Quest® Security Explorer® 9.9.2

Deployment in FIPS Environments

Legend

■ **WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.**

! **CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.**

ⁱ **IMPORTANT NOTE**, **NOTE**, **TIP**, **MOBILE**, or **VIDEO:** An information icon indicates supporting information.

Security Explorer Deployment in FIPS Environments
Updated - February 2024
Software Version - 9.9.2

Contents

Deployment overview and requirements

Overview

Security Explorer 9.9.2 can be successfully deployed in a Federal Information Processing Standard (FIPS) environment by following the procedure described in this document.

Audience

This document is intended for technical implementation consultants responsible for deploying Security Explorer.

Cryptographic usage

Security Explorer 9.9.2 relies on the following third-party cryptographic libraries for its cryptographic needs:

Table 1. Cryptographic usage

Cryptographic Usage	Cryptographic Algorithm	Cryptographic Parameters	Third-Party Libraries
Communication	WCF TCP/HTTP Transport; Security Schannel; SMB v2.1, SMB v3.x; Kerberos;	System.Net.Security.ProtectionLevel.EncryptAndSign	bcryptprimitives.dll or bcrypt.dll
Symmetric encryption of bulk data	N/A	N/A	N/A
Symmetric encryption of secrets	.Net DPAPI ProtectedData	DataProtectionScope.LocalMachine DataProtectionScope.CurrentUser	System.Security.dll Bcryptprimitives.dll or Bcrypt.dll
Asymmetric encryption of secrets	N/A	N/A	N/A
Signing	N/A	N/A	N/A
Hashing	N/A	N/A	N/A

Background

To execute in a FIPS compliant mode, a Windows environment requires the Microsoft Policy "System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing" setting enabled.

Microsoft states that "This policy is only advisory to applications. Therefore, if you enable the policy, it does not make sure that all applications will comply".

Security Explorer 9.9.2 leverages Microsoft's CryptoAPI (CAPI) and CryptoAPI Next Generation (CNG) for its cryptographic needs.

Microsoft Product Relationship with CNG and CAPI libraries is documented here:
https://technet.microsoft.com/en-us/library/cc750357.aspx

"Rather than validate individual components and products, Microsoft chooses to validate only the underlying cryptographic modules. Subsequently, many Windows components and Microsoft products are built to rely on the Cryptographic API: Next Generation (CNG) and legacy Cryptographic API (CAPI) FIPS 140 validated cryptographic modules. Windows components and Microsoft products use the documented application programming interfaces (APIs) for each of the modules to access various cryptographic services.

Prerequisites

The following prerequisites are necessary to set up an environment for FIPS Mode.

- Windows Server 2008 R2 or later (latest)

- The following group policies must be enabled:

    - System Cryptography: Use FIPS compliance algorithms for encryption, hashing and signing. Ensure this policy is enabled.

    - Network Security: Configure encryption types allowed for Kerberos. Ensure the "AES128_HMAC_SHA1" and "AES256_HMAC_SHA1" values are selected.

Installation and operation

Installing Security Explorer 9.9.2 in a new environment automatically enforces all FIPS Mode requirements. No updates are required.

In order to ensure FIPS compliance in the environment, older components must be upgraded or uninstalled.

About us

Quest provides software solutions for the rapidly-changing world of enterprise IT. We help simplify the challenges caused by data explosion, cloud expansion, hybrid datacenters, security threats, and regulatory requirements. We are a global provider to 130,000 companies across 100 countries, including 95% of the Fortune 500 and 90% of the Global 1000. Since 1987, we have built a portfolio of solutions that now includes database management, data protection, identity and access management, Microsoft platform management, and unified endpoint management. With Quest, organizations spend less time on IT administration and more time on business innovation. For more information, visit www.quest.com.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request.
- View Knowledge Base articles.
- Sign up for product notifications.
- Download software and technical documentation.
- View how-to-videos.
- Engage in community discussions.
- Chat with support engineers online.
- View services to assist you with your product.