Quest

Quest® Change Auditor 7.6.3
Installation Guide

© 2026 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.
10801 N. Mopac Expressway
Building 3, Suite 400
Austin, TX 78759

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, the Quest logo, and Join the Innovation 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

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 Installation Guide
Updated - August 2026
Software Version - 7.6.3

Contents

Installation Overview 5
Before you begin 5
System requirements 6
System statistics and facilities 6
Network traffic 6
Interval settings 7
System overview 7
Installation overview 8
Using group Managed Service Accounts (gMSA) 9

Install Change Auditor 10
Installation workflow 10
Install the first coordinator 11
Required permissions 12
Install the client 16
Install multiple coordinators 17
SSL certificate configuration and deployment 18

Add Users to Change Auditor Security Groups 20
Introducing Change Auditor security groups 20
Add accounts to security groups 21
Add accounts to ChangeAuditor database role 22

Connecting to the Clients 23
Connect to the client 23
Open the web client 24
Access product information 24

Deploy Change Auditor Agents 25
Change Auditor agents 25
Deploy agents 26

Upgrade Change Auditor 28
Pre-upgrade considerations 28
Upgrade Change Auditor 29
Step 1: Upgrade all coordinators (and database schema) 30
Step 2: Upgrade all clients 30
Step 3: Upgrade the agents 31
Post upgrade considerations 31

Installation Notes and Best Practices 33
Licensing Change Auditor products 33
Permissions 34
Other installation notes 35

Change Auditor for Windows File Servers . . . 37
Change Auditor for Exchange . . . 38
Change Auditor for Authentication Services . . . 40
Change Auditor for SharePoint . . . 40
Backup notes . . . 41
Agent behavior notes . . . 41
Client notes . . . 42
ADAM (AD LDS) auditing . . . 42
Change Auditor for SQL Server — SQL auditing . . . 43

Deployment Options . . . 44
Multi-forest deployment . . . 44
Requirements . . . 44
Example deployment scenario . . . 45
Configuration . . . 46
Foreign forest agent deployment . . . 49
Supported functionality . . . 50
Requirements . . . 50
Workflow . . . 50
Harvesting the foreign forest topology . . . 51
Deploying agents to a foreign forest . . . 51
Installing agents in a foreign forest . . . 52
Example deployment scenario . . . 54

Workstation Agent Deployment . . . 56
Recommendations and deployment requirements . . . 56
All workstation agents . . . 56
Deploying workstation agents (domain workstations) . . . 56
Deploying foreign forest workstation agents (domain workstations) . . . 56
Manual workstation agent deployment . . . 57
Deploying workgroup agents (non-domain workstations) . . . 58

Agent Comparison . . . 60

Install an agent to audit ADAM (AD LDS) on workgroup servers . . . 62
Agent installation . . . 62

Windows Installer Command Line Options . . . 63
Agent options . . . 63
Coordinator options . . . 64
Web Client options . . . 65

About us . . . 67
Our brand, our vision. Together. . . . 67
Contacting Quest . . . 67
Technical support resources . . . 67

1

Installation Overview

Change Auditor provides auditing and security coverage for your enterprise network. You can audit the activities taking place in your infrastructure and receive real-time alerts on vital changes and activities as they occur. Instantly know who made changes including the IP address of the originating workstation, where and when it occurred along with before and after values. Then automatically turn that information into intelligent, in-depth forensics for auditors and management — and reduce the risks associated with day-to-day modifications.

- Audit critical changes across your enterprise including Active Directory, Microsoft Entra ID, Microsoft 365 (Exchange Online, SharePoint Online, and OneDrive for Business), Windows File Servers, NetApp, EMC, SQL Server, and SharePoint.
- Collect user login and log out activity for regulatory compliance and user activity tracking.
- Automate ongoing compliance with tracking and reporting for best practices and regulatory compliance mandates for SOX, PCI-DSS, HIPAA, FISMA, GLBA, and more.
- Speed troubleshooting through real-time insight into changes with a comprehensive audit library including built-in audit alerts, reports, and powerful searches.
- Proactively protect critical Active Directory objects, Exchange Mailboxes, and Windows files and folders from harmful changes that could open security holes or cause resources to become unavailable.
- Separate product deployment and management for key environments including Active Directory, Exchange, Windows File Servers, NetApp, EMC, SQL Server, Active Directory Query, SharePoint, and Logon Activity.
- Integrate with other products to track, audit, report, and alert on critical changes made using Safeguard Authentication Services and Quest Defender.

This guide contains the information required to install and configure Change Auditor and upgrade from a previous release. It is intended for network administrators, consultants, analysts, and any other IT professionals installing the product.

See the following information to get you started:

- Before you begin
- System requirements
- System statistics and facilities
- System overview
- Installation overview
- Using group Managed Service Accounts (gMSA)

Before you begin

If you do not already have Change Auditor, download it from https://support.quest.com/.

- Before you can download the product, you must register with Quest. If you are a registered Quest user, log on using your email address and password.
- After you have registered or logged in, locate the product and version to download from the product list.

- On the download window, click the link and save the file to an appropriate directory (such as c:\temp).

  NOTE: If you have purchased multiple Change Auditor products, download one instance of Change Auditor only. The code is the same for all and the license keys determine what features are enabled or disabled.

Before you install Change Auditor:

- Review the system requirements
- Review the complete installation process
- Review Installation Notes and Best Practices
- Read the Release Notes for updated information
- Ensure that you have the appropriate license to enable Change Auditor auditing modules. (A separate license is required to enable the functionality of each of the Change Auditor auditing modules.)

  NOTE: Change Auditor prompts you for a valid license during the coordinator installation. You cannot proceed with an invalid or expired license.

System requirements

Change Auditor includes the following components, all which have specific system requirements:

- Change Auditor coordinators
- Change Auditor client
- Change Auditor agents
- Change Auditor workstation agents
- Microsoft SQL Server database
- Change Auditor web client

NOTE: Each module also has specific auditing and system requirements.

See the Change Auditor Release Notes for details.

System statistics and facilities

Network traffic

- 1 to 3 KB of TCP traffic is generated per audit event sent from a Change Auditor agent to a Change Auditor coordinator.
- 1 to 3 KB of TCP traffic is generated per record upon a successfully run search query.
- 1 KB of TCP traffic is generated every five minutes to update the Change Auditor agent statistics, which are displayed on the Agent Statistics page.

NOTE: There are other network communications, primarily the agent downloading licensing, or configuration data from the coordinator. This configuration can be large, depending on the auditing modules licensed and how they are configured.

Interval settings

Table 1. Interval settings

Setting	Description
Connection Interval	Every five minutes a Change Auditor agent tries to establish a connection or communication channel with a Change Auditor coordinator. **NOTE:** Connection attempts can also be triggered when an agent loses its connection to the coordinator, where the agent tries to re-establish a connection.
Forwarding Interval	Every five seconds an agent forwards all the audited events stored in the local queue (agent's database) to a Change Auditor coordinator. These audited events have not been previously sent to the coordinator. This interval is configurable using the Configuration Setup dialog.
Polling Interval	Every 900 seconds (15 minutes) the agent checks to determine if there have been any modifications to the agent's configuration. This interval is configurable using the Configuration Setup dialog.
Retry Interval	If the agent does not receive an immediate success acknowledgment from the coordinator for the audited events it transmitted, the agent resends all unacknowledged events after five minutes (300 seconds) from the previous attempt. This interval is configurable using the Configuration Setup dialog.

To display the Configuration Setup page

1. Select **View| Administration** to open the Administration Tasks tab.
2. Select **Configuration | Agent** from the navigation pane.
3. On the Agent Configuration page click **Configurations** to display the Configuration Setup dialog, open the **System Settings** tab to view and modify the **Forwarding Interval, Polling Interval** or **Retry Interval** settings.

System overview

Change Auditor agents are deployed to all servers (domain controllers and member servers) tracking configuration changes in real time. When a change is made on a server running a Change Auditor agent, the change information (audit event) is captured by the agent, batched and forwarded to a Change Auditor coordinator, which then inserts the event details into the Change Auditor database.

NOTE: If the Change Auditor for Logon Activity Workstations auditing module is licensed, you must deploy agents to the workstations that you want to monitor.

For each change detected, an audit event entry is created in the Change Auditor database with the following information:

- Type of configuration change event
- Time and date of the configuration change event
- Identity of the machine the change was made on
- Identity of the managed object the change pertains to
- Old and new value of the change (if applicable)
- IP address of the workstation and client where the change originated

The coordinator fulfills client and agent requests and generates alerts. Multiple coordinators can be installed in a single forest and an agent can be connected to multiple coordinators simultaneously. All connected coordinators

can participate in receiving events from the agent, allowing a high volume of events to be distributed for processing.

NOTE: Server agents submit events to all available coordinators to load balance automatically. However, workstation agents randomly connect to a single coordinator. This design enables ‘scaling out’ options for large workstation agent deployments within a single site.

The Change Auditor client provides immediate access to key configuration change information. From the client you can:

- Install, upgrade, or uninstall agents
- Define search criteria to return specific events and view the search results
- Enable and disable alerts and view the events that triggered these alerts
- Enable and schedule email reporting for individual search queries
- View agent and coordinator statistics
- Define custom Active Directory and ADAM (AD LDS) objects and attributes to audit
- Define the SharePoint farm and paths to audit
- Define file system auditing for Windows File Servers and EMC and NetApp devices
- Specify the SQL Server instances to audit
- Specify the Exchange mailboxes to audit
- Specify the Microsoft 365 Exchange Online organizations and SharePoint Online and OneDrive for Business sites to audit
- Specify the containers to exclude from Active Directory query auditing
- Configure object protection for Active Directory, Exchange, File Systems, and Group Policies
- Define and assign agent configurations
- Configure SMTP for alerting and reporting
- Create and schedule purge jobs for maintaining the database
- Define who is authorized to use the Change Auditor client (Windows and web) features

Installation overview

Before installing Change Auditor, choose the SQL database to use. If you want to install the Change Auditor database to a SQL instance other than the default instance of the selected SQL Server, create the instance before running the installer.

During the coordinator installation, you have the option of adding the current user to the Change Auditor Administrators security group. If you select not to do this during the coordinator installation process, you need to add your user account (and any other appropriate user accounts) to one of the Change Auditor security groups. Quest also recommends that you add the Change Auditor Administrators and Change Auditor Operators groups to the appropriate SQL database role. See Add Users to Change Auditor Security Groups for more information regarding these security groups.

Open the client to deploy agents to the required servers. Also, if you have the Change Auditor for Logon Activity Workstation auditing module licensed, deploy agents to the domain workstations you want to monitor. See Deploy Change Auditor Agents for more details.

IMPORTANT: You must be a member of the Change Auditor Administrators group and have local permissions to deploy agents.

You can optionally install the Change Auditor web client to access (search and report on) the data collected by Change Auditor and create custom search queries Change Auditor. See the Change Auditor Web Client User Guide for information about installing and running the web-based client.

Using group Managed Service Accounts (gMSA)

NOTE: By default, all services run as LocalSystem. Using gMSA accounts as the service account is not supported.

When using group Managed Service Accounts:

- The account must end with '$' and the password must be blank.
- The local Administrator group must be added to the group policy debug programs. (Found under Local Computer Policy | Windows Settings | Security Settings | Local Policies | User Rights Assignments | Debug programs.)

Additional Requirements

- Coordinator database connection
  - The coordinator host must be correctly configured to retrieve the managed password for the specified group Managed Service Account.
  - The coordinator installer must be run as the administrator. (Right-click and select Run as administrator.)
- Agent deployment and configuration
  - The domain should be entered in the Fully Qualified Domain Name format.
  - The Windows client must be run as the administrator. (Right-click and select Run as administrator.)
  - The agent host must be correctly configured to successfully retrieve the managed password for the specified group Managed Service Account.
  - For manual installations, the agent installer must be run as the administrator. (Right-click and select Run as administrator.)
  - For foreign domain agent deployments, the account name for the agent to connect to the coordinator should be specified with the Fully Qualified Domain Name (For example: domain.com\user.)
  - For foreign domain agent deployments, a trust relationship with the foreign domain and the coordinator's domain is required.
  - The Coordinator Credential Configurator must be run as the administrator. (Right-click and select Run as administrator.)
- Coordinator configurations that allow users to send reports to a shared folder.
  - The Windows client must be run as the administrator. (Right-click and select Run as administrator.)
  - The coordinator host must be correctly configured to retrieve the managed password for the specified group Managed Service Account.

For information on group Managed Service Account implementations and requirements, refer to Microsoft documentation.

2

Install Change Auditor

- Installation workflow
- Install the first coordinator
- Install the client
- Install multiple coordinators

Installation workflow

Quest recommends installing the Change Auditor components in the following order:

- Database (SQL Server) — Ensure the SQL server is available and the installation account has SQL Server role as dbcreator. To host the Change Auditor database on a SQL instance other than the default instance of the selected SQL Server, create the instance before running the installer.

  NOTE: The database name must not include embedded spaces, special characters, or supplementary characters. For more details, see Microsoft's database identifier documentation.

- Coordinator — When prompted, specify the SQL server to use and the installation account. The Change Auditor database is created remotely on this server during the installation.

  NOTE: During the coordinator installation, you are have the option of adding the current user to the Change Auditor Administrators security group. If you did not add the current user during the installation process or want to add extra user accounts to the Change Auditor security groups, add them before running the client.

  Quest also recommends that you add these security groups to the appropriate SQL database role (that is, Change Auditor Administrators — <*InstallationName*> group to the Change Auditor_Administrators role and ChangeAuditor Operators — <*InstallationName*> group to the ChangeAuditor_Operators role). See Add Users to Change Auditor Security Groups.

- Client — After you have confirmed that the coordinator is functioning correctly, install the client.

  TIP: Quest recommends that you install the first coordinator and client, but do not deploy agents until you have installed required coordinators. When deploying agents, you can select which installation to use for each of the agents.

- Agents — Open the client to deploy agents to your domain controllers and member servers. Also, if you have Change Auditor for Logon Activity Workstation licensed, deploy agents to the domain to monitor for logon activity.
- Web client — Optionally, install the web client on the IIS web server.

This section provides instructions for installing Change Auditor coordinators and the Change Auditor client. See Deploy Change Auditor Agents for instructions on deploying agents. See the Change Auditor Web Client User Guide for instructions on installing and running the web-based client.

Install the first coordinator

The coordinator fulfills client and agent requests and generates alerts. You can install multiple coordinators in a single forest to provide fault tolerance of the Change Auditor service tier. See Install the client.

NOTE:

- You cannot use an existing database. The database must be created by the coordinator installation.
- UDP port 389 must be open on initial installs and upgrades for the coordinator to start.

The coordinator installation creates the following components:

- The coordinator
- A coordinator system tray icon, where you can enable or disable the coordinator, display the status of the coordinator installed on the current computer, change the database instance or service accounts used to access the database, or specify a static port to use to communicate with the coordinator.

  NOTE: See the Change Auditor User Guide for more information about the Change Auditor coordinator system tray icon.

- Three installation-specific Active Directory security groups to enable access to the Change Auditor client and shared overviews distributed using the Change Auditor web client.
  - ChangeAuditor Administrators — <*InstallationName*>
  - ChangeAuditor Operators — <*InstallationName*>
  - ChangeAuditor Web Shared Overview Users — <*InstallationName*>

  Where <*InstallationName*> is a unique name selected during the coordinator installation to isolate your components from any other Change Auditor installation in your Active Directory forest.

