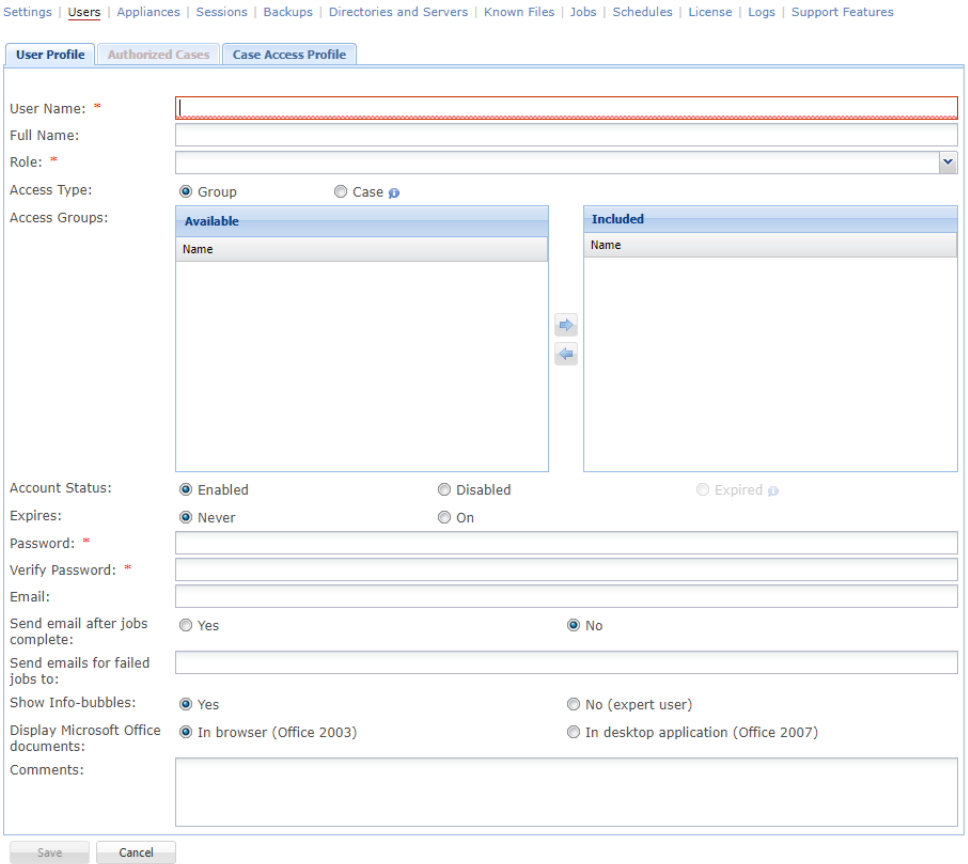
Defining Collections Administration User Accounts

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 192*. 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 190*. 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

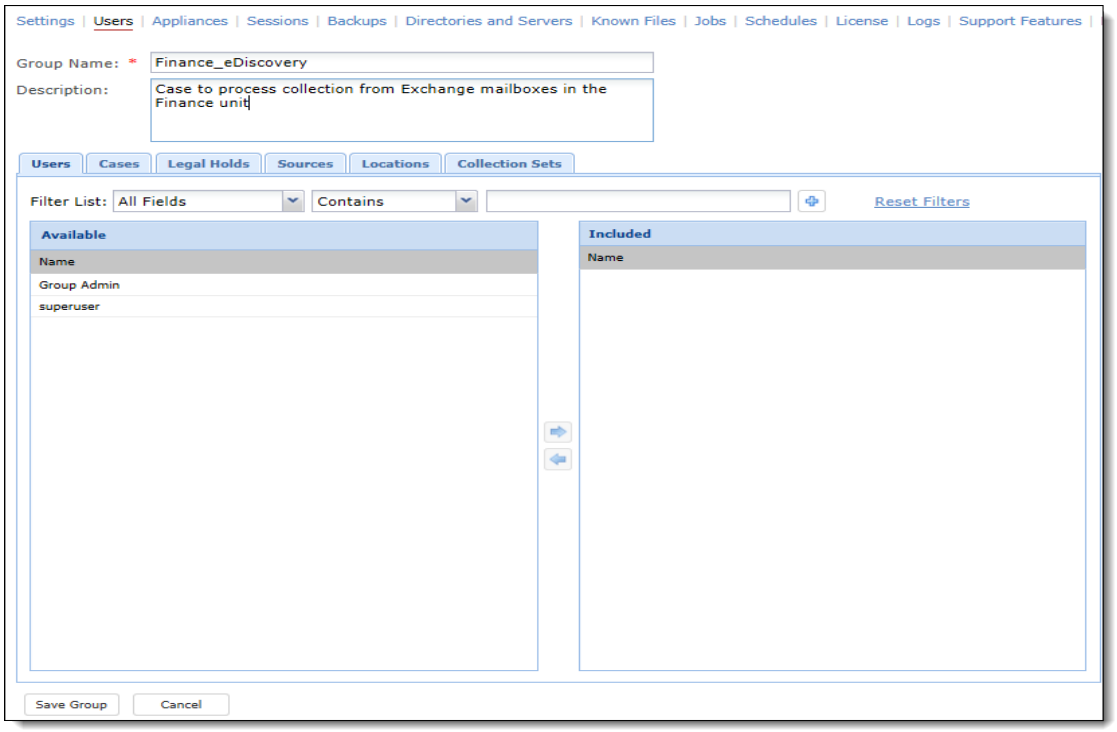
Create access groups and map the users, legal holds, sources, locations, and collection sets as:

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:

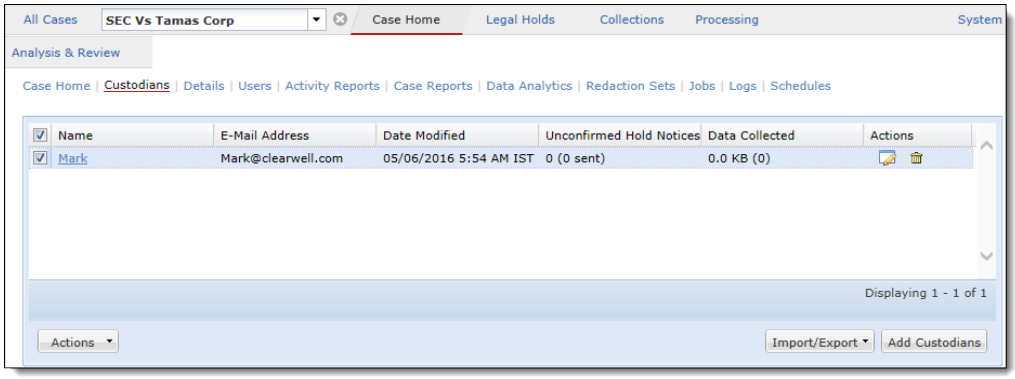
- View/sort consolidated custodian information
- Edit custodian data, with options to view details, changes made, and all Legal Hold and Collection activity for a selected custodian in the case

  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.

