



The latest version of this document is available from the Veritas Support website at <https://www.veritas.com/docs/100041266>.

For the latest news about this release, including any hotfixes, subscribe to <https://www.veritas.com/docs/100041268>.

This document describes the new features in Veritas Enterprise Vault 12.3.

If you are performing a new installation of Enterprise Vault, follow the installation instructions in the Enterprise Vault *Installing and Configuring* guide. If you are upgrading, follow the instructions in *Upgrade Instructions*. These guides are in the `Veritas Enterprise Vault\Documentation\English\Administration Guides` folder on the Enterprise Vault media.

Contents

- **New features in Enterprise Vault 12.3**

- [General data protection enhancements](#)
- [Classification-defined storage to "smart" partitions](#)
- [Updated version of the Veritas Information Classifier](#)
- [Enterprise Vault Search enhancements](#)
- [Enhancements to SMTP archiving](#)
- [Enhancements to storage expiry](#)
- [Enhancements to the retention folders feature](#)
- [Enterprise Vault web applications are secured by default](#)
- [Auditing enhancements](#)
- [New options for managing OCR conversion of embedded images](#)
- [Migrating Enterprise Vault data using the AWS C2S storage migrator](#)
- [Support for new Microsoft releases](#)

- **Changes in Enterprise Vault 12.3**

- [Changes to prerequisite software for Enterprise Vault 12.3](#)
- [Support for Outlook 2016 on the Enterprise Vault server](#)

- [New and enhanced PowerShell cmdlets](#)
 - [Silently installing Enterprise Vault from the command line](#)
 - [Changes to Enterprise Vault registry values](#)
 - [Weak protocols and ciphers are blocked for HTTPS communications](#)
 - [Oracle Outside In Technology content converters updated](#)
 - [Known issues and limitations](#)
 - [Documentation](#)
-

New features in Enterprise Vault 12.3

Enterprise Vault 12.3 includes the following new features. For information about the new features in earlier releases, see the release notes for [Enterprise Vault 12](#), [Enterprise Vault 12.1](#), and [Enterprise Vault 12.2](#).

General data protection enhancements

This release includes the following enhancements to help you comply with data protection legislation, such as the "right to be forgotten":

- In Discovery Accelerator, certain privileged users can now delete items permanently from Enterprise Vault archives.
- Third-party applications with suitable access permissions can now delete archived items programmatically.
- Enhanced auditing and reporting capabilities now show when items have been deleted for compliance reasons.

Classification-defined storage to "smart" partitions

Earlier versions of Enterprise Vault archived all items to a single, open vault store partition on a storage device. Enterprise Vault 12.3 removes this limitation by letting you archive different items to different partitions, depending on how the Enterprise Vault classification feature has tagged the items. For example, if you have configured the classification engine to detect and tag items that contain personally identifiable information (PII), you can choose to archive these items to one partition. Other types of items, such as bids and business proposals, can be archived to a different partition.

These new types of partitions are called *smart* partitions. They are identical to standard vault store partitions except in the following ways:

- Using the Vault Administration Console, you can associate a smart partition with one or more classification tags that you have defined in your chosen classification engine (Veritas Information Classifier or Microsoft File Classification Infrastructure). Only items to which the classification engine has assigned the chosen tags are archived to the smart partition.

- Multiple smart partitions can be open for archiving at the same time. This is not true of standard vault store partitions, which are limited to one open partition for each vault store.

Note: If you normally use the NetBackup Agent for Enterprise Vault to perform backups of your data, see [below](#) for a known issue in how it handles multiple open partitions in the same vault store.

- You can configure a standard vault store partition so that Enterprise Vault automatically rolls over to the next available partition when certain criteria are met. This rollover capability is not available for smart partitions.

As with standard vault store partitions, you can create smart partitions on any storage device that Enterprise Vault supports.

For more information on smart partitions, see the *Installing and Configuring* guide.