  NOTE: See the Change Auditor Web Client User Guide for more information about the ChangeAuditor Web Shared Overview Users security group.

- Two SQL database roles (ChangeAuditor_Administrators and ChangeAuditor_Operators). These roles are added to the Change Auditor database to facilitate database connections from an untrusted forest with the least amount of privileges. The two roles allow administrators to control access to the Change Auditor database through SQL security.

Required permissions

IMPORTANT: Minimum permissions

User account installing the coordinator:

The user account that is installing the coordinator must have permission to perform the following tasks on the target server:

- Windows permissions to create and modify registry values.
- Windows administrative permissions to install software and stop or start services.

The user account must also be a member of the **Domain Admins** group in the domain where the coordinator is being installed.

Service account running the coordinator service (LocalSystem by default):

- Active Directory permissions to create and modify SCP (Service Connection Point) objects under the computer object that is running a Change Auditor coordinator.
- Local Administrator permissions on the coordinator server.

By default, the Coordinator service runs as LocalSystem. To run the Change Auditor service as a Domain User or service account other than Local System, the Change Auditor SPN (Service Connection Point) must be removed from the Coordinator computer (local system) account and added to the Domain Account used to run the Coordinator service.

To do so, open a command prompt on a Domain Controller and perform the following:

1. Remove the SPN from the computer object by entering:

   setspn -D NPRepository4(INSTALLATION_NAME)/SERVER.DOMAIN.TLD SERVERNAME

2. Add the SPN to the service account by entering:

   setspn -A NPRepository4(INSTALLATION_NAME)/SERVER.DOMAIN.TLD USERNAME

   INSTALLATION_NAME = Change Auditor Installation (Default name is DEFAULT)

   SERVER.DOMAIN.TLD = FQDN of the coordinator server

   SERVERNAME = Short name of the coordinator server

   USERNAME = SAM account name of the service account

3. Update the Coordinator service to run under the user name context in question.
4. Restart the Coordinator service.

SQL Server database access account specified during installation:

Create an account that the coordinator service can use on an ongoing basis for access to the SQL Server database. This account must have a **SQL Login** and be assigned the following SQL permissions:

- Must be assigned the **db_owner** role on the Change Auditor database
- Must be assigned the SQL Server role of **dbcreator**

To install the first coordinator:

NOTE:

- You should have received separate licenses from Quest to enable the Change Auditor products you purchased. Before you begin the installation, copy the appropriate license to the local hard drive where you are installing Change Auditor.
- You cannot use an existing database. The database must be created by the coordinator installation.

1. Verify that the user account used to run the coordinator installation is at least a Domain Admin in the domain to which the coordinator server belongs.
2. Use an existing account or create a user account that Change Auditor will use to access the SQL Server.

3 Create a SQL Login for this user account and assign the following permissions to this login: Server role: **dbcreator**

4 From the member server, browse to the folder where the Change Auditor package was downloaded, and run the **Quest Change Auditor Coordinator (x64).msi** file to open the Change Auditor Coordinator Setup wizard.

5 Enter the information requested in the Coordinator Setup wizard.

Review the table for additional information. This table only covers unfamiliar information. It does not include all the wizard screens or field descriptions.

Table 2. Coordinator Setup wizard — installing first coordinator

Product Licensing screen	
Licenses	Click **Open License Dialog** to locate and apply a license. **NOTE:** As of Change Auditor 7.0 a new license is required for all modules.
Installation Name screen	
After licensing the product, the setup wizard prompts you to enter a unique installation name to identify the database to which the coordinator will connect. **NOTE:** If you plan on installing multiple coordinators, see Install the client for more details regarding the ChangeAuditor installation name.	
ChangeAuditor Installation Name	Enter a unique Change Auditor installation name that identifies the current installation within your Active Directory environment. An installation name is required; has a limit of 22 characters; can only contain alphanumeric characters and underscores; and is converted to all caps. **NOTE:** Quest recommends that you use the default (DEFAULT) installation name. **NOTE:** If you entered an existing installation name, confirm that you want to join this component to an existing installation. Click **Yes** to proceed or **No** to reenter a unique installation name.

Table 2. Coordinator Setup wizard — installing first coordinator

SQL Server Information screen	
SQL Server and Instance	Enter the server name or IP address (member server running the SQL instance) and the SQL instance name for the Change Auditor coordinator database such as, <*FQDN of the SQL server*>\<*instance name*> or browse your Active Directory network to locate the required instance. Azure SQL Managed Instance: • For a private endpoint, specify the managed instance host name in the following format: MyHostName.dns_zone.database.windows.net For private endpoint with default port, port specification is not explicitly required. For example: MyHostName.b1b2a3d4e5f7.database.windows.net or MyHostName.b1b2a3d4e5f7.database.windows.net,1433 • For a public endpoint, specify the managed instance host name and port in the following format: MyHostName.public.dns_zone.database.windows.net,3342 For public endpoint, port specification is required. For example: MyHostName.public.b1b2a3d4e5f7.database.windows.net,3342 **NOTE:** Visit the support portal knowledge base for more information about migrating from SQL on-premises to SQL Managed Instance. **NOTE:** Performance may vary depending on network configuration, topology, and Azure SQL Managed Instance configuration. **NOTE:** Azure SQL Managed Instance (PaaS) is supported using SQL authentication or Microsoft Entra authentication with an encrypted connection. Windows authentication is not supported. **NOTE:** Single User Mode is not supported during installation or upgrade when using Azure SQL Managed Instance. Ensure that all SQL connections to the Change Auditor database are closed before and during the upgrade. **NOTE:** Azure SQL Managed Instance (HA) high availability is supported using the read-write listener endpoint. **NOTE:** If you are using Windows security to access your SQL Server, ensure that the domain user is granted access to the SQL Server. **NOTE:** If you plan to add the Change Auditor database to a SQL AlwaysOn Availability Group, ensure that the availability group has already been configured and then specify the name of the availability group listener for SQL server name.
Name of database catalog	Enter the name to assign to the Change Auditor database. **NOTE:** If an existing Change Auditor database is present, you should provide a unique name for the Change Auditor database. If a database with the name entered is found, a warning message explains the need to provide a unique name for your new Change Auditor database. On this warning dialog, click **Cancel** to specify a different database name. Clicking **OK** proceeds to the Ready to Install the Program screen.

Table 2. Coordinator Setup wizard — installing first coordinator

Authentication/ Credentials	Use the authentication section to specify whether the authentication to use when communicating with the SQL database instance. (The authentication method is set up when SQL is installed.) **NOTE:** If **Windows Authentication** is used to access the designated SQL instance, a verification screen is displayed. Verify that the server name, SQL instance name, and credentials are correct before proceeding. Incorrect entries cause the Change Auditor coordinator service to fail on startup. **NOTE:** For Azure SQL Managed Instance (PaaS), SQL authentication or Microsoft Entra Authentication with an encrypted connection must be used. **NOTE:** If you are using a group Managed Service Account: • The account must end with '$' and the password must be blank. • The coordinator host must be correctly configured to retrieve the managed password for the specified group Managed Service Account. • The coordinator installer must be run as the administrator. (Right-click and select Run as administrator.) • The local Administrator group must be added to the group policy debug programs. (Found under Local Computer Policy | Windows Settings | Security Settings | Local Policies | User Rights Assignments | Debug programs.)
Encryption **NOTE:** • Change Auditor supports TLS 1.3; however, TLS 1.2 remains a requirement since SQL Server 2022 satellite services require TLS 1.2 to be enabled. For more information on TLS support, see Microsoft documentation.	Select the appropriate level of encryption for the data sent between the coordinator and SQL server. • **Strict (SQL Server 2022)**: Select this option for SQL Server 2022 and Azure SQL Managed Instance or when the instance has **Force Strict Encryption** enabled. • **Mandatory**: Select this option when the instance has **Force Encryption** enabled. It can also be used when no encryption is configured for the instance, but **Trust server certificate** is enabled. While this method is less secure than installing a trusted certificate, it does support an encrypted connection. • **Optional** Enabling **Trust server certificate**, when 'Optional' or 'Mandatory' encryption is selected, or if the server enforces encryption, means that SQL Server will not validate the server certificate on the client computer when encryption is enabled for network communication. Under **Host name in certificate**, you can provide an alternate, yet expected, Common Name (CN) or Subject Alternative Name (SAN) in the server certificate. You would use this option when the server name does not match the CN or SAN, for example, when using DNS aliases. Leaving this option blank allows certificate validation to confirm that the CN or SAN matches the server name.
ChangeAuditor Administrators screen	
Add the current user to the "ChangeAuditor Administrators - <*InstallationName*>" security group	This check box is selected by default and adds the current user to the ChangeAuditor Administrators — <*InstallationName*> group. Any user that is running a Change Auditor client must be added to either this security group or the ChangeAuditor Operators security group. In addition, users responsible for deploying Change Auditor agents must be a member of the ChangeAuditor Administrators group in the specified ChangeAuditor installation. See Add Users to Change Auditor Security Groups for more information about these security groups and how to add more user accounts.

Table 2. Coordinator Setup wizard — installing first coordinator

Specify Port Information screen	
By default Change Auditor dynamically assigns communication ports to use to communicate with each installed coordinator. However, using the port settings on this screen you can specify static SCP listening ports to use instead. **NOTE:** A zero (0) indicates that a dynamic port is being used. These port assignments can also be set using the Coordinator Configuration Tool which is accessed by right-clicking the Change Auditor coordinator system tray icon.	
Client Port	Enter the static port number for the Change Auditor client to communicate with the coordinator. **TIP:** If you are planning on installing the Change Auditor web client, enter a static client port.
Public SDK Port	Enter the static port number for external applications to access the coordinator.
Agent Port (Legacy)	Enter the static port number for legacy (5.x) Change Auditor agents to communicate with the coordinator.
Agent Port	Enter the static port number for Change Auditor agents to communicate with the coordinator.
Specify LDAP Authentication Type	
Specify the authentication method to use to make Active Directory requests. • Select Simple Authentication and Security Layer (SASL) to use Kerberos or NTLM. • Select Secure Socket Layer (SSL) to use certificates. See SSL certificate configuration and deployment for more details. **NOTE:** When making Active Directory requests, credentials and message content are encrypted for both authentication methods.	

6 After you have entered all the requested information, click **Install** to start the installation process.

7 After the coordinator is installed, you can install the client.

NOTE: Reboot the server if you have any other Quest solutions installed on this server.

8 If you are using the SQL AlwaysOn Availability Groups functionality, you now need to put the database in an SQL availability group.

a Stop the coordinator.

b Put the database is in full recovery mode.

c Backup the database.

d Move the database to a previously configured availability group.

e Allow database replication to complete.

f Start the coordinator.

Install the client

The client connects directly to the coordinator or to an archive database and is the user interface that provides immediate access to key configuration change information.

To install the client:

1 On a workstation, laptop or member server, browse to the folder where the Change Auditor package was downloaded, and run the **Quest Change Auditor Client (x64).msi** file to open the Change Auditor Client setup wizard.

2 Select **Install Change Auditor Client** to open the Client Setup wizard.

> **NOTE:** If Microsoft .NET is not installed on the computer, an extra screen is displayed explaining that this application was not found and the install cannot continue. Click **Close** to stop the client install. Download and install the required .NET version. After .NET is successfully installed, restart the client installation.

3 Read and accept the license agreement and click **Next**.

4 Select the installation directory and click **Next**.

5 Select your shortcut options and click **Next**.

6 Specify the authentication method to use to make requests to Active Directory.

Select Simple Authentication and Security Layer (SASL) to use Kerberos or NTLM.

Select Secure Socket Layer (SSL) to use certificates. See SSL certificate configuration and deployment for more details.

> **NOTE:** When making Active Directory requests, credentials and message content are encrypted for both authentication methods.

7 Click **Install**.

If you are installing multiple coordinators, install your additional coordinators now.

Install multiple coordinators

When installing multiple coordinators in your Active Directory forest, the Change Auditor installation name entered during the coordinator installation determines if they connect to the same SQL database or to different database installation. That is,

- If you use an existing installation name for each coordinator, these coordinators all connect to the same SQL database installation.
- If you enter a unique installation name for each coordinator, these coordinators connect to different SQL database installations.

A unique installation name allows you to isolate your installation of Change Auditor from any other installations of Change Auditor in your Active Directory forest. When all Change Auditor installations are upgraded in the forest, the installation name:

- Allows all coordinators to use your central SQL database, while ensuring no other installation's coordinators use your SQL database.
- Ensures that only agents in your installation connect to your coordinator. See Deploy Change Auditor Agents.
- Ensures only users in your installation's security groups can use the Change Auditor client to manipulate your configuration and view your data.

> **TIP:** Quest recommends that you install the first coordinator and client, but do not deploy agents until after you have installed all additional coordinators required. When deploying agents, you can select which installation to use for each of the agents.

To install more coordinators:

1 On the individual member servers that are to host a coordinator, browse to the folder where the Change Auditor package was downloaded, and run the **Quest Change Auditor Coordinator (x64).msi** file to open the Change Auditor Coordinator Setup wizard.

2 Enter the information requested in the Coordinator Setup wizard.

Review the following table for additional information. This table only covers information regarding multiple coordinator installations. It does not include all the wizard screens or field descriptions.

Table 3. Coordinator Setup wizard — installing multiple coordinators

Product Licensing screen	
Licenses	Use the same license files used for the first coordinator. **NOTE:** If you have installed or licensed multiple auditing modules, apply the appropriate license for each of the installed auditing modules.
Installation Name screen	
Change Auditor Installation Name	Enter a unique installation name to use a different database. Enter an existing installation name or browse to connect to an existing Change Auditor installation. **NOTE:** By selecting an existing Change Auditor installation, you are joining this component to the specified installation. (For example multiple coordinators will be connected to the same database and agents can connect to any of the coordinators in this installation). **NOTE:** If you entered an existing installation name, confirm that you want to join this component to an existing installation. Click **Yes** to proceed or **No** to enter a unique installation name. **NOTE:** If the Change Auditor database is in a SQL availability group, specify the name of the availability group listener for the SQL server name.
Specify Port Information screen By default Change Auditor dynamically assigns communication ports used to communicate with each installed coordinator. However, using the port settings on this screen you can specify static SCP listening ports to use. **NOTE:** A zero (0) indicates that a dynamic port is being used. These port assignments can also be set using the Coordinator Configuration Tool which is accessed by right-clicking the Change Auditor coordinator system tray icon.	
Client Port	Enter the static port number for the client to communicate with the coordinator.
Public SDK Port	Enter the static port number for external applications to access the coordinator.
Agent Port (Legacy)	Enter the static port number to for legacy (5.x) agents to communicate with the coordinator.
Agent Port	Enter the static port number for Change Auditor agents to communicate with the coordinator.
Specify LDAP Authentication Type Specify the authentication method to use to make Active Directory requests. • Select Simple Authentication and Security Layer (SASL) to use Kerberos or NTLM. (This is the default.) • Select Secure Socket Layer (SSL) to use certificates. See SSL certificate configuration and deployment for more details. **NOTE:** When making Active Directory requests, credentials and message content are encrypted for both authentication methods.	

