Quest

Quest® Secure Copy® 7.7

Deployment in FIPS Environments

© 2025 Quest Software Inc.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept.
20 Enterprise, Suite 100
Aliso Viejo, CA 92656

Refer to our website (https://www.quest.com) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at https://www.quest.com/legal.

Trademarks

Quest Software, Quest, and the Quest logo are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit https://www.quest.com/legal/trademark-information.aspx. All other trademarks and registered trademarks are property of their respective owners.

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.

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

Secure Copy Deployment in FIPS Environments
Updated - August 2025
Software Version - 7.7

Contents

Deployment overview and requirements **4**
Overview 4
Audience 4
Cryptographic usage 4
Background 4
Prerequisites 5
Installation and operation 5

About us **6**
Technical support resources 6

1

Deployment overview and requirements

Overview

Secure Copy 7.7 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 Secure Copy.

Cryptographic usage

Secure Copy 7.7 relies on the following third-party cryptographic libraries for its cryptographic needs:

Table 1. Cryptographic usage

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

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 7.7 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 Secure Copy 7.7 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.