VERITAS

Veritas Enterprise Vault™ 12 and FIPS 140-2

About this document

Read this document if you want to know about using Enterprise Vault in an environment that complies with the FIPS 140-2 standard. This document describes:

- What the FIPS 140-2 standard specifies.
- What we mean by a “FIPS 140-2-compliant” version of Enterprise Vault.
- How Enterprise Vault achieves FIPS 140-2 compliance.
- Which versions and components of Enterprise Vault are compliant.
- Points to note when using Enterprise Vault in a FIPS 140-2-compliant environment.

About FIPS 140-2

The Federal Information Processing Standards (FIPS) define U.S. and Canadian Government security and interoperability requirements for computer systems. The FIPS 140-2 standard specifies the security requirements for cryptographic modules. It describes the approved security functions for symmetric and asymmetric key encryption, message authentication, and hashing.

For more information on the FIPS 140-2 standard and its validation program, see the National Institute of Standards and Technology (NIST) and the Communications Security Establishment Canada (CSEC) Cryptographic Module Validation Program website at http://csrc.nist.gov/groups/STM/cmvp.

What does “FIPS 140-2 compliant” mean?

Where the Enterprise Vault documentation states that a version of Enterprise Vault is “FIPS 140-2-compliant”, it means the following:

- Enterprise Vault uses FIPS 140-2-validated instances of algorithms and hashing functions in all instances where data is encrypted or hashed.
- Enterprise Vault manages cryptographic keys and message authentication in a secure manner, as required of FIPS 140-2-validated cryptographic modules.

How Enterprise Vault achieves FIPS 140-2 compliance

To achieve FIPS 140-2 compliance, Enterprise Vault uses a FIPS 140-2-validated cryptographic module to provide the required cryptographic functionality. The Veritas Enterprise Vault Cryptographic Module handles the encryption and decryption of passwords, the hashing of data, and random number generation.

The certificate numbers for the cryptographic modules that are used within the Veritas Enterprise Vault Cryptographic Module are **1012**, **1337**, and **1894** on the list of validated FIPS 140-2 modules that the NIST publishes. See the following:

- http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2008.htm#1012
- http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2010.htm#1337
- http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2013.htm#1894

About the cryptographic boundary

The cryptographic boundary of the Veritas Enterprise Vault Cryptographic Module is described in the module's *Security Policy* document. This document is available from the NIST website at the following address:

http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2012.htm#1732

Where an Enterprise Vault version is FIPS 140-2-compliant, the following components and features of Enterprise Vault use the Cryptographic Module:

- The Veritas Enterprise Vault archiving agents: Exchange Server, Domino Server, File System (FSA), SharePoint Server, IMAP and SMTP
- Compliance Accelerator and Discovery Accelerator

The following Veritas add-ons do not use the Cryptographic Module:

- Veritas Enterprise Vault EnCase Ingest Connector
- Veritas NetBackup for Enterprise Vault Agent
- Veritas Backup Exec Agent for Enterprise Vault, and Backup Exec Migrator for Enterprise Vault

For other Veritas add-ons, consult the documentation for the add-on. For third-party products that integrate with Enterprise Vault, check with the third party whether the product uses a FIPS 140-2-validated cryptographic module.

Using Enterprise Vault in a FIPS 140-2-compliant environment

Note the following points if you want to use Enterprise Vault in a FIPS 140-2-compliant environment:

- FIPS 140-2-compliant versions of Enterprise Vault store data on your storage devices using FIPS-compliant algorithms. However, you may want to check with the storage provider whether your storage devices are FIPS-compliant.
- If you want to run Windows in FIPS 140 compliance mode, you must enable the Windows group policy setting or local policy setting for FIPS-compliant algorithms. This setting restricts the use of non-compliant algorithms in the Microsoft .NET Framework.

  See the Microsoft knowledge base article at http://support.microsoft.com/kb/811833.
- To use File System Archiving with placeholder shortcuts on an EMC Celerra device, you must configure the Celerra DataMover to use the Secure Sockets Layer (SSL) protocol. See the *Setting up File System Archiving* guide for instructions.

  Note: Celerra DART 5.5 may not support SSL. Check your Celerra documentation for details of FIPS compliance, if required.
- If you use Enterprise Vault Reporting, see the following technical note on the Veritas Enterprise Support website for guidance on Microsoft SQL Server Report Manager:

  http://www.veritas.com/docs/000014160
- If you use Enterprise Vault Operations Manager, you must rerun the Operations Manager Configuration utility after you enable the Windows policy setting for FIPS-compliant algorithms.

  See “Running the Enterprise Vault Operations Manager Configuration utility” in the *Installing and Configuring* guide.

About the Enterprise Vault CryptoModule event log

An event log view named Veritas Enterprise Vault CryptoModule logs the events that the Veritas Enterprise Vault Cryptographic Module generates.