SSL certificate configuration and deployment

When selecting to use SSL for LDAP authentication, ensure that you adhere to the following guidelines:

- A public-key certificate for the domain controller is required on the host of each Change Auditor component that makes Active Directory requests to a domain controller.

- A valid certificate must be provisioned, and your domain controller policy must be configured to use it.
- SSL authentication settings are global. Once enabled, domain controllers within all domains known to the coordinator must be configured to support this authentication method. Domains which do not support SSL will not be searchable for Change Auditor auditing, protection or agent deployment.
- For details on configuring certificates on domain controllers, see Microsoft documentation.
- Certificates are deployed to all computers in the forest automatically when using Active Directory Certificate Services. Certificates must be manually deployed to foreign forests.

  NOTE: Visit the support portal knowledge base for more information.

- A sample script is available that you can use to set or reset the authentication mode used for your Change Auditor components. By default, the script is located here: C:\Program Files\Quest\ChangeAuditor\Client\PowerShell Sample Scripts\ SetCALdapBindingOptions.ps1.

3

Add Users to Change Auditor Security Groups

- Introducing Change Auditor security groups
- Add accounts to ChangeAuditor database role
- Add accounts to security groups

Introducing Change Auditor security groups

During the coordinator installation, the following security groups are created to allow access for performing various functions within Change Auditor:

- **ChangeAuditor Administrators — <*InstallationName*> Group** — provides access to all aspects of Change Auditor and to deploy agents.
- **ChangeAuditor Operators — <*InstallationName*> Group** — provides access to Change Auditor except for making configuration changes.
- **ChangeAuditor Web Shared Overview Users — <*InstallationName*> Group** — provides access to the web client shared overviews, while restricting access to only what has been shared. See the Change Auditor Web Client User Guide for more information about sharing overviews.

The installation name assigned during the coordinator installation is appended to these security groups. For example, when using the default installation name, these groups are named:

- ChangeAuditor Administrators — DEFAULT
- ChangeAuditor Operators — DEFAULT
- ChangeAuditor Web Shared Overview Users — DEFAULT

Two Domain Local Security Groups are created in the same domain as the coordinator. The Group Scope can be changed to Universal as long as the Group Names remain ChangeAuditor Administrators — <*InstallationName*> and ChangeAuditor Operators — <*InstallationName*>.

NOTE: If the domain's Functional Level is in Windows 2000 Mixed mode, then Local Security groups are created on each coordinator member server.

Membership in the ChangeAuditor Administrators and ChangeAuditor Operators groups enable the client to connect and authenticate to a coordinator; therefore, any user that is running a Change Auditor client must be added to one of these groups. In addition, all users responsible for deploying agents must also be a member of the ChangeAuditor Administrators group in the specified Change Auditor installation. If you are not a member of this security group for this installation, you get an access denied error.

NOTE: If multiple coordinators are installed in a mixed mode environment, to connect to each coordinator, you must add your user account to one of these groups on each of the member servers where the coordinators reside.

All users running a client must also have the proper SQL credentials for accessing a Change Auditor archive database. One way of accomplishing this would be to add the ChangeAuditor Administrators and ChangeAuditor Operators groups into the appropriate SQL database roles which were also created during the coordinator installation: ChangeAuditor_Administrators and ChangeAuditor_Operators.

Add accounts to security groups

During the coordinator installation process, you could add the current user to the ChangeAuditor Administrators security group in the specified Change Auditor installation. If you selected not to add the current user during the installation process or want to add more user accounts, use the following procedure.

To add user accounts to security groups:

Use the Active Directory Users and Computers MMC snap-in to add the appropriate user accounts to one of the Change Auditor groups:

1. Open the **Active Directory Users and Computers** snap-in.
2. Connect to the domain where the coordinator was installed.
3. Right-click and select **Properties** on the group called ChangeAuditor Administrators — <*InstallationName*> or ChangeAuditor Operators — <*InstallationName*>.
4. Select the **Members** tab.
5. Click **Add** and browse to the appropriate user object.
6. Click **OK** to close the Active Directory Users and Computers snap-in.
7. To apply this change, log out and back in.

Adding the appropriate users to one of these groups allow the client to successfully connect to the coordinator.

To add user accounts to security groups (Domain in Windows 2000 mixed mode):

Use the Microsoft Computer Management tool to add the appropriate user accounts to one of the Change Auditor groups:

1. From the member server where the Change Auditor coordinator is installed, right-click **My Computer** and select **Manage**.
2. From the Computer Management dialog, expand **Local Users and Groups** and select **Groups**.
3. Right-click and select **Properties** on the group called ChangeAuditor Administrators — <*InstallationName*> or ChangeAuditor Operators — <*InstallationName*>.
4. Click **Add** and browse to the appropriate user object.
5. Click **OK** to close the Computer Management tool.
6. To apply this change, log out and back in.

Adding the appropriate users to one of these groups allow the client to successfully connect to the coordinator.

Add accounts to ChangeAuditor database role

NOTE: This process only applies to archive databases and must be modified each year to apply to the new archive for that year

To add accounts to the ChangeAuditor database role:

Use the Microsoft SQL Management Studio to add the appropriate user or group accounts to one of the ChangeAuditor database roles:

1. Open the Microsoft SQL Server Management Studio and connect to the SQL database server.
2. Navigate to the ***<SQL Server(Instance)>*** **| Security | Logins** directory. Expand the Logins node.
3. Right-click the Logins node and select **New Login**.
4. On the Select User or Group dialog, click **Object Types** and make sure that the **Groups** check box is selected. Click **Location** to search either the Entire Directory or local SQL server (depending on where the group was created, which is determined by the domain functional level). Click **Check Names** to select the user or group account (for example, ChangeAuditor Administrators) to be added.
5. In the Select a Page pane (left pane), select **User Mapping**.
6. In the Users mapped to this login pane (top pane), select the Change Auditor database.
7. In the bottom pane, Database role membership for: ChangeAuditor, select the ChangeAuditor_Administrators role.
8. Click **OK**. Your SQL Login account for Change Auditor database access is now mapped to the appropriate role.

   Repeat these steps to create a SQL Login for the ChangeAuditor Operators group and assign this login to the ChangeAuditor_Operators role for the Change Auditor database.

4

Connecting to the Clients

- Connect to the client
- Open the web client
- Access product information

Connect to the client

The following conditions must be met to properly connect:

- Communications are successful, meaning the coordinator service is running and has a valid SCP listening port (no firewall implications). If this condition fails, the client displays an error dialog stating the appropriate issue.
- The current authenticated user running the client has the proper credentials for accessing the coordinator service. If this condition fails, the client displays the Coordinator Credentials Required dialog where you can enter the proper login credentials to access the coordinator.
- The current authenticated user is a member of either the ChangeAuditor Administrators or ChangeAuditor Operators AD group. If this condition fails, the Change Auditor logon screen displays an error and allows you to enter the appropriate credentials.
- When using a direct database connection, the current authenticated user running the client has the proper SQL credentials for accessing the SQL database. If this condition fails, the client displays the Database Credentials Required dialog where you can enter the proper logon credentials to access the SQL database.
- To access an archive database, the account that you use to log into the client must not have the 'Deny logon over the network' right set.

To open the client

1 Select **Start | All Programs | Quest | Change Auditor | Change Auditor Client**.

The Connection screen opens where you can connect to the ‘default connection’ profile or define or specify a different connection profile.

A connection profile defines the connection method used to connect to a coordinator in trusted or untrusted forests, or to the database directly without connecting with the coordinator. See Manage Connection Profiles in the Change Auditor User Guide for more information about defining connection profiles.

2 Initially, select **Connect** to use the default connection profile.

After you have defined alternate connection profiles, select the appropriate profile from the drop-down list and click **Connect**.

3 If you do not have the proper credentials required for access, the credentials dialog opens allowing you to enter the required credentials.

Depending on how your system has been configured:

- Enter a user account and password or a smart card certificate and personal identification number.

- Select Disconnect client after 30 minutes of inactivity to disconnect from the coordinator after 30 minutes of inactivity.

4 You are now ready to deploy agents. See Deploy Change Auditor Agents for details.

Open the web client

The web client enables you to search for configuration changes and view Change Auditor data using a web browser rather than the Change Auditor client.

NOTE: The web client's appearance is different based on whether you have started it using a standard browser or a mobile browser. The procedures in this guide illustrate the standard browser version of the web client.

NOTE: **Upgrading the web client**
After you have upgraded the web client, you may need to force your browser to reload the Change Auditor web pages from the web server (CTRL-F5 for IE, Chrome ,or Firefox) to ensure you are seeing the most up-to-date changes made to style components within the web client (for example, icons, text or images). See the documentation for your browser for further details.

To open the web client:

1 Open your web browser and enter the URL of the web application server.

https://<*Web Server Host Name*>/ChangeAuditor

2 When the web client is opened, log on by entering the user name (<*Domain*>\<*UserName*>) and password of an authorized Active Directory account.

NOTE:
- By default you only have 3 attempts to log on to the web client. Once locked out you will need to wait 15 minutes before you can try to log on again.
- Selecting the **Remember Me** check box retains your <*Domain*>\<*UserName*> on subsequent sessions.

3 Click **Log In**.

Access product information

The first time the client is opened, the Start page provides access to news and updates, support, and knowledge base content, online documentation, links to the latest releases, and essential contact links.

If you do not want to see this page each time that you open the client, then clear the **Display this page each time I log in** option. One this option has been cleared, the next time you log in you will be directed automatically to the Overview page. However, Quest suggest you keep the Start page active as it contains the most up-to-date access to the supporting information you may require.

5

Deploy Change Auditor Agents

- Change Auditor agents
- Deploy agents

Change Auditor agents

Once you have installed the coordinators and client, you are ready to deploy agents to the servers and workstations.

NOTE:

- If you have not added the appropriate user accounts to either the ChangeAuditor Administrators or ChangeAuditor Operators group, you are denied access to the coordinator when you open the client. See Add Users to Change Auditor Security Groups for more information about these security groups and SQL database roles.
- The user account used to deploy agent must have:
  - Administrative authority to install software on every target computer.
  - Interactive logon rights.

Quest recommends that you deploy a server agent to all servers (domain controllers and member servers) to track configuration changes in real time. For workstations, deploy a workstation agent to only those that you want to monitor for login activity. See Agent behavior notes for information about how the different types of agents connect to the coordinators in your environment and the limits set for agent connections.

When a change is made on a server running an agent, the change information (audited event) is captured and forwarded to the specified database.

NOTE: The agent database supports up to 3 GB. After the database size reaches this limit, no new events are audited and the 'Agent service has reached a critical load' event is generated. This typically occurs when an agent is disconnected from a coordinator for an extended period.

NOTE: See the Installation Notes and Best Practices for notes on deploying agents for Change Auditor for Exchange and Change Auditor for Authentication Services.

NOTE: To install Change Auditor agents to monitor ADAM (AD LDS) instances on workgroup servers, run the agent installer package (Quest Change Auditor Agent 6 (x64)).msi. See Install an agent to audit ADAM (AD LDS) on workgroup servers for details.

NOTE: When you are using Active Roles, there is an extra integration step that you can take to capture the user who initiated the change. See the Change Auditor for Active Directory User Guide for details.

The Deployment page in the client displays all the servers and workstations discovered in your Active Directory environment. From here, you specify the servers (and workstations) to host an agent. For a description of the Deployment page, see the online help or Change Auditor User Guide.

NOTE: The Deployment page does not display nonmember objects, such as ADAM workgroup servers or nondomain workstations, because agents cannot be deployed to non-member objects using the Deployment tab. See Install an agent to audit ADAM (AD LDS) on workgroup servers for more information about manually installing agents to workgroup servers. See Workstation Agent Deployment for more information about manually installing agents to non-domain workstations.

Deploy agents

The following procedures step you through the process of deploying agents. See the Change Auditor User Guide for procedures on using the advanced options and setting up auto deployment of new servers.

To deploy agents:

NOTE:

- If required, agents running on a domain-joined server or domain controller can connect to coordinators in a foreign Active Directory forest. For details, see Foreign forest agent deployment.
- When deploying agents using remote deployment from the Deployment tab, the LDAP Authentication option for the deployed agent will be set according to the current LDAP Authentication setting of the connected coordinator.

1. Verify that the agent deployment account has at least administrator permissions in every domain that contains servers or workstations where agents will be deployed.
2. Verify that the logged on user account is a member of the Change Auditor Administrators group in the specified Change Auditor installation.
3. Open the client. If agents have not yet been deployed, select the **Deployment** tab. Otherwise, use **View | Deployment**.

   The Deployment page is populated with the servers (domain controllers and member servers) and workstations in your Active Directory environment.

   NOTE: The Deployment page may initially be empty until the current forest's server topology has been initially harvested. Topology scan takes a long time when the environment contains many workstations. This page is automatically refreshed after this task has completed.

4. From this list, select an entry and select **Credentials | Set** to enter the proper user credentials for installing agents on the selected domain.

   On the Domain Credentials dialog, select the domain from the list and click **Set**. On the Logon Credentials dialog, enter the credentials of a user with administrator rights on the selected domain.

   NOTE: If you are using a group Managed Service Account, see Using group Managed Service Accounts (gMSA) for additional requirements.

5. After entering the proper credentials, select the entry back on the Deployment page and select **Credentials | Test**. If you get a **Valid Creds** status in the **Deployment Result** column, you can start deploying agents to that domain.

   If you get a **Logon Failure** status in the **Deployment Result** column, use the **Credentials | Set** command to enter the proper credentials for installing agents.

6. By default, the Change Auditor agent folders (Agent, Systray) are installed to %ProgramFiles%\Quest\ChangeAuditor\. You can, however, change the location of the installation folder by clicking **Advanced Options**.
7. Select one or more servers or workstations on the Deployment page and click **Install or Upgrade**.
8. On the Install or Upgrade dialog select one of the following options to schedule the deployment task:

   - Now (default)
   - When

   If you select the **When** option, enter the date and time when you want the deployment task to initiate. Click **OK** to initiate or schedule the deployment task.

   Back on the Deployment page, the **Agent Status** column displays 'Pending' and the **When** column displays the date and time specified.

   NOTE: To cancel a pending deployment task, select the server or workstation and then click **Install or Upgrade**. On the Install or Upgrade dialog, click **Clear Pending**.

9 As agents are successfully connected to the coordinator, the corresponding **Deployment Result** cell displays ‘Success’, the **Agent Status** cell displays ‘Active’ and a desktop notification displays in the lower right-hand corner of your screen.

NOTE: To deactivate these desktop notifications, select **Action | Agent Notifications**.

Once agents are deployed and you open the client, the Overview page opens and provides a real-time stream of events based on a ‘favorite’ search definition and other summary information.

NOTE: After the deployment, the Version cell might display a previous version of an agent if you installed the agent on an unsupported platform.

6

Upgrade Change Auditor

This section contains information about upgrading Change Auditor. Before proceeding with an upgrade, read the following information carefully and consider all steps that apply to your deployment.

NOTE: The Change Auditor 7.0.2 and higher agent cannot connect to a coordinator version 7.0.1 or earlier. When upgrading the Change Auditor agent to 7.0.2 and higher, ensure the Change Auditor coordinator has also been upgraded to 7.0.2 and higher.

You can upgrade from the following upgrade paths.

