Overview

This section includes the following topics:

Overview

Overview

These release notes describe updates related to installation, upgrades, and operational considerations, including resolved and known issues related to Veritas eDiscovery Platform software.

Detailed information on how to use the appliance and the new features can be found in the documentation for that particular feature or enhancement. Each manual has a guide to the documentation in the *Product Documentation* section.

Operational notes

This section includes the following topics:

What files to download

Please sign in and use the Veritas Support portal for downloading product software, licensing, and support: https://www.veritas.com/content/support/en_US.html

- For cumulative hotfix information and downloads, visit the eDiscovery Platform support site: https://www.veritas.com/content/support/en_US/article.100038329.html
- For information on how to obtain license key and installation download:https://www.veritas.com/support/en_US/article.000100418

A number of Veritas eDiscovery Platform installation files are available from the Veritas Support Portal Downloads area. Use the information below to help you choose the appropriate set of files to download for your license and deployment.

If you are upgrading to 9.1.1, use the following incremental installer (for the Master node and all nodes in the cluster, the Confirmation Server and the Utility Node):

- `Veritas_eDiscovery_Platform_v91_CHF1_Win_EN_Fix1.zip`

If you are upgrading from a previous version, run the full product installer.

- Full product installer

`Veritas_eDiscovery_Platform_Installer_9.1-Win-EN.zip`

- Legal Hold installer (only applicable if you are licensed for the Legal Hold module):

`Veritas_eDiscovery_Platform_ConfServer_Installer_9.1-Win-EN.zip`

- Utility Node installer (only applicable if you are licensed for the Review, Redaction and Production module

`Veritas_eDiscovery_Platform_UtilityNode_Installer_9.1-Win-EN.zip`

Install/upgrade instructions

Veritas eDiscovery Platform 9.1.1 supports the following upgrade path:

- Veritas eDiscovery Platform Release 9.1

If you are running above listed version, you must run the incremental installer to install 9.1.1 on the following:

- Master Node and all other nodes in the cluster
- Confirmation Server

  > “ ”

  Note: Note: If you are using a dedicated Confirmation Server, then you must run the 9.1.1 incremental installer on the Confirmation Server.

  > “ ”

- Utility node

eDiscovery Platform does not support release upgrades that extend past a previous version release (for example, you cannot perform a direct upgrade from 9.0 to 9.1.1). Instead, eDiscovery Platform requires intermediary upgrades to update the product to the latest version. In the case of 9.1.1, your system must be running 9.1 before running and applying the 9.1.1 incremental install.

IMPORTANT! You may need to restart your system after upgrading to 9.1.1, if prompted.

Distributed architecture deployment updates

If you are using a distributed architecture deployment, the 9.1.1 installation retains the product version as 9.1.1.0.

All nodes in a cluster must be upgraded to the same version; otherwise nodes will not be available.

To uppgrade the nodes

1. Stop all services on all nodes.
2. Install 9.1.1 on the Master node first.
3. Continue to install 9.1.1 on all other nodes in the cluster.

For more information about distributed architecture system requirements, refer to the Distributed Architecture Deployment Guide.

Product documentation

For more information on supported upgrade paths, refer to:

https://www.veritas.com/support/en_US/article.000095769

For more information on the supported operating systems and third-party applications, refer to:

https://www.veritas.com/support/en_US/article.000019811

9.1.1 and hotfixes product documentation:

https://www.veritas.com/support/en_US/article.100044239

9.1 Late Breaking News:

https://www.veritas.com/support/en_US/article.100043230

Need help?

Customer Support portal: https://www.veritas.com/support/en_US.html

Contact numbers: https://www.veritas.com/content/support/en_US/contact-us.html

> “ ”

Note: Access to some areas of the Support Portal may require a Veritas Account. If you do not already have one, register for a new Veritas Account from the Support Portal Licensing area.

> “ ”

New in Release 9.1.1

This section includes the following topics:

Ability to configure footer text in the Legal Hold settings

Legal Hold administrator - Edit the text and look of the text currently being inserted automatically for Legal Hold notices.

In previous releases, eDiscovery generated a complete Legal Hold message by combining the automated static message (like Hold Confirmation link text) and a configured text in message body by Legal Hold administrator.

Now, a Legal Lold administrator can edit the content and format the automated footer text which would be used within the body of different Legal Hold messages. A Legal Hold administrator can configure the footer text in the global settings or within a specific hold's settings. Changes made to a hold's settings supersedes the global settings.