Updated version of the Veritas Information Classifier

Enterprise Vault 12.3 comes with an updated version of the Veritas Information Classifier engine, with which you can assign classification tags to all new and existing archived content. This new version first appeared in the Enterprise Vault 12.2.2 release update, and it provides the following additional features:

- **Document similarity.** Locate documents that are similar to a template that you supply. For example, you can find completed forms by using a blank form as a template.
- **Import/export feature.** Move policies, patterns, and tags by exporting them from one environment and importing them in another. Share with other Veritas applications that use the Information Classifier.
- **New Personally Identifiable Information policies.** New personal data policies are available to help you comply with regulations in Belgium, Denmark, the Netherlands, Norway, and Sweden.
- **Language detection.** Detect the primary language of an item, find documents containing multiple languages, and restrict policy matching to documents in a particular language.
- **Analyze.** You can now classify a folder of documents to test new or existing policies. Watch real-time statistics as policy matches occur, and then download a PDF report when the scan has completed.

For more information on these features, see the online Help for the Veritas Information Classifier.

Enterprise Vault Search enhancements

This release adds the following features and enhancements to Enterprise Vault Search:

- **Hit highlight navigation.** You can find specific instances of search terms in a selected item in the reading pane using the hit highlighting navigation bar.
- **Enhanced simple search suggestions.** The simple search suggestions feature now provides additional criteria that help you refine your search.
- **Live simple search.** If you select a search suggestion when using simple search, Enterprise Vault Search updates the search results.
- **Advanced search suggestions.** Search suggestions are now available with advanced search as well as simple

search.

- **Advanced search size ranges.** You can now select size ranges in an advanced search.
- **Option to restore items from journal archives to other users' mailboxes.** If you have full access rights to other users' Exchange mailboxes, you can now restore items from Enterprise Vault journal archives to the **Restored Items** folders in these mailboxes.

Enhancements to SMTP archiving

This release adds the following features and enhancements to SMTP archiving:

- **SMTP Provisioning groups.** Enterprise Vault 12.3 now supports SMTP provisioning groups. This is now the recommended way to configure targets for SMTP Mailbox Journaling and SMTP Group Journaling (formerly known as Selective SMTP Journaling). You can choose an Active Directory user group, and then provision all the users in the group for SMTP archiving at the same time. When processing an SMTP Mailbox Journaling provisioning group, Enterprise Vault automatically creates an Internet Mail archive for each user in the group, or links a user's existing Internet Mail archive.
- **Adding multiple archives and specifying type of journaling.** You can now assign multiple archives to targets for SMTP Journaling and SMTP Group Journaling. Enterprise Vault automatically maintains the consistency of the retention settings across the archives assigned to a target address or group. If the archives for a target are spread across Enterprise Vault storage servers, Enterprise Vault also performs archiving load-balancing across the servers.
- **Manual targets.** In the Administration Console, you now add routing addresses under **Targets > SMTP > Manual targets**. You select the type of journaling when you add a manual target. Although you can also add manual targets for SMTP Mailbox and Group Journaling, we recommend that you use provisioning groups to configure targets for these types of journaling.

Existing targets that you added in the previous release of Enterprise Vault are listed under **Manual targets**. During the upgrade to Enterprise 12.3, the journaling type of existing targets is determined based on the archive type. For more information, see the *Upgrade Instructions*.

- **Improved journal report processing.** To improve the performance of SMTP archiving when processing journal reports, Enterprise Vault 12.3 includes a new advanced SMTP policy setting called **Process journal reports for journal archives only**. This new value is now the default value for journal report processing. For more information, see the *Upgrade Instructions*.

For more information, see the *Setting up SMTP Archiving* guide.

Enhancements to storage expiry

Enterprise Vault 12.3 includes the following enhancements to storage expiry:

- Improved performance when deleting items during storage expiry processing.
- Consistent implementation of storage expiry across NTFS and Centera partitions.

The following new advanced settings for customizing storage expiry processing for individual Enterprise Vault storage servers:

- **Maximum vault stores for concurrent storage expiry processing**
- **Number of threads per vault store for storage expiry processing**

In the Enterprise Vault Administration Console, these settings are in the properties for the Enterprise Vault storage server. In **Computer properties**, click the **Advanced** tab, and list the settings for **Storage** to view the new settings.

Enhancements to the retention folders feature

Enterprise Vault 12.2 introduced a feature with which you can create one or more *retention folders* in your users' Exchange mailbox archives. With Enterprise Vault 12.3, you can now create retention folders in Internet Mail archives as well.