Table 4. Available upgrade paths

Upgrade from...	Details
Change Auditor 6.x through 7.x	You can upgrade directly to the latest version. If the upgrade cannot proceed because 5.x events are still present in the database, upgrade to 6.8 first to complete the upgrade of the 5.x events, then upgrade to the latest version. Ensure that upgrade of the 5.x events has fully completed before you upgrade.
Change Auditor 5.9 or below	You cannot upgrade directly to the latest version. You must upgrade to 6.8 first.

- Pre-upgrade considerations
- Upgrade Change Auditor
- Post upgrade considerations

Pre-upgrade considerations

IMPORTANT: Agent upgrade

- As of version 7.6.2, Change Auditor utilizes SQLite for the agent's local event storage. Events that are stored locally and waiting to be sent to the coordinator will be lost on agent upgrade because the existing agent database will be discarded and replaced with the new SQLite database. We suggest that you upgrade servers during a time when there is the least amount of event traffic.
- If upgrading agents to version 7.6.2 from 7.5 or later, you may remove SQL Server 2022 LocalDB and the Microsoft VC++ redistributable 2015-2022 from the agent host computer after the upgrade is complete if you determine there are no other dependencies and are not being used by other applications. These components will not be removed automatically with the upgrade.

Review these special considerations before running an upgrade.

Coordinator upgrades

Coordinator upgrades may take longer than expected due to additions to the Changes Auditor database schema. The duration of the upgrade is dependent on the number of events generated in the last 45 days prior to the upgrade. The estimated time is approximately 1 minute for 1 million events.

Larger, more active environments should prepare for coordinator downtime of several hours during the upgrade process. You can view the upgrade progress in the coordinator logs or by connecting the upgraded client to the coordinator.

Upgrading a coordinator that is using Azure SQL Managed Instance for the database configuration

Single User Mode is not supported during installation or upgrade when using Azure SQL Managed Instance.

NOTE: Do not open a connection to the SQL database while upgrading.

Upgrading a coordinator that is using SQL AlwaysOn Availability Groups for the database configuration

When upgrading Change Auditor databases that are part of a SQL AlwaysOn Availability Group, the upgrade can be performed while connected to the availability group listener. The upgrade will take place on the primary database and SQL will replicate any changes to the other databases in the availability group. Ensure that all SQL connections to the primary database are closed before and during the upgrade.

Services using Change Auditor SDK

Stop any services that use the Change Auditor SDK, such as Active Roles or GPOADmin, before starting the upgrade process.

Server collation differences

Starting with Change Auditor 6.0, on the coordinator startup the database collation is checked against SQL server collation. If they are different, the coordinator stops and logs the “Database collation differs from server collation” warning. If it is not possible to update collation of the SQL server, use the AllowCollationSwitch registry key to allow proceeding with rebuilding Change Auditor database according to the new collation. However, using this in environment with large number of events in the database significantly increases the load on SQL server. See the Change Auditor Technical Insight Guide for more information about setting this registry key.

Upgrading Change Auditor agents on high volume Exchange servers

It is critical that Change Auditor for Exchange agent upgrades be scheduled for maintenance intervals or other periods of low user mailbox activity for any configuration of Exchange Server. Change Auditor for Exchange agent upgrades should not be attempted on an active Exchange Server cluster node in any case.

To eliminate the possibility of unscheduled Exchange Server downtime, perform agent upgrades to Exchange Servers during periods of low or no mailbox activity. When upgrading agents on busy Exchange Servers, it is also recommended that you manually stop the agent before upgrading to avoid a possible timeout on the stop command. Verify that the Change Auditor agent service is stopped on the Exchange Server before proceeding with the agent upgrade.

NetApp Auditing

HTTP application access must be assigned to all accounts that are assigned to agents for NetApp auditing templates prior to upgrading to 7.5 or later. See system requirements in Release Notes for additional details.

Alert Configuration (Evaluation Frequency)

This setting is no longer available. If you want to reduce the amount of email produced from alert-enabled searches, you must set the "AlertScanPeriod" registry key setting on the coordinator computer:

HKLM\SOFTWARE\Quest\ChangeAuditor\Coordinator

Value: AlertScanPeriod

Type: DWORD

Default value: 60 seconds

Description: Specifies the time interval between generating alerts.

Upgrade Change Auditor

To ensure success, upgrade the Change Auditor components in the following order:

- Step 1: Upgrade all coordinators (and database schema)
- Step 2: Upgrade all clients
- Step 3: Upgrade the agents

Step 1: Upgrade all coordinators (and database schema)

During an upgrade of the first coordinator, the Change Auditor database is upgraded. Before proceeding with the coordinator upgrade, backup the database.

NOTE: Change Auditor 7.0 and above requires a new license for all modules.

IMPORTANT: As of Change Auditor version 7.0.4, Microsoft Graph API permissions are required for the web application to audit Microsoft Entra ID and Microsoft 365. Due to this, any existing Microsoft Entra ID and Microsoft 365 templates must be updated.

Microsoft Entra ID and Microsoft 365 auditing will not occur if the permission requirements are not met.

See the Microsoft 365 and Microsoft Entra ID auditing User Guide for details on updating the templates and the required permission.

To upgrade all coordinators (and database schema):

1. Stop all coordinators.
2. Log on to the coordinator server to upgrade and browse to the folder where the Change Auditor package was downloaded, and run the **Quest Change Auditor Coordinator (x64).msi** file to open the Change Auditor Coordinator Setup wizard.
3. Follow the Change Auditor Coordinator Setup wizard.
4. After the Change Auditor Coordinator Setup wizard has successfully finished, wait until the coordinator goes from an 'Initializing' status to a 'Running' status. To determine the coordinator's status, right-click the Change Auditor coordinator system tray icon and select the **Coordinator Status** option.
5. Continue to upgrade the remaining coordinators one at a time following steps 2 to 4.

Step 2: Upgrade all clients

To upgrade a client:

1. From a workstation, laptop, or member server, browse to the folder where the Change Auditor package was downloaded, and run the **Quest Change Auditor Client (x64).msi** file to open the Change Auditor Client Setup wizard.
2. Follow the Change Auditor Client Setup wizard.

   See Install the client for more detailed information about the Client Setup wizard.

To upgrade a Change Auditor web client:

1. On the IIS server, browse to the folder where the Change Auditor package was downloaded, and run the **Quest Change Auditor Web Client (x64).msi** file to open the Change Auditor Web Client Setup wizard.
2. Follow the Change Auditor Web Client Setup wizard.

   See the Change Auditor Web Client User Guide for more detailed information about the Change Auditor Web Client Setup wizard.

Step 3: Upgrade the agents

NOTE: Previous versions of Change Auditor agents (6.x, and 7.x) can connect and work with a Change Auditor 7.x coordinator and client. Direct upgrades to the latest version are supported from versions 6.x and 7.x.

The Change Auditor agent requires .NET 4.8. See the System statistics and facilities system requirements for the list of supported platforms.

To upgrade Change Auditor agents:

1. Open the client and select **View | Deployment**.
2. Select the agents to upgrade and click **Install or Upgrade**.

   NOTE: If you get an **Access Denied** status in the Deployment Results column, use the **Credentials | Set** command to enter the proper credentials for installing agents.

3. Select one of the following options to schedule the deployment task:
   - Now (default)
   - When

   If you select the **When** option, enter the date and time when you want the deployment task to initiate. Click **OK** to initiate or schedule the deployment task.

Post upgrade considerations

Querying the Change Auditor database directly is not supported

Querying the database directly is not supported. Any 5.x scripts previously created to manipulate the 5.x (or earlier) events do not work with Change Auditor 7.0 and later.

Data gateway service

The Data Gateway Service is no longer used in Change Auditor for capturing user logon activity events. If you had an earlier version of this service running, you can remove it.

Active Roles integration

If the Active Roles scripting module has been deployed in a previous Change Auditor version, refer to the following knowledge base article which details the process to move to the updated version of these scripting modules that are available in Change Auditor 6.x: https://support.quest.com/change-auditor/kb?k=119136

Exchange Online auditing templates

When you upgrade the client and coordinator from Change Auditor version 6.8 or earlier:

- Previously created Exchange Online auditing templates are deleted from the database and no longer display in the client.

- Agents previously assigned to audit Exchange Online stop auditing the tenant.

NOTE: You can still search and report on previously captured events. All legacy events are shown in the Microsoft 365 subsystem, or Microsoft 365 Exchange Online Mailbox and Microsoft 365 Exchange Online Administration facilities.

To capture new events and avoid losing any audited activities after an upgrade:

1. Upgrade an existing agent to the latest version.
2. Create an Microsoft 365 auditing template.

Microsoft Entra ID and Microsoft 365 auditing templates

As of Change Auditor version 7.0.4, additional Microsoft Graph API permissions are required to audit Microsoft Entra ID and Microsoft 365. If you are updating from version 7.0.3 or older see Updating Microsoft Entra ID templates in the Microsoft 365 and Microsoft Entra ID User Guide.

7

Installation Notes and Best Practices

This section contains notes and best practices that should be considered when installing Change Auditor. These notes and best practices are listed under the following topics:

- Licensing Change Auditor products
- Permissions
- Other installation notes
- Change Auditor for Windows File Servers
- Change Auditor for Exchange
- Change Auditor for Authentication Services
- Change Auditor for SharePoint
- Backup notes
- Agent behavior notes
- Client notes
- ADAM (AD LDS) auditing
- Change Auditor for SQL Server — SQL auditing

Licensing Change Auditor products

Upgrading Change Auditor

You can upgrade from the following versions of Change Auditor: 6.x and 7.x.

NOTE: As of Change Auditor 7.0 a new license is required for all modules.

Applying licenses for multiple Change Auditor products

The following Change Auditor products all require separate licenses which can be applied during the coordinator installation process:

- Change Auditor for Active Directory
- Change Auditor for Exchange
- Change Auditor for Windows File Servers
- Change Auditor for SQL Server
- Change Auditor for Active Directory Queries

- Change Auditor for EMC
- Change Auditor for NetApp
- Change Auditor for SharePoint
- Change Auditor for Logon Activity User (captures login activity on monitored server agents)
- Change Auditor for Logon Activity Workstation (captures login activity on monitored workstation agents)

NOTE: Change Auditor now has a Change Auditor Government Cloud license available that enables the creation of Microsoft Entra ID and Microsoft 365 auditing templates specifically for GCC and GCC High tenants. However, it does not include auditing capabilities on its own. To audit specific services, you must also have the appropriate Change Auditor license types:

- Entra ID directory auditing requires the Change Auditor for Active Directory license.
- Entra ID sign-on and risk auditing requires the Change Auditor for Logon Activity User license.
- Microsoft 365 Exchange Online auditing requires the Change Auditor for Exchange license.
- Microsoft 365 SharePoint Online and OneDrive auditing requires the Change Auditor for SharePoint license.

If you are licensing multiple Change Auditor products, you can apply the licenses in any order but must apply all the licenses provided.

Applying licenses after initial installation

If you purchased more Change Auditor products after the initial installation, you can apply new licenses from the coordinator icon in the system tray.

1. Right-click the coordinator icon in the system tray and select **Licensing**.
2. From the **Licenses** tab, click **Select License**.
3. Locate and apply the new product licenses.

   The new licenses are applied once the configuration is updated.

Permissions

Coordinator required permissions

User account performing the coordinator installation:

The user account installing the coordinator needs permission to perform the following tasks on the target server:

- Windows permissions to create and modify registry values.
- Windows administrative permissions to install software and stop/start services.

The user account performing the installation, must be a member of the **Domain Admins** group in the domain where the coordinator is being installed.

Service account running the coordinator service (LocalSystem by default):

- Active Directory permissions to create and modify SCP (Service Connection Point) objects under the computer object running a coordinator.
- Local Administrator permissions on the coordinator server.

By default, the Coordinator service runs as LocalSystem. To run the Change Auditor service as a Domain User or service account other than Local System, the Change Auditor SPN (Service Connection Point) must be removed from the Coordinator computer (local system) account and added to the Domain Account used to run the Coordinator service.

To do so, open a command prompt on a Domain Controller and perform the following:

1 Remove the SPN from the computer object by entering:

   setspn -D NPRepository4(INSTALLATION_NAME)/SERVER.DOMAIN.TLD SERVERNAME

2 Add the SPN to the service account by entering:

   setspn -A NPRepository4(INSTALLATION_NAME)/SERVER.DOMAIN.TLD USERNAME

   INSTALLATION_NAME = Change Auditor Installation (Default name is DEFAULT)

   SERVER.DOMAIN.TLD = FQDN of the coordinator server

   SERVERNAME = Short name of the coordinator server

   USERNAME = SAM account name of the service account

3 Update the Coordinator service to run under the user name context in question.

4 Restart the Coordinator service.

SQL Server database access account specified during installation:

An account must be created to be used by the coordinator service on an ongoing basis for access to the SQL Server database. This account must have a **SQL Login** and be assigned the following SQL permissions:

- Must be assigned the **db_owner** role on the Change Auditor database
- Must be assigned the SQL Server role of **dbcreator**

Required permissions for deploying agents

The Agent Deployment wizard runs under the security context of the currently logged on user account. Therefore, you must have administrative authority to install software on every target machine. This means you must be a **Domain Admin** in every domain that contains servers that you are targeting for installation.

If you are targeting domain controllers only, membership in the **Enterprise Admins** group will grant you authority to all domain controllers in the forest.

All users responsible for deploying agents must also be a member of the ChangeAuditor Administrators group in the specified Change Auditor installation. If you are not a member of this security group for this installation, you will get an access denied error.

Required permissions to deploy agents using the Windows Installer (MSIEXEC.exe)

The user account used to install the agent by running the Windows Installer directly on the domain controller or member server or workgroup server or workstation needs permissions to perform the following tasks on the server:

- Windows permissions to create and modify registry values.
- Windows administrative permissions to install software and start or stop services.

Other installation notes

Stopping MMC modules

Certain MMC modules disrupt or hinder the addition or removal of services, therefore, MMC modules can not be running (directly on the server or in a Terminal Services session) when installing or uninstalling Change Auditor. Stop the MMC files before installing or uninstalling Change Auditor.

Event Log Viewers in Windows 2008 (and higher) environments

Before installing or upgrading the coordinators or server agents, Quest recommends to close all Event Log Viewers. If a user has an Event Viewer open and opens a Change Auditor event log to load and display a message, the Windows EventLog locks the event message DLL which can cause the Windows Installer Restart Manager to restart dependent services.

Microsoft .NET framework

- Microsoft .NET 4.8 framework is required in the Change Auditor coordinator.
- Microsoft .NET 4.8 framework is required in the Change Auditor clients.
- Microsoft .NET 4.8 framework is required for agents (server and workstation).

If you try to install these components on a computer with an earlier version, the installation fails and you are notified that a newer version is required. To verify that you are running the appropriate version of Microsoft's .NET framework, use Add or Remove Programs.

Component installation order

Quest recommends installing the Change Auditor components in the following order:

- Database (SQL Server) - Make sure the SQL server you are going to use is available and the installation account has SQL Server role as dbcreator. If you want to host the Change Auditor database on a SQL instance other than the default instance of the selected SQL Server, create the new instance before running the installer.

  NOTE: The database name must not include embedded spaces, special characters, or supplementary characters are also not allowed. For more details, see Microsoft's database identifier documentation.