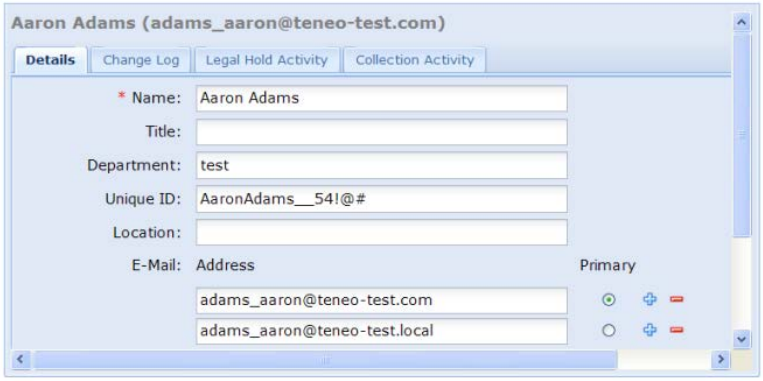


   This view displays a consolidated list of employee information showing all activity for each custodian in a specific case. The columns *Unconfirmed Holds* and *Data Collected* show both Legal Hold and Collection activity in a single dashboard view. From here, you can search and sort by attributes and date range (based on the same criteria used for employee attributes as described in *"Mapping Employee Attributes" on page 36*).

2. Do one or more of the following custodian management tasks:

   A. *Edit Custodians*.

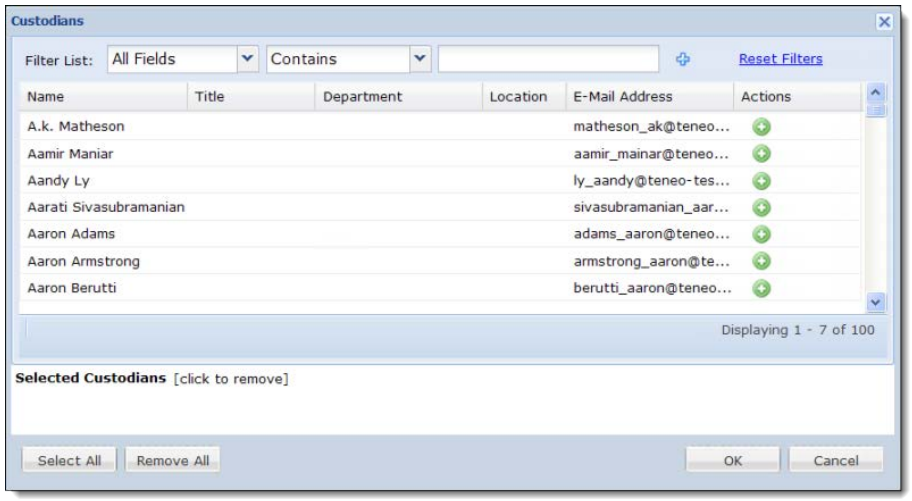
   › Either click the (edit) icon from the Actions column, or click a name in the list to edit the custodian's information.



   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 36*.

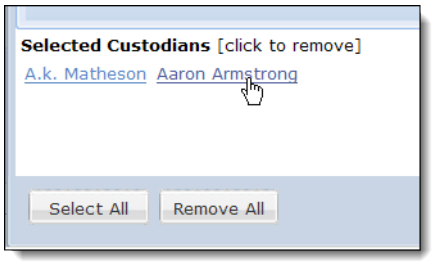
   B. *Add Custodians*.

   › 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 39*.) 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 150*. 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.

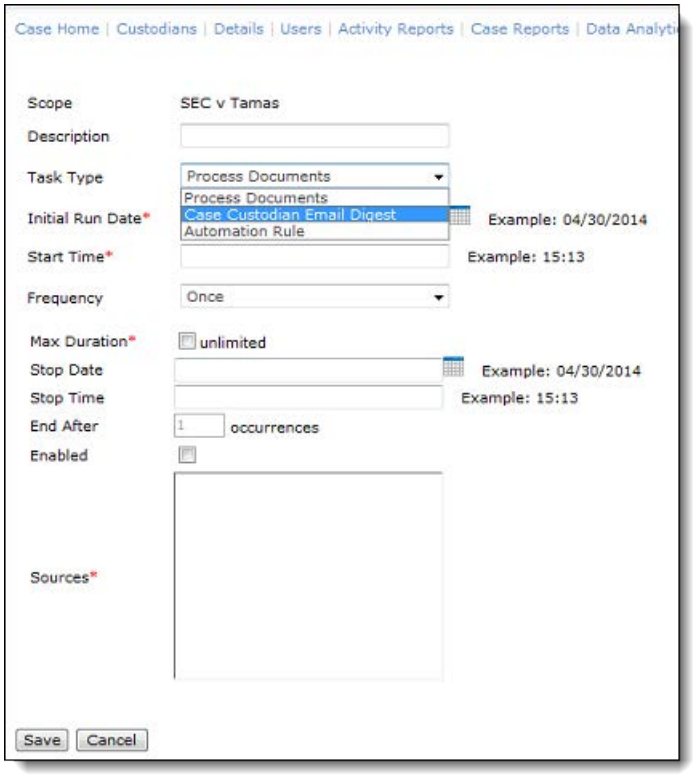
› From there, click the icon under the status column to view custodian reports for all custodians in the selected case.

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 137*. 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.

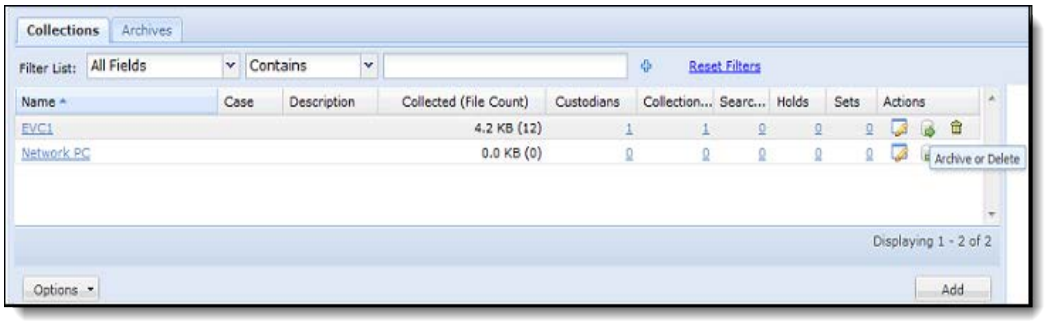
When a collection is deleted, its contents (collections and tasks) are removed from Veritas eDiscovery Platform. The data itself is not actually deleted or moved, but cannot be recovered from its current location. (The default location for the selected legal hold's data is provided. For example: D:\CaseData.)

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

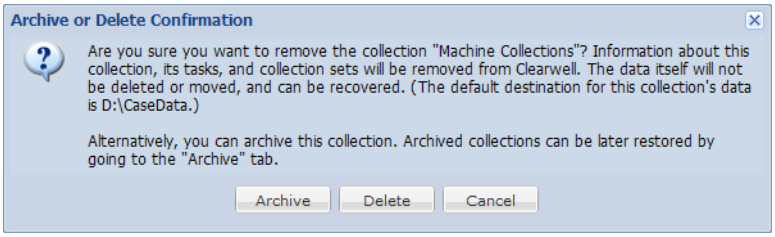
1. From **All Collections** > **Collections** screen, click the **Collections** tab.

   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 206*.