In addition, when defining the properties of retention folders, you can now supply alternative names for them in multiple languages. For example, suppose that some users in your organization employ English and others employ French. You can now supply one folder name to suit the English users and an alternative name to suit the French users. This feature overcomes a limitation in earlier versions of Enterprise Vault: the need to create multiple, language-specific retention plans in order to supply retention folder names in different languages.

For more information on retention folders, see the *Administrator's Guide*.

Enterprise Vault web applications are secured by default

In new installations of Enterprise Vault 12.3, connections to Enterprise Vault web applications require HTTPS with Secure Sockets Layer (SSL) by default.

Enterprise Vault web applications are configured in the Default Web Site in IIS. When configuring a new installation, the Enterprise Vault configuration wizard creates and installs a self-signed certificate. The configuration wizard adds to the Default Web Site an HTTPS binding on port 443, if this binding does not already exist, and enables SSL on all Enterprise Vault virtual directories.

Note: The self-signed certificate uses the SHA512 hashing algorithm. Some versions of Windows disable this algorithm on computers where the TLS 1.2 protocol is used. See the following Microsoft article for instructions on how to enable SHA512 for TLS 1.2, so that you can use the self-signed certificate:

<http://support.microsoft.com/kb/2973337>

We strongly recommend that you replace the self-signed certificate as soon as possible with a certificate obtained from a trusted authority. For more information, see "Default security for the Enterprise Vault Web Access components" in the *Installing and Configuring* guide.

If you are upgrading from an earlier version of Enterprise Vault, the existing configuration of Enterprise Vault web applications in IIS remains unchanged. To ensure the security of these web applications, we recommend that you manually configure HTTPS with SSL on all the Enterprise Vault virtual directories. For instructions on how to do this, see

"Securing Enterprise Vault web applications" in the *Upgrade Instructions*.

Auditing enhancements

Auditing of administrative activity (**Admin Activity** auditing category) has been enhanced. In particular, the quality of information relating to administrative activity in the following areas is significantly improved:

- Exchange, SMTP, and Search policies
- Exchange and SMTP tasks
- Exchange and SMTP targets
- Exchange Message Classes
- Archives

Improvements have also been made to the auditing of roles-based administration, vault store and partition administration, and advanced settings.

For more information, see the new *Auditing* guide.

New options for managing OCR conversion of embedded images

The following new Content Conversion site settings give you greater control over how Enterprise Vault applies Optical Character Recognition (OCR) content conversion to embedded images:

- **File types for OCR conversion of embedded images.** This setting lets you limit OCR conversion to selected file types.
- **OCR conversion of scanned pages.** This setting lets you control whether to apply OCR conversion to scanned pages in PDF documents.

The Content Conversion site settings are described in the *Administrator's Guide*.

Migrating Enterprise Vault data using the AWS C2S storage migrator

Enterprise Vault now supports the migration of archived data to Amazon Web Services (AWS) Commercial Cloud Services (C2S) storage using the AWS C2S storage migrator.

The AWS C2S migrator plug-in is installed as part of the Enterprise Vault 12.3 installation. For more information, see [Migrating Enterprise Vault Data Using the AWS C2S Storage Migrator](#).

Support for new Microsoft releases

Enterprise Vault 12.3 includes support for the following Microsoft releases:

- Windows Server 2016

Enterprise Vault classification using Microsoft File Classification Infrastructure is not supported on Windows

Server 2016.

- SQL Server 2017



Changes in Enterprise Vault 12.3

Changes to prerequisite software for Enterprise Vault 12.3

There are no changes to prerequisite software since Enterprise Vault 12.

The Enterprise Vault installer requires Microsoft .NET Framework 4.5.2, and all Enterprise Vault servers require both Microsoft .NET Framework 4.5.2 and .NET Framework 3.5 SP1.

For full details of all supported versions of software and devices, see the Enterprise Vault [Compatibility Charts](#). Appendix A provides details of the versions of software that have been dropped since Enterprise Vault 11.0.

Support for Outlook 2016 on the Enterprise Vault server

Archiving from Exchange public folders is now supported with Outlook 2016 on the Enterprise Vault server.