Support for Enterprise Vault 12.4

Starting from eDiscovery Platform 9.1.1 release, Enterprise Vault 12.4 Server is certified as a collection source specifically including deployment scenarios where mailboxes were first created using on-premise Exchange Server and then were migrated to Office® 365.

This requires Enterprise Vault API 12.4 Runtime to be present on Veritas eDiscovery Platform Server.

See instructions below on how to obtain this API Runtime and perform the upgrade. This activity is required to be done on a Standalone eDiscovery Platform Server, Cluster Master and all Worker Nodes in Distributed Architecture environment.

Figure: Veritas eDiscovery Platform compatibility chart

Enterprise Vault Server Versions	Veritas eDiscovery Platform Versions							
	8.0	8.1	8.1.1	8.2	8.3	9.0	9.1	9.1.1
9.0	N	N	N	N	N	N	N	N
9. 1	N	N	N	N	N	N	N	N
9. 2	N	N	N	N	N	N	N	N
9. 3	N	N	N	N	N	N	N	N
9. 4	N	N	N	N	N	N	N	N
9. 5	N	N	N	N	N	N	N	N
10.0	Y	Y	N	N	N	N	N	N
10.1	Y	Y	N	N	N	N	N	N
10.2	Y	Y	N	N	N	N	N	N
10.3	Y	Y	N	N	N	N	N	N
10.4	Y	Y	Y	Y	Y	Y	Y	Y
11.0	Y	Y	Y	Y	Y	Y	Y	Y
11.1	N	N	Y	Y	Y	Y	Y	Y
12.0#	N	N	Y*	Y*	Y	Y	Y	Y
12.1	N	N	Y*	Y*	Y	Y	Y	Y
12.2	N	N	Y*	Y*	Y	Y	Y	Y
12.3	N	N	N	N	N	N	Y##	Y##
12.4	N	N	N	N	N	N	N	Y##

Legend:

EV 11.0 supports IMAP while EV 11.0.1 supports both IMAP and SMTP

*Veritas eDiscovery Platform 8.1.1 Cumulative Hotfix 2 (and later) and 8.2 Cumulative Hotfix 5 (and later) with Enterprise Vault 11.0.1 API Runtime are certified to work with Enterprise Vault 12.0 to 12.0 SP2.

Starting with 9.1.1, environments where mailboxes were first created using on-premises Exchange and then were migrated to Office® 365 must use Enterprise Vault 12.4 (or higher) API Runtime client

You need to manually upgrade the Enterprise Vault API Runtime client. Contact Veritas customer support for further assistance.

Note the following:

- If you are targeting Enterprise Vault 12.3 (or higher) as a collection source, you are required to upgrade to Enterprise Vault 12.4 API Runtime on the eDiscovery Platform Server.
- If you are targeting Enterprise Vault 12.2 (or lower) as a collection source, you can continue using Enterprise Vault 11.0.1 API Runtime already installed on the eDiscovery Platform Server.

How to install Enterprise Vault Runtime

A separate standalone installer for Enterprise Vault 12.4 API Runtime is available as part of the eDiscovery Platform 9.1.1.

To install Enterprise Vault Runtime using the standalone installer

1. Download the file `Veritas_eDiscovery_Platform_9.1.1.zip` from the eDiscovery Platform 9.1.1 Release Technote.
2. Extract the content. You will see a folder `Veritas_Enterprise_Vault_12.4_API_Runtime` containing the following files:
   - `Veritas Enterprise Vault 12.4 Runtime Installer.bat`
   - `Veritas Enterprise Vault 12.4 Runtime.exe`
   - ReadMeFirst
3. Read the `ReadMeFirst.txt` for the detailed installation instructions.
4. Run `Veritas Enterprise Vault 12.4 Runtime Installer.bat` to perform a silent installation of Enterprise Vault 12.4 API Runtime.
5. Perform these steps on all eDiscovery Platform appliances (Standalone, Cluster Master, Worker) in the environment.

Support for Java SE Development Kit 8, Update 201 (JDK 8u201)

Veritas eDiscovery Platform 9.1.1 is certified to work with Java SE Development Kit 8, Update 201 (JDK 8u201). After the eDiscovery Platform environment is upgraded to the 9.1.1 release, you need to update the Java SDK on the eDiscovery Platform server using the installer available as part of `Veritas_eDiscovery_Platform_9.1.1.zip`.