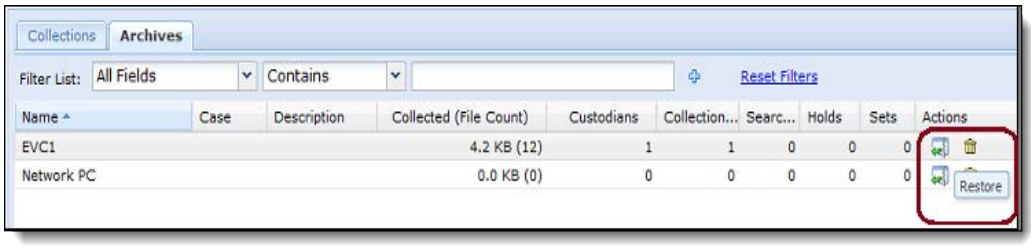
Restoring an Archived Collection

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**.

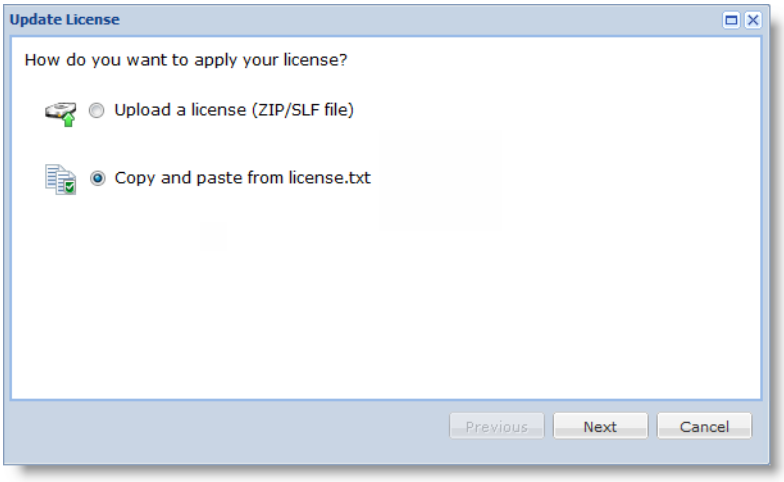
   In this example, the current capacity is for 50 custodians. Periodically note the custodian count, particularly each time you archive a collection or task.

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.

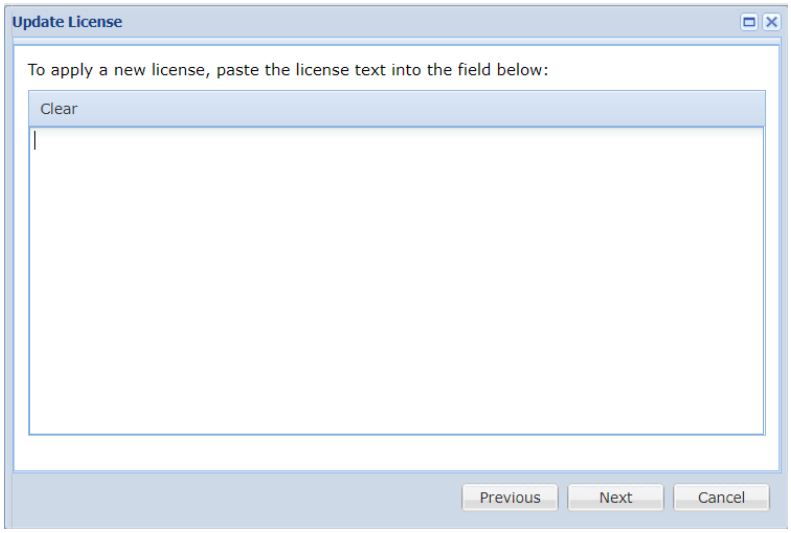
   (As shown in this example, you can choose to copy and paste the license information instead, from "license.txt" file, attached in an email message you received.)



   Click **Next**.

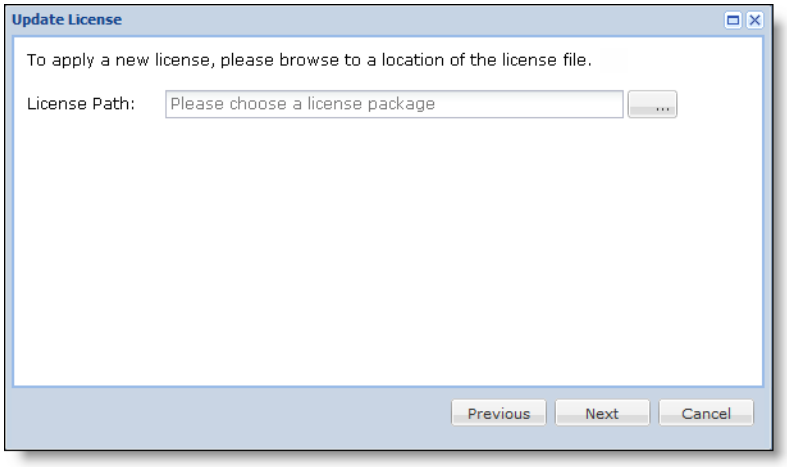
5. Do one of the following:

   A. If copying/pasting the license information, press Ctrl+V to the place the copied text into the window. (Click **Clear** to delete.)

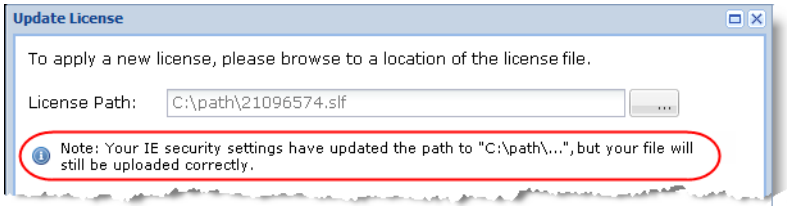


Note: Depending on your browser's security settings, pressing Ctrl+V may prompt you to allow access to the System Clipboard. Clicking **Allow access** is safe and will stay in effect until the page is refreshed again.

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 browser security settings are updated to that location, though your license file will still be properly uploaded.

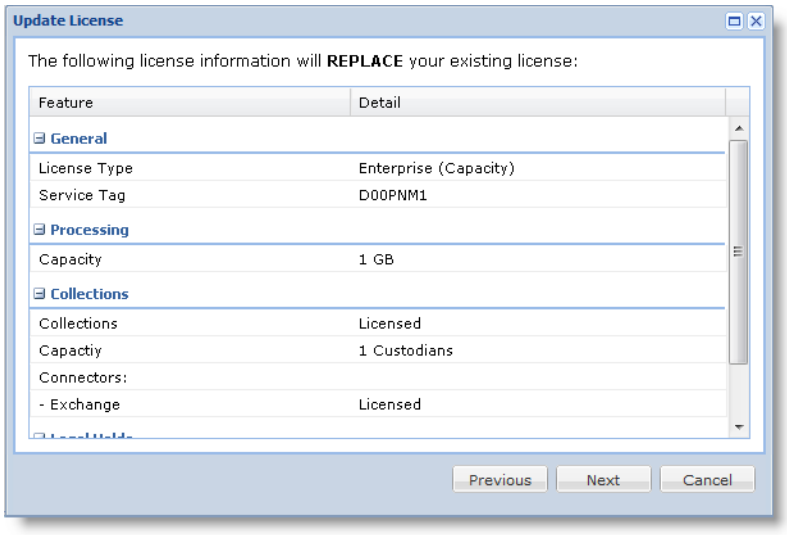


Note: Uploading a file will *add/merge* the license information with the current license on the server where it is installed.