Testing has shown that performance of public folder archiving is affected if Outlook 2016 is installed on the Enterprise Vault server. If you are already using Outlook 2013, we recommend that you continue to use it on the Enterprise Vault server.

If you choose to install Outlook 2016, you may need to configure legacy (Exchange 2010 or earlier) public folders so that users whose mailboxes are on Exchange Server 2013/2016 can access them. See the following Microsoft article for instructions:

[https://technet.microsoft.com/en-us/library/dn690134\(v=exchg.150\).aspx](https://technet.microsoft.com/en-us/library/dn690134(v=exchg.150).aspx)

Note the following:

- Enterprise Vault supports Outlook 2016 (32-bit version). Enterprise Vault supports the Windows Installer (.msi) package, which is available with the volume license.
- The following versions of Outlook 2016 are not supported:
 - Outlook 2016 (64-bit version)
 - Outlook 2016 (Click-to-Run version)
- Connections to Exchange 2010 with Outlook 2016 are not supported. If you want to use Exchange 2010, you must use Outlook 2013.
- Outlook 2016 supports Exchange 2013 and 2016 connections, but only using MAPI over HTTP.
- Outlook Anywhere and RPC are not supported connection methods.

New and enhanced PowerShell cmdlets

In earlier versions of Enterprise Vault, you needed to import certain modules to use PowerShell cmdlets that the Enterprise Vault Management Shell did not automatically load. For example, you needed to import the module `Symantec.EnterpriseVault.PowerShell.Monitoring.dll` to make available cmdlets like `Get-EVServiceState` and `Get-EVTaskState`. This is not the case in Enterprise Vault 12.3, where all the Enterprise Vault PowerShell cmdlets are immediately available in the Management Shell.

Enterprise Vault 12.3 includes the following new PowerShell cmdlets:

Cmdlet	Description
<code>Remove-EVArchive</code>	Deletes the specified archive and the items that it contains.

Enterprise Vault 12.3 includes the following changes to existing PowerShell cmdlets:

Cmdlet	Change
<code>Get-EVFSFolder</code>	Can now retrieve details of all folders, including retention folders.
<code>Get-EVRetentionPlan</code>	In cases where you have used the specified retention plan to supply alternative names of retention folders in multiple languages, now returns information about these alternative names.
<code>Get-EVSMTPTarget</code>	Now returns in tabular format the details of the archives that are associated with the target.
<code>New-EVRetentionPlan</code>	For the retention folders that you have associated with a new retention plan, now lets you supply alternative names of the folders in multiple languages.
<code>New-EVSMTPTarget</code>	Can now associate multiple archives with SMTP Journaling and SMTP Group Journaling targets, and set the target type. For targets that are associated with other archives, updates the retention plan of all affected archives.
<code>Set-EVArchive</code>	For archives that are associated with one or more targets that are associated with other archives, updates the retention plan of all affected archives.
<code>Set-EVFSFolder</code>	Can now disable archiving on retention folders and sub-folders.
<code>Set-EVRetentionPlan</code>	For the retention folders that you have associated with an existing retention plan, now lets you supply alternative names of the folders in multiple languages.
<code>Set-EVSMTPTarget</code>	Can now associate multiple archives with SMTP Journaling and SMTP Group Journaling targets. For targets that are associated with other archives, updates the retention plan of all affected archives. Can also use the output of <code>Get-EVSMTPTarget</code> to update the list of archives and archive types.

Start-EVDatabaseUpgrade

Now has multiple timeout parameters with which you can adjust the time that the cmdlet allows for executing SQL Server commands and scripts.

See the *PowerShell Cmdlets* guide for more information on these cmdlets.

Silently installing Enterprise Vault from the command line

The command-line syntax for silently installing Enterprise Vault has changed. You must now include two new parameters, `/wait` and `/clone_wait`. The syntax is as follows:

```
start /wait "" "setup (x64).exe" /s /clone_wait /v"COMPONENTS=Option[|Option][...]"
```

For more information, see the "Installing Enterprise Vault (command line)" section in the *Installing and Configuring* guide.

Changes to Enterprise Vault registry values

The following Enterprise Vault registry value has been withdrawn:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KVS\Enterprise Vault\Storage\EMCCenteraExpiryThreads

The registry value is not removed on upgrade, but it is now ignored.