How to install Java SE Development Kit 8, Update 201 (JDK 8u201)

A separate standalone installer for Java SE Development Kit 8, Update 201 (JDK 8u201) is available as part of the eDiscovery Platform 9.1.1.

To install Java SE Development Kit 8, Update 201 (JDK 8u201) using the standalone installer

1. Download the file `Veritas_eDiscovery_Platform_9.1.1.zip` from the eDiscovery Platform 9.1.1 Release Technote.
2. Extract the content. You will see a folder `Java_SE_Development_Kit_8_Update_201(JDK 8u201)` containing the following files:
    - `JDKUpgrader.exe`
    - ReadMeFirst
3. Read the `ReadMeFirst.txt` for the detailed installation instructions.
4. Run `JDKUpgrader.exe` to install the Java_SE_Development_Kit_8_Update_201(JDK 8u201).
5. Perform these steps on all eDiscovery Platform appliances (Standalone, Cluster Master, Worker, Utility Node, Confirmation Server, Remote MySQL Database) in the environment.

Support for MySQL Server 5.6.43

After the eDiscovery Platform environment is upgraded to the 9.1.1 release, run the MySQL Upgrade installer to upgrade the MySQL to version 5.6.43 to meet the security needs. Perform the MySQL upgrade using the installer available as part of the `Veritas_eDiscovery_Platform_9.1.1.zip`.

How to install MySQL Server 5.6.43

To install MySQL Server 5.6.43

1. Download the file `Veritas_eDiscovery_Platform_9.1.1.zip` from the eDiscovery Platform 9.1.1 Release Technote.
2. Extract the content. You will see a folder `MySQL Server 5.6.43` containing the following files:
    - `o MySQLUpgrader.exe`
    - ReadMeFirst
3. Read the `ReadMeFirst.txt` for the detailed installation instructions.
4. Run `MySQLUpgrader.exe` to install MySQL Server 5.6.43.

5. Perform these steps on all eDiscovery Platform appliances (Standalone, Cluster Master, Worker, Utility Node, Legal Hold Confirmation Server, Remote MySQL Database) in the environment.

Support for password hardening

For security reasons, you must ensure that the passwords that are used by the end users are secure. This feature enables an eDiscovery administrator to harden the end user password. The passwords are checked against the password policies whenever a new system user gets added or password for existing user is changed.

The administrator can use the configuration properties to configure the following:

- The minimum password length.
- The number of numeric characters that the password must have.
- The number os special characters that the password must have.
- The number os uppercase characters that the password must have.
- Whether white spaces should be allowed in a password.

Administrator can set the following configuration properties to control the strength of the password.

PROPERTY NAME	TYPE	DEFAULT VALUE
esa.common.user.minPasswordLen	Integer	6
esa.common.user.minNumericCharCount	IntegerRequired	0
esa.common.user.minSpecialCharCount	IntegerRequired	0
esa.common.user.minUpperCaseCharCount	IntegerRequired	0
esa.common.user.noWhiteSpaceChar	BooleanAllowed	False

Inclusion of Access Groups is now configurable

In previous releases, by default, all the existing access groups were included at the time of creating a new case or user. Also, a user had no option to configure this default inclusion. This inclusion process is opposite to standard security practice of being least inclusive.

To overcome this problem, a new capability has been added in version 9.1.1 where the user can make the access group inclusion configurable using properties. These configurable properties can be set to true or false from support features depending on the customer needs.

From 9.1.1 onwards, the behavior of access groups' inclusion is as follows:

- By default, all the access groups are shown in INCLUDED section at the time of creating a new case or user.
- Access group inclusion has been made configurable by the new separate properties for cases and users. These properties can be added from the UI through System > Support Features > 'Property Browser page.
- For new cases, following property has been introduced that can be set as `true` or `false`:
  - `esa.new.case.all.access.groups.included` \- `true` signifies that all the access groups are in INCLUDED section; '`false` signifies that all the access groups are in 'AVAILABLE section.
- For new users, the following property has been introduced that can be set as `true` or `false`:
  - `esa.new.user.all.access.groups.included` \- `true` signifies that all the access groups are in INCLUDED section; '`false` signifies that all the access groups are in 'AVAILABLE section.

eDiscovery Platform logs enhanced to print information when license usage has reached beyond threshold limit

The enhancement implements a logging framework in `Server.Log` for the license capacity when a threshold value is reached (CFT-1732). The enhancement ensures that log messages for Processing, ICP, and Legal Hold are printed only when the threshold value is reached and it will log this information once per day. The default value of the license threshold is set to 70% and it is also configurable under the System > Support Features Property Browser tab.