- Coordinator - Install the coordinator. When prompted, specify the SQL server you are going to use and the installation account. The Change Auditor database is created remotely on this server during the installation.
- Client - Once you have confirmed that the coordinator is functioning correctly, install the client.

  TIP: Quest recommends that you install the first coordinator and client, but do not deploy agents until after you have installed all of the additional coordinators required. When deploying agents you can select which installation is to be used for each of the agents.

  NOTE: During the coordinator installation, you can add the current user to the ChangeAuditor Administrators security group. If you selected not to add the current user during the installation process or want to add additional user accounts to the Change Auditor security groups, you need to add them prior to launching the Change Auditor client. Quest also recommends that you then add these security groups to the appropriate SQL database role (i.e., ChangeAuditor Administrators - <*InstallationName*> group to the ChangeAuditor_Administrators role and ChangeAuditor Operators - <InstallationName> group to the ChangeAuditor_Operators role). See Add Users to Change Auditor Security Groups in the Change Auditor Installation Guide.

- Agents - Start the client to deploy agents to your domain controllers and member servers. Also, if you have the Change Auditor for Logon Activity Workstation auditing module licensed, deploy agents to the domain workstations to be monitored for logon activity.
- Web-based client — Optionally, install the web client on the IIS web server to allow users access to Change Auditor data through a standard or mobile browser. See the Change Auditor Web Client User Guide for information about installing and using the web client.

Deploying Change Auditor agents

For a complete and comprehensive Active Directory change auditing solution, Quest recommends deploying agents to every server in the forest.

For best results in capturing Group Policy changes, Quest recommends installing an agent on the domain's PDC operations master role holder.

Security groups

During the coordinator installation, three installation-specific security groups are created in the domain where the member server hosting a coordinator resides.

- **ChangeAuditor Administrators — <*InstallationName*> Group** — provides access to all aspects of Change Auditor and to roll out Change Auditor agents.
- **ChangeAuditor Operators — <*InstallationName*> Group** — provides access to Change Auditor except for making configuration changes.
- **ChangeAuditor Web Shared Overview Users — <*InstallationName*> Group** — provides access to the Change Auditor web client shared overviews, while restricting access to only what has been shared. See the Change Auditor Web Client User Guide for more information about sharing overviews.

Where <*InstallationName*> is a unique name selected during the coordinator installation to isolate your components from any other Change Auditor installation in your Active Directory forest.

Add your user account to either the ChangeAuditor Administrators or ChangeAuditor Operators group before running the client. If multiple coordinators are installed in a mixed mode environment, to connect to each coordinator, add your user account to one of these groups on each of the member servers where a coordinator resides.

In addition, users responsible for deploying agents must also be a member of the ChangeAuditor Administrators group in the specified Change Auditor installation.

During the coordinator installation, you are presented with the option to add the current user to the ChangeAuditor Administrators security group. If you selected not to do this during the coordinator installation process or you want to add more user accounts, add your user account (and any other appropriate user accounts) to one of the Change Auditor security groups before running the client.

See Add Users to Change Auditor Security Groups for more detailed information about the security groups that are created when the coordinator is installed.

NOTE: When the first foreign workstation agent is manually installed, a ChangeAuditor Agents - <*InstallationName*> security group is created. User accounts must be added to this security group to properly authenticate.

Change Auditor for Windows File Servers

Change Auditor for Windows File Server agents may fail to provide origin information if remote users are already connected when the agent is initialized or started. Therefore, it is suggested that you restart the server as soon as possible after an agent installation or upgrade.

Change Auditor for Exchange

Agent deployment

High volume Exchange Servers. Agent processing of large Exchange auditing and protection configurations may slow down initial user login access or cause timeouts if many user logins are occurring at the same time. To avoid this issue, Quest recommends that the following actions be performed during maintenance intervals or other periods of low user mailbox activity:

- Change Auditor Exchange agent deployment
- Change Auditor Exchange agent upgrade
- Change Auditor Exchange Mailbox auditing or protection configuration changes

Before the system returns to a normal load, one user should log in to Outlook Web Access (OWA), Outlook, and Exchange Web Services (EWS, Outlook for Mac) clients. This triggers the Change Auditor agent to process Exchange Mailbox auditing and protection configuration changes when the fewest logins are occurring.

Exchange 2016. Exchange 2016 stores its configuration data in Active Directory, and installing Change Auditor agents on the domain controller captures all these change actions. However, Microsoft changed how they process configuration changes. Therefore, in order for Change Auditor for Exchange to retrieve the correct 'who' information for these Active Directory based events it now audits Windows PowerShell. So you can:

- Deploy an agent to all Active Directory domain controllers in the forest. However, the 'who' value is missing (reported as the Exchange server computer account) from all the Exchange 2016 Active Directory based events.
- Depending on the Exchange version you are running, deploy an agent to Exchange servers as described below. This captures the correct 'who' value for many of the Exchange 2016 Active Directory based events, but not all Exchange 2016 events are being audited in this scenario.
    - **Exchange 2016:** Deploy an agent to all Exchange 2016 servers with the Mailbox role.
- **Recommended:** Deploy an agent to all Active Directory domain controllers and to all required Exchange servers. However, duplicate events are generated for Exchange Active Directory events: one from the agent auditing attribute changes on a domain controller (contains no 'who' value) and one from the new agent auditing PowerShell on an Exchange server (contains the correct 'who' value).

To capture Exchange mailbox access events:

- **Exchange 2016:** Deploy an agent to all Exchange 2016 Mailbox role servers.

Deploy agents to all Exchange Servers. When a Change Auditor 5.6 (or higher) agent is deployed on Exchange Server, it automatically enables the scripting extension in Active Directory. This is a forest-wide setting and applies to all Exchange servers in the Exchange organization. This extension requires that the ScriptingAgentConfig.xml file be present in the Exchange Server folder; otherwise, Exchange management tools display error messages each time the Scripting Agent cmdlet runs. The Change Auditor 5.6 (or higher) agent automatically creates the required ScriptingAgentConfig.xml file in the Exchange Server folder if one is not already present. Therefore, it is highly recommended that an agent be installed on all Exchange servers to ensure that all servers are using the same scripting agent.

> **NOTE:** If the scripting agent was not enabled on your Exchange servers before deploying agents, you should perform backups of your Exchange servers in accordance with your company's disaster recovery plan once you have successfully deployed agents to all your Exchange servers.
>
> If you need to restore your Exchange servers and they were NOT backed up after you deployed agents that enabled the scripting agent, you will need to disable the CmdletExtensionAgent BEFORE recovering your Exchange 2016 servers.

If Change Auditor cannot be installed on all your Exchange servers, use the following procedure on all Exchange servers where an agent is not yet deployed:

1 Create an empty ScriptingAgentConfig.xml file under the following directory:

%ProgramFiles%\Microsoft\Exchange Server\V14\Bin\CmdletExtensionAgents\

Enter the following text into this ScriptingAgentConfig.xml file:

```
<?xml version="1.0" encoding="utf-8"?>
<Configuration version="1.0"/>
```

2 Save and close the file.

Exchange cluster node servers. When deploying or upgrading agents on Exchange cluster node servers, use the following recommended procedure:

1 Deploy or upgrade the agent on the passive Exchange cluster nodes.

2 Perform a scheduled fail-over on the active cluster nodes.

3 Then deploy or upgrade the agent on the newly passive cluster nodes.

If you find the need to deploy or upgrade an agent on an active cluster node, schedule the deployment during low-utilization periods. A visual check of the server utilization to ensure that utilization is below 20% should be sufficient.

Exchange 2003, 2007, and 2010 — Not supported

Exchange 2003, 2007, and 2010 are no longer supported. For supported versions, see the Change Auditor Release Notes.

SMTP authentications and alerts on Exchange

Exchange denies authentication to all well-known accounts, including 'Administrator'. Use Hub Transport servers to allow SMTP email to go through. This references the setting for **My Server Requires Authentication** on the SMTP Configuration pane on the Coordinator Configuration page (Administration Tasks tab) in the Change Auditor client. It may also be necessary to configure more Transport settings (authentication and permissions) to allow email relay from the Change Auditor coordinator machine to receive SMTP alerts.

Microsoft Outlook 2000 and 2002 — Not supported

Change Auditor for Exchange does not support Microsoft Outlook 2000 or 2002.

Change Auditor Exchange Server monitoring and Outlook cached mode

For improved performance, Outlook offers an option to 'cache' requests to Exchange Server. This option is enabled by default when you configure an email account for Exchange Server. To disable this setting, select the Outlook **Tools | Account Settings** menu command, open the E-mail tab and click **Change**, and then clear the **Use Cached Exchange Mode** check box on the Microsoft Exchange Settings dialog.

While Change Auditor Exchange monitoring events closely track user input in non-cached Outlook and Outlook Web Access clients, this is not the case with cached-mode Outlook.

User activity in cached-mode Outlook can provide complex results with Change Auditor Exchange monitoring; the timing and order of Exchange requests is not obvious or intuitive.

A few of the effects you will see when monitoring an Outlook cached connection to Exchange Server include:

- Cached-mode Outlook frequently defers message copy, move and delete requests until seconds or even minutes later.
- When opening cached-mode Outlook, several folders may be 'opened' at the same time. Outlook examines all folders with recent changes at startup.

- When opening cached-mode Outlook or selecting a different mail folder, several message read events may occur at the same time. Outlook reads all new Inbox messages as they become available (independent of user activity) and then keeps local copies for reading.
- When opening messages that have previously been read (or selecting messages with the preview pane enabled) you will not see a 'message read' event. Since cached-mode Outlook keeps local copies of the messages they never need to be read from the server again, even after closing and re-starting Outlook. The original read from the server does produce a 'message read' event.
- When deleting messages (moving them to the Deleted Items folder), instead of 'message deleted and moved to the Deleted Items folder' events as in non-cached mode you will receive two events: 'message created' in the Deleted Items folder, and 'message permanently deleted' in the original folder. This is an accurate report of how cached-mode Outlook implements message deletions to the Deleted Items folder.
- When permanently deleting messages (emptying the Deleted Items folder) you will see a 'message read' event as cached-mode Outlook obtains information from the message followed somewhat later by a 'message permanently deleted' event.
- If the user closes cached-mode Outlook before it has a chance to synchronize permanently deleted items with the Exchange Server, it will do so the next time Outlook is started. Other clients viewing the mailbox will be able to access the 'deleted' items until cached-mode Outlook synchronizes with the server.

You will still receive all notifications of critical non-owner events from cached-mode Outlook clients, but the timing and sequence may not be obvious. Understanding the effect that cached-mode Outlook has on your Change Auditor Exchange monitoring will give you confidence that the results you are seeing are accurate.

Change Auditor for Authentication Services

Agent deployment

Change Auditor for Authentication Services requires agents deployed on all Active Directory domain controllers in the forest to capture modifications to the Authentication Services configuration container.

Change Auditor for SharePoint

The Microsoft SharePoint requirements must be met. Change Auditor for SharePoint does not need any additional requirements.

See the Change Auditor for SharePoint User Guide for information about installing, configuring, and using Change Auditor for SharePoint.

Agent deployment

You need deploy an agent on one of the SharePoint servers in the SharePoint farm that you want to monitor.

Required rights and permissions

The agent selected to connect to and collect events from the SharePoint farm must have the following permissions:

- At a minimum, the account must have full access to all SharePoint sites. It must also have read permissions on all SharePoint SQL databases.

- **Recommended:** Use the SharePoint farm administrator account that was supplied when SharePoint was installed.

For proper auditing of the sites within the MySite Site Collection or Web Application, add the account Change Auditor uses to access the SharePoint database as a Site Collection Administrator (primary or secondary) or to the User Web Policy for the MySite host. Depending on how your MySite host is initially set up, use the Central Administration website to verify, and if necessary add, this account.

SharePoint settings

For Change Auditor to capture some of the SharePoint events, the following settings must be enabled:

- **Native Auditing** enabled for all SharePoint web applications (including each user site under MySite)Change Auditor

  NOTE: Log trimming is off by default. Enable log trimming to meet your policies. If the Change Auditor agent is offline or is otherwise unable to retrieve event information from the SharePoint database for a period longer than the trim period, events could be lost.

- **Versioning** enabled for each individual Library and List Item pertaining to the Sites, if you want Change Auditor to capture versioning activities.

See the Change Auditor for SharePoint User Guide or Event Reference Guide for a list of the events that require these additional settings.

Backup notes

Backup and protect the coordinator database

The coordinator uses Microsoft SQL Server as the main database for collecting and reporting audit information. This data must be protected and backed up regularly, acceptable to your data retention policies. There are several third-party tools available, including Microsoft's SQL Tools, which provide backup and restore functions.

Exclude the local agent directory and files from your backup

The agent uses a SQLCE database file (ChangeAuditorAgent.sdf) on the local drive of each agented DC/member server. This database is primarily used to capture the state values for Active Directory® objects, File System values, and Windows registry changes. The agent files are not required as part of the backup job since the data contained in the database files can be recreated upon agent installation. Quest recommends that you exclude the agent files (%ProgramFiles%\Quest\ChangeAuditor\Agent\DBScripts) from your backup solution.

Agent behavior notes

Agent connection behavior

When an agent comes online, it queries the Active Directory Catalog (GC) for a list of all coordinator SCPs within its same installation to determine which to connect to.

When there are available coordinators within the agent's site, the agent connects to all coordinators in the site. When there are no coordinators running within the agent's site, the agent connects to any online coordinator. However, when coordinators within the site come back online, the agent switches to connect to just the

coordinators within the same site and drop nonsite coordinator connections. If this behavior is problematic for your environment, contact Quest Technical Support to discuss possible configuration options.

The connection behavior after these initial steps depends on the type of agent:

- **Change Auditor server agents**: Starting with Change Auditor 6.0, server agents submit events to all coordinators in the site and load balancing occurs automatically. All connected coordinators can then participate in receiving events from the server agent, allowing a high volume of events to be distributed for processing.
- **Change Auditor workstation agents**: The workstation agents randomly connect to a single coordinator. This enables 'scaling out' options for large workstation agent deployments within a single site.

NOTE: A maximum of 10,000 agents (server and workstation) can connect to a single coordinator. If this connection limit is problematic for your environment, contact Quest Technical Support to discuss possible configuration options.

Incompatibility with Symantec Backup Exec CPS agent

Junction point creation may fail on a server where both a Symantec™ Backup Exec™ CPS agent and a Change Auditor agent are running. To resolve the problem, upgrade the CPS agent to 12.5 or later.

Client notes

Disabled audit events

Some events are disabled by default to improve the initial deployment process and reduce the amount of audited event information initially collected. These audited events can easily be enabled on the Audited Events page of the Administration Tasks tab.

See the online help or appropriate Event Reference Guide for a list of the events that are disabled by default.

Enabling encrypted SQL Server connections

By default, connections to a SQL Server are not encrypted; however to encrypt all data transmitted between an application computer and a computer running a SQL Server instance, you can use the Secure Sockets Layer (SSL). For more details on configuring client network protocols, see the following Microsoft article: http://msdn2.microsoft.com/en-us/library/ms190425.aspx

ADAM (AD LDS) auditing

Monitoring ADAM (AD LDS) instances on workgroup servers

Run the appropriate Change Auditor Agent.msi file on the workgroup server to install an agent to monitor ADAM (AD LDS) instances on nondomain servers. See Install an agent to audit ADAM (AD LDS) on workgroup servers for more information.