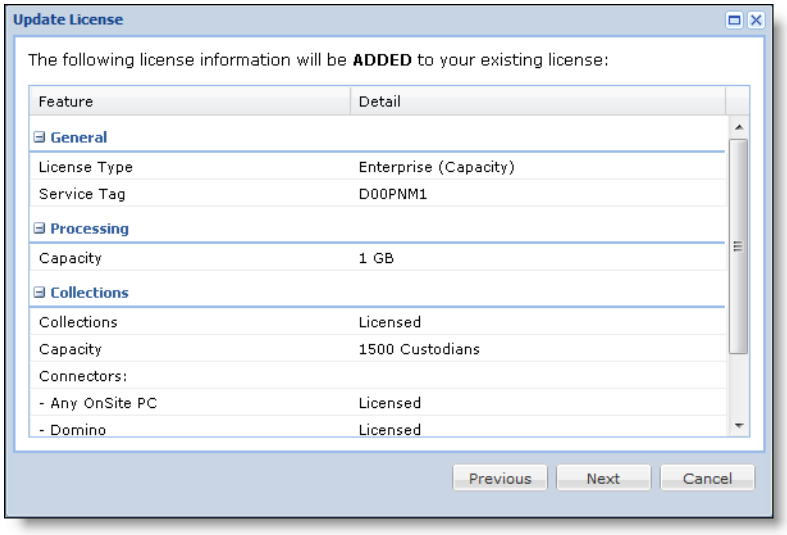
Click **Next**.

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:

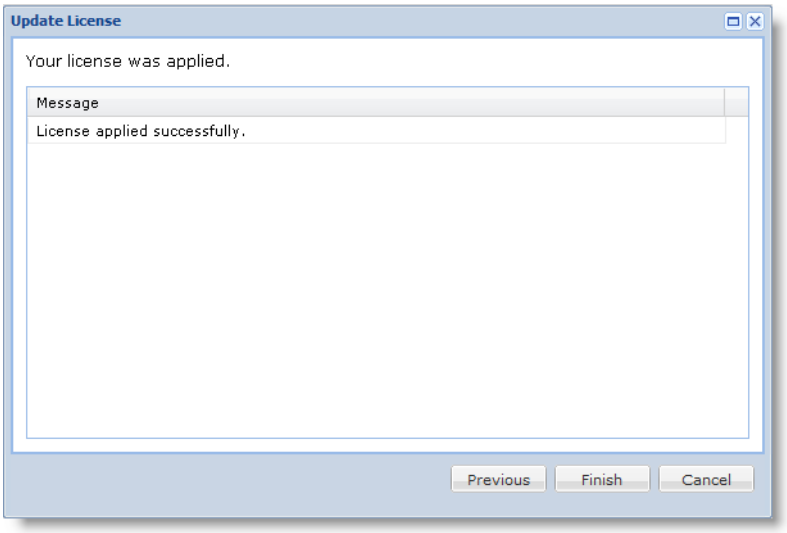


   B. If you uploaded your license (from a ZIP or SLF file), note that the information, as shown, will be *added to* your existing license:



   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 190*.
Managing Task Collections	Data collections can be scheduled to occur automatically. See *"Run or Schedule a Collection Task" on page 137*. (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 206*.
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 213*.

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" on page 214*
- *"Troubleshooting Exchange collections" on page 216*
- *"Troubleshooting Exchange collections failure in a cross-domain environment" on page 217*
- *"Troubleshooting Exchange 2013 collections" on page 218*
- *"Troubleshooting File Server or PC collections" on page 221*
- *"Troubleshooting SharePoint collections" on page 223*
- *"Troubleshooting Collector Sources" on page 224*
- *"Enabling Scaleout Mode (for Enterprise Vault Collection)" on page 225*
- *"Troubleshooting the EV.cloud discovery" on page 227*
- *"Troubleshooting Enterprise Vault Retry Failures" on page 227*
- *"Improving the Enterprise Vault collection task concurrency" on page 228*
- *"Custodian assignment for Enterprise Vault User Mailbox Archives" on page 229*
- *"Changing Source Accounts" on page 231*
- *"Troubleshooting the Microsoft 365 collections" on page 231*
- *"Microsoft 365 Collection Performance Tuning" on page 233*
- *"Troubleshooting Microsoft Teams collections" on page 236*
- *"Technical Support" on page 238*