- Property name - **`esa.common.license.threshold`**
- Default value - 70

Increased email body limit for Legal Hold Notices (CFT-1824)

The email body limit of Legal Hold notices is now enhanced from 14000 to 30000.

Additionally, the email body limit is also configurable via property which can be set in the System > Support Features > Property Browser tab.

- Property name - `esa.ui.legalHolds.noticeElementSizeMaximum`
- Default value - 30000 (the value can be between 1 and 65000)

Known issues

This section includes the following topics:

Known issues in 9.1.1

This section describes the known issues in Veritas eDiscovery Platform™ Release 9.1.1.

ESA-51548 - Footer text columns do not get created in 't_lithold_settings' table in database when V91 ICLH backup is restored on V911 appliance

When user restores any previous version of ICLH backup on V911, the following UI pages fail to load and the error message - *Unable to load hold settings details* is displayed.

- Global as well as Per Legal Hold Settings
- Details of Legal Hold Notices that are restored from ICLH backup

As a result, the user fails to create new Legal Holds or use existing legal hold notices to send reminders, escalation etc.

Workaround

Remote Desktop into the eDiscovery appliance and restart the Tomcat (*EsaApplicationService: FireDaemon*) service from Services panel.

ESA-51411 - Unable to remove the hyperlink from the footer text

The user is not able to remove the hyperlink from the footer text that is specified in Footer Text section. If user selects the already hyperlinked text and clicks the 'Hyperlink' button again, it does not remove the hyperlink.

Workaround

Delete the hyperlinked text, type the text again and then select text to insert the hyperlink.

Fixed issues

This section includes the following topics:

Fixed issues in Release 9.1.1

The following issues are fixed in Release 9.1.1:

Identification and collection

Table: Fixed issues in Identification and collection

ISSUE NUMBER	DESCRIPTION
CFT-1472	Forbidden error when a user creates an Enterprise Vault collection task.
	A Forbidden error was displayed when a user with a custom role creates an Enterprise Vault collection task. This issue is now fixed and users can create an Enterprise Vault collection task.
CFT-1569	Date filter in Enterprise Vault.Cloud collections allow incorrectly formatted dates to be entered manually.
	Invalid date formats are not recognized while creating Enterprise Vault.Cloud collection task causing incorrect results to be collected This issue is now fixed.
CFT-1653	Enterprise Vault Hold tasks showing mismatched search hit counts for items held counts.
	Retries of Enterprise Vault Hold Task wrongly increased Item Held counts on eDiscovery

ISSUE NUMBER	DESCRIPTION
	Platform UI (CFT-1604) : This fix resolves a problem of inaccurate statistics of Item Held count for Enterprise Vault Hold task during task retry situations.
CFT-1667	Incomplete ADSync disables valid Exchange mailbox display flag.
	Exchange Mailboxes are marked as disabled after an incomplete ADSync run. This fix resolves the way eDiscovery Platform deals with environment situations during the AD Sync process. The fix is multifold and solves different environmental problems observed in the field.
	- Retry on DirectoryServicesCOMException (0x800700EA) The solution will make 5 retry attempts after receiving this exception. Number of retries is configurable using the following property: Property name - lang=txt esa.adscrawler.searcher lang=txt .directoryserviceexception_maxretrycount Default value is 5.
	- Disable mailboxes only if it is not discovered in the current ADSync run and its last discovered date is older than a specific number of days. This solution resolves problems around transient errors received from Active Directory. A mailbox will be consider disabled during ADSync only when it is not discovered in the current ADSync and the last discovered date for the mailbox is older than a specific number of days (Default is 15 Days). Property name - esa.ad.discovery.validate.maxundiscovereddays Default value - 30 The functionality of disabling mailboxes during validation is configurable using the following property. • • Property name -