Change Auditor for SQL Server — SQL auditing

Auditing events on SQL Server

Due to a Microsoft hotfix, agents do not capture SQL-related events unless the following action is taken on the SQL Server:

- Using SQL Server Configuration Manager, add a startup parameter called '-T1906' on the **Startup Parameters** tab in the SQL Server Properties dialog.
- Restart the SQL Server service.

SQL Server auditing for Itanium platform — Not supported

Auditing of SQL Servers running on Itanium platforms is not supported.

8

Deployment Options

Change Auditor can be configured to audit and report on one or many Active Directory forests to facilitate searching for compliance audit data. There are two deployment options available to you:

- Multi-forest deployment which requires at least one coordinator in each monitored forest. This option provides full auditing support.
- Foreign forest deployment with agents running on a domain-joined server, domain controller, or workstation connected to coordinators in a foreign Active Directory forest. This option allows for improved centralization of agent management while providing most core Change Auditor functionality. For details on the level of support, see Supported functionality.

The following section outlines the support, requirements, recommendations and steps for deploying agents, and example deployments for these deployment options:

- Multi-forest deployment
- Foreign forest agent deployment

Multi-forest deployment

- Requirements
- Example deployment scenario
- Configuration

Requirements

The following must be in place for multi-forest deployments:

- Network connectivity between each monitored forest.

  Coordinators in all forests connect directly to the SQL server that is hosting the Change Auditor audit database.

  Coordinators must resolve the host name of the SQL server or must be configured to use the IP address of the SQL server.

- At least one coordinator deployed in each forest.

  The coordinator collects and maintains the topology information for each forest. This includes domains, sites, domain controllers, and member servers. The coordinator is also responsible for:

  - Sending alerts by email, SMNP, or WMI
  - Sending agent configuration settings, auditing and protection templates
  - License enforcement
  - Agent status updates
  - Agent installation and upgrade
  - Auto deployment

- Event statistics
- Group membership expansion

- Change Auditor groups created in each forest.

  To connect to coordinators in other forests, users must be added to either the 'ChangeAuditor Administrators — <*InstallationName*>' OR 'ChangeAuditor Operators — <*InstallationName*>' in the forest where the coordinator is joined.

- Credentials for the Microsoft SQL server backend.

  Depending on whether the Active Directory forests have a trust in place, you need to configure Change Auditor to use the appropriate SQL credentials.

  Scenario A — One or more of the forests do not have a valid trust in place.

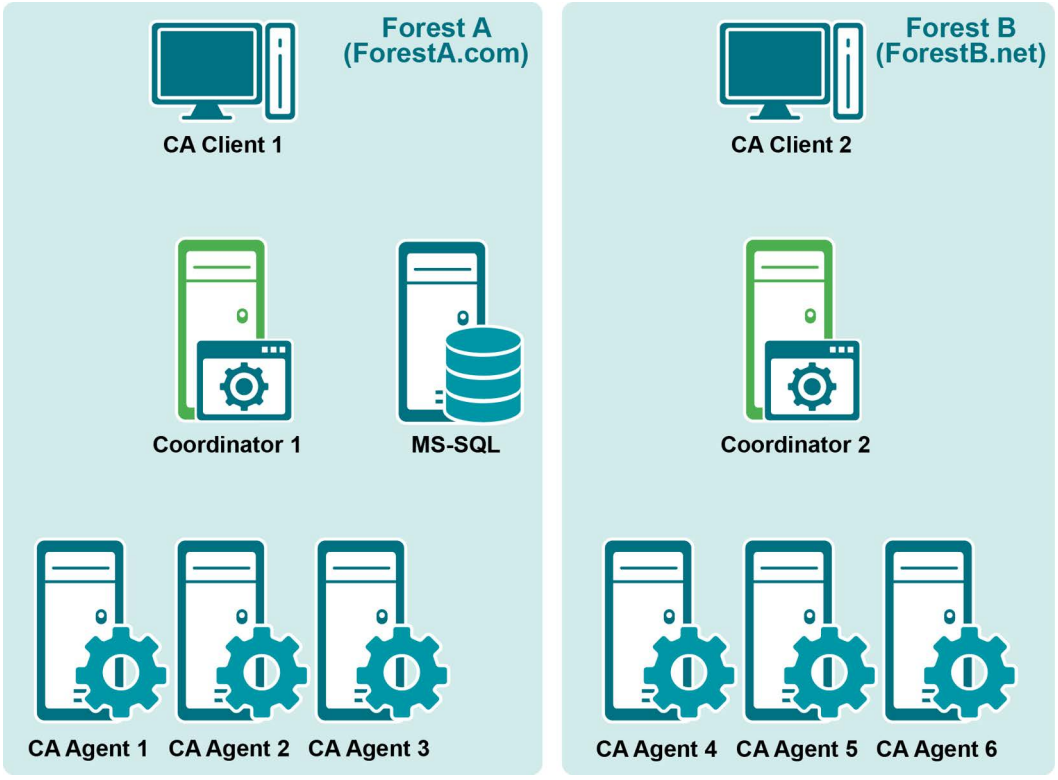
  The coordinator that is not part of the same forest where the SQL server is joined to, must be configured to use a SQL user account or a Domain Account from the forest where the SQL server resides.

  Scenario B — All forests have a valid trust in place.

  Each of the coordinators may be configured to use either authentication type. Both Windows or SQL user accounts may be used in each of the forests.

Example deployment scenario

The following diagram shows two separate forests where Change Auditor will be deployed. Forest A is deployed first and the Forest B is added.



Forest A installation

1. Install the coordinator on a member server in Forest A. In this example, Coordinator1.ForestA.com is used as the coordinator server.

- While installing the first coordinator, make note of the “Installation name”. The same installation name is used to deploy the coordinator in Forest B (ForestB.net).
- Also take note of the SQL Server host and credential information. This server and account will also be used in the second forest. The required information is as follows:
  - SQL Server host name or IP address AND Instance name if applicable
  - Database or Catalog name
  - User name, password, and domain if applicable

2 Install the client on either a workstation or member server. In this example, CAClient1.ForestA.com is used as the client computer.

3 Using the client, connect to the coordinator in Forest A to deploy Change Auditor agents on to the domain controllers and/or member servers in Forest A. See Deploy Change Auditor Agents for more details about deploying agents.

4 At this point, Change Auditor should be fully deployed to the first forest in the organization (ForestA.com in this example).

Forest B installation

5 Install the coordinator on a member server in Forest B. In this example, Coordinator2.ForestB.net is used as the coordinator server.

- While installing the second coordinator, you must use the ‘Installation name’ that was selected in the first forest.
- During the installation of the second coordinator, use the same SQL server and database name used in the first coordinator’s installation. The Windows or SQL user account may be different than the account used in the first installation.
- Quest recommends that the same database access account used in the first forest is also used in the second forest. If a different user account for database access is used in the second coordinator's installation, the following permissions must be granted before the installation is started:
  - **db_owner** database role on the Change Auditor database
  - **dbcreator** server role

6 Install the client on either a workstation or member server. In this example, CAClient2.ForestB.net is used as the client computer.

7 Using any client, connect to the coordinator in Forest B to deploy agents on to the domain controllers and/or member servers in Forest B.

8 Change Auditor is now fully configured to collect audit data from both forests into a single database. Reports and alerts can be run from any client to return data related to one or all the deployed forests.

9 You can deploy more forests by following steps 5 through 8.

Configuration

- Audit and protection configuration flow
- Event flow
- Reports and queries from the client

Audit and protection configuration flow

Audit and protection configurations are maintained using the client that is installed on either workstations or member servers. Configuration changes are stored in the SQL database by the coordinator service.

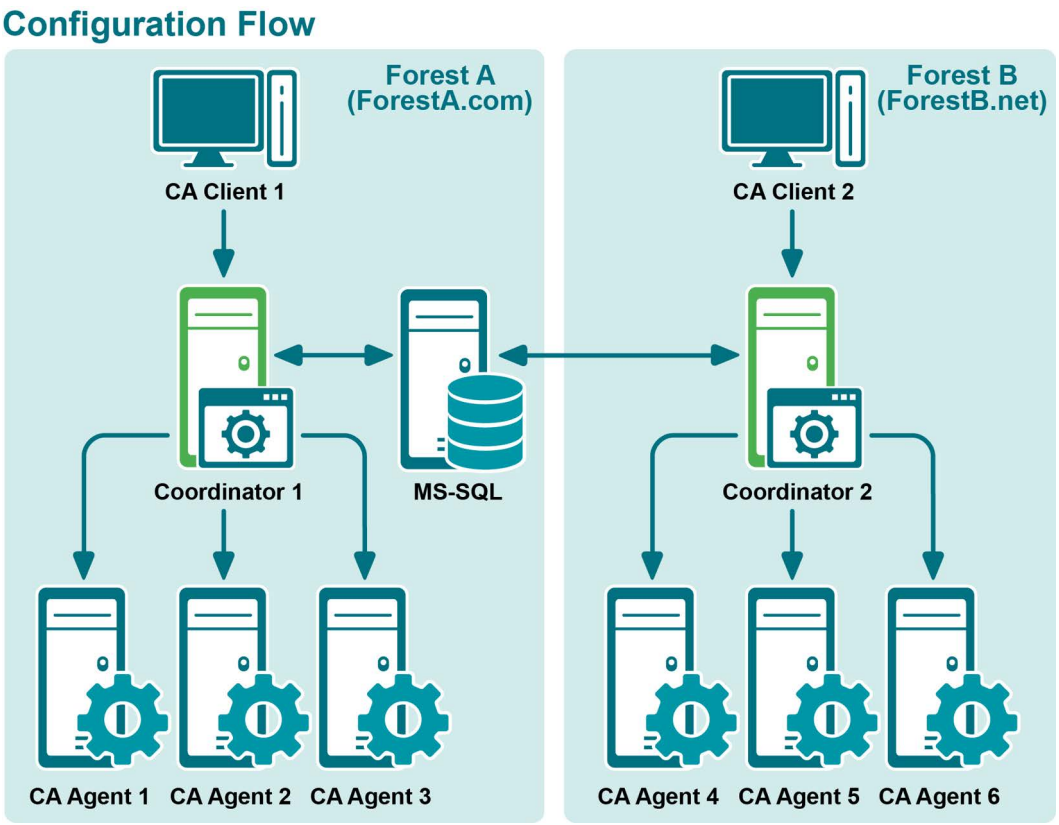
The following configurations can be shared across forests regardless of the forest trust level:

- Active Directory Auditing — Object Class\Attributes
- ADAM\AD (LDS) Auditing — Object Class\Attributes
- Excluded Accounts templates
- File System Auditing templates
- Registry Auditing templates
- Service Auditing templates
- SQL Auditing templates
- Audit Event configurations (for example, enabled or disabled, severity level)

The following configurations can be shared when a two-way trust exists:

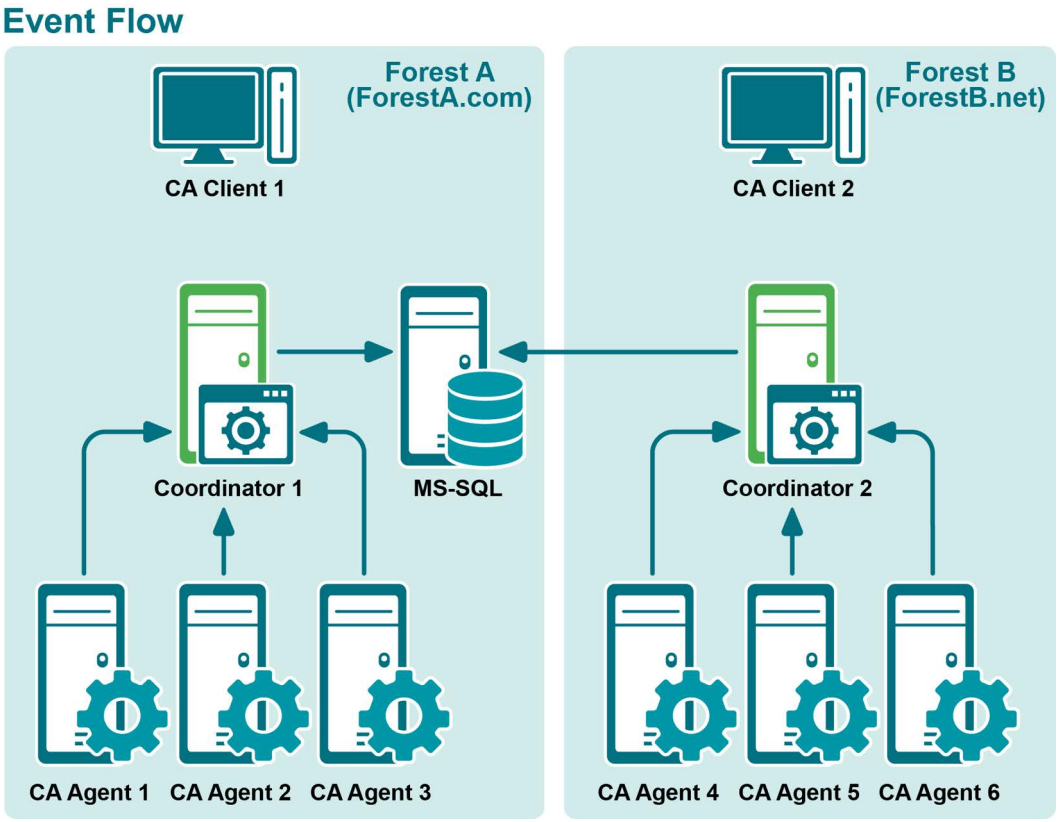
- Active Directory Protection templates
- ADAM\AD (LDS) Protection templates
- Exchange Protection templates
- File System Protection templates
- Group Policy Protection templates

NOTE: A trust is required to view the Active Directory accounts in the other forest for protection account exclusions.



