Enterprise Vault 9.0.3 Feature Briefing

FIPS Support

This document is one of several that details major new or changed features in Enterprise Vault 9.0.3. This document covers the changes made to Enterprise Vault in order to support the US Government Federal Information Processing Standard (FIPS) 104-2.

If you have any feedback or questions about this document please email them to **EV-TFE-Feedback@symantec.com** stating the document title.

.

Feature Description

Enterprise Vault 9.0.3 offers support for Federal Information Processing Standard (FIPS) 104-2. A new Enterprise Vault Cryptographic Module (EVCM) provides FIPS-certified hashing, encryption and random number generation, which will now be used throughout the Enterprise Vault code.

Business Value

FIPS is a US government security standard used to accredit cryptographic modules. Federal agencies typically require software and hardware to be FIPS certified. None of Enterprise Vault's major competitors are FIPS 140-2 compliant at the time of writing this document.

There are no use cases for this feature, except eligibility for sales to US Federal customers.

Underlying Principles

Previously Enterprise Vault used a combination of FIPS-certified and non-certified algorithms for hashing, encryption and random number generation. A new Enterprise Vault Cryptographic Module (EVCM) has been developed for both 32 and 64-bit platforms, and existing EV code has been modified to use this module.

Enterprise Vault 9.0.3, 10.0.1 and future releases will only use the FIPS certified EVCM for hashing, random number generation and Encryption/Decryption.

Discovery and Compliance Accelerator products were also modified to use the new EVCM.

Test Drive

Enterprise Vault will always use FIPS certified algorithms via the EVCM, irrespective of the environment. Even if the Operating System is running in non-FIPS mode, only FIPS certified algorithms will be used by EV.

The FIPS certified module is not visible to administrators or end users. It is recommended that administrators go one step further and enable their Operating Systems to work in FIPS mode. This will ensure compliance for managed code (.NET).

Enterprise Vault will always be in FIPS mode, it cannot be disabled.

There are no pre-requisites for enabling the FIPS EVCM module, and no actions required by the administrator following an upgrade from an earlier version of EV.

Licensing and support considerations

Windows 2000 and Windows XP SP2 do not support FIPS 104-2 certified algorithms, and will therefore no longer be supported by Enterprise Vault.

Note the following when you upgrade from Enterprise Vault 9.0.3 to Enterprise Vault 10.0 original release:

- Enterprise Vault 10.0 is not FIPS-compliant. Before upgrading from 9.0.3 to 10.0 you must disable the security option "System cryptography: Use FIPS-compliant algorithms for encryption, hashing, and signing" in Windows Security Settings > Local Policies > Security Options.
- Enterprise Vault 10.0.1 is not fully FIPS-compliant. For additional information see **http://www.symantec.com/docs/DOC4820**).

About Symantec:

Symantec is a global leader in providing storage, security and systems management solutions to help consumers and organizations secure and manage their information-driven world.

Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

For specific country offices and contact numbers, please visit our Web site: **www.symantec.com**

Symantec Corporation

World Headquarters

350 Ellis Street

Mountain View, CA 94043 USA

+1 (650) 527 8000

+1 (800) 721 3934