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:
```

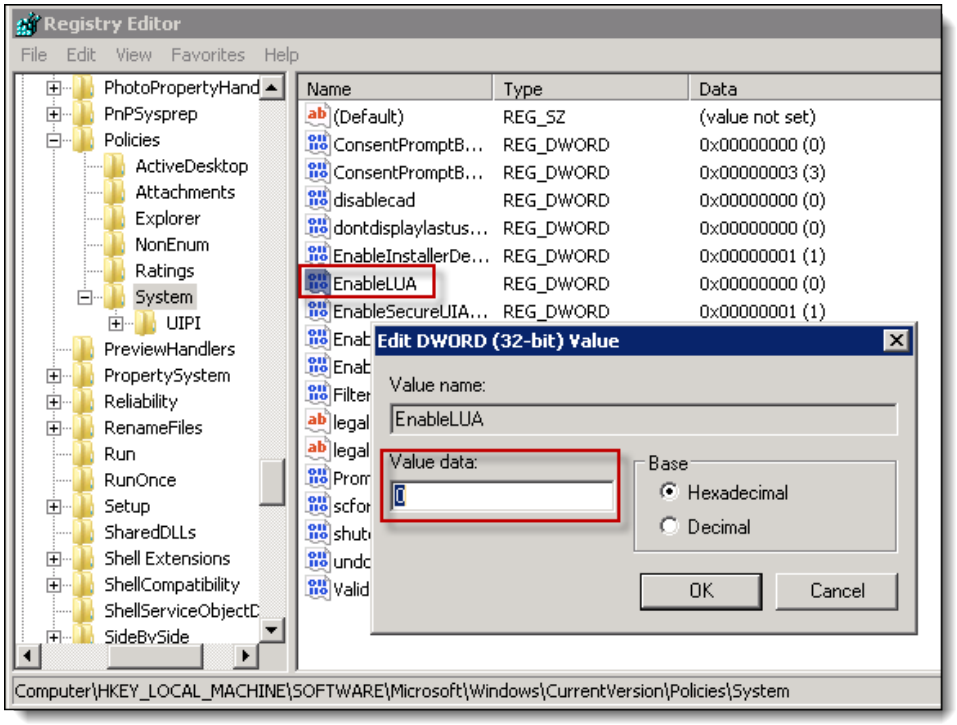
How to deactivate UAC on your appliance:

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.

   Note: On Windows Server 2019 with Outlook 2019, if Exchange collection fails because the Exchange Server does not have a Trusted CA signed certificate, you need to import the Exchange Server certificate in Trusted root certificate authorities.
   To import certificate, run any of the following commands:

   - Import-Certificate -FilePath "<.cer file path>" -CertStoreLocation Cert:\LocalMachine\Root command.
     For example, Import-Certificate -FilePath "C:\CA-PublicKey.Cer" -CertStoreLocation Cert:\LocalMachine\Root
   - certutil.exe -addstore root <.cer file path>
     For example, certutil.exe -addstore root c:\capublickey.cer

4. Check your security settings for the mailbox. The security settings may be preventing mailbox access.

Troubleshooting Exchange collections failure in a cross-domain environment

Exchange Server fails when the collection task is run from a Windows Server 2019 appliance present in a different domain.

To understand the issue, consider the following network domains having individual domain controllers connected in a two-way trust.

- Domain A contains an Exchange Server
- Domain B contains eDiscovery Platform installed on Windows Server 2019

In the above scenario, if a task to collect the data from Exchange Server is run on eDiscovery Platform, the collection fails. And the logs indicate that Autodiscover to Exchange Server is not reachable. To resolve this issue, create a host "Autodiscover" entry to the Exchange Server in the domain where the Exchange Server resides.

To create the DNS entry, complete the following steps:

1. Log on to the domain that hosts the Exchange Server, for example Domain A.
2. On the command prompt, run **dnsmgmt.msc** command.
3. Under the DNS Manager, expand domain name, and then expand the forward look-up zone.
4. Right-click the first entry and select "Host (A)".
5. In the Name field, type "Autodiscover".
6. In the IP field, type the IP address for Exchange Server.
7. Click **Add Host**.
8. Close the DNS Manager.

Note: For a domain with multiple Exchange Servers, a separate host entry for each Exchange Server must be created.

On the machine where eDiscovery Platform is installed, verify that the Outlook that is run as the source account, can:

- Connect to the Exchange Server
- Fetch emails

The eDiscovery Platform should now be able to collect emails from Exchange Server that is located in other domain.

Troubleshooting Exchange 2013 collections

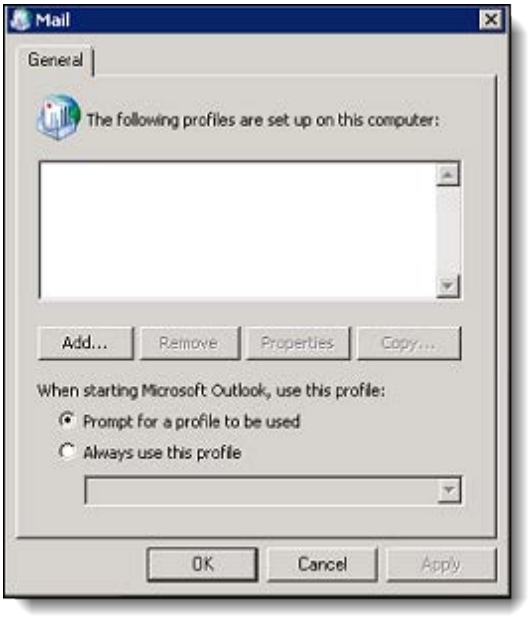
The Exchange 2013 mailbox uses the built-in Auto-discover feature which automatically detects your Microsoft Outlook settings. Your collection task to collect from the Exchange 2013 mailboxes may fail if the profile information for your Exchange server is not retrieved correctly.

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.

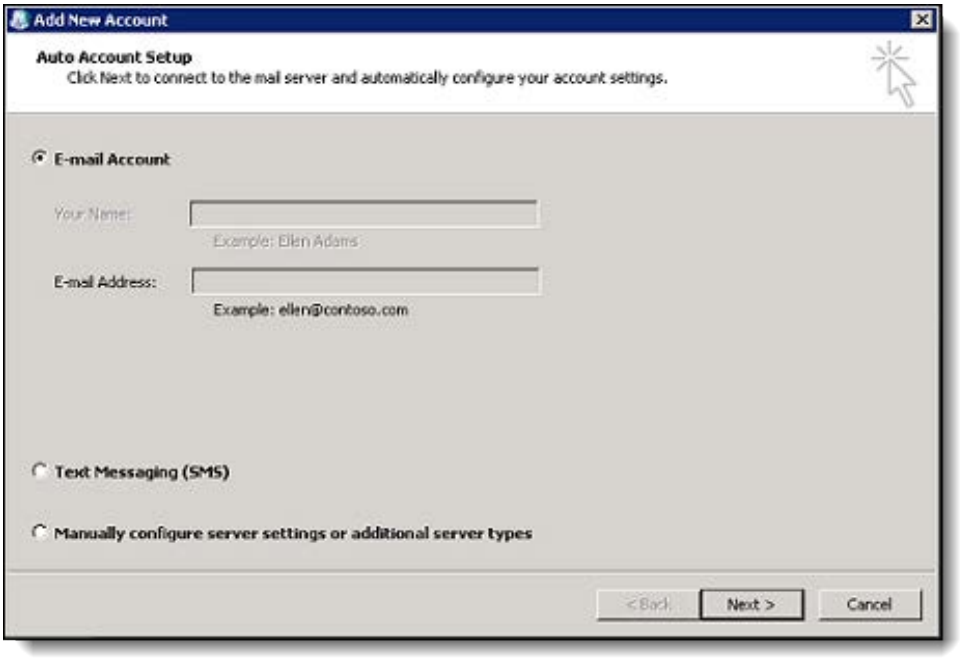
To configure the Outlook template profile

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.



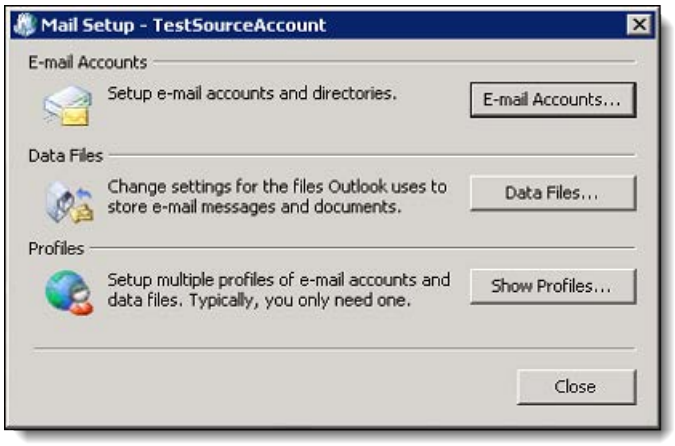
3. Click **Add**. The **New Profile** dialog appears.

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

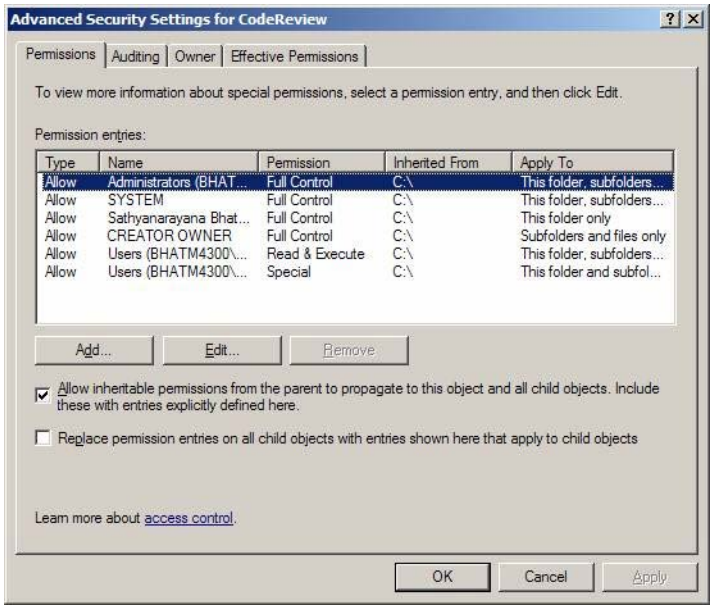
To perform the collection, run Microsoft's "net use" command, which requires 'RunAs' privileges, and do the following:

- 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 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.
- 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.

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 226*

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_Primary*, *CWA_Node1*, *CWA_Node2*, and *CWA_Node3*, the Veritas_Appliance_Primary 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 Primary 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 Primary 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.

Improving the Enterprise Vault collection task concurrency

Release 9.0.2 and later provide an ability to improve the concurrency of multiple Enterprise Vault Collection, Search, or Hold tasks. The Enterprise Vault lease is now claimed/released at a batch level within a task, instead for the entire length of the task. This gives an equal opportunity to all the tasks running to make progress.

To improve the concurrency of multiple Enterprise Vault tasks, a user can configure the property ***esa.icp.ev.contentretriever.leaseWaitTimeMills*** by using **System** > **Support Features** > **Property Browser** feature, and setting the value as low as 1 millisecond.

Custodian assignment for Enterprise Vault User Mailbox Archives

In the current mechanism of custodian assignment, eDiscovery Platform identifies the custodians based on the mapping between an Active Directory User, the user's Exchange Mailbox DN, and the user's Exchange Mailbox Archive in Enterprise Vault.

When a mailbox is moved to Microsoft 365, Enterprise Vault loses the Exchange Mailbox DN information that is associated with the archive and subsequently it becomes NULL in the Enterprise Vault databases. When eDiscovery Platform performs Enterprise Vault discovery, a *NULL* value of the user's Exchange Mailbox DN is stored in the eDiscovery Platform database. As a result, the custodian assignment fails to identify the custodian that is associated with the archives.

A new mechanism to correctly identify and assign custodians is introduced in 8.3 CHF4, 9.0.2, and 9.1.

The custodians are identified using the Display Name or E-mail Address that is associated with the *MailboxId*. If the *MailboxId* information is not available, then *ArchiveId* is used to determine E-mail Address for searching the right employee. The Archive Id is used to query the Archive to SMTP target (i.e. email address) mapping.

To implement this mechanism, you must set the ***esa.icp.ev.CustodianAssign.by.EVSmtpTargets*** property to *True* by using **System** > **Support Features** > **Property Browser**. By default, this property is set to *False*.