Event flow

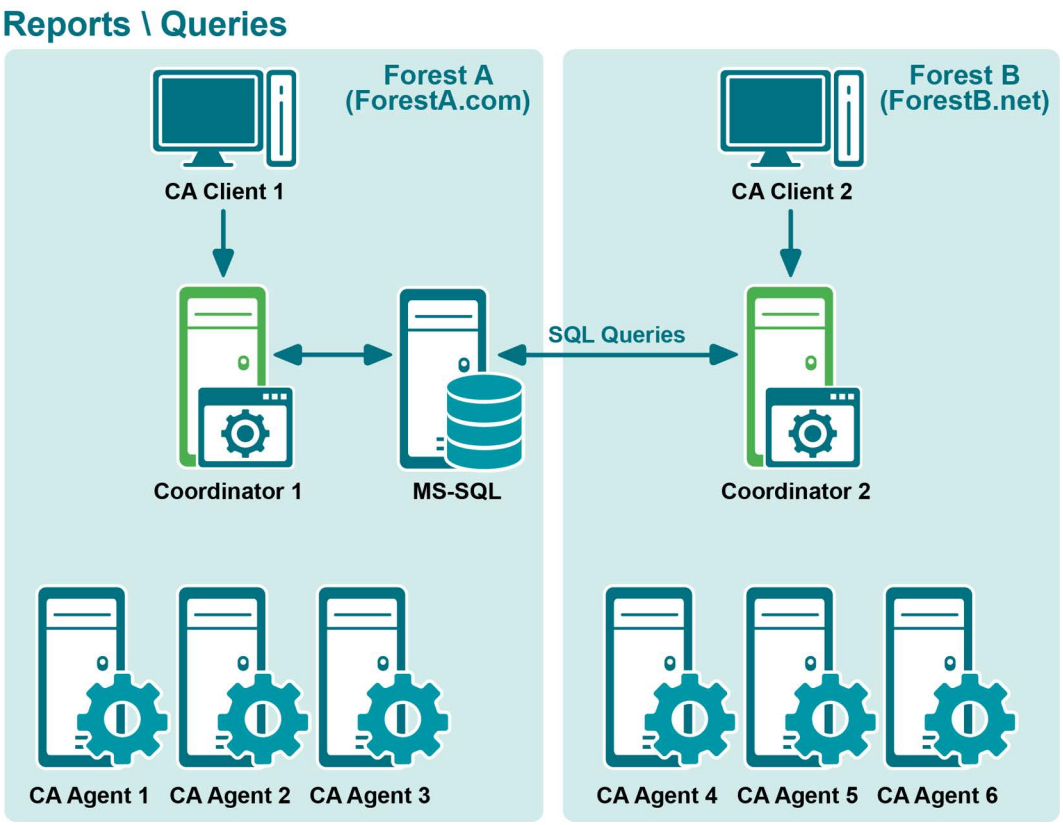
Recorded audit events are first queued in a local database on each agent computer. Events are then batched and forwarded to a coordinator. The coordinator checks for new events every 10 seconds and does a bulk insert of the event details to the SQL database.



Reports and queries from the client

Change Auditor clients do not connect directly to the SQL database. Instead, the coordinator to which the client is connected processes search results and change requests. Clients can connect to any coordinator if the logged on user is a member of either the ChangeAuditor Administrators — <*InstallationName*> or the ChangeAuditor Operators — <*InstallationName*> group in the respective forest.

By default, user-configured alerts (SMTP, SNMP, and WMI) are generated and sent from the first installed coordinator in the Change Auditor installation.



Foreign forest agent deployment

- Supported functionality
- Requirements
- Workflow
- Harvesting the foreign forest topology
- Deploying agents to a foreign forest
- Installing agents in a foreign forest
- Example deployment scenario

Supported functionality

The support available for agents connected to a foreign forest includes the following:

Table 5. Foreign forest support

Functionality	Supported features

Auditing	• Directory auditing:
	  ▪ GPO
	  ▪ Active Directory objects and attributes
	  ▪ AD Query
	  ▪ ADAM
	• Logon Activity
	• Windows File System

Protection	• Windows File System • Active Directory • Group Policy Objects • Exchange mailboxes

Requirements

- Network connectivity between the foreign server and coordinators in the remote forest.
- A routable network path between the foreign forest computer and the coordinator servers.
- Name resolution of domain controllers and the coordinator servers from the foreign forest server. This is required regardless of whether DNS server configuration, NetBIOS/WINS configuration or local hosts file entries are used.
- Ensure that the account you are using to deploy agents is at least a **Domain Admin** in every domain that contains servers or workstations where agents will be deployed.

Workflow

- Harvest the foreign forest topology. See Harvesting the foreign forest topology.
- Deploy an agent in a foreign forest.

  You can deploy agents either by installing agents on the required computers or using the deployment option in the Change Auditor client. See Installing agents in a foreign forest and Deploying agents to a foreign forest for details).

  NOTE:
  - If the agent fails to connect to the coordinator, check the network connection, ensure that the coordinator name can be resolved, the group "ChangeAuditor Agents - <InstallationName>" is created in the domain where the coordinator is located, and the account has been added.
  - You may need to pre-stage\create the "ChangeAuditor Agents – <InstallationName>" domain local security group and manually add the configured user account to the security group in additional domains within the forest where coordinators reside.
- Create any auditing templates as required and assign to the agent.
- Events will be audited by the agent and displayed in the client once they are collected.

Harvesting the foreign forest topology

1 From the Change Auditor client, select the **Deployment** tab.

2 Click **Foreign Forest** to open the Foreign Forest Credentials dialog where you will provide the foreign forest DNS name and credentials required to collect the foreign forest topology.

3 Click **Add** to enter the credentials of a user with administrator rights on the selected domain and the required forest, and click **OK**.

4 Click **Force Refresh** to populate the available servers or workstations in the forest.

Deploying agents to a foreign forest

NOTE: When deploying agents using remote deployment from the Deployment tab, the LDAP Authentication option for the deployed agent will be set according to the current LDAP Authentication setting of the connected coordinator.

To deploy agents to a foreign forest from the client:

1 From the Change Auditor client, select the **Deployment** tab.

The Deployment page is populated with the servers (domain controllers and member servers) and workstations in your Active Directory environment.

NOTE: The Deployment page may initially be empty until the current forest's server topology has completed. The topology scan takes a long time when the environment contains many workstations. This page is automatically refreshed after this task has completed.

2 From this list, select an entry and select **Credentials | Set** to enter the proper user credentials for installing agents on the selected domain.

NOTE: If you are using a group Managed Service Account, see Using group Managed Service Accounts (gMSA) for additional requirements.

3 Select one or more servers or workstations on the Deployment page and click **Install or Upgrade**.

4 On the Install or Upgrade dialog select one of the following options to schedule the deployment task:

- Now (default)
- When

If you select the **When** option, enter the date and time when you want the deployment task to initiate. Click **OK** to initiate or schedule the deployment task.

5 Enter the Active Directory credential information to allow the agent to connect to the coordinator in the remote forest, and click **OK**.

- Coordinator Root Domain Name (example.com): Enter the coordinator forest root domain name and an account to be used by the agent to connect to the coordinator.
- Account Name (example.com\user): Enter the name of the user that can find and connect to a coordinator in the Active Directory forest.
- Account Password: Enter the password associated with the specified account.
- Account Type: Select the account type of the specified account.

NOTE: If you are using a group Managed Service Account, see Using group Managed Service Accounts (gMSA) for additional requirements.

- Add this user to the ChangeAuditor Agents security group: This is selected by default indicating that the specified user account will be added to the ChangeAuditor Agents security group in the supplied

Active Directory domain. User accounts must be added to this security group to properly authenticate.

NOTE: You may need to pre-stage\create the "ChangeAuditor Agents – <InstallationName>" domain local security group and manually add the configured user account to the security group in additional domains within the forest where coordinators reside. If using a group Managed Service Account this step is required and must be performed manually.

You can add the domain user account to the ChangeAuditor Agents – <InstallationName> security group, if appropriate LDAP and network protocol access is available.

Back on the Deployment page, the **Agent Status** column displays 'Pending' and the **When** column displays the date and time specified.

NOTE: To cancel a pending deployment task, select the server or workstation and then click **Install or Upgrade**. On the Install or Upgrade dialog, click **Clear Pending**.

As agents are successfully connected to the coordinator, the corresponding **Deployment Result** cell displays 'Success', the **Agent Status** cell displays 'Active' and a desktop notification displays in the lower right-hand corner of your screen.

NOTE: To deactivate these desktop notifications, select **Action | Agent Notifications**.

Once agents are deployed and you open the client, the Overview page opens and provides a real-time stream of events based on a 'favorite' search definition and other summary information.

Installing agents in a foreign forest

To manually install an agent in a foreign forest:

1. Copy the appropriate agent installer package from the Change Auditor service installation directory to the required computers.
2. Run the installer file to open the Change Auditor Agent Setup wizard which steps you through the installation.
3. Accept the license agreement and click **Next**.
4. Select **This agent connects to a coordinator in a foreign forest**.
5. Enter the Active Directory credential information to locate the Change Auditor Installation and allow the agent to connect to the coordinator in the remote forest.
   - Coordinator Forest Root (example.com): Enter the coordinator forest root domain name and an account to be used by the agent to connect to the coordinator.
   - Account Name (example.com\user): Enter the name of the user that can find and connect to a coordinator in the Active Directory forest.
   - Account Password: Enter the password associated with the specified account.
   - Account Type: Select the account type of the specified account.

     NOTE: If you are using a group Managed Service Account, see Using group Managed Service Accounts (gMSA) for additional requirements.

   - Add this user to the ChangeAuditor Agents security group: This is selected by default indicating that the specified user account will be added to the ChangeAuditor Agents security group in the forest where the coordinator is located. User accounts must be added to this security group to properly authenticate.

     NOTE: You may need to pre-stage\create the "ChangeAuditor Agents – <InstallationName>" domain local security group and manually add the configured user account to the security group in additional domains within the forest where coordinators reside. If using a group Managed Service Account this step is required and must be performed manually.

You can add the domain user account to the ChangeAuditor Agents – <InstallationName> security group, if appropriate LDAP and network protocol access is available.

6 The Installation Name screen prompts you to enter the installation name to identify the database where the coordinator is located. Click **Browse** to select the required installation

7 Choose the destination folder and click **Next**.

8 Specify the authentication method to use to make Active Directory requests.

- Select Simple Authentication and Security Layer (SASL) to use Kerberos or NTLM.
- Select Secure Socket Layer (SSL) to use certificates. See SSL certificate configuration and deployment for more details.

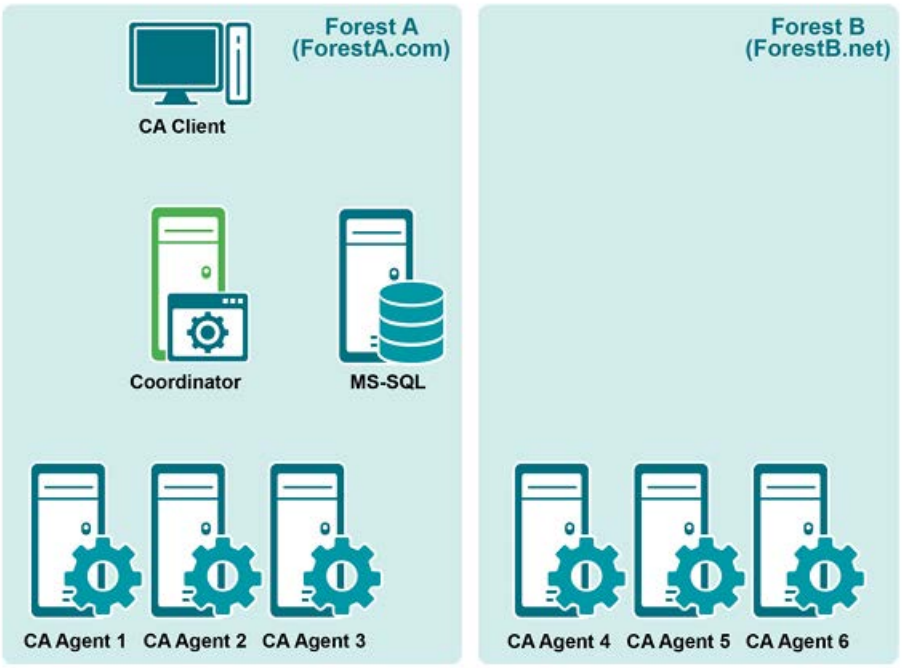
NOTE: When making Active Directory requests, credentials and message content are encrypted for both authentication methods.

9 Click **Next** to begin the installation.

Once the agent starts and connects to coordinator, the foreign forest computers will be available in the Deployment tab.

Example deployment scenario

The following diagram shows two separate forests where Change Auditor will be deployed. Forest A is deployed first and then Forest B is added.



Forest A installation

1. Install the coordinator on a member server in Forest A. In this example, Coordinator.ForestA.com is used as the coordinator server.

   While installing the first coordinator, make note of the “Installation name”. The same installation name is required when deploying agents to Forest B.

2. Install the client on either a workstation or member server. In this example, CAClient1.ForestA.com is used as the client computer.

3. Using the client, connect to the coordinator in Forest A to deploy agents to computers in Forest A. See Deploy Change Auditor Agents for more details about deploying agents.

   At this point, Change Auditor should be fully deployed to the first forest in the organization (ForestA.com in this example).

Forest B installation

Option 1: Deploying agents to a foreign forest through the Change Auditor client

1. Using the client, connect to the coordinator in Forest A.
2. Deploy agents to the required computers in Forest B. (See Deploying agents to a foreign forest for details.)

Option 2: Installing agents manually in a foreign forest

1. Run the appropriate Agent MSI on the required computers in Forest B where the installation is required. The MSI should be launched from an elevated command prompt.
2. When prompted, select the **This agent connects to a coordinator in a foreign forest** option.
3. Enter the Active Directory root domain name of the remote forest where the agent will connect.

4 Enter a domain administrator account for the coordinator domain and click **Next**. Ensure that you use the following format: fully-qualified-domain-name\user.

5 Enter the Installation Name that the agent needs to join and click **Next**.

6 Click **Install.**

The agent will now connect to the coordinator in Forest A and the computer will be available in the Deployment tab of the Change Auditor client.

9

Workstation Agent Deployment

Workstation agents are required to capture login activity events when a Change Auditor for Logon Activity Workstation license is applied. This section provides recommendations for deploying agents necessary for auditing both domain workstations and non-domain workstations. It also includes instructions on manually deploying workstation agents.

- Recommendations and deployment requirements
- Manual workstation agent deployment
- Deploying workgroup agents (non-domain workstations)

Recommendations and deployment requirements

All workstation agents

- See the Release Notes for a full list of the minimum system requirements for workstation agents.
- Quest recommends a phased approach to deploying workstation agents. Deploying a maximum of 100 workstation agents at a time allows you to monitor the coordinator performance before deploying another batch of agents
- When deploying agents using remote deployment from the Deployment tab, the LDAP option for the deployed agent will be set according to the current LDAP setting of the connected coordinator.

Deploying workstation agents (domain workstations)

- The recommended installation is from the Deployment tab of the client. See Change Auditor agents.
- Alternately, you can manually deploy workstation agents. See Manual workstation agent deployment.

Deploying foreign forest workstation agents (domain workstations)

- The recommended installation is from the Deployment tab of the client. See Deploying foreign forest agents.
- Alternately, you can manually deploy workstation agents. See Manual workstation agent deployment.

Manual workstation agent deployment

When installed manually, the workstation agent installer must be run as an account with the local administrator account privileges and with elevated User Account Control (UAC) permissions.

NOTE: Depending on the UAC policies (see User Account Control (UAC) Settings), elevated UAC permissions may require starting the installer using one of the following methods:

- Shift + Right-click installer to select 'Run as a different user'
- From the Windows Task Manager, select File | Run New Task, browse and select the Change Auditor Workstation Agent installer file, and select the 'Create this task with administrative privileges' option, then click OK.

