Quest

Quest® Change Auditor 7.0

Deployment in FIPS Environments

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

Quest Software Inc.
Attn: LEGAL Dept.
4 Polaris Way
Aliso Viejo, CA 92656

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

Legend

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.

Change Auditor Deployment in FIPS Environments
Updated - March 2019
Software Version - 7.0

Contents

1

Deployment Overview and Requirements

Overview

Change Auditor 7.0.2 can be deployed in a FIPS environment by following the procedure in this document.

Audience

This document is intended for technical implementation consultants responsible for deploying Change Auditor.

Background

To run a Windows environment in FIPS compliant mode, the Microsoft Policy “System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing” must be 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”.

As of version 7.0.2, Change Auditor 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
- Enable the following group policies on all Change Auditor components (agent, coordinator, windows client, web client, and workstation agent):
  - System Cryptography: Use FIPS compliance algorithms for encryption, hashing and signing. Ensure the “AES128_HMAC_SHA1” and “AES256_HMAC_SHA1” values are selected.
  - Network Security: Configure encryption types allowed for Kerberos.

Installation and Operation

To ensure FIPS compliance for your Change Auditor deployment, all Change Auditor components must be v7.0.2 or later.

- Environments with existing Change Auditor deployments:

  All components (clients, coordinators, and agents) must be upgraded to v7.0.2 or later. Begin by upgrading all coordinators and clients. Once this is complete, upgrade all agents either remotely using the client or manually using the agent x64 installer.

- New environments:

  Installing Change Auditor v7.0.2 or later automatically enforces all FIPS Mode requirements. No updates are required.

Supported subsystems

FIPS compliant practices are implemented in Change Auditor wherever possible. The following subsystems guarantee FIPS compliant communications:

- Active Directory
- AD Queries
- AD LDS
- Windows File Server
- SharePoint
- SQL
- Exchange
- Logon Activity

All other subsystems are not considered completely FIPS compliant due to limitations related to handling and passing of data through communications with external products.

Webhooks and FIPS compliance

With the introduction of webhooks and event subscriptions in Change Auditor 7.0, you can configure Change Auditor to send event data to external sources. As the receiver of the data is customized and defined by each individual customer, you are responsible to verify the FIPS Compliance of the event data receiver. This includes generic webhook subscriptions created with Change Auditor PowerShell commands and subscriptions created in the Windows client for supported SIEM tools such as Splunk, ArcSight and QRadar.

In addition, when configuring subscriptions, you must use TLS enabled communication between Change Auditor and the event receivers to ensure FIPS compliance.

- For Splunk and generic webhook subscriptions, the URL specified for the receiver of events must begin with HTTPS.
- For ArcSight and QRadar subscriptions, the TLSEnabled flag must be set to True.

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.

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 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.

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.