In this release, there are new storage expiry settings that you can configure for a storage server using the Enterprise Vault Administration Console. These settings apply to all storage devices. See [Enhancements to storage expiry](#).

Weak protocols and ciphers are blocked for HTTPS communications

In a new installation of Enterprise Vault 12.3, or an upgrade to Enterprise Vault 12.3, the Enterprise Vault installer now disables weak protocols and ciphers for all applications that require HTTPS communications.

Weak protocols

Enterprise Vault disables the following protocols, if you have not enabled them manually:

- SSL 2.0
- SSL 3.0

Weak protocols are managed using registry values under the following subkey:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols

If you have manually enabled the weak protocols listed above, registry values will exist under the **Protocols** subkey. Enterprise Vault does not disable a protocol that you have enabled in this way.

You can also manually disable the TLS 1.0 protocol, but this may prevent some Enterprise Vault functionality from

working properly. The following article describes how to disable TLS 1.0 and explains the consequences of doing so:

<https://www.veritas.com/docs/100041638>

Weak cyphers

Enterprise Vault disables the following ciphers:

- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

Ciphers are managed using the registry value called **functions** under the following key:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Cryptography\Configuration\SSL\00010002

Enterprise Vault disables all the weak ciphers listed above, even if you have enabled any of them using the **functions** registry value.

Oracle Outside In Technology content converters updated

This release includes the following patch for Oracle Outside In Technology content converters:

- Oracle Outside In SDK Library Patch for 8.5.3 (Release date: 15 November, 2017)



Known issues and limitations

Classification using Microsoft File Classification Infrastructure on Windows Server 2016 [3909224]

Classification using the Microsoft File Classification Infrastructure is not supported on Windows Server 2016.

NetBackup Agent for Enterprise Vault cannot back up data from multiple open partitions in the same vault store [3928569]

With the introduction of [smart partitions](#) in Enterprise Vault 12.3, vault stores can now contain multiple, open vault store partitions. Previously, each vault store could contain just one open partition.

The NetBackup Agent for Enterprise Vault does not currently support this enhanced functionality. Instead of backing up the data from every open partition in a vault store, the agent backs up the data from the most recently opened partition only. The other partitions are not backed up and marked as secured.

This issue will be fixed in a future version of the NetBackup Agent. If you normally use the agent to perform backups of your Enterprise Vault data, see the *Backup and Recovery* guide for alternative methods to back up the data.

Policy Manager scripts fail if you specify the name of the system mailbox [3941033]

To use the Enterprise Vault Policy Manager, you must specify the SMTP address of the Enterprise Vault system mailbox, irrespective of the version of Outlook that is installed on the Enterprise Vault server. The script fails to run if you specify the name of the system mailbox.

Files not deleted on placeholder deletion on NetApp 9.2 devices [3941424]

On NetApp 9.2 devices, archived files are not deleted when the placeholders are deleted.

Any change that you have made to the site-level port setting is discarded after you upgrade to Enterprise Vault 12.3 [3943567]

In Enterprise Vault 12.2 and earlier, the default ports for client connections to Enterprise Vault Search are HTTP over TCP port 80 and HTTPS over TCP port 443. However, you can choose an alternative port when you edit the properties of your Enterprise Vault site with the Vault Administration Console.

After you upgrade to Enterprise Vault 12.3, any change that you have made to the site-level port setting is discarded. As a result, some Enterprise Vault Search, OWA and the Office Mail app functions do not work.

To resolve this issue, follow these steps after you have upgraded to Enterprise Vault 12.3:

1. On the Enterprise Vault server, browse to the folder that contains the **Web.config** file for the affected feature. For Enterprise Vault Search, the **Web.config** file is in the **EVSearch\EVSearchClient** subfolder of the Enterprise Vault installation folder; for example, **C:\Program Files (x86)\Enterprise Vault\EVSearch\EVSearchClient**.
2. Open the **Web.config** file in a plain-text editor such as Windows Notepad.
3. In every **<endpoint>** entry, change the target address so that it includes the required port number.

For example, if you set the default port to 8080 then you might change the first **<endpoint>** entry to the following:

```
<endpoint name="normal"  
address="http://localhost:8080/EnterpriseVault/Search/ClientDataService.svc" ...
```

4. Save and close the file.



Documentation

The Enterprise Vault media includes the Enterprise Vault documentation in all supported languages.