Note: You must first perform Active Directory sync and Enterprise Vault discovery before you can use this enhancement and start collecting data from Enterprise Vault User Mailbox Archives. You should perform Active Directory sync and Enterprise Vault discovery at regular intervals to ensure that the eDiscovery Platform database stays current and that custodian assignment works correctly.

On Enterprise Vault, multiple SMTP targets can be configured to store data in the same archive. In this case, multiple email addresses are identified when eDiscovery Platform searches for *ArchiveId*.

When an archive is mapped with more than one email address, you should configure the following properties using **System** > **Support Features** > **Property Browser**:

Property 1:

esa.icp.ev.CustodianAssign.SmtpTargetsAmbiguity.ResolveBy.PreferredDnsList

Value: The values can be comma-separated list of DNS names listed in a preference order. The default value is set to "" (i.e. null).

Property 2:
esa.icp.ev.CustodianAssign.MultipleEmployeesAmbiguity.ResolveBy.PrimaryEmail

Value: *True* or *False*. The default value is set to *True*.

When all records have the same primary email address, then the employee with the least *EmpId* is selected as a custodian. If the primary email addresses are not identical, then *NONE* is assigned as a custodian.

When an archive is associated with multiple email addresses, then you can set a preferred order to choose between multiple email addresses.

For example, "MMOORE" archive is mapped with three email addresses:

Email address	Archive Name
mMoore@ONCLOUD.CLEARWELL.COM	*MMOORE*
mMoore@GO.CLEARWELL.COM	MMOORE
mMoore@CLEARWELL.COM	MMOORE

Records in the "t_employee" table:

EMPID	DISPLAYNAME	PRIMARYMAIL
1	*MMoore*	*mMoore@oncloud.clearwell.com*
2	*Michael.Moore@clearwell.com*	mMoore@oncloud.clearwell.com

Scenario 1:

When the properties are set as:

esa.icp.ev.CustodianAssign.SmtpTargetsAmbiguity.ResolveBy.PreferredDnsList="GO.CLEARWELL.COM","ONCLOUD.CLEARWELL.COM"

esa.icp.ev.CustodianAssign.MultipleEmployeesAmbiguity.ResolveBy.PrimaryEmail=true

In this case, the "*mMoore@GO.CLEARWELL.COM*" is first searched in the *t_employee* table. As no employee is found, then "*mMoore@ONCLOUD.CLEARWELL.COM*" is searched. As a result, two employee records are found. If the primary email address is same, then the employee with the least *EmpId* is selected as a custodian. Else, *NONE* is assigned as a custodian.

Scenario 2:

When the properties are set as:

esa.icp.ev.CustodianAssign.SmtpTargetsAmbiguity.ResolveBy.PreferredDnsList="GO.CLEARWELL.COM","ONCLOUD.CLEARWELL.COM"

esa.icp.ev.CustodianAssign.MultipleEmployeesAmbiguity.ResolveBy.PrimaryEmail=false

In this case, the "*mMoore@GO.CLEARWELL.COM*" is first searched in the *t_employee* table. As no employee is found, then "*mMoore@ONCLOUD.CLEARWELL.COM*" is searched. As a result, two matching employee records are found. The employee with the least *EmpId* is directly selected as a custodian without checking for the primary email address. Here, if no matching records are found, then *NONE* is assigned as a custodian.

Scenario 3:

When the properties are set as:

esa.icp.ev.CustodianAssign.SmtpTargetsAmbiguity.ResolveBy.PreferredDnsList=""

esa.icp.ev.CustodianAssign.MultipleEmployeesAmbiguity.ResolveBy.PrimaryEmail=true

In this case, if all three records have the same primary email address, then the employee with the least *EmpId* is selected as a custodian. If the primary email addresses are not identical, then *NONE* is assigned as a custodian. The database is queried for DNS in an unordered manner. The first DNS name is used for searching the employee records. If no record is found, then the second DNS name is used, and so on. If no records are found, then *NONE* is assigned as a custodian.

Scenario 4:

When the properties are set as:

esa.icp.ev.CustodianAssign.SmtpTargetsAmbiguity.ResolveBy.PreferredDnsList=""

esa.icp.ev.CustodianAssign.MultipleEmployeesAmbiguity.ResolveBy.PrimaryEmail=false

In this case, then the first matching employee for the first matching email address is selected as a custodian.

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.

Troubleshooting the Microsoft 365 collections

Use the information in this section to troubleshoot issues related to Cloud Active Directory discovery or collection for Microsoft 365 Exchange and OneDrive sources.

Owner list is not populated while adding a new collection task

- Check if the Microsoft 365 Cloud Discovery is already performed.
- If Cloud Discovery is already performed, but still the owner list is not populated, then check with the Server type of your mailboxes and also verify your respective tables in the database.

Progress of collection set processing is displayed as zero percentage

Check if the *ESAPstcrawler* and *EsaNsfCrawlerService* services are running.

PST files are not created for Exchange collection

Check the log file at *esa-src\logs\icp-logs\icp-remoteicpjob@47024.log*. Check whether *CwEmlToPst.exe* is launched.

Check whether the below files exist or not.

- CwEmlToPst.exe
- CwEmlToPst.pdb
- CwEmlToPst.exe.config
- Interop.Redemption.dll
- log4net.dll
- log4net.xml
- Redemption.dll

If any of the above files do not exist, then the issue is related to the build.

If all of the above files exist, then check the *ErroredItems.csv* available at the destination you have specified and check the root cause for the issue.

Additionally, you can check the log file generated by *CwEmlToPst.exe* at *esa-src\logs\CwEmlToPst_output.log*.

Microsoft 365 collection task failed

1. Check the Job status log.
2. Check the server logs file (such as, *server.2020-09-16.txt*) available inside the *logs* folder.
3. Check the icp-logs for the collection task-related troubleshooting:
   - Find the string "Authority url used for authentication token is" in the log file. It will print the Connection URL used for the Graph API call and verify it is correct. If it is not correct, then set the correct connection URL using Property Browser.
   - If the log contains "InvalidAuthenticationToken" exception, this will be occurred due to invalid Connection URL and Source information added for Microsoft 365. Correct the connection URL and source information.
   - If the log contains “JsonProcessingException “ exception, search for *“Json Url*" in the log, which contains a JSON string. Verify that all filters contain correct entries and valid data.

