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 use the Symantec Enterprise Vault Cryptographic Module.
- 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 Symantec Enterprise Vault Cryptographic Module handles the encryption and decryption of passwords, the hashing of data, and random number generation.

NIST has validated the Symantec Enterprise Vault Cryptographic Module to FIPS 140-2 Level 1. The certificate number for the cryptographic module is 1595 on the list of validated FIPS 140-2 modules that the NIST publishes. See http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2011.htm#1595.

For more information about the Symantec Enterprise Vault Cryptographic Module see the module's Security Policy document, which is available from the same URL.
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

<table>
<thead>
<tr>
<th>Enterprise Vault version</th>
<th>FIPS 140-2 compliant?</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.0 (all versions)</td>
<td>No</td>
</tr>
<tr>
<td>9.0 original release, 9.0.1, 9.0.2</td>
<td>No</td>
</tr>
<tr>
<td>9.0.3 and later</td>
<td>Yes. See About the cryptographic boundary.</td>
</tr>
<tr>
<td>10.0 original release</td>
<td>No</td>
</tr>
<tr>
<td>10.0.1 and later</td>
<td>Yes. See About the cryptographic boundary.</td>
</tr>
</tbody>
</table>

About upgrading to the Enterprise Vault 10.0 original release

The Enterprise Vault 10.0 original release predates the introduction of the Symantec Enterprise Vault Cryptographic Module. If you upgrade from Enterprise Vault 9.0.3 or later to the Enterprise Vault 10.0 original release, you must make sure that the Windows group policy setting or local policy setting for FIPS-compliant algorithms is disabled. Otherwise the Enterprise Vault programs that use the .NET Framework and cryptographic algorithms stop working and generate errors in the event log.

For information about the policy setting, see the following Microsoft knowledge base article: [http://support.microsoft.com/kb/811833](http://support.microsoft.com/kb/811833)

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

Note the following points if you want 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](http://support.microsoft.com/kb/811833).
- If you run Windows in FIPS 140 compliance mode, you cannot use FSA to archive data from Windows 2000 file servers, or use Windows 2000 file servers as proxy servers for FSA Reporting. Microsoft’s FIPS-compliant encryption and hashing algorithms are available on Windows Server 2003 and later versions of Windows.
- 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.

About the cryptographic boundary


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

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

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

- Symantec Enterprise Vault Discovery Collector
- Symantec Enterprise Vault IM Manager
- Symantec Enterprise Vault Adapter for Secure Messaging and Rights Management
- Symantec Enterprise Vault EnCase® Ingest Connector
- Symantec NetBackup for Enterprise Vault Agent
- Symantec Backup Exec Agent for Enterprise Vault, and Backup Exec Migrator for Enterprise Vault

For other Symantec 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.
See “Configuring a Celerra connection to use SSL” in the Setting up File System Archiving guide.

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 Symantec Enterprise Support website for guidance on Microsoft SQL Server Report Manager:
  http://www.symantec.com/docs/TECH171120

- 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

The Symantec Enterprise Vault Cryptographic Module generates events in accordance with FIPS 140-2 to indicate when known-answer tests and self-integrity tests are run, and whether they complete successfully. The module logs all these events in a new event log view named Symantec Enterprise Vault CryptoModule.

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.