ISSUE NUMBER	DESCRIPTION
	esa.ad.discovery.disable_undiscovered_mailboxes Default value - true
	- Enable the discovered mailbox again if it is found to be disabled in eDiscovery Platform. This enhancement will ensure that existing disabled mailbox records in eDiscovery Platform database will be re-enabled as part to ADSync run if eDiscovery Platform receives this information from Active Directory.
CFT-1679	No record of who deleted a (non EV-hold) collection task.
	For Enterprise Vault Collection task and Search tasks, logs do not mention the user who deleted them. This fix resolves the problem and enhances logging with by storing details of user who deleted Enterprise Vault Collection and Search tasks.
CFT-1739	Enterprise Vault collection ends in a false SUCCESS when an Index Server fails.
	Enterprise Vault collection task falsely end with Success state when one or more Enterprise Vault Index Server fails to respond in the stipulated time (CFT-1585). This fix resolves the problem and ensures that the Enterprise Vault collection task shows the correct job status at the end of the run.
CFT-1786	Enterprise Vault collections threads causes Enterprise Vault to go down.
	Multiple collection requests to the Enterprise Vault Server causes services to go down. The fix introduces a control mechanism to ensure that Enterprise Vault collection tasks raised by eDiscovery Platform are not overloading

ISSUE NUMBER	DESCRIPTION
	Enterprise Vault services and allow them to function smoothly.
CFT-1795	Collections from Enterprise Vault.Cloud fail with error EVcloud export failed for exportURL due to null after Enterprise Vault.Cloud update.
	Enterprise Vault.Cloud collections tasks fail while collecting data from Enterprise Vault.Cloud environment. This fix resolves the integration related issue between eDiscovery Platform and EV.Cloud. With the fix eDiscovery Platform should be able to collect to Enterprise Vault.Cloud mailboxes and download messages which match the ilter criteria of the collection task.

Infrastructure

Table: Fixed issues in Infrastructure

ISSUE NUMBER	DESCRIPTION
CFT-1706	Node backup is failing with due to Perl version difference.
	eDiscovery Platform appliance backup fails to initialize on the specific schedule. This fix resolves a problem while appliance backup was not initialized on the scheduled time.

Processing

Table: Fixed issues in Processing

ISSUE NUMBER	DESCRIPTION
CFT-1518	The From field has multiple sender email addresses. The source is NSF file.

ISSUE NUMBER	DESCRIPTION
	NSF file that has multiple mail addresses in the Sender field is not correctly processed. The fix has resolved the issue where the processing engine incorrectly strips our email addresses stamped on each message coming from the NSF file of Lotus Domino.
CFT-1535	EMLs with embedded images never index
	EML messages with embedded images cause the Indexer to crash. This fix resolved an issue where the indexer was crashing because of EML messages with embedded images.
	As a workaround, you can truncate the message body to process EML messages successfully by changing the value of the esa.crawler.eml.droplargebodyeml property to false. As a result, EML messages will not be dropped even if the body size is greater than the defined value. You can define the body size for the truncated messages by reducing the value of PROPERTY_ESA_EML_MSG_BODY_SIZE property. The default value is 1024000 bytes.
CFT-1599	All entries in BCC fields are not index due to too many listed.
	Emails with multiple Bcc fields in message header are not getting indexed correctly (CFT-1486).This fix resolves dataset specific issue where items with multiple Bcc fields in message header were not getting indexed in its entirety. This change ensures that all the recipient values are indexed and searchable in eDiscovery Platform.

Search

Table: Fixed issues in Search

ISSUE NUMBER	DESCRIPTION
CFT-1699	Custom field Advanced Search fails until the first eDiscovery Platform restart (or first case of backup and restore).
	Advanced Search using the Custom Fields section fails to find responsive documents until the eDiscovery Platform services are restarted or until the case is backed-up and then restored. This fix resolves a problem where advanced search using the Custom Fields section fails to find responsive documents.

Export

Table: Fixed issues in Export

ISSUE NUMBER	DESCRIPTION
CFT-1264	When generating the Production Export Slipsheet, the `IGC TargetFile` path to be greater than 255 characters when you select Create downloadable (zip) file .

System Administration

Table: Fixed issues in System Administration

ISSUE NUMBER	DESCRIPTION
CFT-1497	`ADSCrawler_Output` log file is filled with unclear and confusing log messages when Exchnage Server 2013 or 2016 is present in the environment.
	This issue is now fixed.

Review

Table: Fixed issues in Review

ISSUE NUMBER	DESCRIPTION
CFT-1635	Retrieval of EML files failing with error: \ [#41047\] Unable to retrieve email content: Retrieval timed out.
	Reviewing specific EML files results in an error "\[#41047\] Unable to retrieve email content: Retrieval timed out" (CFT-1383).
	This issue is now fixed.