Active Directory Sync for Microsoft 365 Cloud Discovery failed

1. Verify that the added tenant details, such as App ID, Client Secret, Tenant ID are correct.
2. Check the server logs file (such as, *server.2020-09-16.txt*) inside the "logs" folder, search for string "Authority URL used for authentication token is" in the log file. It shows the connection URL used for Graph API call. Verify that it is correct. If the connection URL is not correct, then set Connection URL using Property Browser.
3. Check whether All Permission are set for the App ID.

4. Analyze the *ADSCrawler_output.txt log* files if the error occurred during Sync.

Specify a connection URL to get an authentication token for O365 Discovery

If you are using multiple connection URLs, you need to specify a connection URL to get an authentication token for the Microsoft 365 discovery.

1. From the **System** view, click **Support Features**.
2. Select **Property Browser**.
3. Enter the property: **esa.o365.collection.authority.url**
   - Default value for this property is: **https://login.microsoftonline.com/**
   - For collection from GCC High, set the value to: **https://login.microsoftonline.us/**

   Note: In case the property value is set for collection from GCC High and you want to collect from GCC or public cloud, you must reset the property value to default.
4. Click **Submit**.

Microsoft 365 Collection Performance Tuning

Below listed properties can be used to improve the Microsoft 365 collection.

Microsoft 365 Properties for performance tuning

Scenarios	Property details
If the application throttling is frequent, then you can change it. In case of getting throttling issue (error code 429:too many requests), this value should be increased. To improve collection speed, this value can be decreased.	Property: ***esa.o365.collection.waitTime*** Default value: 100000 (in Milliseconds) **Note:** Do not change the value greater than 10 minutes.
	Property: ***esa.o365.collection.retries*** Default value: 3
By default, Exchange and OneDrive collection runs in sequential order. If you need the Exchange and OneDrive collection to run in parallel, you can change the default value. After changing the value to 2, the overall collection performance improves.	Property: ***esa.o365.collection.connectorInSequential*** Default value: 1 Allowed Values: [1,2] 1 = Exchange and OneDrive collection run in sequence 2 = Exchange and OneDrive collection run in parallel.

Microsoft 365 Properties for performance tuning

Scenarios	Property details
To improve the performance of EML to PST conversion.	Property: ***esa.icp.collection.o365graphcollection.emltopst.maxThreadsForEMLToMSG*** Default value: 8 Allowed value: Any Positive Integer Value **Note:** Better performance can be achieved if the value is set to 16; however, check your appliance configuration. Do not set the value to 0.
Enable or disable validation of a mailbox.	Property: ***esa.ad.discovery.validate_and_purge_stale_mailboxes*** Default value: true Allowed value: true or false If the value it set to true, then the following properties should be set: Property: ***esa.ad.discovery.validate.maxundiscovereddays*** Default value: 30 Allowed value: Positive Integer Property: ***esa.ad.discovery.disable_undiscovered_mailboxes*** Default value: true Allowed value: true or false Disable the mailbox not found in this AD sync (On-premise and cloud AD) if ***lastDiscoveredDate*** is older than the value of ***esa.ad.discovery.validate.maxundiscovereddays.***
Skip employee sync job of for On-premises AD sync and Cloud AD sync.	Property: ***esa.icp.employee.skipEmployeeSync*** Default value: false Allowed value: true or false
Set the maximum proxy address of the user to persist when an Employee is created.	Property: ***esa.employeemanager.max.emails*** Default value: 20 Allowed value: Positive Integer

Microsoft 365 Properties for performance tuning

Scenarios	Property details
In case of occurrence of application throttled issue.	Property: ***esa.o365.collection.recordsFetchSize*** Default value: 2000 Allowed value: Any Positive Integer It should be in the inclusive range from 500 to 2000. Setting value less than 500 decreases the collection speed, and setting the value above 2000 increases the throttling occurrence in the application during collection.
Though it is not recommended to change this property value, it can be changed only if Microsoft allows more Graph requests at a time.	Property: ***esa.o365.collection.usersInABatch*** Default value: 3 Allowed value: Any Positive Integer Value
Apply limit on the number of collection jobs processes to run at a time and This property will be used for the type manager execution throttle.	Property: ***esa.jobmanager.type.O365_COLL.executionThrottle*** Default value: 2 Allowed value: Any Positive Integer Value
Apply limit on the number of collection jobs processes to run at a time. This property will be used for the type manager node execution throttle.	Property: ***esa.jobmanager.type.O365_COLL.nodeExecutionThrottle*** Default value: 2 Allowed value: Any Positive Integer Value
When we stop the thread pool executor, this property value will make this number of attempts to terminate the thread pool.	Property: ***esa.o365.collection.conversion.exeTaskExecutor.stopRetryCount*** Default value: 3 Allowed value: Any Positive Integer Value
After a thread pool shutdown request, the system waits for 20 seconds by default till the thread pool terminates. Configure this wait time based on your requirements. When we stop the thread pool executor, this property value will make this number of attempts to terminate the thread pool.	Property: ***esa.o365.collection.conversion.exeTaskExecutor.shutDownAwaitTime*** Default value: 20 Allowed value: Any Positive Integer Value
Specify how many EML files can reside in a single folder.	Property: ***esa.o365.collection.conversion.folderInsideFileLimit*** Default value: 1000 Allowed value: Any Positive Integer Value