The Enterprise Vault documentation is available in PDF and HTML format in the Veritas [Documentation Library](#).

Administration documentation

The Enterprise Vault administration documentation is available in English, Japanese, and Simplified Chinese from the following locations:

- **Veritas Enterprise Vault\Documentation** folder on the Enterprise Vault media
- Administration Console (click **Help > Help on Enterprise Vault**)

Document	Comments
Enterprise Vault Documentation Library	<p>Includes all the following documents in Windows Help (.chm) format so that you can search across them all. It also includes links to the guides in Acrobat (.pdf) format.</p> <p>You can access the library in several ways, including the following:</p> <ul style="list-style-type: none">• In Windows Explorer, browse to the Documentation\language\Administration Guides subfolder of the Enterprise Vault installation folder, and then open the EV_Help.chm file.• On the Help menu in the Administration Console, click Help on Enterprise Vault.
Introduction and Planning	Provides an overview of Enterprise Vault functionality.
Deployment Scanner	Describes how to check the required software and settings before you install Enterprise Vault.
Installing and Configuring	Provides detailed information on setting up Enterprise Vault.
Upgrade Instructions	Describes how to upgrade an existing Enterprise Vault installation to the latest version.
Setting up Domino Server Archiving	Describes how to archive items from Domino mail files and journal databases.
Setting up Exchange Server Archiving	Describes how to archive items from Microsoft Exchange user mailboxes, journal mailboxes, and public folders.
Setting up File System Archiving	Describes how to archive files that are held on network file servers.
Setting up IMAP	Describes how to configure IMAP client access to Exchange archives and Internet Mail archives.
Setting up SharePoint Server Archiving	Describes how to archive documents from Microsoft SharePoint servers.
Setting up Skype for Business Archiving	Describes how to archive Skype for Business sessions.
Setting up SMTP Archiving	Describes how to archive SMTP messages from other messaging servers.
Classification using the Microsoft File Classification Infrastructure	Describes how to use the classification engine that is built into recent Windows Server editions to classify all new and existing archived content.
Classification using the Veritas Information	Describes how to use the Veritas Information Classifier to evaluate all new and archived content against a comprehensive set of industry-standard classification policies.

Classifier	If you are new to classification with Enterprise Vault, we recommend that you use the Veritas Information Classifier rather than the older and less intuitive File Classification Infrastructure engine.
Administrator's Guide	Describes how to perform day-to-day administration procedures.
PowerShell Cmdlets	Describes how to perform various administrative tasks by running the Enterprise Vault PowerShell cmdlets.
Auditing	Describes how to collect auditing information for events on Enterprise Vault servers.
Backup and Recovery	Describes how to implement an effective backup strategy to prevent data loss, and how to provide a means for recovery in the event of a system failure.
Reporting	Describes how to implement Enterprise Vault Reporting, which provides reports on the status of Enterprise Vault servers, archives, and archived items. If you configure FSA Reporting, additional reports are available for file servers and their volumes.
NSF Migration	Describes how to import content from Domino and Notes NSF files into Enterprise Vault archives.
PST Migration	Describes how to migrate content from Outlook PST files into Enterprise Vault archives.
Utilities	Describes Enterprise Vault tools and utilities.
Registry Values	A reference document that lists the registry values with which you can modify many aspects of Enterprise Vault behavior.
Help for Administration Console	The online Help for the Enterprise Vault Administration Console.

Guides for end users

The following guides for end users are provided in .PDF format on the Enterprise Vault media, in the folder **Veritas Enterprise Vault\Documentation\Language\Client User Guides**:

- *Enterprise Vault Search Mobile edition: Quick Reference*
- *Guide for Notes Users*
- *Guide for Mac OS X Users*
- *Guide for Outlook Users*



Legal notice

Copyright © 2018 Veritas Technologies LLC. All rights reserved.

Veritas, the Veritas Logo, Enterprise Vault, Compliance Accelerator, and Discovery Accelerator 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 document

accompanying this Veritas product or available 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
500 E Middlefield Road
Mountain View, CA 94043

<https://www.veritas.com>