VERITAS

Enterprise Vault and FIPS 140-2

How Enterprise Vault achieves FIPS 140-2 compliance

Veritas™ White Paper | September 2020

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 FIPS140-2 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 about 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 that:

- 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 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 Enterprise Vault Cryptographic Module are 1894, 2357, 2937 and 3197 on the list of validated FIPS 140-2 modules that the NIST publishes. See the following:

- http://csrc.nist.gov/groups/stm/cmvp/documents/140-1/1401val2013.htm#1894
- https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/2357
- https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/2937
- https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/3197

WHICH VERSIONS OF ENTERPRISE VAULT ARE FIPS 140-2-COMPLIANT?

The following table shows which versions of Enterprise Vault are FIPS 140-2-compliant.

Table 1 Versions of Enterprise Vault that are FIPS 140-2 compliant

Enterprise Vault version	FIPS 140-2 compliant?
10.0 original release	No
10.0.1	Yes. See About the cryptographic boundary.
11.0 (all versions)	
12.0 (all versions)	

ABOUT THE CRYPTOGRAPHIC BOUNDARY

The cryptographic boundary of the Enterprise Vault Cryptographic Module is described in the module's Security Policy document. This document is available from the NIST website at http://csrc.nist.gov/groups/STM/cmvp /documents/140-1/1401val2011.htm#1595.

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

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

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

- Enterprise Vault Discovery Collector
- Enterprise Vault IM Manager
- Enterprise Vault Adapter for Secure Messaging and Rights Management
- Enterprise Vault Encase® Ingest Connector
- NetBackup for Enterprise Vault Agent
- Backup Exec Agent for Enterprise Vault, and Backup Exec Migrator for Enterprise Vault
- Veritas Information Classifier (VIC).

Please note FIPS 140-2 certification for VIC is part of the backlog and it will be addressed soon.

For other 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 following Microsoft knowledge base article: http://support.microsoft.com/kb/811833.
- Microsoft's FIPS-compliant encryption and hashing algorithms are available on Windows Server 2003 and later versions of Windows.
- If you use Enterprise Vault Operations Manager, then 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 Enterprise Vault CryptoModule logs the events that the Cryptographic Module generates.

ABOUT DISCOVERY ACCELERATOR AND FIPS COMPLIANCE

Note the following points if you used Discovery Accelerator before Enterprise Vault 9.0.3.

All the following types of cases are FIPS-compliant:

- Cases that you create with Discovery Accelerator 9.0.3.
- Pre-9.0.3 cases in which analytics is disabled.
- Cases that you create by promoting research folders that you have added with Discovery Accelerator 9.0.3.
- Cases that you create by promoting pre-9.0.3 research folders in which analytics is disabled.

FIPS compliance can be achieved for pre-9.0.3 cases and research folders by disabling analytics and then reenabling it with Discovery Accelerator 9.0.3.

2625 Augustine Drive, Santa Clara, CA 95054
+1 (866) 837 4827
www.veritas.com

For specific country offices and contact numbers, please visit our website.
www.veritas.com/company/contact

V1031 09/20