Configure the number of EML batch items after which a batch EML batch is created for PST. For example, if this property is set to 100, then after 100 items downloaded based on this property, one batch for those EMLs are created inside the database and that will be submitted for EML to PST conversion.	Property: ***esa.o365.collection.conversion.batchGuiDLimit*** Default value: 1000 Allowed value: Any Positive Integer Value

Microsoft 365 Properties for performance tuning

Scenarios	Property details
Specify the number of items that a single PST can hold.	Property: ***esa.o365.collection.conversion.maxFilesInsideSinglePST*** Default value: 50000 Allowed value: Any Positive Integer Value lesser than the default value.
Configure whether to delete the EMLs after they are injected inside a PST. If property value is true, then after PST conversion, EML files are deleted.	Property: ***esa.o365.collection.conversion.EMLToPSTEXE.deleteEmlLater*** Default value: true Allowed value: true OR false
Download EML files at a destination other than the default destination.	Property: ***esa.o365.collection.conversion.scratch.dir*** Default value: esa-src\\scratch\\temp\\o365collection\\ Allowed value: Any folder inside scratch folder
Specify the number of PSTs that can be created in parallel.	Property: ***esa.o365.collection.conversion.maxPstToProcessInParallel*** Default value: 5 Allowed value: Any Positive Integer Value
Specify the time interval in which the thread will look for downloaded batch of EML files inside the database.	Property: ***esa.o365.collection.conversion.recordFetchInterval*** Default value: 2 Allowed value: Any Positive Integer Value (in seconds)

Troubleshooting Microsoft Teams collections

Use the following pointers to troubleshoot issues related to the collection from Microsoft Teams sources.

- **Debug logs**: For more information about an issue, enable debug logs for the following packages.

  Login to eDiscovery web UI > **System** > **Logs** > **Setting** > **Add**.

  Set Log Level as "Debug" and Duration as "Permanent" for following module names.

  - **log4j.category.com.teneo.esa.icp.collection**
  - **log4j.category.com.teneo.esa.icp.collection.o365.teams.apis**
- **Errors**: Check for any error stack in server<date>.log, icp-logs, and jobs-related web UI logs.
- **Understanding log messages**: For any issue in the collection run, check for the following log messages in the latest log file under icp-logs folder. Ensure that you have debug logs enabled, as stated earlier.

  - **MS Teams Collection is starting now**: This indicates that the base work of the eDiscovery job is over and now, Teams collection execution will start.
  - **Trying Merge1 URL now**: This indicates various URLs that eDiscovery server fire on Merge1 server as Restful web request.
  - **JSON Body sends with URL request to Merge1**: While sending a restful web service request, some parameters are sent as request body. They are printed with this message.
  - **Successfully involved Merge1 URL**: This message indicates successfully invoked Merge1 restful web requests.
  - **JSON Response from Merge1 is**: This message indicates the return of the Merge1 server in response of the above request. This is useful, in case of any error at the Merge1 end.
  - **Failure while invoking API**: This message shows errors in case of any issue in execution of Merge1 requests.
  - **Merge1 job submitted successfully now. There won't be any further update here until the Merge1 job is over**: This is the last message from eDiscovery to Merge1. This indicates that everything went well and the Merge1 job is triggered.

- **Troubleshooting with tools like Postman**: Tools like postman can be used to troubleshot Merge1 web services. Capture exact request, with the body as stated above and try it with the postman. Use the same credential that are supplied in eDiscovery source creation.
- **Investigating Merge1 server**: If this message is seen, follow the steps:

  A. Go to Merge1 web UI https://localhost/Configuration/ and login.

  B. Navigate to IMPORTERS menu on left side.

  C. Check for the status of your Merge1 job that is triggered from eDiscovery.

  D. Check for the machine-generated name of your job in icp-logs after the message: "JSON Body send with URL request to Merge1--> {"InstanceName":"

- **Inspecting destination**: Check for new file being collected at: \\destinaion\0.27.6.3-20211019-143435-411\content\Teams\Merge1JSONs

Technical Support

To contact Veritas Technical Support, use any of the following methods:

- **MyVeritas Technical Support Portal**
  - *https://my.Veritas.com*

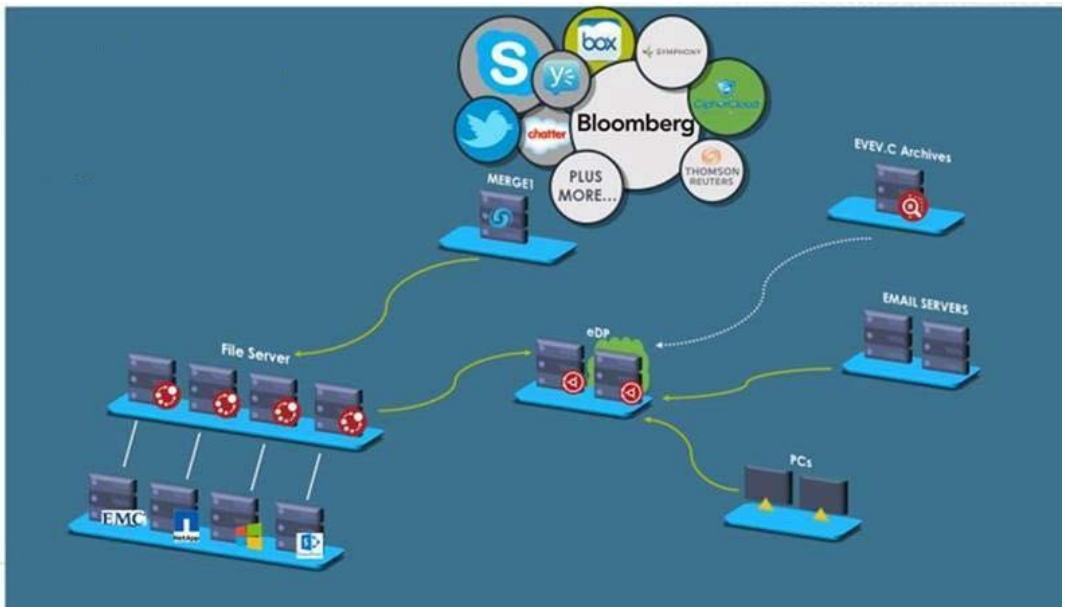
  Note: Access to the MyVeritas Technical Support Portal requires a SymAccount. If you do not already have on, register for a new SymAccount from the MyVeritas Technical Support Portal.
- **Phone** — Toll-Free (North America):
  - 1-800-342-0652
    For regional contact numbers: *http://www.Veritas.com/business/support/techsupp_contact_phone.jsp*

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 16*.

Appendix A: Using Merge1 with eDiscovery Platform

A standalone Merge1 needs to be installed separately from eDiscovery Platform. Once authentication credentials are provided to Merge1, a user needs to set up filters and collect the data onto a file share. Once the data is collected, an administrator can point eDiscovery Platform, processing to the file share location. Any data that is added to that folder can be automatically processed once added.

The following diagram shows the architecture of Merge1 and eDiscovery Platform.



Merge1 can collect data from more than 80 sources. For a complete list of the supported sources, see the article: https://www.veritas.com/insights/merge1

Appendix B: 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
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 10.x compared to 9.x, 8.x compared to 7.x and 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
Imaging Tool Upgrade Guide	Provides details about the Imaging Tool Upgrade feature and how to perform Imaging Tool Upgrade after the eDiscovery Platform appliance is upgraded to version 10.0, workflows affected when the cases are upgraded or not upgraded, and frequently asked questions (FAQs).
Export and Production Guide	Describes how to use and produce exports, productions, and logs (privilege and redaction logs)
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