Quest

Quest® Secure Copy 7.5.1

Deployment in FIPS environment

Trademarks

Legend

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

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

Quest® Secure Copy
Updated – Jun 3, 2019

Contents

Contents

A. Overview 5

B. Audience 5

C. Cryptographic usage 5

D. Background 5

E. Prerequisites 6

F. Installation and operation 6

G. References 6

Document Control

Version		1.0
Author	Director Cybersecurity	Olivier Le Rudulier
Owner	Director Cybersecurity	Olivier Le Rudulier
Approver	Director Cybersecurity	Olivier Le Rudulier
Date Approved		

Version Control

Version	**Date**	**Name**	**Description**
1.0	June 27, 2018	Olivier Le Rudulier	Original Template
2.0	June 4, 2019	Rex Ren	Secure Copy specifics for version 7.5.1

A. Overview

Secure Copy 7.5.1 can be successfully deployed in a FIPS environment by following the procedure described in this document.

B. Audience

The audience for this document are technical implementation consultants deploying Secure Copy.

C. Cryptographic usage

Secure Copy relies on the following Third-Party cryptographic libraries for its cryptographic needs

Cryptographic usage	**Cryptographic algorithm**	**Cryptographic parameters**
Communication	SMB v2, SMB V3	HMAC-SHA256, AES-128-CMAC, AES-128-GCM
Symmetric encryption of bulk data(*email password*)	ProtectedData	DataProtectionScope.LocalMachine AES256 – CBC Mode
Symmetric encryption of secrets(licensed server list)	ProtectedData	DataProtectionScope.LocalMachine AES256 – CBC Mode
Asymmetric encryption of secrets	N/A	N/A
Signing	N/A	N/A
Hashing	DPAPI SHA512	DataProtectionScope.LocalMachine SHA512

D. 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".

Secure Copy 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.

E. Prerequisites

External to Secure Copy, there are several server configurations necessary to set up the environment for FIPS Mode.

1. Windows Server 2008 R2 or later must be installed and up to date.
2. The following group policies must be enabled:
    a. System Cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing. Ensure this policy is enabled.
    b. Network Security: Configure encryption types allowed for Kerberos. Ensure the "AES128_HMAC_SHA1" and "AES256_HMAC_SHA1" values are selected.

F. Installation and operation

For new environments, installing Secure Copy 7.5.1 or later 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.

G. References

N/A

About us

We are more than just a name

We are on a quest to make your information technology work harder for you. That is why we build community-driven software solutions that help you spend less time on IT administration and more time on business innovation. We help you modernize your data center, get you to the cloud quicker and provide the expertise, security and accessibility you need to grow your data-driven business. Combined with Quest's invitation to the global community to be a part of its innovation, and our firm commitment to ensuring customer satisfaction, we continue to deliver solutions that have a real impact on our customers today and leave a legacy we are proud of. We are challenging the status quo by transforming into a new software company. And as your partner, we work tirelessly to make sure your information technology is designed for you and by you. This is our mission, and we are in this together. Welcome to a new Quest. You are invited to Join the Innovation.

Our brand, our vision. Together.

Our logo reflects our story: innovation, community and support. An important part of this story begins with the letter Q. It is a perfect circle, representing our commitment to technological precision and strength. The space in the Q itself symbolizes our need to add the missing piece — you — to the community, to the new Quest.

Contacting Quest

For sales or other inquiries, visit https://www.quest.com/contact.

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.