To manually install a workstation agent:

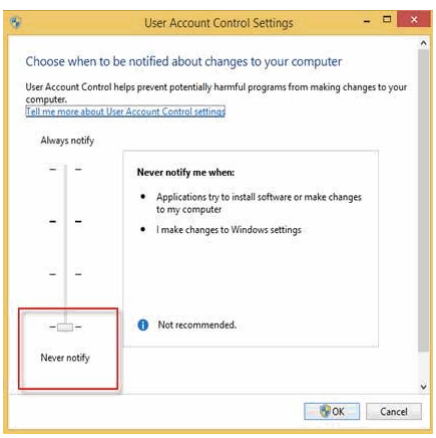
1. Copy the appropriate agent installer package from the Change Auditor service installation directory to the workstation to monitor. The default directory is %ProgramFiles%\Quest\ChangeAuditor\Service\Change Auditor Workstation Agent (x64).msi.
2. Run the installer file on the workstation to open the Workstation Agent Setup wizard which steps you through the installation.
3. If the computer is member of the local forest where coordinator resides, select **This agent connects to a coordinator in the local forest**. If the computer is a workgroup member or member of a foreign forest where no coordinator resides, select **This agent connects to a coordinator in a foreign forest**. For more information see Installing agents in a foreign forest.
4. The Installation Name screen prompts you to enter the installation name to identify the database where the coordinator is located. Click **Browse** to select the required installation.
5. Choose the destination folder and click **Next**.
6. Specify the authentication method to use to make Active Directory requests.
    - Select Simple Authentication and Security Layer (SASL) to use Kerberos or NTLM.
    - Select Secure Socket Layer (SSL) to use certificates. See SSL certificate configuration and deployment for more details.

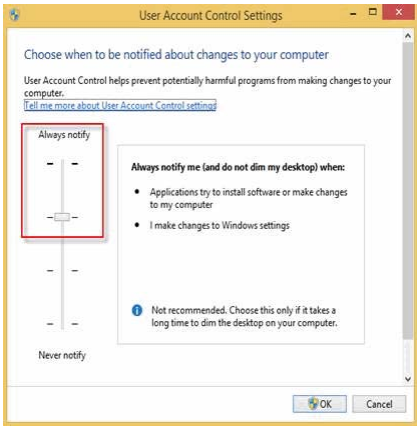
NOTE: When making Active Directory requests, credentials and message content are encrypted for both authentication methods.

7. Click **Next** to begin the installation.

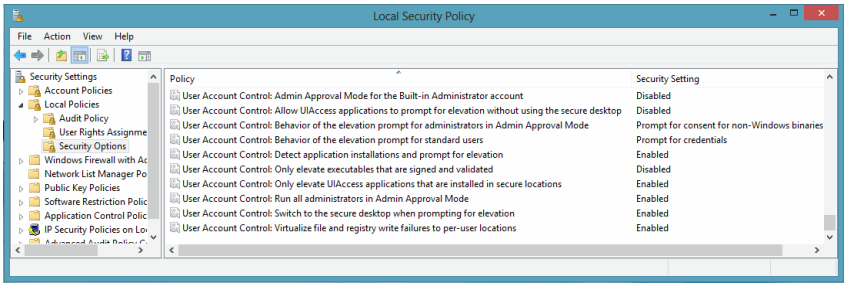
User Account Control (UAC) Settings

- UAC policies typically use different settings for the 'Administrator' account and other accounts with Administrative privileges, so it may be easier to run the Change Auditor Workstation Agent installer with elevated UAC permissions if the Administrator account is used.
- General UAC elevation and prompt level configurations can be accessed through the Control Panel User Access Control configuration.





- More specific UAC policies can be configured in the Local Security Policy or a Group Policy Object (where appropriate) to determine whether all Administrators or the built-in Administrator account are run in Admin Approval Mode, the elevation prompt level, whether the secure desktop is used for prompting, whether elevation is possible without prompting, and so forth.



Deploying workgroup agents (non-domain workstations)

- A workgroup agent requires NetBIOS over TCP enabled and access to the following ports inbound to the domain controllers:
  - UDP port 137 (name services)
  - UDP port 138 (datagram services)
  - TCP port 139 (session services)
- A routable network path must exist between the workgroup computer, domain controllers, and the coordinator servers. Name resolution of domain controllers and the coordinator servers is also required from the non-domain computer, whether DNS server configuration, NetBIOS/WINS configuration or local hosts file entries are used.
- Agents must be deployed manually. See Manual workstation agent deployment.
- During installation, the agent installer prompts for Active Directory domain and credential information to locate a coordinator and installation name.
- When the first agent is installed on workgroup computer, a ChangeAuditor Agents - <InstallationName> security group is created. User accounts must be added to this security group to properly authenticate.

- The agent installer allows you to add the domain user account to the ChangeAuditor Agents – <InstallationName> security group, if appropriate LDAP and network protocol access is available.

NOTE: Sometimes, you might need to pre-stage\create the ChangeAuditor Agents – <InstallationName> security group and manually add the configured workstation agent user account to the security group.

- You can also use the Coordinator Credential Configurator to change between coordinator domains at any time after the agent is installed.

NOTE: The Coordinator Credential Configurator application can be launched using the CoordinatorCredentialConfigurator.exe file in the agent installation folder on the workstation. The default agent installation location is: %ProgramFiles%\Quest\ChangeAuditor\Agent

NOTE: If User Account Control is enabled, you may need to authorize the Coordinator Credential Configurator tool to use the required elevated permissions by right-clicking on the tool and selecting 'Run as administrator' option

10

Agent Comparison

There are a few client features that are not available for workstation agents. The following table displays the agent-related features that are available for server and workstation agents.

Table 6. Agent comparison

Page and Feature	Available for server agents?	Available for workstation agents?
Deployment Page		
The Deployment page does not display non-member objects, such as ADAM workgroup servers or non-Active Directory workstations, because agents cannot be deployed to non-member objects using the Deployment tab.		
Included in topology harvest	Yes	Yes
Install or Upgrade (deploy agent)	Yes	Yes
Advanced Options | Specify Agent Installation Location	Yes	Yes
Advanced Options | Specify a Custom Share on the Remote Server	Yes	Yes
Advanced Options | Launch ServiceStatusTray on startup	Yes	No
Advanced Options | Restart Agent on failure	Yes	Yes
New Servers | Enable Auto Deployment on New Servers	Yes	No
Overview Page		
Agent Status Pane		
▪ Enterprise View (member objects)	Yes	No
▪ Workstation View (member objects)	No	Yes
▪ Other View (non-member objects)	Yes	Yes
▪ <*Domain*> (member and non-member objects)	Yes	Yes
Count of Events Pane		
▪ Location (member and non-member objects)	Yes	Yes
Top Agent Activity Pane		
▪ All (member and non-member objects)	Yes	Yes
▪ DCs (member objects)	Yes	No
▪ Servers (member objects)	Yes	No
▪ Workstations (member objects)	No	Yes
▪ Others (non-member objects)	Yes	Yes
Search Properties Tabs		
Where Tab	Yes	Yes
Origin Tab	Yes	Yes
Agent Statistics Page		
Included in Agent Statistics page	Yes	Yes
Start | Stop | Restart agent (member objects)	Yes	Yes
Start | Stop | Restart agent (non-member objects)	No	No

Table 6. Agent comparison

Page and Feature	Available for server agents?	Available for workstation agents?
Set Agent Uninstalled	Yes	Yes
Hide | Show Uninstalled agents	Yes	Yes
View agent logs	Yes	Yes (See Note below)
View resource properties	Yes	Yes
Administration Tasks Page — Agent Configuration		
Included in Agent Configuration page	Yes	No
Assign agent configurations	Yes	No (Uses Default Configuration)
Configuration Setup dialog | System Settings	Yes	Yes (From Default Configuration)
Configuration Setup dialog | File System settings (Change Auditor for Windows File Servers, Change Auditor for EMC or Change Auditor for NetApp)	Yes	No
Configuration Setup dialog | AD Query settings (Change Auditor for Active Directory Queries)	Yes	No
Configuration Setup dialog | Exchange settings (Change Auditor for Exchange)	Yes	No
Agent system tray icon	**Yes**	**No**

NOTE: For workstation log management (such as Get Logs and View Agent Logs), the following must be enabled on the workstation:

- Windows Management Instrumentation (WMI) in the firewall rule set (usually domain) on the workstation
- Network Discovery and File Sharing
- Remote Registry Service set to ‘Start Automatically’. By default, this service is stopped and set to ‘Manual’ for Windows 10.

11

Install an agent to audit ADAM (AD LDS) on workgroup servers

Change Auditor audits Active Directory Application Mode (ADAM) or Active Directory Lightweight Directory Services (AD LDS) events. This section provides information regarding the agent installation necessary for auditing ADAM (AD LDS) instances on workgroup servers.

Agent installation

NOTE: An agent must be installed on the server where the ADAM (AD LDS) instance to audit resides.

To install agents to audit ADAM (AD LDS) on workgroup servers:

NOTE: A workgroup agent requires NetBIOS over TCP enabled and access to the following ports inbound to the domain controllers:

- UDP port 137 (name services)
- UDP port 138 (datagram services)
- TCP port 139 (session services)

1. Copy the appropriate agent installer package from the Change Auditor service installation directory to the workgroup server to monitor. The default directory is %ProgramFiles%\Quest\ChangeAuditor\Service\Change Auditor Agent (x64).msi.
2. Run the installer file on the workgroup server to open the Change Auditor Agent wizard which steps you through the installation.
3. Review the following table for additional requested information in this wizard. This table only covers unfamiliar information. It does not include all the wizard screens or field descriptions.

Table 7. Change Auditor Agent wizard

Active Directory Information screen	
On the Active Directory Information screen, enter the Active Directory information required for the agent to establish a coordinator connection.	
Name of Active Directory Root Domain (domain.com)	Enter the DNS name (domain.com) of the root domain of Active Directory.
Account Name (domain\user)	Enter the name of the user (domain\user) that can find and connect to a Change Auditor coordinator in the Active Directory forest.
Account Password	Enter the password associated with the previously entered user account.
Installation Name screen	
The Installation Name screen prompts you to enter the installation name to identify the database to which the coordinator is to be connected. A workgroup agent must join an existing Change Auditor installation.	
ChangeAuditor Installation Name	Enter an existing Change Auditor installation or click **Browse** to select from a list of existing installations.

12

Windows Installer Command Line Options

This section lists the Windows Installer command line options (MSIEXEC.exe) that are available for deploying an agent or installing a coordinator.

- Agent options
- Coordinator options
- Web Client options

For more information on using the Windows Installer (MSIEXEC.exe) see: http://msdn.microsoft.com/en-us/library/aa367988(VS.85).aspx

Agent options

Table 8. Change Auditor agent command line options

Option	Use this to...
AD_LDAP_USE_SSL	Specify whether to use SASL or SSL for LDAP binding. • Set to "0" to use SASL • Set to "1" to use SSL If not specified it will set the option to SASL for new installations. If not specified in the case of an upgrade, it will use the current setting of the installed component.
INSTALLATION_NAME="<*name*>", INSTALLATION_NAME_VALID="1"	Specify the Change Auditor installation name.
APPDIR="<*install directory*>"	Specify the installation path.
INSTALLER_ITAD_GPTBACKUP="<*path*>"	Specify a GPO backup path.
SYSTRAY_AUTOSTART="1" SYSTRAY_AUTOSTART="0"	Specify whether to open the agent system tray icon on startup. • Set to "1" to launch agent system tray icon • Set to "0" to not launch the agent system tray icon
RESTARTONFAILURE="3" RESTARTONFAILURE="0"	Specify whether to automatically restart the agent on failure. • Set to "3" to automatically restart the agent • Set to "0" to not automatically restart the agent

Table 8. Change Auditor agent command line options

Option	Use this to...
EVENTLOG_BLOCK_OVERRIDE="1"	Specify whether to override event log block detection. • Set to "1" to enable this override When this setting is set to "0" (default), the event log detection is active which detects whether or not the system EventLog service is holding one of Change Auditor's event log message DLLs open. If one of these DLLs are open, the Windows Installer Restart Manager can cause unpredictable restarts of dependent services.
FOREIGN_LOGON_ACCOUNT="<example.com\user>" FOREIGN_PASSWORD="<*password*>"	For foreign agents (non-domain members), specify the foreign credentials to be used to find and connect to a coordinator in the Active Directory forest.
FOREIGN_FOREST_ROOT_DOMAIN="<*FQDN*>"	For foreign agents (non-domain members), use this option to specify the fully-qualified domain name (domain.com) of the root domain of Active Directory.
FOREIGN_CREATE_AGENT_GROUP="1"	For foreign agents (non-domain members), specify whether the logged in user is to be added to the ChangeAuditor Agents security group. • Set to "1" to add the user to this security group.

Coordinator options

Table 9. Change Auditor coordinator command line options

Option	Use this to...
AD_LDAP_USE_SSL	Specify whether to use SASL or SSL for LDAP binding. • Set to "0" to use SASL • Set to "1" to use SSL If not specified it will set the option to SASL for new installations. If not specified in the case of an upgrade, it will use the current setting of the installed component.
AGENT_PORT="<*static port number*>"	Assign the static port number to be used by the agents to communicate with the coordinator.
AGREETOLICENSE="YES"	Agree to the Software License Agreement.
CLIENT_PORT="<*static port number*>"	Assign the static port number to be used by the client when communicating with the coordinator.
INSTALLATION_NAME="<*installation name*>"	Set the Change Auditor installation name.
SDK_PORT="<*static port number*>"	Assign the static port number to be used by external applications to access the coordinator.
SQLSERVER_DATABASE="<*database name*>"	Provide the name of the Change Auditor database.

Table 9. Change Auditor coordinator command line options

Option	Use this to...
SQLSERVER_AUTH="1"	SQLSERVER_AUTH="1" SQLSERVER_AUTH="2" Specify whether to use SQL, Windows or Microsoft Entra authentication. • Set to "1" to use SQL authentication. • Set to "2" to use Microsoft Entra authentication. **NOTE:** For Azure SQL Managed Instance (PaaS), Microsoft Entra or SQL authentication with an encrypted connection must be used.
SQLSERVER_SQLSERVER="<*IP address\server name*>"	Specify the SQL instance used to store the Change Auditor database.
SQLSERVER_LOGINID="<*user name*>"	Specify the user name used to connect to the SQL instance.
SQLSERVER_PASSWORD="<*password*>"	Specify the password used to connect to the SQL instance.
SQLSERVER_DOMAIN="<*domain name*>"	If Windows authentication is being used, specify the domain of the user credentials used to connect to the SQL instance.
ADD_USER_CAADMINS="1"	Specify whether the logged in user is to be added to the ChangeAuditor Administrators security group. • Set to "1" to add the user to this security group.
EVENTLOG_BLOCK_OVERRIDE="1"	Specify whether to override event log block detection. • Set to "1" to enable this override When this setting is set to "0" (default), the event log detection is active which detects whether or not the system EventLog service is holding one of Change Auditor's event log message DLLs open. If one of these DLLs are open, the Windows Installer Restart Manager can cause unpredictable restarts of dependent services.

Web Client options

Table 10. Change Auditor web client command line options

Option	Use this to...
AD_LDAP_USE_SSL	Specify whether to use SASL or SSL for LDAP binding. • Set to "0" to use SASL • Set to "1" to use SSL If not specified it will set the option to SASL for new installations. If not specified in the case of an upgrade, it will use the current setting of the installed component.
AGREETOLICENSE="YES"	Agree to the Software License Agreement.

Table 10. Change Auditor web client command line options

Option	Use this to...
MY_WEBSITE="<Name of website>"	Specify the web site in IIS where the web client should be installed. For example, Default Web Site.
COORDINATOR_IP_PORT=<fqdn of Coordinator>:<Client SCP Port of the coordinator>	Specify the connection to the coordinator that will be used by the web client by entering the FQDN of the coordinator and the coordinator client SCP port.

About us

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Microsoft 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now. 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.